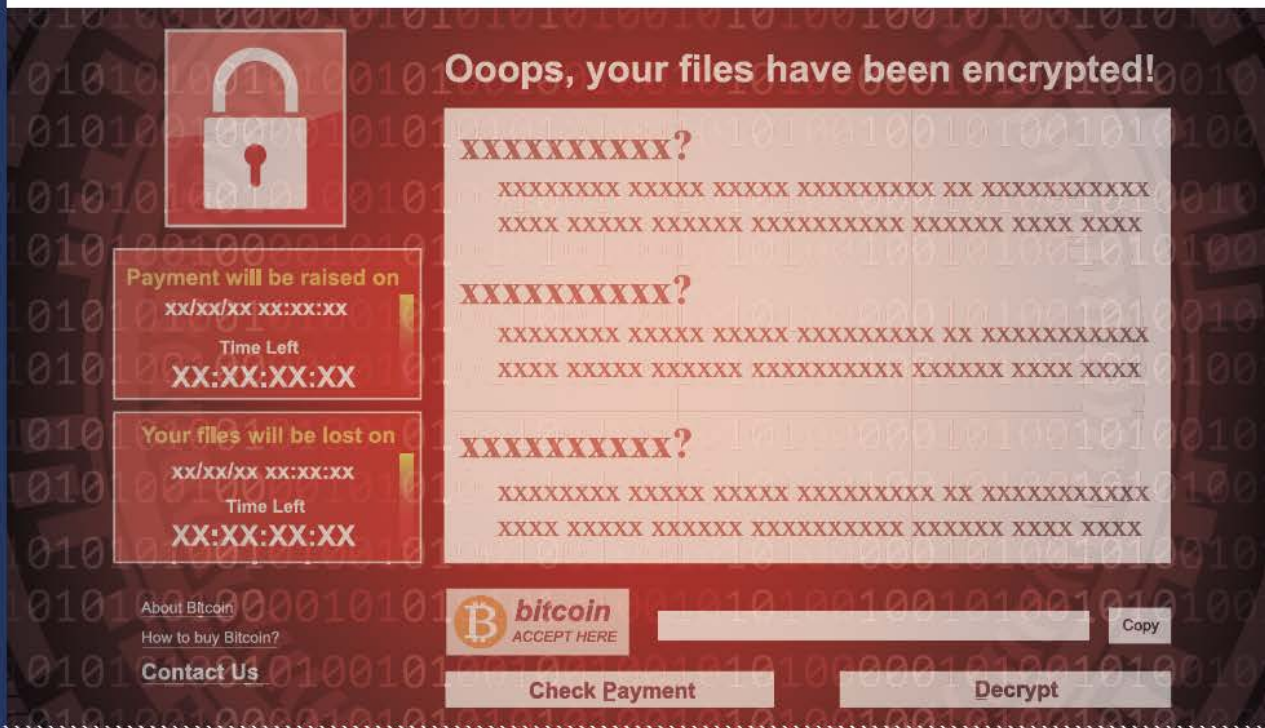
POLITIE & Wetenschap

Interactieve PDF

Onderhandelen, betalen en melden na slachtofferschap van ransomware

Sifra Matthijsse, Susanne van 't Hoff-de Goede, Rutger Leukfeldt



DE HAAGSE HOGESCHOOL

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
telefoon: 070 - 378 98 80
website: www.sdu.nl/service

Omslagontwerp: Imago Mediabuilders, Amersfoort
Afbeelding omslag: ANP foto

ISBN: 9789012410700
NUR: 600

PK 127 Onderhandelen, betalen en melden na slachtofferschap van ransomware

Een mixed methods onderzoek naar de factoren die bijdragen aan beslissingsgedrag van burgers en ondernemers

Sifra Matthijsse
Susanne van 't Hoff-de Goede
Rutger Leukfeldt

Halfweg, januari 2025

POLITIE & Wetenschap

Leestips - *Navigeren door de interactieve PDF*

Voor u ligt de interactieve PDF-versie van het onderzoeksrapport 'Onderhandelen, betalen en melden na slachtofferschap van ransomware'. Deze interactieve versie stelt u als lezer in staat om eenvoudig door het rapport heen te navigeren, resultaten op deelonderwerpen te vergelijken en de verdieping te zoeken.

Via de blauwe knoppen in het hoofdmenu navigeert u naar:

Literatuurstudie (H2)

De deelstudies over zelfgerapporteerd slachtofferschap (deel I en II) en advisering van slachtoffers (deel III)

Deel 1: Resultaten burgers (H4 en H5)

Deel II: Resultaten ondernemers (H6 en H7)

Deel III: Resultaten experts (H8)

Conclusie en discussie (H9)

Hierbinnen navigeert u via het grijze submenu naar de terugkerende thema's :

Prevalentie

Onderhandelen

Betalen

Melden

Implicaties

Klik op ⊕ voor meer informatie over factoren die bijdragen aan de bereidheid om te onderhandelen, betalen en/of melden.

Bekijk hier ook de factsheets 'Slachtofferschap van ransomware in Nederland' over (1) de prevalentie, aard en impact, (2) meldingsbereidheid en (3) het beslissingsgedrag van niet-slachtoffers.

Inhoudsopgave

Voorwoord / 9

Samenvatting / 11

1 **Inleiding** / 25
1.1 Achtergrond / 25
1.2 Doelstelling / 26
1.3 Vraagstelling / 28
1.3.1 Hoofdvraag / 28
1.3.2 Deelvragen / 28
1.4 Leeswijzer / 30

2 **Literatuurstudie** / 31
2.1 Definities / 31
2.2 Prevalentie van ransomware / 31
2.3 Aard en impact van ransomware / 32
2.4 Betalingsbereidheid / 34
2.5 Meldingsbereidheid / 37

3 **Methodologie** / 39
3.1 Deelstudie 1 & 2 / 39
3.1.1 Steekproef / 39
3.1.2 Meetinstrument / 46
3.1.3 Analyse / 51
3.2 Deelstudie 3 / 55
3.2.1 Steekproef / 55
3.2.2 Meetinstrument / 56
3.2.3 Analyse / 57
3.3 Ethische toestemming / 57

DEEL I RESULTATEN BURGERS

4 **Prevalentie, aard en impact van zelfgerapporteerd slachtofferschap van ransomware onder burgers** / 61
4.1 Prevalentie / 61
4.2 Achtergrondkenmerken / 61

4.3 Frequentie, incidentie en type ransomware / 62
4.4 Aard van incident / 63
4.5 Eerste reactie / 66
4.6 Onderhandelen / 68
4.7 Betalen / 69
4.8 Impact / 72
4.9 Melden / 74
4.10 Resumé / 77

5 Factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap van ransomware onder burgers / 81
5.1 Achtergrondkenmerken / 81
5.2 Eerste reactie / 82
5.3 Onderhandelen / 84
5.4 Impact / 85
5.5 Betalen / 88
5.6 Melden / 92
5.7 Resumé / 97
5.8 Vergelijking deelstudie 1A en 2A / 99

DEEL II RESULTATEN ONDERNEMERS

6 Prevalentie, aard en impact van zelfgerapporteerd slachtofferschap van ransomware onder ondernemers / 105
6.1 Prevalentie / 105
6.2 Achtergrondkenmerken / 106
6.3 Frequentie, incidentie en type ransomware / 108
6.4 Aard van incident / 109
6.5 Eerste reactie / 113
6.6 Onderhandelen / 115
6.7 Betalen / 117
6.8 Impact / 120
6.9 Melden / 124
6.10 Resumé / 128

7 Factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap van ransomware onder ondernemers / 131
7.1 Achtergrondkenmerken / 131
7.2 Eerste reactie / 133
7.3 Onderhandelen / 135
7.4 Impact / 137
7.5 Betalen / 141

7.6 Melden / 146
7.7 Resumé / 152
7.8 Vergelijking deelstudie 1B en 2B / 154

DEEL III RESULTATEN EXPERTS

8 Advisering van slachtoffers vanuit publieke en private organisaties / 159
8.1 Hulpbronnen en voorzieningen / 159
8.1.1 Cybersecuritybedrijven / 160
8.1.2 Politie / 161
8.2 Advisering en ondersteuning van slachtoffers / 163
8.2.1 Communicatie/onderhandelen / 163
8.2.2 Betalen / 166
8.2.3 Melden / 171
8.3 Sterke- en verbeterpunten in de ondersteuning van slachtoffers / 174

9 Conclusie en discussie / 179
9.1 Conclusies / 180
9.1.1 Prevalentie, aard en impact van slachtofferschap van ransomware / 180
9.1.2 Onderhandelen / 182
9.1.3 Betalen / 184
9.1.4 Melden / 187
9.2 Discussie / 189
9.2.1 Implicaties / 190
9.2.2 Beperkingen / 195

Literatuur / 199

Bijlage 1 Vragenlijst 1A / 207

Bijlage 2 Vragenlijst 2A / 225

Bijlage 3 Vragenlijst 1B / 237

Bijlage 4 Vragenlijst 2B / 257

Bijlage 5 Verdeling vignetten over groepen (deelstudie 2) / 271

Bijlage 6 Informatiebrief en informed consent interviews / 273

Bijlage 7 Interviewprotocol / 277

Uitgaven in de reeks Politiekunde / 281

Voorwoord

Voor u ligt een rapport over slachtofferschap van ransomware. Ransomware wordt door verscheidene Nederlandse en internationale organisaties beschouwd als een van de grootste (cyber)dreigingen van dit moment. Dit vraagt dan ook om een effectieve aanpak. Vanuit een wetenschappelijk gezichtspunt is er echter weinig bekend over hoe vaak slachtofferschap voorkomt, wie de slachtoffers zijn en wat de aard en impact van ransomware is. Bovenal is er meer inzicht nodig in hoe slachtoffers reageren, bijvoorbeeld als het gaat om onderhandelen, betalen en melden, de factoren die deze beslissingsprocessen beïnvloeden en hoe zich dit tot verhoudt tot de adviezen van verschillende partijen die slachtoffers van ransomware ondersteunen. Het huidige onderzoek is dan ook uitgevoerd om meer inzicht in deze aspecten te krijgen en zo aanknopingspunten te bieden voor de aanpak door publieke en private partijen die zich bezighouden met ransomware. Een van de experts die we interviewden wees ons erop dat een effectieve aanpak vereist dat alle puzzelstukjes afkomstig van verschillende plekken bij elkaar gelegd worden. We hopen met dit onderzoek een klein deel van de puzzel te hebben gelegd.

Dit onderzoek had niet tot stand kunnen komen zonder de medewerking van velen. Ten eerste bedanken we alle respondenten die hun inzichten met ons wilden delen. Hierbij gaat het om respondenten die de vragenlijsten hebben ingevuld, maar ook de experts van de Nederlandse politie, van Slachtofferhulp Nederland, uit de cybersecuritysector en uit de wetenschap die we hebben geïnterviewd. Steve van de Weijer en Asier Moneva danken we voor hun kritische blik op de voor dit onderzoek ontwikkelde vragenlijsten en het vignetexperiment. Liesbeth Holterman, Matthijs Jaspers, Wouter Landman, Richard Nijeboer, Wouter Stol en Franck Wagemakers danken we voor hun deelname aan de expertbijeenkomst waarin de implicaties van het onderzoek besproken zijn. Onze dank gaat bovendien uit naar de leden van de leescommissie voor hun bijdragen: Pauline Aarten, Jildau Borwell en Sophie van der Zee. Tot slot danken we Adriaan Rottenberg en Seran de Leede voor de begeleiding vanuit Politie & Wetenschap.

Sifra Matthijsse
Susanne van ’t Hoff-de Goede
Rutger Leukfeldt

Samenvatting

Achtergrond
Ransomware wordt vandaag de dag beschouwd als een van de voornaamste online dreigingen. Naast de financiële impact kan slachtofferschap ook leiden tot andere schade zoals verlies van data, reputatieschade, faillissement of gezondheidsproblemen. Daarnaast kan een ransomware-aanval een bredere maatschappelijk impact hebben. Tot op heden is er echter nog weinig bekend over de prevalentie van slachtofferschap van ransomware onder burgers en bedrijven in Nederland en de stappen die zij nemen na de ransomware-aanval. Daarnaast is onbekend in welke mate Nederlandse slachtoffers zich gedragen volgens de richtlijnen en adviezen van experts. Er is inzicht nodig in hoe slachtoffers op ransomware reageren, of zij onderhandelen en/of overgaan tot betaling van het losgeld, bij wie ze eventueel melding maken van het incident en welke factoren bijdragen aan deze processen. Dergelijke inzichten zijn van belang om goed en effectief beleid te kunnen voeren om (de gevolgen van) ransomware tegen te gaan.
Het huidige onderzoek heeft als doel om meer inzicht te verkrijgen in slachtofferschap van ransomware onder Nederlandse burgers, zelfstandigen zonder personeel (zzp'ers) en het midden- en kleinbedrijf (mkb[1]), en om aanknopingspunten te bieden voor de aanpak door publieke en private partijen die zich bezighouden met preventie van ransomware.

Onderzoeksvragen
Binnen het onderzoek staat de volgende onderzoeksvraag centraal:

Hoe vaak worden Nederlandse burgers en bedrijven slachtoffer van ransomware, hoe reageren zij met betrekking tot onderhandelen, betalen en melden, en hoe verhoudt dit zich tot de adviezen van publieke en private organisaties die slachtoffers van ransomware ondersteunen?

Om deze overkoepelende onderzoeksvraag te beantwoorden, zijn de volgende deelvragen opgesteld:
1. Wat zijn de prevalentie, de aard en de impact van slachtofferschap van ransomware onder Nederlandse burgers en bedrijven?

1 Ondernemingen met minder dan 250 werknemers en waarvan de jaaromzet de 50 miljoen euro of een jaarlijks balanstotaal van 43 miljoen euro niet overschrijdt (art. 2 Recommendation 2003/351/EG, Europese Commissie).

2. In welke mate zijn Nederlandse bedrijven en burgers bij een ransomware-aanval bereid het losgeld te betalen en/of het incident te melden bij politie en/of andere organisaties?
3. In hoeverre beïnvloeden situationele factoren (zoals het hebben van een back-up) de bereidheid van burgers en bedrijven om losgeld te betalen en de ransomware-aanval te melden?
4. Hoe adviseren publieke en private organisaties te handelen in het geval van slachtofferschap van ransomware en wat zijn de overeenkomsten en verschillen tussen organisaties betreffende de advisering?
5. In hoeverre handelen burgers en bedrijven naar de adviezen van publieke en private organisaties in het geval van slachtofferschap van ransomware?

Methoden
Om de onderzoeksvragen te beantwoorden, is het onderzoek opgedeeld in drie deelstudies.

Deelstudie 1
Het doel van deelstudie 1 was om meer inzicht te krijgen in de prevalentie, de aard en de impact van slachtofferschap van ransomware (onderzoeksvraag 1). Om de onderzoeksvraag te beantwoorden, zijn twee online vragenlijsten ontwikkeld en uitgezet onder burgers (deelstudie 1A) en ondernemers (deelstudie 1B). Beide vragenlijsten bestonden uit vijf blokken. Respondenten werden bevraagd over achtergrondkenmerken, de omstandigheden van de aanval, het losgeldbericht en de afpersing, de gevolgen van het incident en het contact met instanties naar aanleiding van het incident. Waar nodig zijn de vraagstelling of antwoordopties bij de vragenlijst voor ondernemers aangepast voor een bedrijfscontext.

Voor de dataverzameling is gebruikgemaakt van het Research Panel en Ondernemerspanel van onderzoeksbureau I&O Research (tegenwoordig Ipsos I&O). Om over een grote representatieve groep Nederlandse burgers uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware, zijn alle panelleden van 18 jaar en ouder (n=35.970) in het Research Panel uitgenodigd om een vragenlijst in te vullen over slachtofferschap van online criminaliteit. Respondenten werd eerst gevraagd om drie screeningsvragen in te vullen om vast te stellen of ze ooit slachtoffer van ransomware zijn geworden in de privésfeer (n=20.659 burgers, respons: 57,4%). De respondenten die ransomware hebben meegemaakt in de privésfeer, zijn vervolgens doorverwezen naar vragen over hun ervaringen met slachtofferschap (n=856 burgers, respons 2,4%). De data van de 20.659 respondenten die de screeningsvragen hebben beantwoord zijn gewogen naar leeftijd, geslacht en opleiding om representatieve uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware onder burgers in Nederland.

Om een zo groot mogelijke groep ondernemers te bereiken, is zowel gebruikgemaakt van het Research Panel als het Ondernemerspanel van onderzoeksbureau I&O Research. Alle ondernemers in deze panels (n=7.072) zijn uitgenodigd om een vragenlijst in te vullen over slachtofferschap van online criminaliteit. Respondenten werd eerst gevraagd om twee screeningsvragen in te vullen om vast te stellen of het bedrijf van de respondenten ooit getroffen is door een ransomware-aanval (n=3.040 ondernemers, 43%). De respondenten die ransomware hebben meegemaakt in hun bedrijf, zijn vervolgens doorverwezen naar vragen over hun ervaringen met slachtofferschap (n=188 ondernemers, respons 2,7%). De data van de 3.040 respondenten die de screeningsvragen hebben beantwoord, zijn gewogen om representatieve uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware onder ondernemers in Nederland. De data van de mkb'ers zijn gewogen naar grootteklasse en sector, de data van de zzp'ers naar sector. Om de eerste onderzoeksvraag over de prevalentie, de aard en de impact van slachtofferschap van ransomware te beantwoorden, is gebruikgemaakt van beschrijvende statistieken.

Deelstudie 2
Het doel van deelstudie 2 was het verkrijgen van inzicht in de factoren die bijdragen aan de bereidheid tot het betalen van losgeld en het melden van het incident bij politie en/of andere organisaties (onderzoeksvragen 2 en 3).

Om de onderzoeksvragen te beantwoorden, zijn twee online vragenlijsten met een vignetexperiment ontwikkeld en uitgezet onder burgers (deelstudie 2A) en ondernemers (deelstudie 2B). Beide vragenlijsten bestonden uit drie blokken. Respondenten werd gevraagd naar enkele achtergrondkenmerken, beslissingen naar aanleiding van een hypothetisch ransomwarescenario en (gepercipieerd) slachtofferschap. Om te onderzoeken welke factoren bepalen of burgers en ondernemers het losgeld betalen en het incident melden in een hypothetisch scenario, is een vignet voorgelegd aan respondenten. Een vignet betreft een korte beschrijving van een persoon, object of situatie dat een systematische combinatie van kenmerken vertegenwoordigt en bedoeld is om attitudes, beslissingen of oordelen uit te lokken. Alle respondenten werd gevraagd om de hypothetische situatie voor te stellen waarbij de respondent zelf (bij de doelgroep burgers) of het bedrijf van de respondent (bij de doelgroep ondernemers) getroffen was door ransomware en de respondent een beslissing moest nemen over het wel of niet betalen van het losgeld en het melden van het incident. Alle respondenten kregen een losgeldbericht en website te zien waarin gevarieerd is met de vignetfactoren. De eerste factor in het vignet betrof de hoogte van het losgeld, variërend tussen 250 euro en 2.500 euro in bitcoin voor burgers en tussen 1% en 25% van de jaaromzet in bitcoin voor ondernemers. De tweede factor betrof of er gedreigd is met het lekken van vertrouwelijke data. De derde factor betrof of er een back-up van de gegevens beschikbaar is. De vierde factor betrof of respondenten geadviseerd is om het losgeld te betalen door een (cybersecurity)organisatie en de mensen om de respondent heen. Vervolgens werd aan respondenten gevraagd hoe waarschijnlijk het is dat ze in dit scenario het

losgeld zouden betalen en het incident zouden melden op een elf-puntenschaal van helemaal niet waarschijnlijk (0%) tot zeer waarschijnlijk (100%). Daarnaast zijn er andere vragen gesteld, onder andere over wat de respondenten zouden voelen en als eerste zouden doen als ze geconfronteerd zouden worden met het losgeldbericht.

Ook in deelstudie 2 is voor de dataverzameling gebruikgemaakt van het Research Panel en Ondernemerspanel van onderzoeksbureau I&O Research. Onder de burgers die bij deelstudie 1A hebben aangegeven geen slachtoffer te zijn geworden van ransomware, is een steekproef getrokken die representatief is op geslacht, leeftijd, opleiding en regio (n=6.000). Deze panelleden zijn uitgenodigd om een vragenlijst in te vullen over beslissingsgedrag in een hypothetisch ransomwarescenario (n=4.082 burgers, respons 68%). De data in deelstudie 2 zijn gewogen naar leeftijd, geslacht en opleiding om de steekproef representatief te maken voor de populatie van burgers in Nederland. Om een zo hoog mogelijke respons te bereiken, zijn alle ondernemers die geen slachtoffer zijn geworden van ransomware direct doorverwezen naar vragen over beslissingsgedrag in een hypothetisch ransomwarescenario (n=2.501 ondernemers, respons, 35,3%).

Om de tweede onderzoeksvraag te beantwoorden over de bereidheid om het losgeld te betalen en het incident te melden in een hypothetisch scenario is gebruikgemaakt van beschrijvende statistieken. Om de derde onderzoeksvraag over de relatie tussen situationele factoren en de bereidheid tot betalen en melden te beantwoorden, is gebruikgemaakt van negatief binomiale- en Poisson-regressiemodellen.

Deelstudie 3
Het doel van deelstudie 3 was om meer inzicht te krijgen in hoe verschillende publieke en private organisaties slachtoffers adviseren te handelen bij een ransomware-incident en de mate waarin slachtoffers zich houden aan deze adviezen (onderzoeksvragen 4 en 5).

Om de onderzoeksvragen te beantwoorden, zijn semigestructureerde interviews (n=10) gehouden met experts van de politie (n=4), uit de cybersecuritysector (n=4), van Slachtofferhulp Nederland (n=1) en uit de wetenschap (n=1). De interviews vonden face to face, via videobellen of telefonisch plaats en zijn afgenomen met behulp van een interviewprotocol. Respondenten zijn eerst gevraagd naar hun achtergrond, functie, de werkzaamheden van de organisatie en waar hun kennis over de ondersteuning van slachtoffers op gebaseerd is. Vervolgens zijn respondenten bevraagd over de ondersteuning en/of advisering van slachtoffers van ransomware vanuit hun organisatie, waarbij onder andere is stilgestaan bij advisering met betrekking tot onderhandelen, betalen, melden en nazorg, en in hoeverre slachtoffers adviezen opvolgen. Daarna zijn de belangrijkste resultaten uit deelstudies 1 en 2 aan respondenten voorgelegd, en is ze gevraagd hierop te reflecteren. Tot slot is aan respondenten gevraagd wat de sterke en

verbeterpunten zijn omtrent de advisering en ondersteuning van slachtoffers van ransomware.

De data in deelstudie 3 zijn geanalyseerd aan de hand van thematische codes die voorafgaand aan de data-analyse zijn opgesteld op basis van het interviewprotocol, de onderzoeksvragen en thema's in de data. Toegekende codes zijn vervolgens vergeleken, gecontrasteerd en verbonden om patronen te identificeren.

Conclusies

Prevalentie
Uit de resultaten van deelstudie 1 blijkt dat 4,5% van de burgers, 4,6% van de zzp'ers en 11,5% van de mkb'ers ooit slachtoffer is geworden van ransomware. Van de totale steekproef is 0,2% van de burgers, 0,3% van de zzp'ers en 0,9% van de mkb'ers in de afgelopen 12 maanden slachtoffer geworden. De meerderheid van de respondenten is eenmalig slachtoffer geworden.

Aard
Als het gaat om de aard van het delict was er bij burgers in de meeste gevallen sprake van lockerware (vergrendeling van (onderdelen van) het systeem), gevolgd door scareware (met een bericht van een zogenaamde wetshandhavingsinstantie of een andere 'neppe' dreiging). Bij de zzp'ers en mkb'ers was in de meeste gevallen sprake van lockerware of cryptoware (versleuteling). De resultaten hebben ook inzicht gegeven in andere kenmerken van het incident, zoals de deadline, de aard van de aangetaste data en aanvullende dreiging naast de vergrendeling of versleuteling.

In deelstudie 1 onder slachtoffers en deelstudie 2 onder niet-slachtoffers is daarnaast meer inzicht verkregen in de eerste handeling na slachtofferschap. Een deel van de respondenten in beide deelstudies heeft geprobeerd of zou zelf proberen het probleem op te lossen. De meeste burgers en zzp'ers die wel en niet eerder slachtoffer zijn geworden, zouden dit doen door de verbinding met internet te verbreken. De mkb'ers die niet eerder slachtoffer zijn geworden zouden hetzelfde doen, terwijl de meeste mkb'ers die wel slachtoffer zijn geworden geprobeerd hebben te herstellen vanaf een back-up. Bij de meerderheid van de daadwerkelijke slachtoffers die zelf heeft gepoogd het probleem op te lossen, is het gelukt om de toegang tot het apparaat of systeem te herstellen. Een ander deel van de respondenten die wel en niet eerder slachtoffer is geworden, heeft hulp gezocht of zou hulp zoeken om het probleem op te lossen. In de meeste gevallen betrof dit een bekende of een organisatie, instantie, ICT-deskundige, computerzaak of provider.

Impact
Hoewel een groot aandeel van de niet-slachtoffers emotionele of psychische gevolgen verwachtte te ervaren (tussen de 68% en 80%) was dit bij minder respondenten die

slachtoffer zijn geworden het geval (tussen de 34% en 45%). De meest voorkomende verwachte en daadwerkelijke gevolgen waren voor burgers een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden, terwijl het bij de meeste ondernemers ging om een minder veilig gevoel, gevolgd door minder vertrouwen in andere mensen (onder slachtoffers) en minder vertrouwen in de eigen digitale vaardigheden (onder niet-slachtoffers). Het meest voorkomende andere gevolg voor burgers was bij zowel slachtoffers als niet-slachtoffers het besteden van tijd aan het oplossen van het incident. Voor ondernemers die wel en niet eerder slachtoffer zijn geworden ging het met name om kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk.

Waar ongeveer 60% van de burgers die geen slachtoffer is geworden financiële gevolgen (met uitzondering van het betaalde losgeld) verwachtte, werd dit in werkelijkheid ervaren door ongeveer 29% van de burgers die slachtoffer zijn geworden van ransomware. Bij beide groepen betrof de (verwachte) financiële schade in de meeste gevallen minder dan 1.000 euro. Bij ondernemers was er meer overeenstemming tussen slachtoffers en niet-slachtoffers, waarbij tussen de 68% en 73% van de niet-slachtoffers een financiële impact verwachtte en tussen de 60% en 75% van de slachtoffers een financiele impact heeft ervaren. De meeste ondernemers die geen slachtoffer zijn geworden schatten de kosten enigszins hoger in dan de door slachtoffers gerapporteerde kosten, tussen de 1.000 en 5.000 euro ten opzichte van minder dan 1.000 euro aan daadwerkelijke schade. Een kleiner aandeel van de burgers en ondernemers ervaarde een hogere financiële impact. Bij slechts een klein deel van de slachtoffers is de financiële schade (gedeeltelijk) vergoed door een verzekeringsmaatschappij, bank of andere instantie. Voor een groot deel van de respondenten die wel en niet eerder slachtoffer is geworden heeft het ransomware-incident daarnaast geleid of zou het leiden tot veranderingen in online gedrag of genomen beveiligingsmaatregelen, waaronder het (vaker) maken van externe-back-ups.

Onderhandelen

In deelstudie 1, 2 en 3 is ook stilgestaan bij de mate waarin slachtoffers van ransomware onderhandelen met daders, welke beweegreden(en) hierbij een rol spelen en wat de uitkomst van de onderhandeling is.

Slechts een klein aandeel van de respondenten heeft contact opgenomen (slachtoffers) of zou contact opnemen (niet-slachtoffers) met de daders, hoewel de aantallen onder daadwerkelijke slachtoffers (tussen de 4% en 7%) lager zijn dan in het hypothetische scenario (tussen de 8% en 18%). Er liggen bovendien andere motivaties aan het contact ten grondslag voor de slachtoffers en niet-slachtoffers. Waar zowel de burgers als ondernemers die niet eerder slachtoffer zijn geworden vooral contact zouden opnemen om vast te stellen of het losgeldbericht echt is, hebben de burgers die slachtoffer zijn geworden vooral contact opgenomen om te informeren over de hoogte van het losgeld

en de ondernemers die slachtoffer zijn geworden om vast te stellen welke data waren gestolen.

Terwijl 27,4% van de burgers, 40% van de zzp'ers en 36% van de ondernemers die niet slachtoffer is geworden contact zou opnemen om te onderhandelen (respectievelijk 2,2%, 4,9% en 6,3% van de totale steekproef), heeft in werkelijkheid geen enkele burger of zzp'er en slechts een enkele mkb'er die slachtoffer is geworden onderhandeld. Zij deden dit om het losgeldbedrag te verlagen of langer de tijd te krijgen. Hoewel de bereidheid om contact op te nemen of te onderhandelen laag is onder de respondenten van de vragenlijsten, blijkt uit de expertinterviews dat dit door cybersecuritybedrijven (vrijwel) altijd geadviseerd wordt. Mogelijke verklaringen voor dit verschil zouden volgens experts kunnen zijn dat de onderzochte doelgroep onvoldoende inzicht heeft in wat contact of onderhandeling hun zou kunnen opleveren, dat ze er niet toe in staat zijn door een gebrek aan kennis of voorzieningen of dat ze het advies opvolgen van de politie en No More Ransom om niet in te gaan op losgeldeisen. Een kanttekening bij de resultaten is bovendien dat het niet bij alle typen ransomware mogelijk is om contact op te nemen met de daders.

Betalen

In deelstudie 1, 2 en 3 is daarnaast stilgestaan bij de mate waarin slachtoffers van ransomware het losgeld betalen en welke beweegreden(en) en situationele factoren hierbij een rol spelen. Als het gaat om de hoogte van het losgeldbedrag dat van slachtoffers in deelstudie 1 is geëist, was dit het laagst onder burgers en het hoogst onder mkb'ers die slachtoffer werden van ransomware. Gemiddeld werd bij de burgers 3.676,37 euro, bij zzp'ers 13.919 euro en bij mkb'ers 231.343 euro aan losgeld geëist.

Zowel bij de respondenten die eerder slachtoffer zijn geworden als bij de respondenten die niet eerder slachtoffer zijn geworden, is de betalingsbereidheid laag. Gemiddeld genomen was het voor de burgers en ondernemers die geen slachtoffer zijn geworden niet waarschijnlijk dat ze zouden betalen. Daarnaast heeft minder dan een op de tien slachtoffers het geëiste losgeld betaald, waarbij dit percentage het hoogst was onder zzp'ers (7,6%), gevolgd door de mkb'ers (6,1%) en burgers (4,1%). De gemiddelde losgeldbetaling onder slachtoffers die betaald hebben was voor burgers 700 euro, voor zzp'ers 1.250 euro en voor mkb'ers 3.134 euro.

De experts uit deelstudie 3 schatten de betalingsbereidheid hoger in. Mogelijke verklaringen die zij aandragen voor het verschil zijn dat de doelgroepen in deelstudie 1 (slachtoffers) en 2 (niet-slachtoffers) minder snel een cyberverzekering hebben, minder impact ervaren, of als gevolg van de tevens lage onderhandelingsbereidheid onder deze doelgroepen. Daarnaast zijn sommige slachtoffers in de steekproef slachtoffer geworden toen het ransomwarelandschap er nog anders uitzag, hoewel betalingspercentages niet wezenlijk lager zijn onder slachtoffers die langer geleden slachtoffer zijn geworden, of tussen de verschillende typen ransomware waar respondenten slachtoffer

van zijn geworden. Tot slot kan deze lagere betalingsbereidheid ook het gevolg zijn van ontwikkelingen in de maatschappij, zoals een beter begrip van de impact van het betalen van losgeld, de advisering vanuit verschillende instanties om het losgeld niet te betalen, verbeterde beveiligingsmaatregelen en initiatieven zoals No More Ransom.

De voornaamste motieven om te betalen onder niet-slachtoffers betroffen voor burgers het niet willen verliezen van bestanden, gegevens of apparaten en voor ondernemers dat het betalen van losgeld goedkoper is dan geen zaken kunnen doen. De ondernemers die slachtoffer zijn geworden en die betaald hebben, deden dit voornamelijk omdat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen. Daarentegen hadden de burgers die slachtoffer zijn geworden als voornaamste reden om te betalen dat ze erop vertrouwden dat toegang hersteld zou worden na betaling. Voorgenomen motieven om niet te betalen waren voor burgers die wel en geen slachtoffer zijn geworden dat ze niet vertrouwden dat de toegang hersteld zou worden na betaling en voor zzp'ers die wel en geen slachtoffer zijn geworden dat het betalen van losgeld onethisch is. Waar de grootste groep mkb'ers die geen slachtoffer is geworden dit ook als reden aanhaalde, gaven de mkb'ers die slachtoffer zijn geworden als voornaamste reden om niet te betalen dat ze een back-up hadden. De experts in deelstudie 3 wijzen daarnaast op verstoring van de bedrijfscontinuïteit (te erg of te lang) als reden om te betalen, wat mede afhankelijk is van de beschikbaarheid van back-ups.

Er is in deelstudie 2 onder niet-slachtoffers ook gekeken naar situationele factoren die samenhangen met de betalingsbereidheid. De resultaten lopen uiteen tussen groepen. Er is een significant verband tussen de hoogte van het losgeld en de betalingsbereidheid van burgers en mkb'ers, maar niet voor zzp'ers. Een lagere losgeldeis is gerelateerd aan een hogere waarschijnlijkheid van betalen. Voor zzp'ers is het niet hebben van een back-up gerelateerd aan een significant hogere waarschijnlijkheid van betalen. Er is daarnaast een significant verband tussen de dreiging van het lekken van data en een hogere waarschijnlijkheid van betalen onder burgers, maar niet onder ondernemers. Tot slot is er zowel bij burgers als ondernemers sprake van een significant verband tussen geadviseerd worden om te betalen en de betalingsbereidheid, waarbij een advies om te betalen gerelateerd is aan een hogere waarschijnlijkheid van betalen.

Melden

Tot slot is in de deelstudies 1, 2 en 3 meer inzicht verkregen in de mate waarin slachtoffers van ransomware bereid zijn het incident te melden, bij welke partijen dit gebeurt en welke beweegreden(en) en situationele factoren hierbij een rol spelen.

Hoewel de gemiddelde meldingsbereidheid hoog is onder de burgers en ondernemers die geen slachtoffer zijn geworden en meer dan 85% van de respondenten het incident zou melden bij de politie, blijkt dit niet het geval onder de respondenten die daadwerkelijk slachtoffer zijn geworden. Tussen de 12% en 27% van de burgers en ondernemers die slachtoffer zijn geworden heeft contact opgenomen met de politie, waarbij dit percentage het hoogst is onder mkb'ers (26,7%), gevolgd door burgers (15,6%) en zzp'ers (12,3%). Hierbij is het aangiftepercentage tussen de 1% en 10% van de totale steekproef. Slachtoffers blijken bovendien geneigd om advies of ondersteuning te zoeken bij een andere organisatie dan de politie, zoals een cybersecuritybedrijf of IT-leverancier.

De meest voorkomende reden om het incident te melden bij de politie betrof bij zowel burgers als mkb'ers die wel en niet slachtoffer zijn geworden dat ze wilden dat de dader gepakt wordt. Ook de meeste zzp'ers die geen slachtoffer zijn geworden gaven dit als voornaamste reden, terwijl de zzp'ers die slachtoffer zijn geworden met name wilden voorkomen dat het bij een ander gebeurt. Deze motieven zijn in overeenstemming met de uitkomsten van de expertinterviews. De meest voorkomende reden om het incident niet te melden bij de politie was voor zowel de burgers en ondernemers die slachtoffer zijn geworden dat ze het probleem zelf of met behulp van een andere partij hebben opgelost. Daarentegen gaven de burgers en ondernemers die geen slachtoffer zijn geworden als voornaamste reden dat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen. Ook in de interviews in deelstudie 3 is gewezen op het feit dat het voor slachtoffers onvoldoende duidelijk is wat melden hun kan opleveren, dat ze het nut er niet van inzien of het gevoel hebben dat de politie niks doet.

Aan respondenten is ook gevraagd hoe ze aankijken tegen het standpunt en advies van de politie om het losgeld niet te betalen. Hoewel een groot deel van zowel de slachtoffers als niet-slachtoffers het met dit standpunt eens is, heeft ditzelfde standpunt bij 20% tot 30% van de slachtoffers ertoe geleid dat ze geen contact hebben opgenomen met de politie. Ook bij 20% tot 27% van de niet-slachtoffers zou dit tot geen contact leiden. Het heeft bovendien bij een deel van de respondenten invloed op de beslissing om na contact met de politie melding of aangifte te doen.

Tot slot is in deelstudie 2 onder niet-slachtoffers gekeken naar situationele factoren die samenhangen met de meldingsbereidheid. Er is een significant verband tussen de hoogte van het losgeld en de waarschijnlijkheid van melden voor burgers, maar niet voor ondernemers. Een hogere losgeldeis is gerelateerd aan een hogere waarschijnlijkheid van melden. Daarnaast is er voor burgers een positief significant verband tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de respondent heen en de waarschijnlijkheid van melden, maar niet voor ondernemers. Burgers rapporteren een hogere waarschijnlijkheid van melden indien ze geadviseerd worden om het losgeld te betalen. Er is geen significant verband gevonden tussen dreigen met lekken of het hebben van een back-up en de waarschijnlijkheid van melden onder burgers en ondernemers.

Implicaties

De uitkomsten van het onderzoek hebben implicaties voor het voorkomen en mitigeren van (de gevolgen van) ransomware, evenals voor de rol van de politie en andere publieke of private partijen hierin. De implicaties richten zich op drie onderwerpen: 1)

het verlagen van de betalingsbereidheid, 2) verbetering in de positie en ondersteuning van slachtoffers, 3) verbetering in de informatiepositie van de politie en het verhogen van de meldingsbereidheid.

Belangrijkste implicaties

- Er zijn aanknopingspunten voor het **verlagen van de betalingsbereidheid**, zoals een verbeterde informatievoorziening vanuit publieke partijen omtrent de effecten van het betalen van het losgeld voor het slachtoffer en de maatschappij.
- De **positie en ondersteuning van slachtoffers van ransomware kan verbeterd worden**, bijvoorbeeld door effectieve, uniforme informatievoorziening over hulpbronnen en door meer aandacht te besteden aan de fysieke en mentale gevolgen van slachtofferschap.
- De **informatiepositie van de politie kan verbeterd worden,** bijvoorbeeld door het verder ontwikkelen van de samenwerking en informatie-uitwisseling met andere partijen zoals cybersecuritybedrijven of het verhogen van de meldingsbereidheid.

Het verlagen van de betalingsbereidheid

- **Cybersecuritymaatregelen zijn van belang, niet alleen om slachtofferschap te voorkomen, maar ook in het kader van herstel en de beslissing om het losgeld te betalen.**
  Belangrijke beweegredenen om het losgeld te betalen waren onder andere dat respondenten bestanden of gegevens niet wilden verliezen, terwijl de beschikbaarheid van back-ups een van de redenen was om het losgeld juist niet te betalen. Ook een te ernstige of lange verstoring van de bedrijfscontinuïteit hing bij ondernemers samen met een hogere betalingsbereidheid, iets wat ook mede afhankelijk is van maatregelen als het maken van goede, gescheiden back-ups. Dit illustreert het belang van het nemen van voldoende cybersecuritymaatregelen door internetgebruikers.

- **De informatievoorziening vanuit publieke partijen over de effecten van het betalen van het losgeld voor het slachtoffer en de maatschappij kan verbeterd worden.**
  Door onder andere de overheid, politie en Slachtofferhulp Nederland wordt geadviseerd om nooit het losgeld te betalen, omdat losgeldbetalingen het ransomwarebusinessmodel in stand houden. De vraag is echter of voor burgers en ondernemers voldoende duidelijk is wat de gedachtegang achter dit advies is en wat de gevolgen zijn van het betalen van het losgeld voor het slachtoffer en de maatschappij. Zo is een belangrijke beweegreden om het losgeld te betalen voor slachtoffers om te voorkomen dat hun gestolen data gelekt of verkocht wordt, terwijl betalen niet garandeert dat de data ook echt door de daders verwijderd worden. Door een verbeterde informatievoorziening door publieke partijen over de effecten van het betalen van het losgeld voor het slachtoffer en de maatschappij, kan de kosten-batenoverweging om te betalen mogelijk beïnvloed worden zodat minder slachtoffers betalen.

- **Samenwerking tussen de politie en cybersecuritysector is van belang om de betalingsbereidheid te verlagen.**
  Slachtoffers zijn meer geneigd om contact op te nemen met een cybersecuritybedrijf, IT-leverancier of andere deskundige dan met de politie. In het vignetexperiment was de waarschijnlijkheid van betalen voor alle doelgroepen bovendien gerelateerd aan geadviseerd worden om te betalen door een cybersecuritybedrijf en de mensen om de respondent heen. Hoewel cybersecuritybedrijven alleen zullen adviseren om te betalen als er geen alternatieven zijn, hebben ze desalniettemin een sleutelpositie. Het is dus belangrijk dat met verschillende partijen wordt samengewerkt om slachtoffers goed te adviseren en beleid te ontwikkelen om losgeldbetalingen te voorkomen.

- **Er is meer onderzoek nodig naar interventies om de betalingsbereidheid te verlagen.**
  Daarnaast kan gedacht worden aan andere initiatieven om de betalingsbereidheid te verlagen, zoals een subsidie die het nemen van beveiligingsmaatregelen stimuleert, veranderingen in verzekeringseisen, of een fonds om slachtoffers bij te staan in hun herstel van een ransomware-aanval als het losgeld niet betaald wordt. Meer onderzoek is nodig om te achterhalen of dergelijke interventies een effect hebben op de betalingsbereidheid.

Verbetering in de positie en ondersteuning van slachtoffers

- **De informatievoorziening kan verbeterd worden omtrent de acties die slachtoffers kunnen ondernemen en de organisaties waarbij ze terechtkunnen. Er is meer onderzoek nodig naar effectieve manieren om de informatievoorziening te verbeteren en meer uniform te maken.**
  Hoewel voor slachtoffers verschillende hulpbronnen en voorzieningen beschikbaar zijn op internet en bij verschillende organisaties, zijn deze voorzieningen versnipperd. Voor slachtoffers is niet altijd duidelijk wat ze zelf aan actie(s) kunnen ondernemen en bij welke organisaties ze terechtkunnen in elke fase van het incident en met welk doel.

  Er is meer onderzoek nodig naar wat een effectieve manier is om deze informatievoorziening te verbeteren en meer uniform te maken en slachtoffers zo handelingsperspectief te bieden. Hierbij kan bijvoorbeeld gedacht worden aan inhoudelijke afstemming tussen partijen die online al informatie of hulp aanbieden omtrent ransomware, waarbij de inhoud zoveel mogelijk overeen moet komen en slachtoffers steeds naar dezelfde website/partij worden doorverwezen. Dit wordt momenteel al toegepast binnen het thema online fraude door de werkgroep integrale aanpak online fraude. Een voorbeeld hierbij is een website voor slachtoffers van

ransomware, opgezet door de verschillende partijen die zich bezighouden met de aanpak van ransomware, waarop adviezen worden gegeven van wat slachtoffers vooraf, tijdens en na een aanval kunnen doen en bij welke organisaties ze terechtkunnen, vergezeld van een campagne om deze website bekendheid te geven. Daarnaast zouden er interventies ingezet kunnen worden om burgers en ondernemers te helpen bij het nemen van maatregelen.

- **Er moet meer aandacht komen voor de fysieke en mentale gevolgen van slachtofferschap van ransomware, waarbij handvatten aan slachtoffers worden geboden door partijen die slachtoffers bijstaan om hiermee om te gaan of de juiste hulp te vinden.**
  Een aanzienlijk deel van de slachtoffers ervaarde emotionele of psychische gevolgen, waaronder een minder veilig gevoel, minder vertrouwen in de digitale vaardigheden of andere mensen. De experts wijzen tevens op stress en onzekerheid. Deze emoties en gevoelens kunnen bovendien de betalings- en meldingsbereidheid beïnvloeden. Er moet meer aandacht komen voor de fysieke en mentale gevolgen van slachtofferschap van ransomware op de korte en lange termijn, waarbij slachtoffers handvatten worden geboden om hiermee om te gaan. Er is niet alleen een belangrijke rol weggelegd voor Slachtofferhulp Nederland om hier invulling aan te geven, maar ook voor andere partijen die slachtoffers ondersteunen om actief bij de impact stil te staan en door te verwijzen naar Slachtofferhulp Nederland indien nodig. Meer onderzoek is bovendien nodig naar de emotionele impact in alle lagen van een organisatie, mogelijke verklaringen voor de verschillen in ervaren impact tussen burgers die in de privésfeer slachtoffer zijn geworden en ondernemers die in bedrijfsverband slachtoffer zijn geworden, en verklaringen voor de discrepantie tussen de daadwerkelijke emotionele impact onder slachtoffers en de verwachte impact onder niet-slachtoffers.

Verbetering in de informatiepositie van de politie en het verhogen van de meldingsbereidheid

- **Samenwerking en informatie-uitwisseling tussen de politie en andere partijen die zich bezighouden met ransomware is van belang voor de informatiepositie van de politie en moet zich blijven ontwikkelen.**
  Een goede ontwikkeling is dat er meer informatie uitgewisseld wordt tussen publieke en private partijen zoals de politie, het OM en de cybersecuritysector, zoals in Project Melissa. De samenwerking en informatie-uitwisseling kan echter nog verder verbeterd worden. Zo wijzen experts erop dat niet alle cybersecuritybedrijven informatie uitwisselen met de politie, dat er geen informatiedeling is tussen de Autoriteit Persoonsgegevens (AP) en de politie (terwijl sommige slachtoffers mogelijk alleen melding maken van een datalek bij de AP) en dat verschillende partijen in het algemeen nog te ver uit elkaar liggen. De samenwerking moet zich dus blijven ontwikkelen, waarbij ook aandacht uitgaat naar de juridische mogelijkheden voor informatiedeling, en tevens geëvalueerd wordt wat het effect van dergelijke initiatieven is op het verkrijgen van een beter inzicht in ransomware en het voorkomen van slachtofferschap.

- **De meldingsbereidheid na slachtofferschap van ransomware is laag. Er zijn verschillende aanknopingspunten om de meldingsbereidheid te verhogen, zoals verbeterde informatievoorziening vanuit de politie over de mogelijkheden, het belang en de (realistische) gevolgen van een melding of aangifte, of het stimuleren van melden door andere partijen zoals cybersecuritybedrijven of verzekeringsmaatschappijen.**
  De intentie om melding te maken bij de politie is hoog, maar de daadwerkelijke meldings- of aangiftebereidheid na slachtofferschap van ransomware is laag. Slachtoffers zoeken eerder advies of ondersteuning bij een andere organisatie, zoals een cybersecuritybedrijf of de Fraudehelpdesk. Daarnaast blijkt uit de resultaten dat slachtoffers onvoldoende het nut inzien van een melding of aangifte bij de politie. Ze denken bijvoorbeeld dat de politie niets voor ze kan betekenen, terwijl de politie wel degelijk ondersteuning kan bieden, bijvoorbeeld door middel van het delen van kennis of het aanbieden van decryptiemogelijkheden.

  De resultaten bieden aanknopingspunten voor het verhogen van de meldingsbereidheid. Ten eerste zou meer informatie gegeven kunnen worden over wat het belang van een melding of aangifte is voor zowel het slachtoffer als de maatschappij, bijvoorbeeld door informatie op de website van de politie, door het delen van 'succesverhalen' van politieacties of middels campagnes. Er is bovendien een belangrijke rol weggelegd voor andere partijen waar slachtoffers contact mee opnemen zoals cybersecuritybedrijven, de Fraudehelpdesk of verzekeringsmaatschappijen om melding of aangifte bij de politie te stimuleren. Tegelijkertijd is het zaak voor de politie om aan verwachtingsmanagement te doen naar het slachtoffer toe over wat wel en niet mogelijk is. Zo blijkt uit de resultaten dat sommige slachtoffers een melding hebben gemaakt bij de politie omdat ze wilden dat de dader gepakt wordt, terwijl de politie voor ransomware niet altijd in deze behoefte kan voorzien. Ook dit benadrukt het belang van goede informatievoorziening. Ten tweede kan een verbetering in processen volgens experts mogelijk een bijdrage leveren aan het verhogen van de meldingsbereidheid. Hierbij kan gedacht worden aan het verbeteren van de online aangifte voor burgers, het invoeren van online aangifte voor ondernemers, of meer persoonlijk contact, maar ook de terugkoppeling naar slachtoffers na een melding. Ten derde zou er een meldplicht ingevoerd kunnen worden, vergelijkbaar met de meldplicht die geldt voor datalekken. Toekomstig onderzoek moet uitwijzen wat de (juridische) mogelijkheden zijn voor het invoeren van een meldplicht in Nederland, en de mogelijke voor- en nadelen.

- **Het advies van de politie om het losgeld niet te betalen weerhoudt een deel van de slachtoffers ervan om contact op te nemen met de politie. Verder onderzoek**

is nodig naar het effect van dit advies en wat dit betekent voor de communicatiestrategie van de politie.
Een belangrijke uitkomst is, tot slot, dat het standpunt van de politie om het losgeld niet te betalen, een deel van de slachtoffers ervan weerhoudt om contact op te nemen met de politie. Dit roept de vraag op of dit advies effectief is. Er is meer onderzoek nodig naar de mate waarin het advies slachtoffers daadwerkelijk weerhoudt van het betalen van het losgeld. Vervolgens kan inzichtelijk gemaakt worden hoe dit zich verhoudt tot de uitkomst van het huidige onderzoek dat het sommige slachtoffers weerhoudt van het melden bij de politie, en wat dit betekent voor de communicatiestrategie van de politie.

1 Inleiding

1.1 Achtergrond

Ransomware wordt vandaag de dag beschouwd als een van de voornaamste online dreigingen (ENISA, 2021; Europol, 2021; FBI, 2021; NCTV, 2022). Niet alleen is de hoeveelheid aanvallen toegenomen (Europol, 2021; Grauer et al., 2022), ook is er sprake van een professionaliseringslag in de modus operandi, waarbij dadergroeperingen op verschillende wijzen druk zetten op het slachtoffer en zelfs een helpdesk bieden met de mogelijkheid te onderhandelen over de hoogte van het losgeld (Matthijsse et al., 2023). Naast de financiële impact als gevolg van verlies van omzet, de losgeldbetaling of herstelwerkzaamheden, kan slachtofferschap ook leiden tot andere schade zoals verlies van data, reputatieschade of faillissement voor organisaties en gezondheidsproblemen zoals stress of slapeloosheid voor individuen (Brennenraedts et al., 2022; Connolly & Borrion, 2022; Knebel et al., 2021; Northwave, 2022). Daarnaast kan een ransomware-aanval een bredere maatschappelijk impact hebben, bijvoorbeeld vanwege de verstoring van ketenprocessen of vitale sectoren (Brennenraedts et al., 2022; NCTV, 2021).

Tot op heden is er nog weinig bekend over de prevalentie van slachtofferschap van ransomware onder burgers en bedrijven en de stappen die zij nemen na de ransomware-aanval. Ten eerste is informatie over de prevalentie onder bedrijven veelal afkomstig uit rapporten van commerciële cybersecuritybedrijven. Deze rapporten geven mogelijk een vertekend beeld vanwege de commerciële aard van de bedrijven en de steekproef waarop de onderzoeken gebaseerd zijn, veelal consumenten die producten of diensten van het bedrijf kopen. Terwijl dergelijke internationale cybersecurityrapporten wijzen op een hoge prevalentie onder bedrijven van 37% tot 71% (CyberEdge Group, 2022; Kaspersky, 2021; Sophos, 2021), geeft grootschalig empirisch Australisch en Europees onderzoek een genuanceerder beeld en wijst op een slachtofferpercentage bij midden- en kleinbedrijven (mkb) van respectievelijk 4,8% en 4% procent in het afgelopen jaar (European Commission, 2022; Voce & Morgan, 2021).

Ook onder burgers is er mogelijk sprake van een groot aantal slachtoffers. Zo vond een verkennend onderzoek dat 8,9% van de Nederlandse respondenten slachtoffer was van ransomware (Van de Weijer et al., 2020) en wijzen Amerikaanse en Australische cijfers op jaarlijkse slachtofferpercentages van respectievelijk 9% en 2,1% onder burgers (Si-

moiu et al., 2019; Voce & Morgan, 2021). In Nederland is er echter tot op heden weinig grootschalig wetenschappelijk onderzoek gedaan naar slachtofferschap van ransomware onder burgers en bedrijven (zie bijvoorbeeld CBS, 2023). Het is van belang om hier meer inzicht in te krijgen om goed en effectief beleid te kunnen voeren om ransomware tegen te gaan.

Ten tweede is er naast een gebrek aan inzicht in prevalentie zeer beperkt zicht op wat er gebeurt wanneer burgers en bedrijven slachtoffer worden van ransomware. Er is inzicht nodig in hoe slachtoffers op ransomware reageren, of zij onderhandelen en/of overgaan tot betaling van het losgeld, bij wie ze een eventuele melding maken van het incident en welke factoren bijdragen aan deze processen. De eerste internationale onderzoeken hiernaar vonden dat het betalen van het losgeld onder andere gerelateerd zou zijn aan het opvolgen van advies om te betalen, het niet hebben van een verzekering of back-up, de hoogte van het losgeldbedrag, of er data gestolen zijn en de angst dat gestolen data anders gelekt wordt (Connolly & Borrion, 2022; Meurs et al., 2022b; Voce & Morgan, 2021). Niet al deze onderzoeken zijn echter gebaseerd op grote, representatieve steekproeven. Het is daarnaast onduidelijk in hoeverre dergelijke factoren ook een rol spelen bij burgers en bedrijven in Nederland en of deze factoren ook van toepassing zijn op het melden van slachtofferschap. Daarnaast is onbekend in welke mate Nederlandse slachtoffers zich gedragen volgens de richtlijnen en adviezen van experts.

1.2 Doelstelling

Het huidige onderzoek heeft als overkoepelend doel om meer inzicht te verkrijgen in slachtofferschap van ransomware onder Nederlandse burgers, bedrijven (zelfstandigen zonder personeel (zzp'ers) en midden- en kleinbedrijven (mkb)[2] [3] en aanknopingspunten te bieden voor de aanpak door publieke en private partijen die zich bezighouden met preventie van ransomware. Hierbij wordt specifiek gekeken naar de prevalentie, aard en impact van slachtofferschap van ransomware en beslissingsgedrag omtrent onderhandelen, betalen en melden na slachtofferschap. Om deze overkoepelende doelstelling te bereiken, is het onderzoek opgedeeld in drie deelstudies, waarbij voor elke deelstudie een eigen doelstelling is opgesteld (tabel 1.1).

Het doel van deelstudie 1 is om meer inzicht te krijgen in de prevalentie, aard en impact van slachtofferschap van ransomware aan de hand van twee vragenlijsten onder Nederlandse burgers (deelstudie 1A) en bedrijven (deelstudie 1B). In dit deel van het

2 Ondernemingen met minder dan 250 werknemers en waarvan de jaaromzet de 50 miljoen euro of een jaarlijks balanstotaal van 43 miljoen euro niet overschrijdt (art. 2 Recommendation 2003/351/EG, Europese Commissie).

3 De focus ligt op zzp'ers en mkb'ers aangezien deze een aanzienlijk deel uitmaken van de Nederlandse bedrijfeconomie. Zo bestond 99,8% van de bedrijven in Nederland in 2019 uit midden- en kleinbedrijven (Eurostat, 2022) en waren er in 2023 meer dan 1,2 miljoen zzp'ers in Nederland (CBS, n.d.).

onderzoek worden daadwerkelijke slachtoffers van ransomware (burgers en bedrijven) gevraagd te beschrijven wat hun is overkomen en hoe zij hierop hebben gereageerd. Zodoende kan inzicht worden verkregen in het aantal slachtoffers in Nederland, wat hun is overkomen (type ransomware, hoogte losgeld, etc.), de impact van het incident, de mate waarin slachtoffers onderhandelen over het losgeldbedrag, het losgeld betalen en het incident melden en de beweegredenen die hierbij een rol spelen. Te verwachten is dat de meldingsbereidheid gerelateerd is aan eerdere beslissingen, zoals het onderhandelen en betalen. Dergelijke beslissingen kunnen namelijk invloed hebben op de ervaren ernst van het delict en hiermee de meldingsbereidheid (Gottfredson & Hindelang, 1979; Skogan, 1984; Tarling & Morris, 2010), wat maakt dat het van toegevoegde waarde is om dit gelijktijdig te onderzoeken. Het vergelijken van slachtofferschap onder burgers en bedrijven zal tevens duidelijkheid scheppen over het heersende beeld dat ransomware vooral een probleem onder bedrijven is.

Het doel van deelstudie 2 is het verkrijgen van inzicht in de factoren die bijdragen aan de bereidheid tot het betalen van losgeld en het melden van het incident bij politie en/of andere organisaties. In deelstudie 2 zal door middel van het voorleggen van hypothetische scenario's in twee vragenlijsten worden onderzocht hoe Nederlandse burgers (deelstudie 2A) en bedrijven (deelstudie 2B) reageren op een fictieve ransomware-aanval en in welke scenario's ze overgaan tot betalen en/of melden. Door het manipuleren van verschillende scenario's zal inzicht worden verkregen in de invloed van verschillende situationele factoren, zoals het hebben van een back-up en krijgen van advies, op beslissingsgedrag van burgers en bedrijven.

Deelstudie 3 heeft vervolgens als doel om inzicht te verkrijgen in de mate waarin slachtoffers zich houden aan de adviezen van verschillende organisaties. In deelstudie 3 zal door middel van expertinterviews worden geschetst hoe de politie, cybersecurity-experts, en andere organisaties slachtoffers adviseren te handelen in het geval van een ransomware-aanval. Tevens zal worden onderzocht in hoeverre burgers en bedrijven zich aan deze adviezen houden door de uitkomsten van de interviews te vergelijken met de uitkomsten van deelstudies 1 en 2.

Tabel 1.1 Overzicht van deelstudies, doelen, onderzoeksmethoden en populatie

	Deelstudie 1	Deelstudie 2	Deelstudie 3
Doel	Inzicht verkrijgen in de prevalentie, aard en impact van slachtofferschap van ransomware	Inzicht verkrijgen in de factoren die bijdragen aan de betalings- en meldingsbereidheid bij slachtofferschap van ransomware	Inzicht verkrijgen in hoe organisaties slachtoffers adviseren te handelen en in welke mate slachtoffers deze adviezen opvolgen
Methode	Vragenlijst	Vragenlijst met vignetexperiment	Interviews
Populatie	Slachtoffers • Burgers • Ondernemers	Niet-slachtoffers • Burgers • Ondernemers	Experts van publieke en private organisaties
Leeswijzer	Methode (§ 3.1) Resultaten • Burgers (hoofdstuk 4) • Ondernemers (hoofdstuk 6) Resumé • Burgers (§ 4.10) • Ondernemers (§ 6.10)	Methode (§ 3.1) Resultaten • Burgers (hoofdstuk 5) • Ondernemers (hoofdstuk 7) Resumé • Burgers (§ 5.7) • Ondernemers (§ 7.7)	Methode (§ 3.2) Resultaten (hoofdstuk 8)
	Vergelijking deelstudie 1 & 2 • Burgers (§ 5.8) • Ondernemers (§ 7.8)		Vergelijking deelstudie 1, 2 & 3 (§ 8.2.3.3)

1.3 Vraagstelling

1.3.1 *Hoofdvraag*

Binnen het onderzoek staat de volgende onderzoeksvraag centraal:

Hoe vaak worden Nederlandse burgers en bedrijven slachtoffer van ransomware, hoe reageren zij met betrekking tot onderhandelen, betalen en melden en hoe verhoudt dit zich tot de adviezen van publieke en private organisaties die slachtoffers van ransomware ondersteunen?

De onderzoeksvraag zal beantwoord worden aan de hand van vijf deelvragen, onderverdeeld naar de verschillende deelstudies van het onderzoek.

1.3.2 *Deelvragen*

Deelstudie 1. Prevalentie, aard en impact van slachtofferschap van ransomware onder burgers en bedrijven
Deelstudie 1 richt zich op burgers (1A) en bedrijven (1B) die reeds slachtoffer zijn geworden van ransomware. De onderzoeksvraag en deelvragen die hierbij centraal staan zijn:

1. Wat zijn de prevalentie, de aard en de impact van slachtofferschap van ransomware onder Nederlandse burgers en bedrijven?
   a. Wat is de prevalentie en frequentie van slachtofferschap van ransomware onder Nederlandse burgers en bedrijven?
   b. Wat is de aard van het delict (type ransomware, hoogte losgeldbedrag, aard en omvang gegijzelde bestanden en/of apparaten)?
   c. Wat was de eerste reactie van slachtoffers van ransomware op de aanval (wat dachten en deden zij)?
   d. In hoeverre werd er door slachtoffers van ransomware onderhandeld met de daders, welke beweegreden(en) speelden hierbij een rol en wat was de uitkomst van de onderhandeling?
   e. In hoeverre werd er door slachtoffers van ransomware losgeld betaald en welke beweegreden(en) speelden hierbij een rol?
   f. Welke financiële, psychologische, emotionele en/of overige gevolgen ervaarden slachtoffers van ransomware?
   g. In hoeverre maakten slachtoffers van ransomware melding van het incident, bij welke partij(en) gebeurde dit en welke beweegredenen speelden hierbij een rol?

Deelstudie 2. Factoren die bijdragen aan de betalings- en meldingsbereidheid na slachtofferschap van ransomware
In deelstudie 2 krijgen burgers (2A) en bedrijven (2B) een fictief ransomwarescenario voorgelegd. De onderzoeksvragen die hierbij centraal staan zijn:

2. In welke mate zijn Nederlandse bedrijven en burgers bij een ransomware-aanval bereid het losgeld te betalen en/of het incident te melden bij politie en/of andere organisaties?
3. In hoeverre beïnvloeden situationele factoren (zoals het hebben van een back-up) de bereidheid van burgers en bedrijven om losgeld te betalen en de ransomware-aanval te melden?

Deelstudie 3. Advisering van slachtoffers vanuit publieke en private organisaties
In deelstudie 3 worden experts van verschillende organisaties geïnterviewd over hoe zij slachtoffers adviseren te handelen bij een ransomware-incident en wordt onderzocht in hoeverre burgers en bedrijven zich houden aan deze adviezen.

4. Hoe adviseren publieke en private organisaties te handelen in het geval van slachtofferschap van ransomware en wat zijn de overeenkomsten en verschillen tussen organisaties betreffende de advisering?
5. In hoeverre handelen burgers en bedrijven naar de adviezen van publieke en private organisaties in het geval van slachtofferschap van ransomware?

1.4 Leeswijzer

Dit rapport begint met een overzicht van de relevante literatuur met betrekking tot ransomware (hoofdstuk 2), gevolgd door een beschrijving van de gebruikte onderzoeksmethoden in hoofdstuk 3. De resultaten zijn opgedeeld in drie delen, gericht op de burgers, ondernemers en experts. In deel I staan de resultaten centraal van deelstudie 1A met betrekking tot de prevalentie, de aard, en de impact van zelfgerapporteerd slachtofferschap onder burgers (hoofdstuk 4) en de resultaten van deelstudie 2A over de factoren die bijdragen aan de betalings- en meldingsbereidheid na ransomwareslachtofferschap onder burgers (hoofdstuk 5). In deel II staan de resultaten centraal van deelstudie 1B met betrekking tot de prevalentie, de aard, en de impact van zelfgerapporteerd slachtofferschap onder ondernemers (hoofdstuk 6) en de resultaten van deelstudie 2B over de factoren die bijdragen aan de betalings- en meldingsbereidheid na ransomwareslachtofferschap onder ondernemers (hoofdstuk 7). In deel III worden de resultaten van deelstudie 3 over de advisering van slachtoffers vanuit verschillende organisaties besproken (hoofdstuk 8). Tot slot volgen in hoofdstuk 9 de conclusie en discussie.

2 Literatuurstudie

2.1 Definities

Ransomware of gijzelsoftware betreft een vorm van cybercriminaliteit en kan gedefinieerd worden als een type kwaadaardige software (malware) dat zich richt op het gijzelen of ontoegankelijk maken van bestanden of systemen door versleuteling of gewijzigde gebruikersrechten. Het slachtoffer wordt vervolgens onder druk gezet om losgeld te betalen in ruil voor toegang tot de data of het systeem (Al-rimy et al., 2018; Meland et al., 2020). Al-rimy et al. (2018) maken hierbij een onderscheid tussen enerzijds *scareware* en anderzijds *detrimental ransomware. Scareware* is een valse waarschuwing of dreiging, bijvoorbeeld de beschuldiging van het bekijken van kinderpornografisch materiaal of een zogenaamde virusinfectie, bedoeld om het slachtoffer te misleiden tot betaling. In werkelijkheid is er echter niets aan de hand (Al-rimy et al., 2018). *Detrimental ransomware* betreft daarentegen een daadwerkelijke dreiging voor het slachtoffer. Hierbij kan een verdere verdeling gemaakt worden tussen locker-ransomware en crypto-ransomware. Locker-ransomware gijzelt een of meer onderdelen van het systeem, wat resulteert in een systeem met beperkte mogelijkheden (Al-rimy et al., 2018). Het onderliggende besturingssysteem en de data blijven intact en slachtoffers kunnen functies die nodig zijn om het losgeld te betalen, zoals het toetsenbord, blijven gebruiken (Sajjan & Ghorpade, 2017). Crypto-ransomware gijzelt de data van het slachtoffer door middel van versleuteling, wat alleen teruggedraaid kan worden met een decryptiesleutel (Al-rimy et al., 2018).

2.2 Prevalentie van ransomware

Afpersing met behulp van malware bestaat al sinds de late jaren 80 van de vorige eeuw (Ferbrache, 1992; Keane, 1990), maar ransomware is pas wijdverspreid geraakt met de ontwikkeling van sterkere cryptografie en de introductie van cryptocurrencies zoals bitcoin als betaalmethode (Young & Yung, 2017). Het aantal actieve ransomwaresoorten is tussen 2011 en 2021 meer dan tien keer toegenomen. Tegelijkertijd is de levensduur van ransomware afgenomen (Grauer et al., 2022). Zo was de gemiddelde ransomwarevariant in 2022 slechts zeventig dagen actief, mogelijk als gevolg van het feit dat daders hun activiteiten willen verbergen en dus met verschillende ransomwarevarianten werken (Grauer et al., 2023).

Ondanks de grote toename in ransomware-aanvallen, is het moeilijk om de prevalentie van slachtofferschap van ransomware te schatten. Uit onderzoek blijkt dat er tussen 1 januari 2019 en 1 juli 2022 in totaal 453 ransomware-aanvallen gemeld zijn bij de Nederlandse politie (Meurs et al., 2022b). Tegelijkertijd is onduidelijk in hoeverre dit representatieve cijfers zijn, gezien de onderrapportage voor cybercriminaliteit in het algemeen (Van de Weijer et al., 2019) en ransomware in het bijzonder (CBS, 2023; Van de Weijer et al., 2020) (zie ook paragraaf 2.5). Ook zelfrapportagestudies kunnen inzicht geven in de omvang van het probleem. De weinige empirische studies die zelfgerapporteerd slachtofferschap van ransomware onder consumenten of burgers hebben gemeten, rapporteren prevalentiecijfers tussen de 0,2% en 4,8% over een periode van één jaar (Bergmann et al., 2018; Cartwright et al., 2023; CBS, 2019; Conradie, 2023; Ortloff et al., 2021; Simoiu et al., 2019; Van de Weijer & Leukfeldt, 2023; Voce & Morgan, 2023; Yilmaz et al., 2022). Uit empirische studies in Europese landen en Australië blijkt dat de prevalentie van slachtofferschap van ransomware onder bedrijven tussen de 0,7% en 6% ligt over een periode van één jaar (CBS, 2023; European Commission, 2022; Matthijsse et al., 2024; Van de Weijer & Leukfeldt, 2023; Voce & Morgan, 2021). Ook bij deze studies is het echter moeilijk om conclusies over de prevalentie te trekken, mede omdat de steekproefgroottes variëren, niet in alle studies gebruikgemaakt is van representatieve steekproeven en studies betrekking hebben op verschillende landen en tijdsperioden. Dit illustreert dat er meer representatief onderzoek nodig is naar slachtofferschap van ransomware onder burgers en bedrijven.

2.3 Aard en impact van ransomware

Ransomware behelst meer dan slechts de versleuteling van gegevens, afpersing en betaling. Het kan gekarakteriseerd worden als een complex delict bestaande uit meerdere stappen voor zowel daders als slachtoffers (Matthijsse et al., 2023). De modus operandi ontwikkelt bovendien voortdurend (Matthijsse et al., 2023; Whelan et al., 2023). In deze paragraaf wordt in grote lijnen beschreven welke stappen in het delict onderscheiden kunnen worden.

Voor daders begint het delict met het vormen van een criminele samenwerking, het opzetten van de infrastructuur en het ontwikkelen van de malware (Matthijsse et al., 2023). Het slachtoffer raakt betrokken op het moment dat de daders toegang tot het systeem of netwerk van het slachtoffer krijgen, bijvoorbeeld door middel van phishing, een geïnfecteerde website, het misbruiken van kwetsbaarheden in software of systemen of het kopen van toegang (via een zogenoemde *initial access broker*[4]) (Al-rimy et al., 2018; Conti et al., 2018; Dargahi et al., 2019; Matthijsse et al., 2023). Vervolgens voeren de daders verschillende acties in het systeem uit, zoals verkenning van het netwerk, gebruikersrechten verhogen, het verwijderen van back-ups en het stoppen van anti-

4 Een andere partij die zich specialiseert in het verkrijgen van toegang tot systemen en deze vervolgens doorverkoopt (Europol, 2023; Matthijsse et al., 2023).

virusdiensten (Akbanov et al., 2019; Dargahi et al., 2019; Matthijsse et al., 2023). Dit proces kan weken tot maanden duren (Matthijsse et al., 2023). Daarnaast exfiltreren veel ransomwaregroepen tegenwoordig ook data voorafgaand aan de versleuteling, wat tijdens de afpersing gebruikt wordt om het slachtoffer verder onder druk te zetten om te betalen (Matthijsse et al., 2023; Meurs & Holterman, 2023). Zodra dit voltooid is worden de data versleuteld en het slachtoffer geconfronteerd met een losgeldbericht (Al-rimy et al., 2018; Matthijsse et al., 2023). Waar in het verleden meestal alleen gedreigd werd met de versleutelde gegevens, wordt tegenwoordig door veel groeperingen *double* of *triple extortion* toegepast, waarbij naast versleuteling ook gedreigd wordt met bijvoorbeeld het lekken van data of het inlichten van de Autoriteit Persoonsgegevens (Matthijsse et al., 2023). In deze fase heeft het slachtoffer de keuze om wel of niet te betalen. Daarnaast wordt er in sommige gevallen gecommuniceerd of onderhandeld voorafgaand aan betaling, soms met behulp van een incidentresponsebedrijf (Meurs et al., 2022b). Voor het slachtoffer kan dit onder andere nuttig zijn om vast te stellen of het communicatiekanaal nog actief is, hulp te vragen bij het aanschaffen van bitcoins of om te onderhandelen over de hoogte van het losgeld (Caporusso et al., 2019; Matthijsse et al., 2023). Ook voor de daders kan communicatie nuttig zijn om vertrouwen te wekken (bijvoorbeeld door een deel van de gegevens vrij te geven) en het slachtoffer te overtuigen om het losgeld te betalen (Caporusso et al., 2019). Indien het slachtoffer betaald heeft, wordt doorgaans automatisch een decryptieproces gestart of krijgen slachtoffers een decryptiesleutel om zelf hun data te ontsleutelen (Conti et al., 2018; Matthijsse et al., 2023). Sommige groeperingen hebben een klantenservice om slachtoffers te ondersteunen in dit proces (Keshavarzi & Ghaffary, 2020). Indien het slachtofer niet betaalt, worden de data doorgaans verwijderd (Matthijsse et al., 2023).

De impact van ransomware kan groot zijn, en uit zich op verschillende wijzen. Aangezien ransomware een misdrijf met een financieel motief is, is er in de eerste plaats sprake van een financiële impact, ook in gevallen waarin geen losgeld betaald is. Internationaal onderzoek toont aan dat het geëiste losgeldbedrag voor burgers kan oplopen tot $ 8.000, hoewel het gemiddelde rond $ 500 ligt (Ortloff et al., 2021; Simoiu et al., 2019). De losgeldbetaling kan bij bedrijven volgens het CBS (2023) variëren van 1% tot meer dan 50% van de totale omzet van het bedrijf. Naast een eventuele losgeldbetaling, kan er ook sprake zijn van andere kostenposten. Hierbij kan gedacht worden aan productie- of omzetverlies omdat de bedrijfsvoering tijdelijk stil is komen te liggen, het inhuren van ICT-specialisten om de schade te beperken of kosten vanwege herstelwerkzaamheden (Brennenraedts et al., 2022; CBS, 2023; Meurs et al., 2022b). Cijfers van het CBS (2023) laten bijvoorbeeld zien dat bijna de helft van de slachtoffers andere kosten dan de losgeldbetaling heeft gemaakt. Voor veel bedrijven bedroegen deze kosten minder dan 1% van de omzet, maar bij sommige bedrijven waren deze overige kosten tussen de 10% en 50% van de omzet van het bedrijf. Daarnaast kan sprake zijn van boetes, bijvoorbeeld van de privacytoezichthouder, of schadevergoedingen (Brennenraedts et al., 2022; Connolly & Borrion, 2022). Sommige organisaties die slachtof-

fer worden, lopen bovendien het risico op faillissement (Bambenek & Bashir, 2020; Connolly & Borrion, 2022).

Ten tweede kan er sprake zijn van andere type gevolgen, zoals verlies van data, klachten van klanten, reputatieschade of identiteitsdiefstal (Connolly & Borrion, 2022; Matthijsse et al., 2023; Voce & Morgan, 2021). Ten derde kan er sprake zijn van fysieke, emotionele of psychologische gevolgen. Zo blijkt uit een surveyonderzoek van Northwave (2022) onder medewerkers van bedrijven die slachtoffer van ransomware zijn geworden dat in de eerste week van het incident slaapproblemen, vermoeidheid en hoofdpijn veel voorkwamen. Sommige van deze symptomen waren weken tot maanden na het incident nog aanwezig. Bij 1 van de 7 medewerkers was bovendien sprake van dusdanig ernstige symptomen van *distress* (o.a. slaapproblemen, dromen over het incident, ongewenste gedachten aan het incident) dat psychologische traumahulp wenselijk zou zijn (Northwave, 2022). Ook in andere onderzoeken is naar voren gekomen dat slachtofferschap van cybercriminaliteit kan leiden tot fysieke, emotionele of psychische gevolgen (Akkermans et al., 2023; Button et al., 2021; Leukfeldt et al., 2018). Tot slot kan ransomware een bredere maatschappelijke impact hebben, bijvoorbeeld de verstoring van ketenprocessen of vitale sectoren, zoals de politie, overheidsinstellingen of de energiesector (Brennenraedts et al., 2022; NCTV, 2021).

2.4 Betalingsbereidheid

Zodra een slachtoffer wordt geconfronteerd met gegevensversleuteling en een losgeldeis, heeft het slachtoffer de keuze om het losgeld te betalen. Hoewel uit quasi-experimentele studies blijkt dat de bereidheid om het losgeld te betalen in een hypothetisch scenario laag is onder burgers en ondernemers (Cartwright et al., 2023; Matthijsse et al., 2024), schetsen daadwerkelijke betalingspercentages een ander beeld. Op basis van zelfrapportages blijkt dat tussen 0,7% en 25% van de burgers het losgeld heeft betaald na slachtofferschap (Cartwright et al., 2023; CBS, 2019; Ortloff et al., 2021; Simoiu et al., 2019; Yilmaz et al., 2022). Daarnaast blijkt op basis van politieaangiftes, zelfrapportagestudies en informatie van incidentresponsepartijen dat tussen de 14% en 32,2% van de organisaties het losgeld betaalt (CBS, 2023; Meurs et al., 2022b; Project Melissa, 2024; Voce & Morgan, 2021). Kanttekening hierbij is dat dit kan verschillen tussen bedrijfsgroottes. Zo vonden Voce & Morgan (2021) dat meer mkb-eigenaren het losgeld betaalden dan niet-mkb-eigenaren en werknemers. Daarnaast vond het CBS (2023) dat de betalingsbereidheid het hoogste is onder microbedrijven. Minder dan 1% (0,1%) van de zzp'ers, 14% van de microbedrijven, 5,1% van de kleine bedrijven, 5,2% van de middenbedrijven en 4,1% van de grote bedrijven betaalde het losgeld na slachtofferschap (CBS, 2023).

Verschillende factoren kunnen de beslissing om het losgeld te betalen beïnvloeden. Sommige wetenschappelijke studies hebben zich gericht op de mate waarin de kenmerken van het losgeldbericht de betalingsbereidheid kunnen beïnvloeden. Hadlington (2017) analyseerde 76 losgeldberichten om te kijken naar het gebruik van drie psychologische mechanismen gebruikt bij social engineering – schaarste, autoriteit en *liking*[5] – om een slachtoffer te beïnvloeden (zie ook Cialdini, 2006). Een gevoel van schaarste wordt gecreëerd door een timer en andere dreigingen, zoals dat alleen de daders de gegevens kunnen ontsleutelen of dat gegevens verwijderd of gelekt worden nadat de deadline is verstreken. Schaarste kan een gevoel van urgentie creëren dat slachtoffers aanzet tot snelle beslissingen. Een gevoel van autoriteit kan gecreëerd worden door duidelijke, gedetailleerde informatie in het losgeldbericht, het aanbieden van een klantenservice of het gebruik van officiële handelsmerken, logo's (bijvoorbeeld een logo van een wetshandhavingsinstantie) of afbeeldingen. Hierdoor zullen slachtoffers meer vertrouwen hebben in het feit dat ze hun bestanden terugkrijgen na betaling. Tot slot kunnen losgeldberichten met humoristische tekst ervoor zorgen dat het slachtoffer de aanvaller aardig vindt en hem of haar aanzetten tot betaling (Hadlington, 2017). Hoewel de invloed van de psychologische mechanismen niet werd getest in de studie van Hadlington (2017), hebben andere studies wel een experimentele opzet. Arief et al. (2020) onderzochten bijvoorbeeld de relatie tussen het ontwerp van een losgeldbericht (een tekstvariant, een scherm met een timer en een scherm met een meer geavanceerde gebruikersinterface) en de waarschijnlijkheid van betalen. Ze vonden geen significante relatie. Wel gaven respondenten aan dat een autoritaire toon (bijvoorbeeld voordoen als wethandhaving), typfouten, de vermelding van bitcoin, ingewikkelde instructies en geen duidelijke manier om contact op te nemen met de daders hen zou ontmoedigen om het losgeld te betalen (Arief et al., 2020). Ook Yilmaz et al. (2021) onderzochten de relatie tussen het ontwerp van het losgeldbericht (een tekstvariant, een grafische gebruikersinterface of een grafische gebruikersinterface met een timer) en de waarschijnlijkheid van betalen, evenals de waarschijnlijkheid van melden. Ongeveer 5% van de respondenten gaf aan dat ze het losgeld zouden betalen. Er werden geen significante verschillen gevonden tussen de experimentele groepen in de waarschijnlijkheid van betalen.

De resultaten van deze studies geven aan dat mogelijk andere factoren dan het ontwerp van het losgeldbericht een rol kunnen spelen in de betalingsbereidheid. Enkele studies hebben aan de hand van een hypothetisch scenario onderzocht welke aspecten of redenen een rol kunnen spelen in de betalingsbereidheid. Zo werd in een vignetstudie onder ondernemers in het mkb gevonden dat geadviseerd worden om te betalen door een cybersecuritybedrijf en het niet hebben van een back-up de waarschijnlijkheid van betalen van het losgeld significant verhogen (Matthijsse et al., 2024). In een andere studie onder consumenten werd gevonden dat jonge mensen, vrouwen, respondenten die foto's opslaan, respondenten die minder frequent back-ups maken en respondenten die bezorgd zijn over datalekken meer bereid zijn om het losgeld te betalen (Cartwright et al., 2023). Daarnaast vonden de onderzoekers dat respondenten die uit prin-

5 Het idee dat een individu eerder geneigd is om een verzoek in te willigen als hij of zij de persoon aardig vindt (Cialdini, 2006; Hadlington, 2017).

cipe geen geld willen betalen aan criminelen (28%) en weinig waarde hechten aan hun bestanden (25%) de laagste betalingsbereidheid hadden. Respondenten die de daders niet vertrouwen (20%) of hopen met behulp van een expert bestanden terug te krijgen (18%), hebben een hogere betalingsbereidheid, en respondenten die zouden betalen als de prijs goed is (1%) hebben de hoogste betalingsbereidheid (Cartwright et al., 2023).

Aanvullend zijn er studies die de redenering beschrijven van slachtoffers van ransomware betreffende de keuze om het losgeld te betalen. De beslissing om te betalen is vaak gebaseerd op een kosten-batenanalyse en slachtoffers kunnen meerdere motieven hebben om (niet) te betalen (Connolly & Borrion, 2022). Redenen om te betalen voor individuen en organisaties zijn onder andere het niet kunnen herstellen van data via back-ups, het niet willen verliezen van gegevens, geadviseerd worden om het losgeld te betalen, een te lange stilstand van bedrijfsprocessen, de dreiging van faillissement, angst voor beschuldigingen van de gegevensbeschermingsautoriteit, de mogelijkheid dat data gelekt of online verkocht wordt als niet betaald wordt, de overtuiging dat toegang tot de data niet hersteld wordt na betaling, het losgeld kunnen veroorloven, en een gebrek aan computerkennis (Connolly & Borrion, 2022; Matthijsse et al., 2023; Simoiu et al., 2019; Voce & Morgan, 2021). Daarnaast blijkt uit een studie gebaseerd op politieaangiftes dat er een significant verband is tussen de waarschijnlijkheid om het losgeld te betalen en de hoogte van het gevraagde losgeldbedrag na onderhandelingen, het aantal dagen dat onderhandeld is, of er data gestolen zijn, of er sprake is van chantage (bijvoorbeeld dat de daders contact opnemen met werknemers of klanten) en de mogelijkheid om data te herstellen via een back-up (Meurs et al., 2022b).

Op basis van de literatuur zijn redenen om niet te betalen voor individuen en organisaties onder andere: het kunnen herstellen via back-ups of op een andere manier, dat de bestanden het niet waard zijn, het niet kunnen veroorloven van het losgeldbedrag, geadviseerd worden om niet te betalen, de overtuiging dat de dreiging nep is, om verdere afpersing te voorkomen, de overtuiging dat het onethisch is om criminelen te betalen of misdaad te faciliteren, en onzekerheid over de uitkomst omdat de daders een kopie van de gestolen gegevens kunnen bewaren om te verkopen of lekken (Cartwright et al., 2023; Connolly & Borrion, 2022; Matthijsse et al., 2023; Voce & Morgan, 2021, 2022; Yilmaz et al., 2021).

Sommige studies spreken elkaar tegen over de rol van verzekeringen bij bedrijven. Terwijl in een onderzoek op basis van interviews met experts werd gevonden dat slachtoffers het losgeld betalen omdat ze verzekerd zijn (Matthijsse et al., 2023), gaven slachtoffers in een enquêteonderzoek aan dat ze het losgeld betaalden omdat ze geen verzekering hadden (Voce & Morgan, 2021). Hoewel de studies geen verdere details geven, zou deze tegenstrijdigheid verklaard kunnen worden door het feit dat het voor onverzekerde bedrijven mogelijk voordeliger is om het losgeld te betalen dan de financiële kosten te dragen die vaak geassocieerd worden met slachtofferschap van ransom-

ware, zoals herstelkosten of inkomstenderving als gevolg van stilgelegde bedrijfsactiviteiten (Brennenraedts et al., 2022; Connolly & Borrion, 2022; Knebel et al., 2021). Verzekerde bedrijven daarentegen krijgen soms een vergoeding voor de betaling van losgeld, afhankelijk van het type dekking. Dit kan losgeldbetalingen aanmoedigen en vergemakkelijken (Mott et al., 2023).

2.5 Meldingsbereidheid

Tijdens of na het ransomware-incident hebben slachtoffers de keuze om melding te doen bij een organisatie of instantie. Uit eerder onderzoek blijkt dat er sprake is van onderrapportage van cybercriminaliteit bij de politie (Van de Weijer et al., 2019). Onderrapportage ontstaat onder andere doordat slachtoffers het incident niet als ernstig ervaren of weinig tot geen schade ervaren, het incident intern of met behulp van een andere organisatie dan de politie afhandelen, en omdat er een gebrek aan vertrouwen is in de politie als het gaat om de bestrijding van cybercriminaliteit (Conradie, 2023; Cybbar & CSD, 2023; Van de Weijer et al., 2020; Veenstra et al., 2015; Wanamaker, 2019). Wel blijken sommige slachtoffers van cybercriminaliteit een melding of aangifte te doen bij een andere partij dan de politie, zoals de Fraudehelpdesk (Conradie, 2023).

Ook voor ransomware is de meldingsbereidheid bij de politie laag. Hoewel uit onderzoek blijkt dat 69% van de respondenten bereid zou zijn om het incident bij de politie te melden als ze (hypothetisch) slachtoffer zouden worden van ransomware (European Commission, 2022), laten zelfrapportages een ander beeld zien. Uit Nederlands onderzoek blijkt dat 5,7% van de burgers die slachtoffer zijn geworden van ransomware melding van het incident heeft gemaakt bij de politie, terwijl dit voor andere cyberdelicten zoals identiteitsfraude, cyberstalking en marktplaatsfraude hoger is (respectievelijk 47,4%, 30% en 25,6% onder burgers) (Van de Weijer et al., 2020). De meldingsbereidheid is hoger onder bedrijven in vergelijking met burgers. Tussen de 13% en 16,7% van de Nederlandse bedrijven die slachtoffer zijn geworden van ransomware heeft melding gemaakt bij de politie (CBS, 2023; Van de Weijer et al., 2020). Uit cijfers van het CBS (2023) blijkt dat dit percentage hoger is onder midden- en grote bedrijven (ongeveer 35%) ten opzichte van zelfstandigen-zonder-personeel (ongeveer 1-2%) en micro- (ongeveer 5%) en kleine bedrijven (ongeveer 21%). In internationale onderzoeken ligt het meldingspercentage bij de politie door burgers en organisaties tussen de 9% en 23% (European Commission, 2022; Simoiu et al., 2019; Voce & Morgan, 2022).

Terwijl de bereidheid om naar de politie te stappen na slachtofferschap laag is, blijkt tegelijkertijd uit meerdere studies dat slachtoffers van ransomware eerder geneigd zijn om bij andere partijen hulp te vragen, zoals vrienden of familie, externe adviseurs, een cybersecuritybedrijf of een financiële instelling (CBS, 2023; Connolly & Borrion, 2022; Simoiu et al., 2019, 2019; Voce & Morgan, 2022; Yilmaz et al., 2022). In de studie van Van de Weijer et al. (2020) heeft bijvoorbeeld 24,5% van de burgers en 26,7% van midden- en kleinbedrijven die slachtoffer zijn geworden van ransomware het delict gemeld

bij een organisatie anders dan de politie (waarbij onduidelijk is om welke organisatie(s) dit gaat). Daarnaast blijkt uit cijfers van het CBS (2023) dat 39% van alle bedrijven met 2 of meer medewerkers die slachtoffer zijn geworden de hulp inschakelt van een cybersecuritybedrijf (en eventueel ook de politie), ten opzichte van 13% die alleen naar de politie stapt. Dit blijkt ook uit internationale onderzoeken. Zo vond een Australisch onderzoek dat 10% van de slachtoffers van ransomware aangifte deed bij de politie, terwijl een hoger percentage bij niemand hulp zocht (28%) of bij andere partijen, zoals bij vrienden of familieleden (29%), een internetserviceprovider (14%) of een financiële instelling (14%) (Voce & Morgan, 2022).

In het Australische onderzoek is naast de meldingspercentages ook onderzocht welke overwegingen een rol spelen in de beslissing om slachtofferschap van ransomware te melden bij de politie of het Australian Cyber Security Centre (ACSC), de uitkomst van de melding en tevredenheid met de politie en het ACSC. De respondenten die melding hebben gedaan, noemden het vaakst dat ze dit deden om te voorkomen dat het henzelf opnieuw of een ander zou overkomen, om een veiligere online omgeving te creëren, en om geld terug of de schade vergoed te krijgen. De slachtoffers van ransomware die geen aangifte hebben gedaan, noemden als meest voorkomende redenen dat ze het incident zelf hebben opgelost, het incident niet als een serieus misdrijf zagen of niet dachten dat de politie of het ACSC iets kon doen (Voce & Morgan, 2022).

3 Methodologie

3.1 Deelstudie 1 & 2

Om de onderzoeksvragen in deelstudie 1 over de prevalentie, aard en impact van slachtofferschap van ransomware te beantwoorden, zijn twee online vragenlijsten ontwikkeld en uitgezet onder burgers en ondernemers. Om de onderzoeksvragen in deelstudie 2 te beantwoorden, zijn twee online vragenlijsten met een vignetexperiment ontwikkeld en uitgezet onder burgers en ondernemers.

3.1.1 *Steekproef*

3.1.1.1 *Burgers*

Om Nederlandse burgers te bereiken, is gebruikgemaakt van het Research Panel van onderzoeksbureau I&O Research (tegenwoordig Ipsos I&O). Het I&O Research Panel bestaat uit meer dan 37.000 panelleden van 16 jaar en ouder. Panelleden worden geworven via steekproeven uit bijvoorbeeld (gemeentelijke) bevolkingsregisters en adresbestanden. Panelleden ontvangen voor elk ingevuld onderzoek spaarpunten die ze kunnen inwisselen voor een bol.com-tegoedbon of een donatie aan een goed doel. Dankzij de grootte van het panel en de achtergrondkenmerken die over panelleden bekend zijn, is het mogelijk om representatief steekproefonderzoek uit te voeren (Ipsos I&O, n.d.-b).

Om over een grote representatieve groep Nederlandse burgers uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware, zijn alle panelleden van 18 jaar en ouder (n=35.970) tussen 11 en 24 september 2023 uitgenodigd om een vragenlijst in te vullen over slachtofferschap van online criminaliteit. Gedurende de dataverzamelingsperiode is, naast de initiële uitnodiging, één rappel uitgestuurd. De vragenlijst bevatte drie screeningsvragen. Ten eerste zijn respondenten aan het begin van de vragenlijst gevraagd om voor acht vormen van cybercriminaliteit (waaronder phishing, datingfraude en ransomware) aan te geven of ze dit ooit (of een poging hiertoe)[6] hadden meegemaakt. Ransomware werd hierbij gedefinieerd als 'uw bestanden, gegevens of appara(a)t(en) werden geblokkeerd of versleuteld en er werd om losgeld

6 Een poging is hierbij expliciet vermeld om geen respondenten uit te sluiten die wel slachtoffer zijn geworden, maar bijvoorbeeld geen geld hebben betaald of van wie geen geld is gestolen.

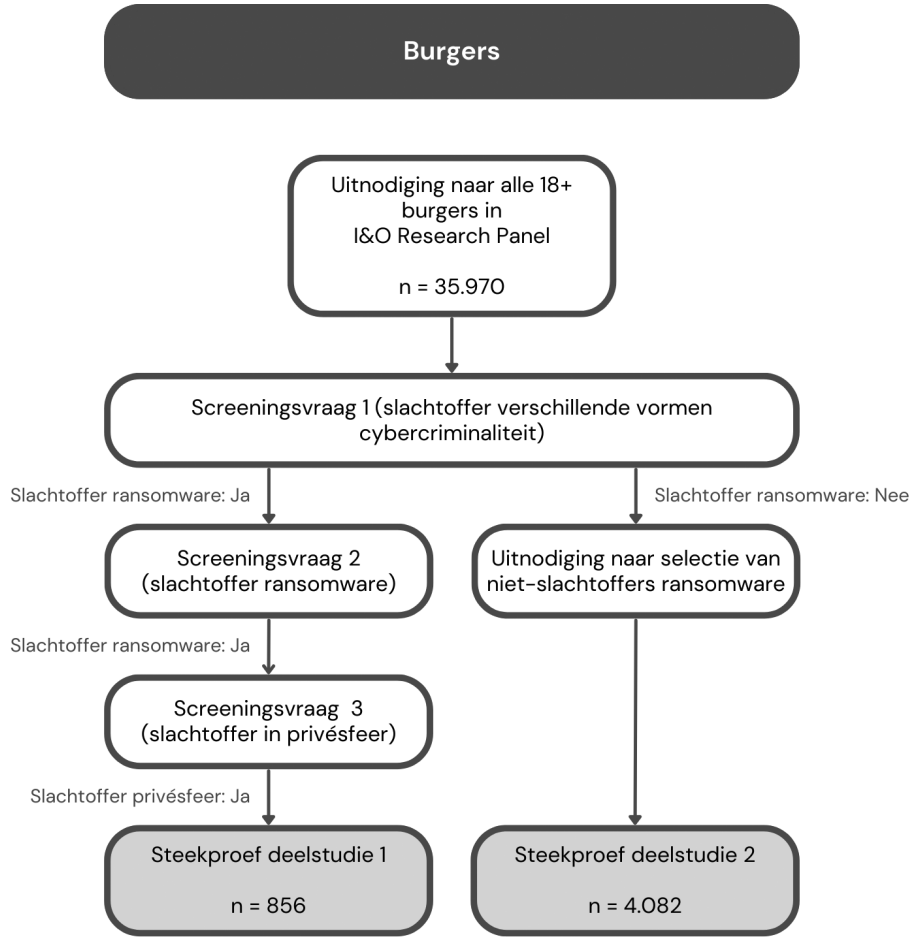
gevraagd om hier weer toegang tot te krijgen'. Slachtofferschap van ransomware omvat zodoende ook de gevallen waarbij er sprake was van een blokkade of versleuteling, maar waarbij individuen niet overgegaan zijn tot betaling van het losgeld.

De respondenten die hadden aangegeven ransomware te hebben meegemaakt, werd vervolgens een tweede screeningsvraag gesteld waarbij nogmaals dezelfde definitie van ransomware werd gegeven en werd gevraagd of de respondenten dit was overkomen. Ten derde werd aan deze respondenten gevraagd of ze zelf slachtoffer waren geworden, of dat de organisatie waar ze werkzaam waren slachtoffer was geworden. De respondenten die ransomware hebben meegemaakt en zelf slachtoffer zijn geworden, zijn vervolgens direct doorverwezen naar vragen over hun ervaringen met slachtofferschap (*deelstudie 1A*). Na het eruit filteren van de speeders,[7] afgebroken vragenlijsten en respondenten die slachtoffer van een ander cyberdelict bleken te zijn op basis van de open antwoorden, zijn de screeningsvragen beantwoord door 20.659 burgers (respons: 57,4%) en bestaat de steekproef voor deelstudie 1 uit 856 burgers (respons: 2,4%). De data van de 20.659 respondenten die de screeningsvragen hebben beantwoord zijn gewogen naar leeftijd, geslacht en opleiding om representatieve uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware onder burgers in Nederland. De data van de 856 respondenten in deelstudie 1 zijn niet gewogen, aangezien het doel was om meer inzicht te krijgen in de groep respondenten die slachtoffer is geworden van ransomware, en niet zozeer om een representatieve steekproef te bereiken. Binnen deze steekproef zijn respondenten relatief vaker man dan in de populatie van burgers in Nederland het geval is. De steekproef wijkt minder sterk af van de populatie als het gaat om leeftijd en opleidingsniveau, maar respondenten zijn relatief minder vaak laag opgeleid en 65 jaar of ouder dan de populatie van burgers in Nederland.

Uit de panelleden die bij de eerste screeningsvraag hebben aangegeven geen slachtoffer te zijn geworden van ransomware, is een steekproef representatief op geslacht, leeftijd, opleiding en regio getrokken van 6.000 panelleden.[8] Deze panelleden zijn tussen 2 en 15 oktober 2023 uitgenodigd om een vragenlijst in te vullen over beslissingsgedrag in een hypothetisch ransomwarescenario (*deelstudie 2A*). Gedurende de dataverzamelingsperiode is, naast de initiële uitnodiging, één rappel uitgestuurd. Na het eruit filteren van de speeders[9] en afgebroken vragenlijsten, bestaat de steekproef voor deelstudie 2 uit 4.082 burgers (respons: 68%). De data in deelstudie 2 zijn gewogen naar leeftijd, geslacht en opleiding om de steekproef representatief te maken voor de populatie van burgers in Nederland.

7 Respondenten die 1/3 van de mediaan of minder lang hebben gedaan over het invullen van de vragenlijst.
8 Deze steekproef is getrokken op basis van de Gouden Standaard van MOA (expertisebureau voor Marketing Insights, Onderzoek en Analytics). Het betreft een ijkingsinstrument voor nationale en regionale steekproeven, gebaseerd op data van het CBS. De steekproef is zodoende een afspiegeling van de Nederlandse samenleving op dat moment.
9 Respondenten die 1/3 van de mediaan of minder lang hebben gedaan over het invullen van de vragenlijst.

Een schematisch overzicht van de steekproeftrekking voor burgers is te vinden in figuur 3.1. De achtergrondkenmerken van de respondenten zijn opgenomen in tabel 3.1.



Figuur 3.1 Steekproeftrekking deelstudie 1 en 2 voor burgers

Tabel 3.1 (Gewogen) achtergrondkenmerken van burgers

	Screeningsvragen (n=20.659)		Deelstudie 1A (n=856)		Deelstudie 2A (n=4.082)	
	N	**%**	**N**	**%**	**N**	**%**
Geslacht	**20.651**		**856**		**4.082**	
Man	10.117	49%	616	72%	2.001	49%
Vrouw	10.454	50,6%	239	27,9%	2.068	50,7%
Genderneutraal	80	0,4%	1	0,1%	12	0,3%
Leeftijd	**20.649**		**854**		**4.082**	
18 t/m 34	5.410	26,2%	232	27,2%	1.033	25,3%
35 t/m 49	3.876	18,8%	196	22,9%	792	19,4%
50 t/m 64	6.547	31,7%	279	32,7%	1.302	31,9%
65+	4.816	23,3%	147	17,2%	954	23,4%
Opleiding	**20.512**		**848**		**4.082**	
Laag	4.324	21,1%	155	18,3%	869	21,3%
Middelbaar	8.145	39,7%	355	41,9%	1.619	39,7%
Hoog	8.044	39,2%	338	39,9%	1.594	39%
Werksituatie	**20.652**		**856**		**4.082**	
Werkzaam in loondienst	11.520	55,8%	536	62,7%	2.330	57,1%
Niet werkzaam (bijv. arbeidsongeschikt, gepensioneerd)	7.161	34,7%	249	29,1%	1.441	35,3%
Studerend/schoolgaand	1.557	7,5%	54	6,3%	229	5,6%
Anders	415	2%	17	1,9%	82	2%
Jaarinkomen (bruto)	**20.514**		**856**		**4.059**	
Minimum (minder dan € 14.100)	1.272	6,2%	69	8,1%	257	6,3%
Beneden modaal (€ 14.100 tot € 29.500)	2.489	12,1%	107	12,5%	503	12,4%
Bijna modaal (€ 29.500 tot € 36.500)	2.539	12,4%	110	12,9%	507	12,5%
Modaal (€ 36.500 tot € 43.500)	3.424	16,7%	144	16,9%	689	17%
Tussen 1 en 2 keer modaal (€ 43.500 tot € 73.000)	4.709	23%	203	23,7%	927	22,8%
Twee keer modaal (€ 73.000 tot € 87.100)	1.524	7,4%	72	8,4%	311	7,7%
Meer dan 2 keer modaal (€ 87.100 of meer)	1.877	9,1%	66	7,7%	384	9,5%
Weet niet/wil niet zeggen	2.680	13,1%	85	9,9%	481	11,8%

3.1.1.2 *Ondernemers*

Het doel was om naast burgers, ook mkb'ers en zzp'ers te bereiken. Om een zo groot mogelijke groep ondernemers te bereiken, is zowel gebruikgemaakt van het eerder beschreven Research Panel als het Ondernemerspanel van onderzoeksbureau I&O Research (tegenwoordig Ipsos I&O). Het I&O Research Panel bevat 2.145 zzp'ers en 559 ondernemers met personeel. Het I&O Ondernemerspanel bestaat uit 2.302 zzp'ers en 1.984 mkb'ers, die grotendeels geworven worden via steekproefonderzoek (Ipsos I&O, n.d.-a).

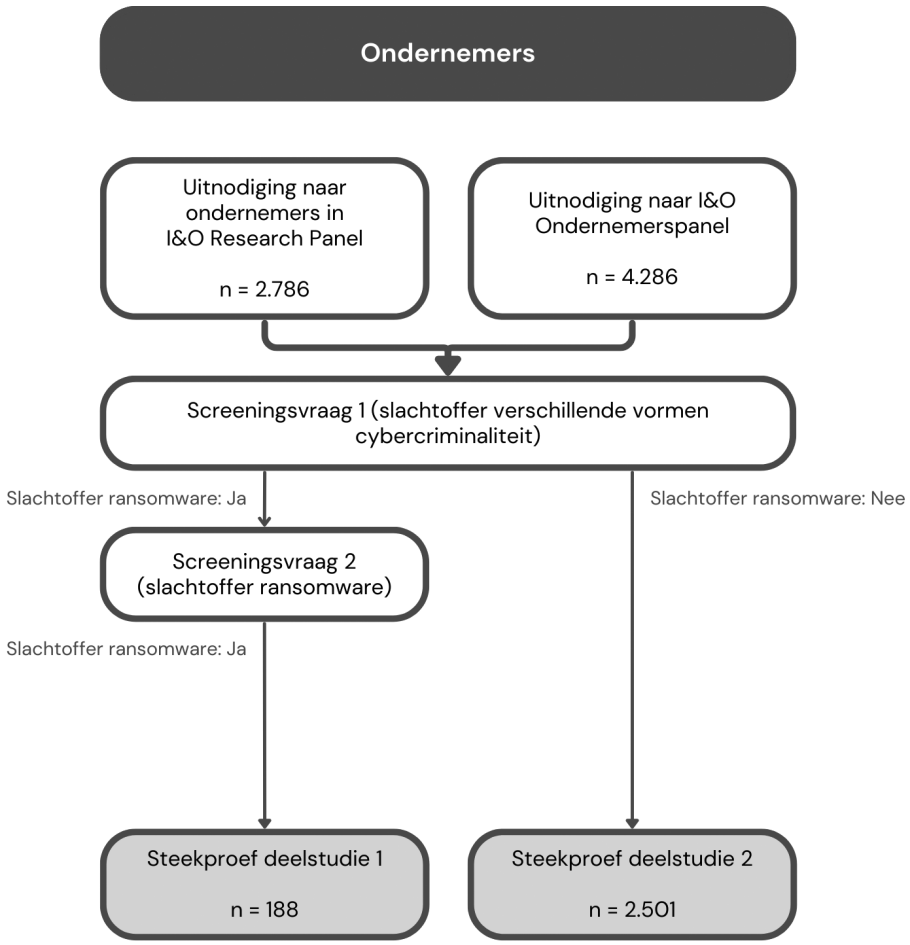
Alle 7.072 ondernemers in het I&O Research Panel en het I&O Ondernemerspanel zijn tussen 25 september 2023 en 29 oktober 2023 uitgenodigd om een vragenlijst in te vullen over slachtofferschap van online criminaliteit. Gedurende de dataverzamelingsperiode zijn, naast de initiële uitnodiging, drie rappels uitgestuurd. Er is gebruikgemaakt van meer rappels in vergelijking met de dataverzameling onder burgers omdat de benodigde nettosteekproef bij ondernemers minder snel bereikt werd. De vragenlijst bestond uit twee screeningsvragen. Ten eerste werd respondenten aan het begin van de vragenlijst gevraagd om voor acht vormen van cybercriminaliteit (waaronder phishing, CEO-fraude en ransomware) aan te geven of ze dit ooit (of een poging hiertoe)[10] in hun bedrijf hebben meegemaakt.[11] Ransomware werd hierbij gedefinieerd als 'de bestanden, gegevens of appara(a)t(en) van uw bedrijf werden geblokkeerd of versleuteld en er werd om losgeld gevraagd om hier weer toegang tot te krijgen'. De respondenten die hebben aangegeven ransomware te hebben meegemaakt, is vervolgens een tweede screeningsvraag gesteld waarbij nogmaals dezelfde definitie van ransomware werd gegeven en werd gevraagd of hun bedrijf dit was overkomen.

De respondenten die beide screeningsvragen bevestigend hebben beantwoord, zijn vervolgens direct doorverwezen naar vragen over hun ervaringen met slachtofferschap (*deelstudie 1B*). Om een zo hoog mogelijke respons te bereiken onder ondernemers, zijn alle ondernemers die geen slachtoffer zijn geworden van ransomware (anders dan bij de steekproeftrekking voor burgers) direct doorverwezen naar vragen over beslissingsgedrag in een hypothetisch ransomwarescenario (*deelstudie 2B*). Na het eruit filteren van de speeders[12], afgebroken vragenlijsten en respondenten waarbij de bedrijfsgrootte niet bekend was, zijn de screeningsvragen beantwoord door 3.040 respondenten (respons: 43%), waarvan 2.077 zzp'ers en 963 mkb'ers. De data van de 3.040 respondenten die de screeningsvragen hebben beantwoord, zijn gewogen om representatieve uitspraken te kunnen doen over de prevalentie van slachtofferschap van ransomware onder ondernemers in Nederland. De data van de mkb'ers zijn gewogen naar grootteklasse en sector, de data van de zzp'ers naar sector. De steekproef voor deelstu-

10 Een poging is hierbij expliciet vermeld om geen respondenten uit te sluiten die wel slachtoffer zijn geworden, maar bijvoorbeeld geen geld hebben betaald of van wie geen geld is gestolen.
11 Een aantal vormen van criminaliteit zijn voor ondernemers aangepast ten opzichte van de vragenlijst voor burgers. Zo is vriend-in-nood-fraude aangepast naar CEO-fraude.
12 Respondenten die 1/3 van de mediaan of minder lang hebben gedaan over het invullen van de vragenlijst.

die 1B bestaat uit 188 ondernemers (respons: 2,7%), waarvan 88 zzp'ers en 100 mkb'ers. De steekproef voor deelstudie 2B bestaat uit 2.501 respondenten (respons: 35,3%), waarvan 1.769 zzp'ers en 732 mkb'ers.

Een schematisch overzicht van de steekproeftrekking voor ondernemers is te vinden in figuur 3.2. De achtergrondkenmerken van de respondenten zijn opgenomen in tabel 3.2 (zzp'ers) en 3.3 (mkb'ers).



Figuur 3.2 Steekproeftrekking deelstudie 1 en 2 voor ondernemers

Tabel 3.2 (Gewogen) achtergrondkenmerken van zzp'ers

	Screeningsvragen (n=2.077)		Deelstudie 1B (n=88)		Deelstudie 2B (n=1.769)	
	N	**%/gem.**	**N**	**%/gem.**	**N**	**%/gem.**
Onderneming actief (in jaren)	1.968	14,9	83	22,8	1.667	14,6
Sector	**2.070**		**87**		**1.763**	
Landbouw/visserij	60	2,9%	3	3,4%	51	2,9%
Industrie, bouw en nutsbedrijven	303	14,6%	13	14,9%	273	15,5%
Handel en logistiek, horeca	345	16,7%	15	17,2%	306	17,3%
Financiële en zakelijke dienstverlening	733	35,4%	33	37,9%	605	34,3%
Overheid, onderwijs, zorg en overig	629	30,4%	23	26,4%	528	30%
Jaaromzet	**2.053**		**88**		**1.769**	
Minder dan 100.000	1.270	61,9%	47	53,4%	1.124	63,5%
€ 100.000 tot € 500.000	468	22,8%	27	30,7%	391	22,1%
€ 500.000 tot € 1.000.000	47	2,3%	3	3,4%	39	2,2%
€ 1.000.000 tot € 2.500.000	29	1,4%	0	0%	27	1,5%
€ 2.500.000 tot € 5.000.000	15	0,7%	1	1,1%	13	0,7%
Meer dan 5.000.000	37	1,8%	1	1,1%	32	1,8%
Zeg ik liever niet	137	6,7%	9	10,2%	102	5,8%
Weet ik niet	48	2,3%	0	0%	42	2,4%

Tabel 3.3 (Gewogen) achtergrondkenmerken van mkb'ers

	Screeningsvragen (n=963)		Deelstudie 1B (n=100)		Deelstudie 2B (n=732)	
	N	%/gem.	N	%/gem.	N	%/gem.
Onderneming actief (in jaren)	**927**	**28,3**	**96**	**31,4**	**708**	**28,1**
Grootte	**963**		**100**		**732**	
Micro (2-9 werkzame personen)	716	74,4%	70	70,3%	555	75,8%
Klein (10-49 werkzame personen)	216	22,4%	27	27,4%	154	21%
Midden (50-250 werkzame personen)	31	3,2%	2	2,4%	23	3,2%
Sector	**961**		**100**		**730**	
Landbouw/visserij	70	7,3%	7	6,9%	54	7,4%
Industrie, bouw en nutsbedrijven	121	12,6%	11	10,8%	91	12,5%
Handel en logistiek, horeca	336	35%	47	47,5%	256	35,1%
Financiële en zakelijke dienstverlening	219	22,8%	22	22,3%	157	21,5%
Overheid, onderwijs, zorg en overig	214	22,2%	12	12,5%	171	23,4%
Jaaromzet	**937**		**100**		**732**	
Minder dan € 100.000	82	8,8%	8	7,6%	64	8,7%
€ 100.000 tot € 500.000	337	35,6%	31	31,5%	280	38,3%
€ 500.000 tot € 1.000.000	151	16,1%	18	18,3%	113	15,4%
€ 1.000.000 tot € 2.500.000	151	16,1%	19	19,1%	112	15,3%
€ 2.500.000 tot € 5.000.000	73	7,8%	8	8,3%	54	7,4%
Meer dan € 5.000.000	72	7,8%	13	13%	52	7,2%
Zeg ik liever niet	54	5,8%	1	1%	43	5,9%
Weet ik niet	17	1,8%	1	1,3%	13	1,8%

3.1.2 *Meetinstrument*

3.1.2.1 *Deelstudie 1*

Om de gegevens voor deelstudie 1 te verzamelen, zijn twee vragenlijsten ontwikkeld over ervaringen met slachtofferschap van ransomware; één voor burgers (1A) en één voor ondernemers (1B). Beide vragenlijsten bestonden uit vijf blokken. Respondenten werden bevraagd over achtergrondkenmerken, de omstandigheden van de aanval, het losgeldbericht en de afpersing, de gevolgen van het incident en het contact met instanties naar aanleiding van het incident. Waar nodig zijn de vraagstelling of antwoordopties bij de vragenlijst voor ondernemers aangepast naar een bedrijfscontext. Een

vraag over de gevolgen bij de ondernemers bevatte bijvoorbeeld extra antwoordopties, waaronder verhindering in de uitvoering van de dagelijkse werkzaamheden, reputatieschade en onderbreking van levering van goederen. De vragen zijn onder andere gebaseerd op eerder onderzoek (CBS, 2022; Johns, 2021; Matthijsse et al., 2024; Simoiu et al., 2019; Van de Weijer et al., 2020; Voce en Morgan, 2021, 2022; Yilmaz et al., 2022). Omdat er veel nog onbekend is over het fenomeen ransomware is daarnaast bij vrijwel elke vraag een 'anders, namelijk…'-optie toegevoegd om de respondenten de kans te geven aanvullingen te doen om zo een completer beeld te krijgen van ervaringen met slachtofferschap van ransomware. De volledige vragenlijsten zijn in bijlage 1 en bijlage 3 opgenomen.

3.1.2.2 *Deelstudie 2*

Om de gegevens voor deelstudie 2 te verzamelen, zijn twee online vragenlijsten ontwikkeld, één voor burgers (2A) en één voor ondernemers (2B). Beide vragenlijsten bestonden uit drie blokken. Respondenten werd gevraagd naar enkele achtergrondkenmerken, beslissingen naar aanleiding van een hypothetisch ransomwarescenario en (gepercipieerd) slachtofferschap. De volledige vragenlijsten zijn in bijlage 2 en bijlage 4 opgenomen.

Om te onderzoeken welke factoren bepalen of burgers en ondernemers het losgeld betalen en het incident melden in een hypothetisch scenario, is een vignet voorgelegd aan respondenten. Een vignet is een korte, zorgvuldig geconstrueerde beschrijving van een persoon, object of situatie, die een systematische combinatie van kenmerken vertegenwoordigt (Atzmüller & Steiner, 2010, p. 128), bedoeld om attitudes, beslissingen of oordelen van respondenten uit te lokken (Aguinis & Bradley, 2014; Atzmüller & Steiner, 2010). Omdat een vignetexperiment gebruikmaakt van een hypothetisch scenario, is het een nuttige methode voor onderzoek naar gevoelige onderwerpen (zoals slachtofferschap van ransomware) waarbij experimenteel onderzoek minder geschikt is vanwege ethische bezwaren, terwijl er toch controle is over de variabelen die de besluitvorming kunnen beïnvloeden (Aguinis & Bradley, 2014). Bovendien verhoogt een vignetexperiment het realisme en de validiteit en vermindert het sociale-wenselijkheidsbias in vergelijking met directe enquêtevragen (Wason et al., 2022).

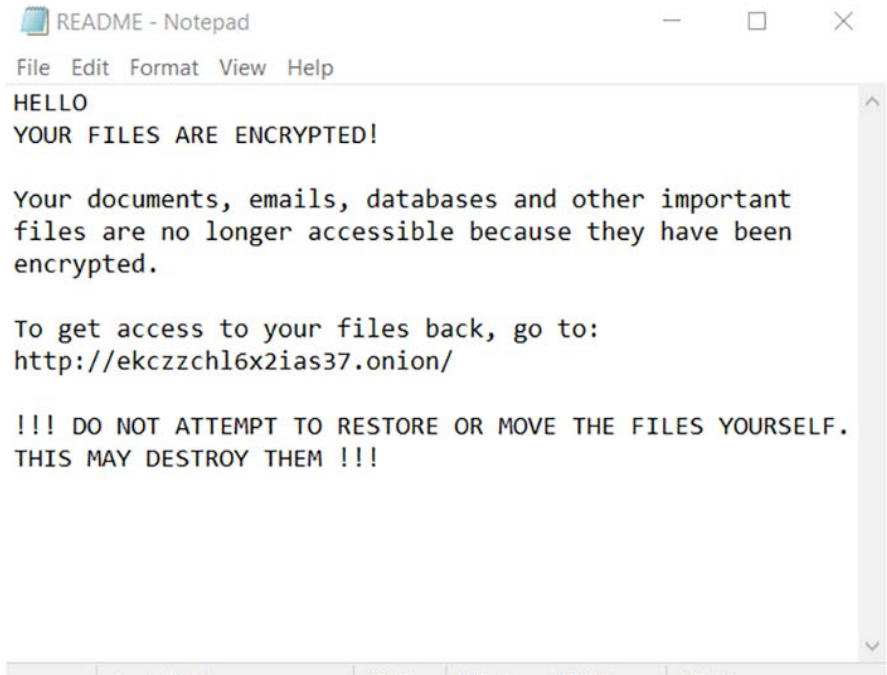
Voorafgaand aan de dataverzameling is er een poweranalyse uitgevoerd om de benodigde steekproefgrootte voor het vignet te bepalen om groepen te vergelijken en statistische verschillen met voldoende betrouwbaarheid te kunnen waarnemen (*power* = 0,8; *alpha* = 0,05) (Cohen, 1988). Omdat het aantal manipulaties gelijk is gehouden voor alle doelgroepen (burgers, zzp'ers en mkb'ers), is de poweranalyse uitgevoerd voor de kleinste steekproef, in dit geval de mkb'ers, ongeacht of er voor andere steekproeven meer manipulaties mogelijk waren. Een poweranalyse voor lineaire regressie gaf aan dat een steekproef van circa ~1.150 mkb'ers ruimte zou bieden aan vier verklarende

factoren om kleine effecten (Cohen's f squared = 0,02) waar te nemen met voldoende statistische power (*power* = 0,8; *alpha* = 0,05) (Cohen, 1988).[13]

Op basis van de poweranalyse zijn er vier factoren met elk twee variaties opgenomen in het vignetexperiment. Dit 2 × 2 × 2 × 2 design resulteerde in 16 verschillende vignetten voor burgers en 16 verschillende vignetten voor ondernemers. De factoren en variaties zijn vastgesteld aan de hand van een literatuurstudie. Zo blijkt uit eerder onderzoek dat de beslissing om het losgeld te betalen onder andere gerelateerd is aan de hoogte van de losgeldeis, of men geadviseerd wordt om te betalen, de beschikbaarheid van back-ups en bezorgdheid om het lekken van data (zie bijv. Cartwright et al., 2023; Connolly & Borrion, 2022; Matthijsse et al., 2024; Meurs et al., 2022b; Voce & Morgan, 2021). Daarnaast is de meldingsbereidheid van cybercriminaliteit onder andere gerelateerd aan de ervaren ernst van een incident of de mate waarin men schade heeft ondervonden (zie bijv. Conradie, 2023; Cybbar & CSD, 2023; Veenstra et al., 2015; Voce & Morgan, 2022; Wanamaker, 2019), wat in het geval van ransomware gerelateerd zou kunnen zijn aan de hoogte van de losgeldeis, de beschikbaarheid van back-ups, dreiging met het lekken van data en advisering om het losgeld te betalen. Er is bovendien advies ingewonnen bij politiemedewerkers bij het vaststellen van de vignetfactoren. Niet alle respondenten kregen dezelfde scenario's voorgelegd omdat er systematisch is gewisseld in de variaties. Er is gebruikgemaakt van een *between persons*-design, wat betekent dat respondenten willekeurig zijn toegewezen aan een groep van ongeveer dezelfde grootte die één scenario te zien kreeg (zie bijlage 5 voor de verdeling over groepen). Het gebruik van een *between persons*-design maakt het mogelijk om vergelijkingen tussen respondenten te maken (Atzmüller & Steiner, 2010).

Alle respondenten werd gevraagd om de hypothetische situatie voor te stellen waarbij de respondent zelf (bij de doelgroep burgers) of het bedrijf van de respondent (bij de doelgroep ondernemers) getroffen was door ransomware en de respondent een beslissing moest nemen over het wel of niet betalen van losgeld en het melden van het incident. Alle respondenten kregen het volgende losgeldbericht (Figuur 3.3) te zien:

13 Deze aantallen zijn wel bereikt voor de groep burgers en zzp'ers, maar niet voor de groep mkb'ers. In de discussie wordt gereflecteerd op wat dit betekent voor de conclusies van het onderzoek.



Figuur 3.3 Losgeldbericht in vignet

Vervolgens werd respondenten meegedeeld dat ze in het scenario door de daders werden doorgestuurd naar een gepersonaliseerde website met een lopende timer. In dit tweede deel is gevarieerd met de vignetfactoren (zie figuur 3.4 voor een voorbeeld). Om het realisme van het vignet te verhogen, zijn zowel het losgeldbericht als de website nagebootst van echte voorbeelden. Zo is het losgeldbericht gebaseerd op losgeldberichten van onder andere de ransomwaregroeperingen Cl0p, Lockbit, BlackCat en Royal. De ransomwarewebsite is gebaseerd op die van de Cl0p-ransomwaregroepering.

Al uw data en systemen zijn ontoegankelijk gemaakt, inclusief bestanden van emotionele waarde. Er is wel een back-up van deze gegevens beschikbaar. U heeft een (cybersecurity)organisatie ingeschakeld voor hulp. De mensen om u heen en deze organisatie adviseren u om niet het losgeld te betalen.

Figuur 3.4 Voorbeeld van een vignet dat is voorgelegd aan een deel van de burgers

De eerste factor in het vignet betrof de hoogte van het losgeld. In het vignet voor burgers stond dit losgeldbedrag vermeld in de afbeelding en varieerde dit tussen 250 euro en 2.500 euro in bitcoin. Voor de ondernemers stond het losgeldbedrag vermeld in de tekst als percentage van de omzet, variërend tussen 1% en 25% van de jaaromzet van de organisatie van de respondent in bitcoin. De losgeldbedragen zijn enerzijds gebaseerd op eerder onderzoek naar ransomware (Conti et al., 2018; Matthijsse et al., 2023; Meurs et al., 2022b, 2022a; zie bijv. Ortloff et al., 2021; Simoiu et al., 2019) en voorbeelden uit de praktijk, en anderzijds op het inzicht van de onderzoekers wat beschouwd zou kunnen worden als een lage en hoge financiële impact voor burgers en ondernemers. De keuze om bij de ondernemers de losgeldeis in een percentage weer te geven, is gemaakt vanwege het feit dat er grote variatie kan zitten in de omzet van de ondernemers, en dus de potentiële financiële impact. Bovendien werd in eerder onderzoek door enkele experts beschreven dat ransomwaregroeperingen zich bij het bepalen van

de losgeldeis baseren op een percentage van de jaaromzet van het bedrijf (Matthijsse et al., 2023).

De tweede factor betrof of er gedreigd is met het lekken van vertrouwelijke data. In een variant van de afbeelding stond niets over lekken vermeld, terwijl in een andere variant de volgende teksten waren opgenomen: 'To decrypt your files and prevent data leakage you need to buy our special software', in combinatie met 'If you do not pay, data will be published on our portal. Anyone will be able to see your confidential information, including your documents photos and videos' (voor burgers) / 'including your financial reports, intellectual property, employee and client data' (voor ondernemers).
De derde factor betrof of er een back-up van de gegevens beschikbaar is, variërend tussen 'Er is wel een back-up van deze gegevens beschikbaar' en 'Er is geen back-up van deze gegevens beschikbaar'.

Ten slotte betrof de vierde factor of respondenten geadviseerd is om het losgeld te betalen, variërend tussen 'U heeft een (cybersecurity)organisatie ingeschakeld voor hulp. De mensen om u heen en deze organisatie adviseren u om wel het losgeld te betalen' en 'U heeft een (cybersecurity)organisatie ingeschakeld voor hulp. De mensen om u heen en deze organisatie adviseren u om niet het losgeld te betalen'.

Na het vignet kregen respondenten een controlevraag voorgelegd voor elke factor (bijvoorbeeld 'Is er binnen de organisatie een back-up van de versleutelde gegevens beschikbaar?' Ja/Nee) om te garanderen dat respondenten zich bewust waren van de omstandigheden van het hypothetische scenario. Vervolgens werd aan respondenten gevraagd hoe waarschijnlijk het was dat respondenten in dit scenario het losgeld zouden betalen en het incident zouden melden op een 11-puntsschaal van helemaal niet waarschijnlijk (0%) tot zeer waarschijnlijk (100%). Daarnaast zijn er andere vragen gesteld, onder andere over wat de respondenten zouden voelen en als eerste zouden doen als ze geconfronteerd zouden worden met het losgeldbericht.

3.1.3 *Analyse*

De data zijn opgeschoond in IBM SPSS Statistics 28.0 en geanalyseerd in IBM SPSS Statistics 28.0, en R-versie 4.3.1 en RStudio-versie 2023.12.0.

Om de deelvragen in deelstudie 1 over de prevalentie, aard en impact van slachtofferschap van ransomware te beantwoorden, is gebruikgemaakt van beschrijvende statistieken. Om de eerste deelvraag in deelstudie 2 te beantwoorden over de bereidheid om het losgeld te betalen en het incident te melden in een hypothetisch scenario is gebruikgemaakt van beschrijvende statistieken. Om de tweede deelvraag in deelstudie 2 over de relatie tussen situationele factoren en de bereidheid tot betalen en melden te beantwoorden, is gebruikgemaakt van regressiemodellen.

Als gevolg van een rechtsscheve verdeling voor de waarschijnlijkheid van betalen onder burgers (*M* = 1,36; *SD* = 2,16; Skewness = 1,700; Kurtosis = 2,233),[14] is de assumptie van een normale verdeling geschonden. Gezien de variantie van de waarschijnlijkheid van betalen hoger was dan het gemiddelde (Variantie = 4,65; *M* = 1,36) is gebruikgemaakt van een negatief binomiaal regressiemodel (Green, 2021; Hilbe, 2011). Het negatieve binomiale regressiemodel dat gebruikt is om de variantie in de waarschijnlijk van betalen te verklaren onder burgers bevat de eerdergenoemde dichotome vignetfactoren. Daarnaast zijn leeftijd, geslacht en opleidingsniveau als controlevariabelen aan het model toegevoegd. De categorische variabelen geslacht en opleidingsniveau zijn gehercodeerd tot dummyvariabelen, met respectievelijk 'vrouw' en 'hoog' als referentiecategorieën.

Aanvullend is er sprake van een linksscheve verdeling voor de waarschijnlijkheid van melden onder burgers (*M* = 7,98; *SD* = 2,86; Skewness = −1,482; Kurtosis = 1,207)[15], waardoor ook hier de assumptie van een normale verdeling is geschonden. Er is gebruikgemaakt van een Poisson-regressiemodel, gezien de variantie van de waarschijnlijkheid van melden vrijwel gelijk is aan het gemiddelde (variantie = 8,20; *M* = 7,98) (Green, 2021). Het Poisson-regressiemodel dat gebruikt is om de variantie in de waarschijnlijk van melden te verklaren onder burgers bevat de eerdergenoemde dichotome vignetfactoren. Daarnaast zijn leeftijd, geslacht en opleidingsniveau als controlevariabelen aan het model toegevoegd. De categorische variabelen geslacht en opleidingsniveau zijn gehercodeerd tot dummyvariabelen, met respectievelijk 'vrouw' en 'hoog' als referentiecategorieën.

De beschrijvende statistieken van de variabelen die zijn opgenomen in de regressiemodellen zijn te vinden tabel 3.4.

14 Blijkens visuele inspectie van de histogram en plots, en een Kolmogorov-Smirnov-test (D(4.082) = 0,323; *p* = 0,000).

15 Blijkens visuele inspectie van het histogram en plots, en een Kolmogorov-Smirnov-test (D(4.082) = 0,263; *p* = 0,000).

Tabel 3.4 Beschrijvende statistieken van geïncludeerde variabelen in de regressiemodellen voor burgers

	N	%	Gem.	SD
Waarschijnlijkheid van betalen (0-10)	4.082		1,36	2,16
Waarschijnlijkheid van melden (0-10)	4.082		7,98	2,86
Leeftijd (18-91)	4.082		1,51	,51
Geslacht	4.082			
– Man (0-1)	2.001	49%		
– Vrouw (0-1)	2.068	50,7%		
– Genderneutraal (0-1)	12	0,3%		
Opleidingsniveau	4.082			
– Laag (0-1)	869	21,3%		
– Middelbaar (0-1)	1.619	39,7%		
– Hoog (0-1)	1.594	39%		
Hoogte losgeld	4.082			
– 250 euro (0-1)	1.999	49%		
– 2.500 euro (0-1)	2.083	51%		
Gedreigd met lekken	4.082			
– Nee (0-1)	2.028	49,7%		
– Ja (0-1)	2.054	50,3%		
Back-up	4.082			
– Nee (0-1)	2.057	50,4%		
– Ja (0-1)	2.025	49,6%		
Geadviseerd om te betalen	4.082			
– Nee (0-1)	2.054	50,3%		
– Ja (0-1)	2.027	49,7%		

Ook bij de ondernemers is de assumptie van een normale verdeling geschonden. Er is sprake van een rechtsscheve verdeling voor de waarschijnlijkheid van betalen onder zzp'ers (*M* = 1,11; *SD* = 1,89; Skewness = 2,016; Kurtosis = 3,799)[16] en mkb'ers (*M* = 1,19; *SD* = 1,98; Skewness = 1,915; Kurtosis = 3,179).[17] Om deze reden zijn bij beide steekproeven negatief binomiale regressiemodellen gebruikt, gezien de variantie van de waarschijnlijkheid van betalen hoger was dan het gemiddelde bij zowel zzp'ers (Variantie = 3,57; *M* = 1,11) als mkb'ers (Variantie = 3,94; *M* = 1,19) (Green, 2021; Hilbe, 2011). Het negatieve binomiale regressiemodel dat gebruikt is om de variantie in de waarschijnlijkheid van betalen te verklaren onder zzp'ers bevat de eerdergenoemde dichotome vignetfactoren. Daarnaast is sector gehercodeerd tot dummyvariabelen en

16 Blijkens visuele inspectie van de histogram en plots, en een Kolmogorov-Smirnov-test (D(1.769) = 0,334; *p* = 0,000).

17 Blijkens visuele inspectie van de histogram en plots, en een Kolmogorov-Smirnov-test (D(732) = 0,328; *p* = < 0,001).

zijn deze als controlevariabelen aan het model toegevoegd, met 'financiële en zakelijke dienstverlening' als referentiecategorie. Het model dat gebruikt is om de variantie in de waarschijnlijkheid van het betalen van het losgeld te verklaren onder mkb'ers bevat de eerdergenoemde dichotome vignetfactoren. Grootteklasse en sector zijn als dummyvariabelen aan het model toegevoegd, met 'financiële en zakelijke dienstverlening' en 'micro' als referentiecategorieën.

Bij de waarschijnlijkheid van melden is sprake van een linksscheve verdeling bij zowel zzp'ers (M = 8,86; SD = 2,34; Skewness = −2,471; Kurtosis = 5,583)[18] als mkb'ers (M = 9,07; SD = 2,10; Skewness = −2,795; Kurtosis = 7,619)[19], waardoor ook hier de assumptie van een normale verdeling is geschonden (Green, 2021). Gezien de variantie van de waarschijnlijkheid van betalen lager is dan het gemiddelde bij zowel zzp'ers (Variantie = 5,50; M = 8,86) als mkb'ers (Variantie = 4,43; M = 9,07), is gebruikgemaakt van negatief binomiale regressiemodellen (Green, 2021; Hilbe, 2011). Het regressiemodel dat gebruikt is om de variantie in de waarschijnlijk van melden te verklaren onder zzp'ers bevat de eerdergenoemde dichotome vignetfactoren. Daarnaast is sector gehercodeerd tot dummyvariabelen en zijn deze als controlevariabelen aan het model toegevoegd, met 'financiële en zakelijke dienstverlening' als referentiecategorie. Het model dat gebruikt is om de variantie in de waarschijnlijk van het melden te verklaren onder mkb'ers bevat de eerdergenoemde dichotome vignetfactoren. Grootteklasse en sector zijn als dummyvariabelen aan het model toegevoegd, met 'financiële en zakelijke dienstverlening' en 'micro' als referentie categorieën.

De beschrijvende statistieken van de variabelen die zijn opgenomen in de regressiemodellen zijn te vinden tabel 3.5.

18 Blijkens de Kolmogorov-Smirnov-test (D(1.769) = 0,380, p = 0,000) en visuele inspectie van de histogram en plots.
19 Blijkens de Kolmogorov-Smirnov-test (D(732) = 0,404, p = 0,000) en visuele inspectie van de histogram en plots.

Tabel 3.5 Beschrijvende statistieken van geïncludeerde variabelen in de regressiemodellen voor ondernemers

	Zzp			Mkb		
	N	**%/gem.**	**SD**	**N**	**%/gem.**	**SD**
Waarschijnlijkheid van betalen (0-10)	1.769	1,11	1,89	732	1,19	1,98
Waarschijnlijkheid van melden (0-10)	1.769	8,87	2,34	732	9,07	2,10
Grootte bedrijf	-			732		
– Micro (0-1)				555	75,8%	
– Klein (0-1)				154	21%	
– Midden (0-1)				23	3,2%	
Sector	1.763			730		
– Landbouw/visserij (0-1)	51	2,9%		54	7,4%	
– Industrie, bouw en nutsbedrijven (0-1)	273	15,5%		91	12,5%	
– Handel en logistiek, horeca (0-1)	306	17,3%		256	35,1%	
– Financiële en zakelijke dienstverlening (0-1)	605	34,3%		157	21,5%	
– Overheid, onderwijs, zorg en overig (0-1)	528	30%		171	23,4%	
Hoogte losgeld	1.769			732		
– 1% van jaaromzet (0-1)	896	50,7%		383	52,3%	
– 25% van jaaromzet (0-1)	873	49,3%		350	47,7%	
Gedreigd met lekken	1.769			732		
– Nee (0-1)	893	50,5%		342	46,7%	
– Ja (0-1)	876	49,5%		390	53,3%	
Back-up	1.769			732		
– Nee (0-1)	919	51,9%		348	47,5%	
– Ja (0-1)	850	48,1%		384	52,5%	
Geadviseerd om te betalen	1.769			732		
– Nee (0-1)	889	50,3%		385	52,6%	
– Ja (0-1)	880	49,7%		347	47,4	

3.2 Deelstudie 3

Om de onderzoeksvragen in deelstudie 3 over de ondersteuning en advisering van slachtoffers vanuit publieke en private organisaties te beantwoorden, zijn semigestructureerde interviews gehouden met experts.

3.2.1 *Steekproef*

Voor dit onderzoek zijn experts van verschillende publieke en private organisaties geïnterviewd die vanwege hun functie in contact staan met slachtoffers van ransomware. Experts zijn geselecteerd op basis van voorkennis van de onderzoekers (n=8), informa-

tie in openbare bronnen waarin hun expertise beschreven is (n=1) en door middel van sneeuwballen (n=5). Op basis hiervan zijn 14 experts benaderd voor een interview. Zoals te zien is in tabel 3.6 bestaat de uiteindelijke steekproef uit 10 respondenten, waarvan 4 van de politie, 4 uit de cybersecuritysector, 1 van Slachtofferhulp Nederland en 1 respondent uit de wetenschap.

De interviews zijn afgenomen tussen 5 maart en 19 juni 2024 en vonden face to face (n=1), via videobellen (n=8) of telefonisch (n=1) plaats. De interviews duurden tussen 28 en 70 minuten, met een gemiddelde lengte van 57,1 minuten. Voorafgaand aan het interview zijn respondenten geïnformeerd over het doel van het onderzoek, en hebben respondenten *informed consent* gegeven (zie bijlage 6). De interviews zijn met toestemming van de respondent opgenomen met beveiligde opnameapparatuur, geanonimiseerd en verbatim getranscribeerd.

Tabel 3.6 Overzicht van geïnterviewde experts

#	Organisatie/sector	Publiek/privaat
R1	Slachtofferhulp	Publiek
R2	Belangenvereniging cybersecurity	Publiek
R3	Cybersecurity/Incident response	Privaat
R4	Politie/Wetenschap	Publiek
R5	Wetenschap	-
R6	Cybersecurity/Incident response	Privaat
R7	Cybersecurity/Incident response	Privaat
R8	Politie	Publiek
R9	Politie	Publiek
R10	Politie	Publiek

3.2.2 *Meetinstrument*

Gedurende het interview is gebruikgemaakt van een interviewprotocol (zie bijlage 7). Respondenten zijn eerst gevraagd naar hun achtergrond, functie, de werkzaamheden van de organisatie en waar hun kennis over de ondersteuning van slachtoffers op gebaseerd is. Vervolgens zijn respondenten gevraagd naar de ondersteuning en/of advisering van slachtoffers van ransomware vanuit hun organisatie, waarbij onder andere is stilgestaan bij advisering met betrekking tot onderhandelen, betalen, melden en nazorg, en in hoeverre slachtoffers adviezen opvolgen. Daarna zijn de belangrijkste resultaten uit deelstudies 1 en 2 aan respondenten voorgelegd, en is hun gevraagd hierop te reflecteren. Tot slot is aan respondenten gevraagd wat de sterke en verbeterpunten zijn en wat er nog ontbreekt als het gaat om de advisering en ondersteuning van slachtoffers van ransomware.

3.2.3 *Analyse*

De data zijn geanalyseerd in het kwalitatieve data-analyseprogramma ATLAS.ti. De data zijn georganiseerd middels thematische codes die voorafgaand aan de data-analyse zijn opgesteld op basis van het interviewprotocol en de onderzoeksvragen en op basis van thema's in de data (Evers, 2015; Saldaña, 2013). Toegekende codes zijn vervolgens vergeleken, gecontrasteerd en verbonden om patronen te identificeren.

3.3 Ethische toestemming

Voor dit onderzoeksproject is ethische toestemming verkregen van de Facultaire Commissie Ethiek Rechtswetenschappelijk & Criminologisch Onderzoek (CERCO) van de Vrije Universiteit Amsterdam en de Ethische Adviescommissie van de Haagse Hogeschool.

Deel I Resultaten burgers

4 Prevalentie, aard en impact van zelfgerapporteerd slachtofferschap van ransomware onder burgers

In dit hoofdstuk worden de resultaten van deelstudie 1A naar slachtofferschap van ransomware onder burgers besproken, waarbij wordt stilgestaan bij de prevalentie, de aard en de impact van slachtofferschap.[20]

4.1 Prevalentie

Aan het begin van de vragenlijst is aan alle respondenten gevraagd om voor acht vormen van cybercriminaliteit aan te geven of ze dit (of een poging ertoe) ooit hebben meegemaakt. Van de 20.659 burgers is 4,5% (n=925) ooit slachtoffer geworden van ransomware in de privésfeer.

De respondenten die gerapporteerd hebben slachtoffer te zijn geworden van ransomware, zijn doorverwezen naar deelstudie 1A, waarin vervolgvragen zijn gesteld over hun ervaringen. Het vervolg van de resultaten heeft betrekking op de groep respondenten die gerapporteerd heeft slachtoffer te zijn geworden van ransomware en de volledige vragenlijst heeft ingevuld (n=856).

4.2 Achtergrondkenmerken

Aan de respondenten in deelstudie 1A is allereerst gevraagd hoeveel tijd ze doorgaans online spenderen voor privédoeleinden en welke beveiligingsmaatregelen ze troffen voordat ze slachtoffer van ransomware werden (tabel 4.1). De meeste burgers spenderen doorgaans dagelijks (29,3%) of meerdere keren per dagen (37,8%) tijd online. Daarnaast waren het niet delen van persoonlijke wachtwoorden met anderen (75,7%), het hebben van een firewall (62,9%) en het hebben van een up-to-date antivirusproduct (59,5%) de meest voorkomende beveiligingsmaatregelen.

20 De frequenties en percentages in tabellen tellen niet altijd op tot de totalen als gevolg van het afronden van getallen in verband met het wegen van de data. Daarnaast tellen sommige percentages niet op tot de totalen omdat respondenten meerdere antwoorden konden selecteren. Dit laatste is aangeduid in de tabellen.

Tabel 4.1 Frequentie van tijd online, en beveiligingsmaatregelen voor slachtofferschap onder burgers (n=856)

	n	%
Tijd online voor privédoeleinden	**856**	
Minder dan 1 keer per maand	37	4,3%
Minimaal 1 keer per maand, maar niet wekelijks	14	1,6%
Minimaal 1 keer per week, maar niet dagelijks	42	4,9%
Dagelijks	250	29,3%
Meerdere keren per dag	323	37,8%
Minstens ieder uur	100	11,7%
Ik ben (bijna) continue online	90	10,5%
Beveiligingsmaatregelen voor slachtofferschap *(meerdere antwoorden mogelijk)*	**856**	
Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	421	49,2%
Unieke wachtwoorden voor alle apparaten en accounts	365	42,7%
Persoonlijk wachtwoorden niet delen met anderen	647	75,7%
Up-to-date antivirusproduct	509	59,5%
Firewall	538	62,9%
Beveiligingssoftware apparaten laten scannen op virussen of andere kwaadaardige software	446	52,1%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	494	57,8%
Voorzichtig met welke websites ik bezoek, wat ik download en welke mails of bijlagen ik open	416	48,6%
VPN-verbinding	54	6,4%
Browserextensies die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren	163	19,1%
Persoonlijke bestanden en gegevens versleuteld	43	5%
Tweestapsverificatie	131	15,3%
Anders	17	2%
Geen van bovenstaande	24	2,9%

4.3 Frequentie, incidentie en type ransomware

Zoals genoemd heeft 4,5% van de burgers gerapporteerd ooit slachtoffer te zijn geworden van ransomware. Van de slachtoffers is 5,6% in de afgelopen 12 maanden, 8,2% tussen 1-2 jaar geleden, 22,6% tussen 2-4 jaar geleden en de meerderheid (63,5%) 5 of meer jaar geleden slachtoffer geworden. Het percentage slachtofferschap van ransomware in het afgelopen jaar binnen de gehele steekproef van burgers is 0,2%. De meerderheid van de respondenten is 1 keer slachtoffer geworden (86,1%), een deel is 2 keer slachtoffer geworden (9,8%) en het kleinste deel is 3 keer (2,1%) of 4 keer of vaker (2%) slachtoffer geworden.[21] Bij meer dan een derde van de respondenten was sprake van

21 Respondenten die meerdere keren slachtoffer zijn geworden, zijn gevraagd om de vervolgvragen in te vullen over de laatste keer dat dit gebeurde.

lockerware (vergrendeling) (37%) of scareware met een bericht van een zogenaamde wetshandhavingsinstantie (35,6%). Een kleiner deel van de respondenten is slachtoffer geworden van cryptoware (versleuteling) (14,7%), een andere type ransomware (7%) of weet het niet meer (5,8%) (tabel 4.2).

Tabel 4.2 Frequentie van incidentie, jaartal en type ransomware onder burgers (n=856)

	n	%
Incidentie	**856**	
1 keer	737	86,1%
2 keer	84	9,8%
3 keer	18	2,1%
4 keer of vaker	17	2%
Laatste keer slachtoffer	**856**	
Een jaar geleden of minder	48	5,6%
1-2 jaar geleden	70	8,2%
2-4 jaar geleden	194	22,6%
5 of meer jaar geleden	544	63,5%
Type ransomware	**856**	
Lockerware (vergrendeling)	317	37%
Cryptoware (versleuteling)	125	14,7%
Scareware wethandhavingsinstantie	304	35,6%
Geen van de bovenstaande opties	60	7%
Ik weet het niet meer	49	5,8%

4.4 Aard van incident

Vervolgens is aan respondenten gevraagd hoe ze (met de kennis van nu) denken dat de ransomware op hun apparaat of systeem is gekomen (tabel 4.3). Iets meer dan een vijfde van de respondenten weet niet hoe hun systeem besmet is geraakt (23,2%). Het grootste deel van de respondenten die dit wel weet, heeft geklikt op een link, advertentie of pop-up tijdens het surfen op internet (25,6%), heeft geklikt op een link of heeft een bijlage geopend in een (phishing-)e-mail (13,9%), of heeft een malafide applicatie of malware geïnstalleerd (15%). Bij een kleinere groep was sprake van een kwetsbaarheid of beveiligingslek (9,9%) of was een bedrijf gehackt waar hun gegevens bekend waren (4,1%). Daarnaast heeft een deel van de respondenten in de open antwoorden aangegeven dat hun systeem vermoedelijk besmet is geraakt door het streamen of downloaden van multimedia (2%), tijdens het surfen op internet of door een bezoek aan een website (2,2%) of doordat ze gebeld zijn door iemand die zich voordeed als een helpdesk (bijvoorbeeld van Microsoft) (0,7%).

In de meeste gevallen stond er geen deadline vermeld in het losgeldbericht (44,9%) of kregen slachtoffers minder dan 24 uur (20,9%) of 1-3 dagen (18,1%) de tijd om te betalen. Bij de meerderheid van de respondenten was er naast de vergrendeling of versleuteling bovendien geen sprake van een aanvullende dreiging (58,8%). Bij een kleiner deel van de respondenten was dit wel het geval, zoals dreigen met het verwijderen van de decryptiesleutel (15,6%) of het lekken van bestanden of gegevens (19,3%). Bij een deel van de respondenten was sprake van een andere dreiging (7,7%), waaronder dreigen met het wissen of aanbrengen van schade aan bestanden, of dreigen met aangifte, vervolging of boete (in gevallen waar het losgeldbericht afkomstig leek te zijn van een wetshandhavingsinstantie en slachtoffers beschuldigd werden van illegale gedragingen).

Tabel 4.3 Frequentie van wijze van besmetting, deadline, aard van de dreiging en aangetaste apparaten of systemen en data onder burgers (n=856)

	n	%
Wijze van besmetting	**856**	
Geklikt op link of bijlage geopend in een e-mail	119	13,9%
Geklikt op een link, advertentie of pop-up op internet	219	25,6%
Bedrijf waar gegevens bekend waren was gehackt	35	4,1%
Kwetsbaarheid of beveiligingslek in gebruikte software of systeem	85	9,9%
Kwaadaardige applicatie of software geïnstalleerd	128	15%
Anders, namelijk …		
– Streamen of downloaden van multimedia (bijv. via een torrentsite)	17	2%
– Tijdens surfen op internet/bezoek aan een website	19	2,2%
– Gebeld door zogenaamde helpdesk	6	0,7%
– Op link geklikt (onduidelijk waar)	6	0,7%
Weet ik niet	199	23,2%
Deadline	**856**	
Minder dan 24 uur	179	20,9%
1-3 dagen	155	18,1%
4-6 dagen	65	7,6%
7 of meer dagen	73	8,6%
Dat stond niet in het losgeldbericht	384	44,9%
Aard dreiging *(meerdere antwoorden mogelijk)*	**856**	
Er is gedreigd met het verwijderen van de decryptiesleutel/permanente blokkade	133	15,6%
Er is gedreigd met het lekken van mijn bestanden of gegevens	166	19,3%
Er is gedreigd met een DDoS-aanval	18	2,1%
Er is gedreigd met iets anders, namelijk …		
– Schade aan/wissen van bestanden	18	2,1%
– Aangifte, vervolging of boete	35	4,1%
– Openbaar maken van zogenaamde compromitterende beelden	5	0,6%
– Weet ik niet meer	8	1%
Geen van bovenstaande	503	58,8%

In veruit de meeste gevallen hadden respondenten door de ransomware geen toegang meer tot hun computer (85,7%) (tabel 4.4). Er was daarnaast een kleinere groep respondenten bij wie andere apparaten of systemen zijn aangetast, zoals een telefoon, tablet, cloudopslag, NAS of toegang tot online accounts. De meest voorkomende bestanden of gegevens die aangetast waren, betroffen bestanden met emotionele waarde (zoals foto's of video's) (54,9%), bestanden voor studie of werk (41,1%) of persoonsgegevens (38,4%). Bijna 1 op de 7 (14,1%) heeft bovendien gespecificeerd dat alles op hun apparaat of systeem ontoegankelijk was gemaakt.

Tabel 4.4 Frequentie van wijze van besmetting, deadline, aard van de dreiging en aangetaste apparaten of systemen en data onder burgers (n=856)

	n	%
Aangetaste apparaten of systemen *(meerdere antwoorden mogelijk)*	**856**	
Computer (desktop of laptop)	733	85,7%
Mobiele telefoon of smartphone	41	4,8%
Tablet	54	6,3%
Computerserver(s)	27	3,2%
Cloudopslag	27	3,2%
Back-up(s)	16	1,9%
Anders, namelijk …		
– NAS	9	1%
– Online accounts (bijv. sociale media, e-mail)	10	1,2%
– Toegang tot browser/website	8	1%
– Diverse apps	1	0,1%
– Er was (nog) niets aangetast, er werd alleen mee gedreigd	4	0,4%
Aangetaste data *(meerdere antwoorden mogelijk)*	**856**	
Persoonsgegevens	329	38,4%
Bestanden met emotionele waarde (bijv. foto's/video's)	470	54,9%
Bestanden voor studie of werk	354	41,4%
Financiële gegevens en boekhouding	202	23,6%
Weet ik niet	107	12,6%
Anders, namelijk …		
– Vrijetijdssoftware (bijv. games) en apps	4	0,5%
– Office-bestanden (o.a. tekstbestanden)	3	0,3%
– E-mails	8	0,9%
– Systeembestanden	6	0,7%
– Alles (hele apparaat/besturingssysteem geblokkeerd)	120	14,1%
– Er was (nog) niets aangetast, er werd alleen mee gedreigd	5	0,6%

4.5 Eerste reactie

Respondenten is vervolgens gevraagd wat hun eerste emotie en handeling(en) waren nadat ze waren geconfronteerd met het losgeldbedrag (tabel 4.5). De meest ervaren emoties betroffen boosheid (63,3%), nervositeit (32%), afkeer (28,8%) en angst (22,4%). Een klein deel van de respondenten heeft daarnaast aangegeven dat ze zich dom of stom voelden, kwaad waren op zichzelf of zich schaamden (2,1%).

Een deel van de respondenten heeft zelf geprobeerd om het probleem op te lossen. De meesten daarvan hebben de verbinding met internet of stroom verbroken (37,1%), het

apparaat opnieuw opgestart (29,1%), het apparaat teruggezet naar fabrieksinstellingen (27,6%) en/of geprobeerd om een programma te gebruiken om de ransomware te verwijderen of de data te ontsleutelen (21,1%). Een kleiner deel heeft iets anders geprobeerd, zoals het herstellen van data vanaf een back-up (18%) of het openen van bestanden door de bestandsextensie te veranderen (4,3%). Van deze respondenten heeft de meerderheid de volledige toegang teruggekregen (64,7%), een kleiner deel geen toegang teruggekregen (21,5%) en het kleinste deel gedeeltelijke toegang teruggekregen (13,8%).

Een ander deel van de respondenten heeft niet zelf geprobeerd om het probleem op te lossen, maar heeft hulp gezocht. De grootste groep zocht hulp van een bekende (27,4%), gevolgd door hulp via internet (22,4%) en hulp van een organisatie (waaronder de politie blijkens de open antwoorden), instantie, ICT-deskundige of computerzaak (18,9%). Uit de open antwoorden blijkt daarnaast dat een kleine groep respondenten andere technische oplossingen heeft geprobeerd (6,2%), als eerste reactie heeft betaald (2,7%), niets heeft gedaan (4%) of het apparaat gelijk heeft weggedaan en een nieuw apparaat heeft gekocht (1,5%).

Tabel 4.5 Frequentie van eerste emotie, eerste handeling en uitkomst onder burgers (n=856)

	n	%
Eerste emotie *(meerdere antwoorden mogelijk)*	**856**	
Boosheid	541	63,3%
Afkeer	246	28,8%
Angst	191	22,4%
Nervositeit	274	32%
Verdriet	114	13,3%
Ontspanning	21	2,5%
Blijheid	2	0,3%
Anders, namelijk …		
– Verrast/verbaasd	6	0,7%
– Dom/stom voelen/kwaad op zelf/schaamte	18	2,1%
– Machteloos/hulpeloos	5	0,6%
– Geschrokken/ontzet	5	0,6%
– Geïrriteerd/gefrustreerd/verontwaardigd	19	2,2%
– Lachwekkend	5	0,6%
– Onverschillig/neutraal	5	0,6%
Geen van de bovenstaande opties	36	4,2%
Weet ik niet	12	1,4%
Eerste handeling *(meerdere antwoorden mogelijk)*	**856**	
Verbinding met internet of stroom verbroken	317	37,1%

Tabel 4.5 Vervolg

	n	%
Apparaat opnieuw opgestart	249	29,1%
Apparaat teruggezet naar fabrieksinstellingen	236	27,6%
Hulp of advies gezocht op internet	192	22,4%
Hulp of advies gezocht van een bekende	235	27,4%
Hulp of advies gezocht van een organisatie, instantie, ICT-deskundige of computerzaak	162	18,9%
Bestanden of gegevens geprobeerd te herstellen vanaf een back-up	154	18%
Geprobeerd om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen	181	21,1%
Geprobeerd bestanden weer te openen door hun extensie terug te veranderen naar het originele formaat	36	4,3%
Losgeld betaald	23	2,7%
Niks gedaan	34	4%
Iets anders gedaan, namelijk …		
– Een nieuw apparaat (computer/schijf) gekocht	13	1,5%
– Andere technische oplossingen (bijv. formatteren, systeemherstel, virusscanner)	53	6,2%
– Account verwijderd	1	0,2%
Uitkomst zelf geprobeerd op te lossen	672	
Volledige toegang terug	434	64,7%
Gedeeltelijke toegang terug	93	13,8%
Geen toegang terug	145	21,5%

4.6 Onderhandelen

Soms is het mogelijk om contact op te nemen met de daders. Respondenten is gevraagd of, door wie, hoe en met welk doel er contact is opgenomen (tabel 4.6). De meerderheid van de respondenten (95,6%) heeft geen contact opgenomen met de daders. Een kleiner deel heeft zelf contact opgenomen (2%), een bekende contact laten opnemen (1,7%) of heeft iemand ingehuurd om contact op te nemen (0,7%). In de meeste gevallen gebeurde dit contact via e-mail (35%) of een chatsysteem op een website of portaal van de daders (33,5%), gevolgd door telefonisch contact (24,9%) of contact via sociale media (4%).

De redenen die respondenten noemden om contact op te nemen waren om te informeren over de hoogte van het losgeld (29,6%), vast te stellen of het losgeldbericht echt was (20,8%), of tijd te rekken (20,8%). Een kleiner deel heeft contact opgenomen om vast te stellen welke data waren gestolen (10,3%), om te informeren hoe het probleem verholpen kon worden (12,5%), om frustratie te uiten (10%), om hulp te vragen *bij* het betalen (5,6%) of hulp te vragen *na* het betalen (2,4%). Geen enkele respondent heeft onderhandeld.

Tabel 4.6 Frequentie van of, door wie en hoe er contact opgenomen is met de daders onder burgers (n=856)

	n	%
Contact opgenomen met daders	**856**	
Zelf contact opgenomen	17	2%
Bekende heeft contact opgenomen	14	1,7%
Ingehuurde partij heeft contact opgenomen	6	0,7%
Geen contact opgenomen	818	95,6%
Communicatiemiddel *(meerdere antwoorden mogelijk)*	**40**	
E-mail	14	35%
Chatsysteem op een website of portaal	13	33,5%
Telefonisch	10	24,9%
Anders, namelijk …		
– Sociale media	2	4%
Doel *(meerdere antwoorden mogelijk)*	**40**	
Om vast te stellen of het losgeldbericht echt was	8	20,8%
Om te informeren over de hoogte van het losgeld (bijvoorbeeld omdat dit in het losgeldbericht niet vermeld stond)	12	29,6%
Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline	0	0,5%
Om vast te stellen welke bestanden of gegevens waren gestolen	4	10,3%
Om hulp te vragen bij het betalen (bijvoorbeeld bij het aanschaffen van bitcoin)	2	5,6%
Om hulp te vragen na het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens)	1	2,4%
Om tijd te rekken	8	20,8%
Anders, namelijk …		
– Om te informeren hoe het probleem verholpen kon worden	5	12,5%
– Om frustratie te uiten/te laten weten niet te gaan betalen	4	10%

4.7 Betalen

Ongeveer 45% van de respondenten (n=385) heeft aan de hand van een bedrag en valutasoort aangeduid wat de hoogte van het geëiste losgeld was, waarvan 75,3% dit heeft aangeduid in euro's (in sommige gevallen omgerekend vanuit een andere koers), 1,8% in guldens, 13,2% in Amerikaanse dollars en 9,6% in bitcoin.[22] De andere helft van de respondenten kon zich de losgeldeis niet herinneren, vermeldde alleen een bedrag (zonder valutasoort) of stelde dat er nog geen concreet bedrag geëist was omdat ze eerst contact moesten opnemen met de daders en dat niet gedaan hebben. Zoals in tabel 4.7 te zien is, lopen de geëiste losgeldbedragen sterk uiteen. De gemiddelde los-

22 De hoogte van het losgeld in bitcoin wordt niet vermeld in tabel 4.7 omdat hierbij te veel onbekende factoren zijn. Zo varieerde de bitcoin koers sterk over de tijd heen en is de precieze datum van het ransomware-incident onbekend, waardoor geen juiste inschatting gemaakt kan worden van de waarde.

geldeis was 3.676,37 euro, 194,58 gulden en 1.784,22 dollar. De mediaan[23] van het geëiste losgeld is 500 euro, 125,86 gulden en 750 dollar. Het meest voorkomende losgeldbedrag was 500 euro, 100 gulden en 1.000 dollar.

Tabel 4.7 Hoogte geëiste losgeld in verschillende valutasoorten [24]

	n	Min.	Max.	Mediaan	Modus	Gem.	Std. dev.
€ (euro)	290	25	250.000	500	500	3.676,37	18.194,25
£ (gulden)	7	75	500	125,86	100	194,58	137,54
$ (dollar)	51	50	10.000	750	1.000	1.784,22	2.793,17
Totaal	348						

De meerderheid (95,9%) van de slachtoffers heeft het geëiste losgeld niet betaald. Een klein deel van de respondenten heeft een gedeelte van (0,8%) of het volledige losgeldbedrag (3,3%) betaald. Bij de 21 respondenten die het betaalde losgeldbedrag vermeld hebben, was de gemiddelde betaling 700,03 euro, met een mediaan van 120 euro.

De respondenten zijn vervolgens gevraagd naar de reden(en) waarom ze wel of niet betaald hebben (tabel 4.8). De meest voorkomende redenen om het losgeld niet te betalen waren dat respondenten niet vertrouwden dat de toegang hersteld zou worden na betaling (36,6%), dat het onethisch is om criminelen te betalen (29,6%) en dat respondenten back-up(s) hadden (23,4%). De meest voorkomende redenen om wel te betalen waren dat respondenten erop vertrouwden dat toegang hersteld zou worden na betaling (48,4%), dat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen (45,8%) en dat het losgeldbedrag niet heel hoog was en ze het zich konden veroorloven (36,7%).

23 Centrummaat, i.e. middelste waarde in dataset.
24 In sommige gevallen moest het losgeld in bitcoin betaald worden, maar hebben respondenten aangeduid dat het om x euro of dollar in bitcoin ging.

Tabel 4.8 Frequentie van reden(en) om (niet) te betalen onder burgers (n=856)

	n	%
Losgeld betaald	**856**	
Een deel van het losgeld betaald	7	0,8%
Losgeld volledig betaald	28	3,3%
Niet betaald	820	95,9%
Reden(en) om niet te betalen *(meerdere antwoorden mogelijk)*	**820**	
Losgeldbedrag te hoog	62	7,6%
Geadviseerd door politie om niet te betalen	79	9,6%
Geadviseerd door bekende om niet te betalen.	100	12,2%
Geadviseerd door IT- of cybersecurityspecialist om niet te betalen	89	10,8%
Back-up(s) van data	192	23,4%
Bestanden, gegevens of apparaten waren niet belangrijk	115	14%
Vertrouwde er niet op dat toegang hersteld zou worden na betaling	300	36,6%
Niet bang voor lekken van data of andere gevolgen bij niet betalen	185	22,6%
Onethisch om criminelen te betalen	243	29,6%
Lukte niet om te betalen	5	0,6%
Anders, namelijk …		
– Zelf (of met behulp van ander) opgelost	127	15,5%
– Uit principe/laat me niet chanteren	9	1,1%
– Wist dat het een valse dreiging was	9	1,1%
– Er was (nog) geen losgeldeis	5	0,6%
Geen van de bovenstaande opties	54	6,6%
Reden(en) om wel te betalen *(meerdere antwoorden mogelijk)*	**35**	
Losgeldbedrag niet heel hoog	13	36,7%
Geadviseerd door bekende om te betalen	3	8,8%
Geadviseerd door IT- of cybersecurityspecialist om te betalen	7	21,1%
Geen back-up(s) van data	4	11,3%
Wilde bestanden, gegevens of apparaten niet verliezen	16	45,8%
Vertrouwde erop dat toegang hersteld zou worden na betaling	17	48,4%
Bang voor lekken van data of andere gevolgen bij niet betalen	3	9,4%
Anders, namelijk …		
– Ik schaamde me	2	5,7%
Geen van de bovenstaande opties	0	0%

Zoals blijkt uit tabel 4.9 is bij de meerderheid van de respondenten die betaald heeft de toegang hersteld (69,4%), terwijl bij een kleiner deel de toegang slechts gedeeltelijk (5,6%) of helemaal niet hersteld is (25%). Tegelijkertijd is het de meerderheid van de respondenten die *niet* betaald heeft ook gelukt om volledig (76,5%) of gedeeltelijk (12,6%) de toegang te herstellen. Slechts in 11% van de gevallen is toegang niet hersteld nadat niet betaald is.

Aan respondenten is daarnaast gevraagd of ze het idee hebben dat hun bestanden of gegevens gedeeld zijn met of verkocht zijn aan anderen. De meerderheid van de respondenten geeft aan dat dit niet het geval is (58,9%), een kleiner deel geeft aan het niet te weten (37,2%) en de minderheid denkt dat dit wel het geval is (3,8%).

Tabel 4.9 Kruistabel van betalen afgezet tegen of toegang hersteld is onder burgers (n=856)

	Niet betaald	Betaald
Toegang terug		
Volledig	627 (76,5%)	25 (69,4%)
Gedeeltelijk	103 (12,6%)	2 (5,6%)
Nee	90 (11%)	9 (25%)
Totaal	820	36

4.8 Impact

Respondenten zijn ook gevraagd naar de impact van het ransomware-incident (tabel 4.10). Ongeveer de helft van de respondenten ervaarde geen emotionele of psychische gevolgen (52,3%). Bij de respondenten die dit wel ervaarden, betroffen de meest voorkomende gevolgen dat respondenten zich minder veilig voelden (28,5%), minder vertrouwen hadden in de eigen digitale vaardigheden (18%), of minder vertrouwen hadden in mensen (13,8%). Een kleiner deel ervaarde andere gevolgen zoals angstklachten en/of paniekaanvallen, slaapproblemen, depressieve klachten of het opnieuw beleven van het voorval.

De meerderheid van de respondenten gaf daarnaast aan dat ze andere gevolgen hebben ervaren. In de meeste gevallen betrof dit het besteden van tijd aan het oplossen van het incident (56,6%), gevolgd door het verliezen van bestanden of gegevens (20%) en kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (17,9%). Een kleine groep geeft daarnaast aan dat ze voorzichtiger zijn geworden online (1,2%).

Wat betreft de financiële impact, gaf een meerderheid van de respondenten (58,3%) aan geen financiële gevolgen te hebben ervaren en gaf een deel aan het niet te weten (13,1%). Bij de respondenten die wel financiële gevolgen hebben ervaren, was dit in de meeste gevallen minder dan 1.000 euro. In veruit de meeste gevallen (92,4%) is de financiële schade (inclusief een eventuele losgeldbetaling) niet vergoed. Een klein deel van de respondenten heeft een gedeelte (1,6%) of het volledige bedrag (2,7%) vergoed gekregen of heeft een vergoeding aangevraagd maar nog geen beslissing ontvangen (3,3%). Bij bijna de helft hiervan is de schade vergoed door of is een aanvraag gedaan bij een verzekeringsmaatschappij (42,7%), terwijl dit bij een kleiner deel bij een bank of financiële instelling (37,8%) of andere instantie is gedaan (19,6%) (tabel 4.10).

Tabel 4.10 Frequentie van emotionele, andere en financiële gevolgen onder burgers (n=856)

	n	%
Emotionele/psychische gevolgen *(meerdere antwoorden mogelijk)*	**856**	
Minder veilig voelen	244	28,5%
Minder vertrouwen in mensen	118	13,8%
Het voorval telkens opnieuw beleven	18	2,1%
Slaapproblemen	37	4,3%
Angstklachten en/of paniekaanvallen	30	3,5%
Depressieve klachten	18	2,1%
Minder vertrouwen in eigen digitale vaardigheden.	154	18%
Andere emotionele of psychische gevolgen, namelijk …		
– Een gevoel van schaamte	3	0,4%
Geen van de bovenstaande opties	447	52,3%
Weet ik niet	25	2,9%
Andere gevolgen *(meerdere antwoorden mogelijk)*	**856**	
Tijd besteed aan het oplossen van het incident	484	56,6%
Kosten gemaakt vanwege reparatie, herstel of aanschaf van bijvoorbeeld een apparaat of netwerk	153	17,9%
Bestanden of gegevens verloren	171	20%
Anders, namelijk …		
– Voorzichtiger geworden online	10	1,2%
Geen van bovenstaande opties	206	24,1%
Financiële gevolgen (m.u.v. betalen losgeld)	**856**	
Geen	499	58,3%
Minder dan € 1.000	183	21,4%
€ 1.000 tot € 5.000	43	5,1%
€ 5.000 tot € 10.000	10	1,1%
€ 10.000 tot € 50.000	3	0,4%
€ 50.000 of meer	6	0,7%
Weet ik niet	112	13,1%
Financiële schade vergoed (incl. betaalde losgeld)	207	
Volledig vergoed	6	2,7%
Gedeeltelijk vergoed	3	1,6%
Niet vergoed	192	92,4%
Aangevraagd en nog geen beslissing ontvangen	7	3,3%
Instantie die financiële schade heeft vergoed/mogelijk gaat vergoeden	16	
Bank of financiële instelling	6	37,8%
Verzekeringsmaatschappij	7	42,7%
Andere instantie	3	19,6%

Daarnaast is aan respondenten gevraagd of het incident gevolgen heeft gehad voor het online gedrag of de beveiligingsmaatregelen, wat bij een groot deel van de respondenten het geval was (tabel 4.11). De grootste groep is voorzichtiger met welke websites ze bezoeken, wat ze downloaden en welke bijlagen ze openen (57,4%), maakt (vaker) externe back-ups van bestanden en gegevens (45,3%), en laat beveiligingssoftware apparaten scannen op virussen of andere kwaadaardige software (35,5%).

Tabel 4.11 Frequentie van genomen beveiligingsmaatregelen na slachtofferschap onder burgers (n=856)

	n	%
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**856**	
Ander besturingssysteem genomen	58	6,8%
(Vaker) back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	388	45,3%
Unieke wachtwoorden voor alle apparaten en accounts	279	32,6%
Persoonlijk wachtwoorden niet (meer) delen met anderen	174	20,4%
(Ander) antivirus product aangeschaft	215	25,1%
Firewall aangeschaft	134	15,7%
Beveiligingssoftware apparaten laten scannen op virussen of andere kwaadaardige software	304	35,5%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	293	34,4%
Ander standaardbrowser genomen	103	12%
Voorzichtiger met welke websites ik bezoek, wat ik download en welke mails of bijlagen ik open	491	57,4%
VPN-verbinding aangeschaft	78	9,1%
Browser extensies geïnstalleerd die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren	101	11,8%
Persoonlijke bestanden en gegevens versleuteld	59	6,8%
Tweestapsverificatie	179	20,9%
Anders, namelijk …		
– Nieuwe externe schijf aangeschaft	1	0,1%
– Overgestapt op online cloudoplossing	1	0,1%
– Laat niemand anders achter pc	2	0,3%
– Periodieke controle/onderhoud door expert	1	0,2%
– Belangrijke documenten offline bewaren	2	0,3%
Geen van bovenstaande	74	8,7%

4.9 Melden

Vervolgens is onderzocht in hoeverre burgers naar aanleiding van het ransomware-incident contact hebben gezocht met organisaties. Slachtoffers hebben het vaakst contact opgenomen met een cybersecuritybedrijf of IT-leverancier (17,3%), de politie (15,6%) of de Fraudehelpdesk (8,6%) voor advies, ondersteuning of om melding van het incident te maken (tabel 4.12). Gemiddeld genomen zijn respondenten (op een schaal van

1 'zeer ontevreden' tot 5 'zeer tevreden') over deze organisaties neutraal tot tevreden, met uitzondering van cybersecuritybedrijven of IT-leveranciers, waar slachtoffers tevreden tot zeer tevreden over zijn.

Tabel 4.12 Frequentie van contact met verschillende instanties en tevredenheid over deze instanties onder burgers *(meerdere antwoorden mogelijk)* (n=856)

	Contact met		Tevredenheid	
Instantie	**N**	**%**	**Gem.**	**Std. dev.**
Politie	134	15,6%	3,47	1,416
Bank of financiële instelling	61	7,2%	3,70	1,549
Verzekeringsmaatschappij	23	2,7%	3,42	1,530
Cybersecuritybedrijf/IT-leverancier/computerzaak	148	17,3%	4,19	1,196
No More Ransom	25	2,9%	3,67	1,137
Slachtofferhulp	17	2%	3,56	1,234
Fraudehelpdesk	74	8,6%	3,73	1,308
Een andere organisatie, namelijk …			3,88	1,119
– Senior Web	1	0,1%		
– Student aan Huis	1	0,1%		
– Telefoonprovider	4	0,5%		
– Belastingdienst	1	0,1%		
– Digitaal vraagpunt/forum	2	0,2%		
– Consumentenbond	1	0,1%		

De meerderheid van de respondenten heeft contact opgenomen met de politie voor hulp en/of informatie (54,1%), en een kleiner deel om het incident te melden (40%) en/of aangifte te doen (36,6%). Van de respondenten die contact met de politie heeft gezocht om melding en/of aangifte te doen, heeft 36,2% daadwerkelijk aangifte gedaan waarbij een proces-verbaal is ondertekend (tabel 4.13). Dit komt neer op een aangiftepercentage van 2,1% onder de 856 slachtoffers.

Tabel 4.13 Frequentie van doel waarmee contact is opgenomen met de politie en aangiftepercentage na contact onder burgers

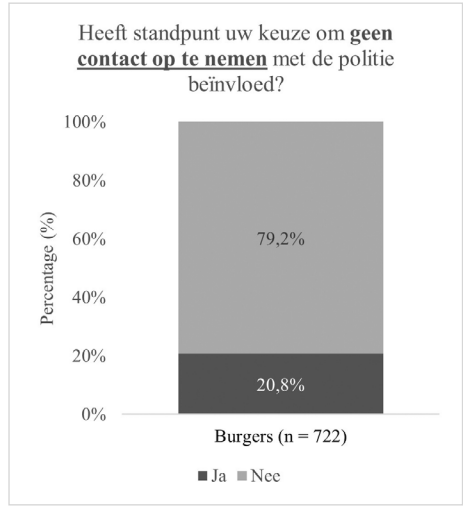
	n	%
Doel contact politie *(meerdere antwoorden mogelijk)*	**134**	
Voor hulp en/of informatie	72	54,1%
Om aangifte te doen	49	36,6%
Om het incident te melden	54	40%
Aangifte gedaan (indien doel contact politie = melden of aangifte)	**49**	
Nee	31	63,8%
Ja	18	36,2%

De meest voorkomende redenen om het ransomware-incident niet te melden en/of geen aangifte te doen bij de politie (tabel 4.14) waren voor burgers dat ze het zelf of met behulp van een andere partij hebben opgelost (68%), het geen zin heeft om melding of aangifte te doen aangezien de politie er toch niets aan doet (28,8%) en dat het incident niet zo belangrijk is (18,6%). De meest voorkomende redenen om wel te melden en/of aangifte te doen, waren dat respondenten wilden dat de dader gepakt wordt (64%), om te voorkomen dat dit bij een ander gebeurt (61%) en om een veiligere (online) wereld te creëren (46,6%).

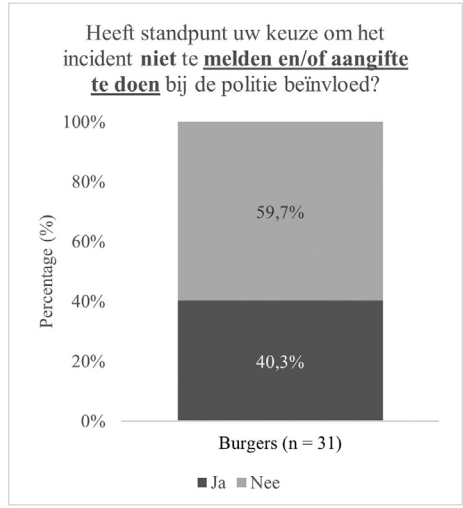
Tabel 4.14 Frequentie van reden(en) om (niet) te melden en/of aangifte te doen bij de politie onder burgers (n=856)

	n	%
Reden(en) om niet te melden *(meerdere antwoorden mogelijk)*	**563**	
Ik heb het zelf of met behulp van een andere partij opgelost	383	68%
Het is niet zo belangrijk	105	18,6%
Het kost te veel tijd/moeite	71	12,6%
Het heeft geen zin, de politie zal er toch niets aan doen	162	28,8%
De politie heeft niet de kennis om dit type delict aan te pakken	45	8%
Het is eerder een zaak voor een andere instantie dan de politie	14	2,5%
Ik heb weinig vertrouwen in de politie	42	7,5%
De politie wilde de melding/aangifte niet opnemen	2	0,4%
Ik heb de schade (losgeld en/of andere kosten) al vergoed gekregen	0	0%
Ik ben bang dat de dader wraak zal nemen	3	0,5%
Ik schaam me dat ik slachtoffer ben geworden	46	8,2%
Ik schaam me dat ik het losgeld betaald heb	4	0,7%
Ik vind dat het eigenlijk mijn eigen schuld is	67	11,9%
Het lukt niet om digitaal aangifte/melding te doen	4	0,6%
Anders, namelijk …		
– Niet aan gedacht/wist niet dat dit mogelijk was	16	2,8%
– Geen schade of een lage impact	8	1,4%
– Had geen informatie om aan de politie door te geven	1	0,2%
Reden(en) om wel te melden *(meerdere antwoorden mogelijk)*	**103**	
Om te voorkomen dat dit opnieuw bij mij gebeurt	38	37,4%
Om te voorkomen dat dit bij een ander gebeurt	63	61%
Ik wil dat de dader gepakt wordt	66	64%
Om een veiligere (online) wereld te creëren	48	46,6%
Het is mijn plicht	40	38,8%
Om de schade vergoed te krijgen	1	1,1%
Anders, namelijk …		
– Om te controleren of de dreiging echt afkomstig van de politie was	5	0,6%
– Omdat de bank dit eiste	1	0,1%

Naast bovenstaande redenen, is ook aandacht besteed aan het feit dat de politie adviseert om het losgeld niet te betalen. Respondenten is gevraagd in hoeverre zij het eens zijn (op een schaal van 1 'helemaal mee oneens' tot 5 'helemaal mee eens') met de stelling 'De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?'. Burgers zijn het gemiddeld (helemaal) eens (M = 4,62, SD = 0,785). Vervolgens is gevraagd of dit standpunt hun beslissing om contact op te nemen met de politie voor advies, ondersteuning of om melding van het incident te maken heeft beïnvloed. Hieruit blijkt dat bij 20,8% van de respondenten die *geen* contact heeft opgenomen met de politie, het standpunt van de politie om niet te betalen hieraan heeft bijgedragen (figuur 4.1). Daarnaast blijkt dat bij bijna de helft (40,3%) van de respondenten die *wel* contact heeft gehad met de politie, dit standpunt eraan heeft bijgedragen dat ze uiteindelijk geen melding en/of aangifte hebben gedaan (figuur 4.2).



Figuur 4.1 Invloed van standpunt politie om niet te betalen op keuze om geen contact op te nemen met de politie



Figuur 4.2 Invloed van standpunt politie om niet te betalen op keuze om niet te melden en/of aangifte te doen

4.10 Resumé

In dit hoofdstuk is stilgestaan bij de prevalentie, de aard en de impact van slachtofferschap van ransomware onder Nederlandse burgers. Uit de resultaten blijkt dat 4,5% van de burgers ooit slachtoffer is geworden van ransomware in de privésfeer, waarvan de meerderheid eenmalig slachtoffer is geworden. Bij de meeste slachtoffers vond het incident meer dan 5 jaar geleden plaats. Het percentage burgers dat in het afgelopen jaar slachtoffer werd van ransomware is 0,2%.

Als het gaat om de aard van het delict was er in de meeste gevallen sprake van lockerware (vergrendeling van (onderdelen van) het systeem) of scareware. Bij de meeste respondenten betrof dit aantasting van de computer en aantasting van bestanden met emotionele waarde, zoals foto's of video's. De meeste respondenten denken dat de ransomware op hun apparaat of systeem is gekomen door het klikken op een link, advertentie of pop-up tijdens surfen op internet. Bij de meerderheid van de respondenten was naast de vergrendeling of versleuteling geen sprake van een aanvullende dreiging. Bij de respondenten bij wie dit wel het geval was, ging het om het dreigen met een permanente blokkade of het lekken van bestanden of gegevens. Wanneer er een deadline in het losgeldbericht stond vermeld, kregen respondenten meestal minder dan 24 uur of tussen de 1 en 3 dagen de tijd om te betalen.

Als het gaat om de eerste emotie en reactie van slachtoffers, was de meest voorkomende emotie boosheid. Een deel van de respondenten heeft zelf geprobeerd om het probleem op te lossen, in de meeste gevallen door de verbinding met internet te verbreken. Bij de meerderheid van de respondenten die zelf heeft gepoogd het probleem op te lossen, is het gelukt om de toegang tot het apparaat of systeem te herstellen. Een ander deel van de respondenten heeft niet zelf geprobeerd om het probleem op te lossen, maar heeft hulp gezocht. In de meeste gevallen betrof dit hulp van een bekende, gevolgd door hulp via internet en hulp van een organisatie, instantie, ICT-deskundige of computerzaak.

Slechts 4,4% van de respondenten heeft zelf contact opgenomen of iemand anders contact laten opnemen met de daders, met name via e-mail of een chatsysteem op een website of portaal. In de meeste gevallen werd dit gedaan om te informeren over de hoogte van het losgeld. Geen enkele respondent heeft onderhandeld.

Gemiddeld werd 3.676 euro aan losgeld gevraagd, met een mediaan van 500 euro. Het meest voorkomende losgeldbedrag was 500 euro. Van de slachtoffers heeft ongeveer 96% het geëiste losgeld niet betaald, met als voornaamste reden dat respondenten niet vertrouwden dat de toegang hersteld zou worden na betaling. De meeste respondenten die wel betaald hebben, gaven als reden dat ze er juist wel op vertrouwden dat toegang hersteld zou worden na betaling. De gemiddelde betaling was 700 euro met een mediaan van 120 euro. Bij de meerderheid van de respondenten is de toegang gedeeltelijk of volledig hersteld, ongeacht of ze het losgeld betaald hebben. De meeste respondenten hadden bovendien niet het idee dat hun data gelekt of verkocht zijn.

Als het gaat om de impact, ervaarde ongeveer de helft van de respondenten emotionele of psychische gevolgen, met name een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden. De meerderheid van de respondenten gaf daarnaast aan andere gevolgen te hebben ervaren, met name het besteden van tijd aan het oplossen van het incident. Ongeveer 29% van de respondenten heeft de financiële gevolgen aangeduid (buiten het eventueel betaalde losgeld), waarbij dit in de meeste gevallen

minder dan 1.000 euro was. In slechts 4,3% van de gevallen is de financiële schade (gedeeltelijk) vergoed door een verzekeringsmaatschappij, bank of andere instantie. Voor een groot deel van de respondenten heeft het ransomware-incident tevens geleid tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In de meeste gevallen zijn respondenten voorzichtiger met welke websites ze bezoeken, wat ze downloaden en welke bijlagen ze openen.

Tot slot is aan respondenten gevraagd met welke organisaties ze contact hebben opgenomen voor advies, ondersteuning of om melding van het incident te maken. Van de respondenten die contact opnamen met een organisatie, namen de meesten contact op met een cybersecuritybedrijf of IT-leverancier (17,3%), gevolgd door de politie (15,6%) en Fraudehelpdesk (8,6%). Van alle respondenten heeft 2,1% daadwerkelijk aangifte gedaan bij de politie waarbij een proces-verbaal is ondertekend. De meest voorkomende reden om het incident niet te melden bij de politie was dat respondenten het zelf of met behulp van een andere partij hebben opgelost. De meest voorkomende reden om wel te melden was dat respondenten wilden dat de dader gepakt werd. Hoewel respondenten het eens zijn met het algemene advies van de politie om het losgeld niet te betalen, heeft ditzelfde standpunt er bij ongeveer 21% toe geleid dat ze geen contact hebben opgenomen met de politie en bij ongeveer 40% dat ze na contact uiteindelijk geen melding en/of aangifte hebben gedaan.

5 Factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap van ransomware onder burgers

In dit hoofdstuk worden de resultaten beschreven van het onderzoek onder burgers naar de factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap (deelstudie 2A).[25] Burgers werd gevraagd om zich de hypothetische situatie voor te stellen waarin ze getroffen waren door ransomware en ze een beslissing moesten nemen over het wel of niet betalen van het losgeld en het melden van het incident aan de hand van een vignet (zie paragraaf 3.1.2.2). In paragraaf 5.8 worden de resultaten van deelstudie 1A en 2A vergeleken.

5.1 Achtergrondkenmerken

Aan de respondenten is allereerst gevraagd hoeveel tijd ze doorgaans online spenderen voor privédoeleinden en welke beveiligingsmaatregelen ze momenteel nemen (tabel 5.1). De meeste burgers spenderen doorgaans dagelijks (33,3%) of meerdere keren per dag (39,9%) tijd online. Daarnaast waren het niet delen van persoonlijke wachtwoorden met anderen (82,3%), voorzichtig zijn met welke websites ze bezoeken, wat ze downloaden, welke mails of bijlagen ze openen (73,2%), en het direct uitvoeren van updates van besturingssystemen, apps en/of software zodra deze beschikbaar zijn (64,3%) de meest voorkomende beveiligingsmaatregelen.

25 De frequenties en percentages in tabellen tellen niet altijd op tot de totalen als gevolg van het afronden van getallen in verband met het wegen van de data. Daarnaast tellen sommige percentages niet op tot de totalen omdat respondenten meerdere antwoorden konden selecteren. Dit laatste is aangeduid in de tabellen.

Tabel 5.1 Frequentie van tijd online, en beveiligingsmaatregelen voor slachtofferschap onder burgers (n=4.082)

	n	%
Tijd online voor privédoeleinden	**4.082**	
Minder dan 1 keer per maand	31	0,8%
Minimaal 1 keer per maand, maar niet wekelijks	36	0,9%
Minimaal 1 keer per week, maar niet dagelijks	253	6,2%
Dagelijks	1.358	33,3%
Meerdere keren per dag	1.627	39,9%
Minstens ieder uur	536	13,1%
Ik ben (bijna) continu online	240	5,9%
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**4.082**	
Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	2.179	53,4%
Unieke wachtwoorden voor alle apparaten en accounts	1.998	49%
Persoonlijk wachtwoorden niet delen met anderen	3.361	82,3%
Up-to-date antivirusproduct	2.164	53%
Firewall	1.704	41,7%
Beveiligingssoftware apparaten laten scannen op virussen of andere kwaadaardige software	1.815	44,5%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	2.624	64,3%
Voorzichtig met welke websites ik bezoek, wat ik download en welke mails of bijlagen ik open	2.989	73,2%
VPN-verbinding	627	15,4%
Browserextensies die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren	1.087	26,6%
Persoonlijke bestanden en gegevens versleuteld	341	8,3%
Tweestapsverificatie	1.594	39,1%
Anders	55	1,3%
Geen van bovenstaande	40	1%

5.2 Eerste reactie

Respondenten is na vertoning van het vignet gevraagd wat hun eerste emotie en handeling(en) zouden zijn nadat ze geconfronteerd zouden zijn met het losgeldbericht (tabel 5.2). De meest ervaren emoties betroffen boosheid (79,7%), nervositeit (48,6%) en afkeer (37%). Een klein deel van de respondenten heeft daarnaast in de open antwoorden aangegeven dat ze zich dom of stom zouden voelen, kwaad zouden zijn op zichzelf, zich zouden schamen of zich machteloos zouden voelen.

Een deel van de burgers zou zelf proberen om het probleem op te lossen (tabel 5.2), waarvan de meesten de verbinding met internet zouden verbreken (42,4%), zouden proberen bestanden of gegevens te herstellen vanaf een back-up (28,5%) of het apparaat opnieuw zouden opstarten (22,3%). Een deel van de burgers zou (ook) hulp zoeken. Ongeveer de helft hiervan zou hulp zoeken van een bekende (49%) of een organisatie, instantie of ICT-deskundige (50,3%) (waaronder de politie blijkens de open antwoorden). Een kleiner deel zou hulp of advies zoeken op internet (32,2%).

Tabel 5.2 Frequentie van eerste emotie, eerste handeling en uitkomst onder burgers (n=4.082)

	n	%
Eerste emotie *(meerdere antwoorden mogelijk)*	**4.082**	
Boosheid	3.252	79,7%
Afkeer	1.509	37%
Angst	1.409	34,5%
Nervositeit	1.984	48,6%
Verdriet	990	24,3%
Ontspanning	63	1,6%
Blijheid	8	0,2%
Anders, namelijk …		
– Verrast/verbaasd/ongeloof	6	0,1%
– Dom/stom voelen/kwaad op zelf/schaamte	19	0,5%
– Machteloos/hulpeloos	18	0,4%
– Geschrokken/ontzet	2	0,1%
– Geïrriteerd/gefrustreerd/verontwaardigd	16	0,4%
– Lachwekkend	12	0,3%
– Onverschillig/neutraal/gelaten	8	0,2%
– Bezorgd	4	0,1%
– Gespannen/gestrest	6	0,2%
– Vermoeid	2	0,1%
– Agressie/moordneigingen	10	0,2%
– Wanhoop	2	0,1%
Geen van de bovenstaande opties	137	3,4%

Tabel 5.2 Vervolg

	n	%
Eerste handeling *(meerdere antwoorden mogelijk)*	**4.082**	
Verbinding met internet verbreken	1.730	42,4%
Apparaat opnieuw opstarten	908	22,3%
Apparaat terugzetten naar fabrieksinstellingen	835	20,5%
Hulp of advies zoeken op internet	1.314	32,2%
Hulp of advies zoeken van een bekende	2.002	49%
Hulp of advies zoeken van een organisatie, instantie of deskundige	2.053	50,3%
Proberen bestanden of gegevens te herstellen vanaf een back-up	1.164	28,5%
Proberen om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen	813	19,9%
Proberen om bestanden weer te openen door hun extensie terug te veranderen naar het originele formaat	241	5,9%
Ik zou niks doen	138	3,4%
Ik zou iets anders doen, namelijk …		
– Een nieuw apparaat (hardware/software) gekocht	11	0,3%
– Andere technische oplossingen (bijv. 2e onafhankelijk systeem opstarten, systeem ontkoppelen, formatteren, reset)	33	0,8%
– Onderzoeken of dreiging legitiem is	2	0,1%
– Nieuwe IP	1	0,1%
– Bericht verwijderen	6	0,1%
– Losgeld betalen	1	0,1%
– Weet ik niet	5	0,1%

5.3 Onderhandelen

Respondenten is daarnaast gevraagd of, door wie, en met welk doel ze contact zouden opnemen met de daders (tabel 5.3). De meerderheid van de burgers zou geen contact opnemen met de daders (92,1%). Een kleiner aandeel zou iemand inhuren om contact op te nemen (3,7%), zou zelf contact opnemen (2,7%) of een bekende dit laten doen (1,6%). De vaakst genoemde redenen om contact op te nemen betroffen: vaststellen of het losgeldbericht echt is (45,8%), tijd rekken (39,2%) of vaststellen welke bestanden of gegevens door de daders zijn gestolen (37,7%). Slechts 89 respondenten (27,4%) zouden contact opnemen om te onderhandelen, wat neerkomt op 2,2% van de totale steekproef. De meerderheid zou onderhandelen om het losgeldbedrag te verlagen (75%). Opvallend is dat een klein deel van de respondenten contact zou opnemen of zou onderhandelen om de identiteit van de daders te achterhalen of informatie te verzamelen die de politie kan helpen in de opsporing.

Tabel 5.3 Frequentie van of, door wie en hoe er contact opgenomen zou worden met de daders onder burgers (n=4.082)

	n	%
Contact opnemen met daders	**4.082**	
Ik zou zelf contact opnemen	109	2,7%
Bekende contact laten opnemen	65	1,6%
Ingehuurde partij contact laten opnemen	150	3,7%
Geen contact opnemen	3.758	92,1%
Doel *(meerdere antwoorden mogelijk)*	**324**	
Om vast te stellen of het losgeldbericht echt is	148	45,8%
Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline	89	27,4%
Om vast te stellen welke bestanden of gegevens waren gestolen	122	37,7%
Om hulp te vragen bij het betalen (bijvoorbeeld bij het aanschaffen van bitcoin)	46	14,2%
Om hulp te vragen na het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens)	54	16,8%
Om tijd te rekken	127	39,2%
Anders, namelijk …		
– T.b.v. achterhalen identiteit/ter ondersteuning opsporing politie	16	4,9%
– Om frustratie te uiten/te laten weten niet te gaan betalen	2	0,6%
– Om meer informatie te krijgen/mogelijkheden te bespreken	3	0,9%
– Om contante betaling aan te bieden	1	0,3%
– Beslag maken op tijd om slachtofferschap bij anderen te voorkomen	2	0,6%
– Om ze terug te kunnen hacken	2	0,6%
Doel onderhandelingen *(meerdere antwoorden mogelijk)*	**89**	
Om het losgeldbedrag te verlagen	67	75%
Om langer de tijd te krijgen	43	49%
Om een andere reden, namelijk …	14	15,7%
– Informatie inwinnen/t.b.v. achterhalen identiteit/ter ondersteuning opsporing politie	6	6,7%
– Nieuwsgierigheid	1	1,1%
– Om na te gaan of ze te vertrouwen zijn/of ze zich na betaling aan de afspraken houden	3	3,4%
– Om probleem te verhelpen	1	1,1%
– Akkoord bereiken over niet betalen	1	1,1%
– Om ze te frustreren	1	1,1%

5.4 Impact

Respondenten is gevraagd wat (naar verwachting) de impact van het ransomware-incident zou zijn (tabel 5.4). Van de burgers verwacht 12,5% geen van de voorgelegde emotionele en/of psychische gevolgen te ervaren. De respondenten die denken wel

emotionele en/of psychische gevolgen te ervaren, verwachten zich voornamelijk minder veilig te voelen (59,5%), minder vertrouwen te hebben in de eigen digitale vaardigheden (50,8%) en minder vertrouwen te hebben in mensen (36,3%).

De meerderheid van de burgers gaf daarnaast aan dat ze andere gevolgen zouden ervaren (tabel 5.4). In de meeste gevallen betrof dit tijd besteden aan het oplossen van het incident (65,6%), gevolgd door het verliezen van bestanden of gegevens (56,3%) en kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (45,4%).

Wat betreft de financiële impact (buiten het eventuele betaalde losgeld), gaf bijna een derde van de respondenten aan het niet te weten (30%) en een kleiner deel dat ze naar verwachting geen financiële gevolgen zouden ervaren (9,6%). Bij de burgers die wel financiële gevolgen denken te ervaren, was dit in de meeste gevallen minder dan 1.000 euro (33,3%) (tabel 5.4).

Tabel 5.4 Frequentie van emotionele, andere en financiële gevolgen onder burgers (n=4.082)

	n	%
Emotionele/psychische gevolgen *(meerdere antwoorden mogelijk)*	**4.082**	
Minder veilig voelen	2.428	59,5%
Minder vertrouwen in mensen	1.480	36,3%
Het voorval telkens opnieuw beleven	424	10,4%
Slaapproblemen	849	20,8%
Angstklachten en/of paniekaanvallen.	452	11,1%
Depressieve klachten	302	7,4%
Minder vertrouwen in eigen digitale vaardigheden	2.075	50,8%
Andere emotionele of psychische gevolgen, namelijk …		
– Gespannen/stress/piekeren/zorgen	16	0,4%
– Gevoel van schaamte/falen/onbekwaamheid/schuldgevoelens/boos op zichzelf	4	0,1%
– Agressie/boosheid/wraakneigingen	42	1%
– Minder vertrouwen in overheid/politie	1	0,1%
– Meer angst/wantrouwen/alerter online	1	0,1%
– Angst op herhaald slachtofferschap van cybercrime	2	0,1%
– Gevoel van machteloosheid	2	0,1%
– Verergering van al bestaande psychische klachten	4	0,2%
– Ongelukkig voelen	1	0,1%
– Onzeker voelen	3	0,1%
– Verdrietig voelen	4	0,2%
Geen van de bovenstaande opties	510	12,5%
Weet ik niet	308	7,5%

Tabel 5.4 Vervolg

	n	%
Andere gevolgen *(meerdere antwoorden mogelijk)*	**4.082**	
Tijd besteden aan het oplossen van het incident	2.677	65,6%
Kosten maken vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	1.852	45,4%
Bestanden of gegevens verloren	2.299	56,3%
Anders, namelijk …		
– Risico op bekendmaking van (privacygevoelige) gegevens	2	0,1%
– Alerter/voorzichtiger geworden online	2	0,1%
– Kosten of tijd besteed aan nemen van beveiligingsmaatregelen/voorkomen van herhaling	16	0,4%
– Weet ik (nog niet)	12	0,3%
Geen van bovenstaande opties	409	10%
Financiële gevolgen (m.u.v. betalen losgeld)	**4.082**	
Geen	390	9,6%
Minder dan €1.000	1.359	33,3%
€1.000 tot €5.000	951	23,3%
€5.000 tot €10.000	128	3,1%
€10.000 tot €50.000	20	0,5%
€50.000 of meer	8	0,2%
Weet ik niet	1.226	30%

Daarnaast is aan respondenten gevraagd of het incident gevolgen zou hebben voor het online gedrag of de beveiligingsmaatregelen, wat bij 79,9% van de respondenten het geval was. De grootste groep burgers zou (vaker) back-ups maken van bestanden en gegevens op een externe harde schijf, clouddienst of server (68,2%), gevolgd door het aanmaken van unieke wachtwoorden voor alle apparaten en accounts (40,9%) en voorzichtiger zijn met welke websites ze bezoeken, wat ze downloaden en welke mails of bijlagen ze openen (37,9%) (tabel 5.5).

Tabel 5.5 Frequentie van genomen beveiligingsmaatregelen na slachtofferschap onder burgers (n=3.262)

	n	%
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**3.262**	
Ander besturingssysteem nemen	221	6,8%
(Vaker) back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	2.223	68,2%
Unieke wachtwoorden voor alle apparaten en accounts	1.336	40,9%
Persoonlijk wachtwoorden niet (meer) delen met anderen	312	9,6%
(Ander) antivirusproduct aangeschaft	855	26,2%
Firewall aanschaffen	754	23,1%

Tabel 5.5 Vervolg

	n	%
Beveiligingssoftware apparaten laten scannen op virussen of andere kwaadaardige software	977	30%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	646	19,8%
Andere standaardbrowser nemen	121	3,7%
Voorzichtiger met welke websites ik bezoek, wat ik download en welke mails of bijlagen ik open	1.236	37,9%
VPN-verbinding aanschaffen	540	16,6%
Browserextensies installeren die helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren	443	13,6%
Persoonlijke bestanden en gegevens versleutelen	799	24,5%
Tweestapsverificatie	813	24,9%
Anders, namelijk …		
– Afhankelijk van advies van specialist/expert/IT-leverancier/computerzaak	79	2,4%
– Afhankelijk van advies bekende(n), bijv. vrienden of familie	18	0,6%
– Afhankelijk van analyse hoe het incident is gebeurd, daarop maatregelen treffen	7	0,2%
– Meer offline werken	1	0,03%
– Periodieke controle/onderhoud door expert	1	0,03%
– Inloggegevens veranderen	2	0,06%
– Belangrijke bestanden op externe schijf/pc	2	0,06%
– Bijscholing/cursus volgen	4	0,1%
– Voorzichtiger met welke persoonlijke gegevens ik online deel	1	0,03%
– (Tijdelijk) stoppen met gebruik computer	2	0,06%
– Ik weet het (nog) niet	31	1%
Geen van bovenstaande	118	3,6%

5.5 Betalen

Na het vignet is aan respondenten gevraagd hoe waarschijnlijk het is dat ze in het hypothetische scenario het losgeld zouden betalen op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). Gemiddeld genomen is dit voor burgers niet waarschijnlijk (M = 1,36; SD = 2,16). Zoals blijkt uit tabel 5.6, is de betalingsbereidheid voor burgers het hoogst onder de groep waarbij 250 euro in bitcoin aan losgeld geëist werd, geadviseerd werd om te betalen, geen back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (M = 2,052; SD = 2,679). De betalingsbereidheid is het laagst onder de groep waarbij 2.500 euro in bitcoin aan losgeld geëist werd, geadviseerd werd om niet te betalen, geen back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (M = 0,746; SD = 1,501).

Tabel 5.6 Betalingsbereidheid per vignet voor burgers (n=4.082)

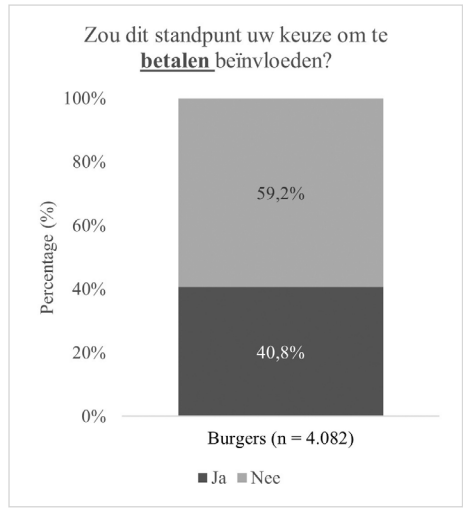
Groep	Vignet				Betalingsbereidheid (0-10)	
	Hoogte losgeld	Geadviseerd om te betalen	Back-up	Gedreigd met lekken	Gem.	Std. dev.
1	250 euro	Nee	Nee	Ja	1,228	2,095
2	250 euro	Nee	Ja	Ja	1,117	1,922
3	250 euro	Ja	Nee	Ja	2,052	2,679
4	250 euro	Ja	Ja	Ja	1,856	2,391
5	2.500 euro	Nee	Nee	Ja	1,151	2,079
6	2.500 euro	Nee	Ja	Ja	0,796	1,604
7	2.500 euro	Ja	Nee	Ja	1,669	2,280
8	2.500 euro	Ja	Ja	Ja	1,815	2,193
9	250 euro	Nee	Nee	Nee	1,177	1,943
10	250 euro	Nee	Ja	Nee	0,974	1,916
11	250 euro	Ja	Nee	Nee	2,027	2,619
12	250 euro	Ja	Ja	Nee	1,642	2,403
13	2.500 euro	Nee	Nee	Nee	0,746	1,501
14	2.500 euro	Nee	Ja	Nee	0,847	1,794
15	2.500 euro	Ja	Nee	Nee	1,345	2,063
16	2.500 euro	Ja	Ja	Nee	1,388	2,130

De respondenten is vervolgens gevraagd wat in dit hypothetische scenario redenen zouden zijn om wel of niet het losgeld te betalen (tabel 5.7). De meest voorkomende redenen om het losgeld niet te betalen waren dat respondenten er niet op zouden vertrouwen dat de toegang hersteld zou worden na betaling (62,5%), dat het onethisch is om criminelen te betalen (53,2%) en dat respondenten niet bang zouden zijn dat de daders data zouden lekken of dat er andere gevolgen zouden zijn voor het niet betalen (22,9%). De meest voorkomende redenen om wel te betalen waren dat respondenten de aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen (25,6%), dat het losgeldbedrag niet heel hoog was en ze het zich zouden kunnen veroorloven (17,2%) en dat ze erop zouden vertrouwen dat de toegang hersteld zou worden na betaling (10,8%).

Tabel 5.7 Frequentie van reden(en) om (niet) te betalen onder burgers (n=4.082)

	n	%
Reden(en) om niet te betalen *(meerdere antwoorden mogelijk)*	**4.082**	
Losgeldbedrag te hoog	814	19,9%
Zou bestanden, gegevens of apparaten niet belangrijk vinden	897	22%
Zou er niet op vertrouwen dat toegang hersteld zou worden na betaling	2.549	62,5%
Niet bang voor lekken van data of andere gevolgen bij niet betalen	936	22,9%
Onethisch om criminelen te betalen	2.172	53,2%
Zou niet weten hoe ik de betaling zou moeten doen	750	18,4%
Anders, namelijk …		
– Ik zou het zelf (of met behulp van een ander) oplossen, bijv. met back-up	65	1,6%
– Uit principe/laat me niet chanteren/houdt criminaliteit in stand/criminaliteit mag niet beloond worden	50	1,2%
– Ik zou denken dat het een valse/ongeloofwaardige dreiging is	6	0,2%
– Bang om opnieuw geraakt te worden of dat meer geld geëist wordt	18	0,4%
– Opvolging advies expert(s)	2	0,1%
– Zou er niet op vertrouwen dat gestolen data niet gelekt of verkocht zouden worden na betaling	3	0,1%
– Ik zou eerst om extern advies vragen	7	0,2%
– Justitie adviseert om niet te betalen	2	0,1%
– Bang dat ze toegang krijgen tot bankgegevens	4	0,1%
– Te veel moeite om cryptocurrency aan te schaffen	2	0,1%
Geen van de bovenstaande opties	136	3,3%
Ik zou het losgeld wel betalen	64	1,6%
Reden(en) om wel te betalen	**4.082**	
Losgeldbedrag niet heel hoog	702	17,2%
Zou bestanden, gegevens of apparaten niet willen verliezen	1046	25,6%
Zou erop vertrouwen dat toegang hersteld zou worden na betaling	443	10,8%
Bang voor lekken van data of andere gevolgen bij niet betalen	391	9,6%
Anders, namelijk …	52	1,3%
– Als expert(s) dit zouden adviseren	17	0,4%
– Als er geen andere mogelijkheid is	3	0,1%
– Dit is de snelste of makkelijkste optie	3	0,1%
– Als ik belangrijke bestanden zou hebben	1	0,1%
– Geen back-up beschikbaar	2	0,1%
– Ik weet het (nog) niet	7	0,2%
Geen van de bovenstaande opties	265	6,5%
Ik zou het losgeld niet betalen	2300	56,3%

De Nederlandse politie neemt het standpunt in dat slachtoffers het geëiste losgeld niet zouden moeten betalen. De respondenten zijn het gemiddeld genomen (helemaal) eens met dit standpunt (M = 4,53; SD = 0,804). Aan respondenten is ook gevraagd of dit standpunt de keuze om te betalen zou beïnvloeden, wat bij iets minder dan de helft van de burgers het geval was (40,8%) (figuur 5.1).



Figuur 5.1 Invloed van standpunt politie om niet te betalen op keuze om te betalen

Verklarende resultaten

Om te onderzoeken of de waarschijnlijkheid van betalen gerelateerd is aan de vignetfactoren is een negatieve binomiale regressie uitgevoerd. Het regressiemodel bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. Leeftijd, geslacht en opleidingsniveau zijn daarnaast als controlevariabelen aan het model toegevoegd. Zoals blijkt uit tabel 5.8, is er een negatieve significante relatie tussen de hoogte van het losgeldbedrag en de waarschijnlijkheid van betalen (B = −0,226, z = −3,989, p = < 0,001). Burgers van wie 2.500 euro aan bitcoin is geëist, achten het minder waarschijnlijk dat zij het losgeld zouden betalen in vergelijking met burgers bij wie 250 euro aan bitcoin is geëist. Dit betekent, met andere woorden, dat burgers een hogere waarschijnlijkheid van betalen rapporteren indien het losgeldbedrag lager is. Tussen dreigen met het lekken van data en de waarschijnlijkheid van betalen bestaat een positief significant verband (B = 0,164, z = 2,889, p = 0,004). Burgers rapporteren een hogere waarschijnlijkheid van betalen indien er gedreigd wordt met het lekken van data. Er is daarnaast een positief significant verband tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de respondent heen en de waarschijnlijkheid van betalen (B = 0,534, z = 9,384, p = < 0,001). Burgers rapporteren een hogere waarschijnlijkheid van betalen indien hen geadviseerd wordt om het losgeld te betalen. Daarentegen is er geen signific-

ant verband tussen het hebben van een back-up en de waarschijnlijkheid van betalen onder burgers (B = −0,053, z = −0,940, p = 0,347).

Wanneer gekeken wordt naar de controlevariabelen blijkt er een negatief significant verband te zijn tussen leeftijd en de waarschijnlijkheid van betalen onder burgers (B = −0,012, z = −6,662, p = < 0,001). Hoe jonger respondenten zijn, hoe hoger de waarschijnlijkheid van betalen is. Bovendien bestaat er een negatief significant verband tussen laag (B = −0,486, z = −5,839, p = < 0,001) en middelbaar opleidingsniveau (B = −0,368, z = −5,796, p = < 0,001) en de waarschijnlijkheid van betalen. Onder laag- of middelbaar opgeleiden is de waarschijnlijkheid van betalen lager in vergelijking met hoogopgeleiden.

Tabel 5.8 Negatieve binomiale regressie van de waarschijnlijkheid van betalen onder burgers (n=4.082)

		B	S.E.	z
	(Intercept)	0,811***	0,110	7,376
Vignet factoren	Hoogte losgeld (0-1)	−0,226***	0,057	−3,989
	Gedreigd met lekken	0,164**	0,057	2,889
	Back-up (0-1)	−0,053	0,057	−0,940
	Geadviseerd om te betalen (0-1)	0,534***	0,057	9,384
Controle-variabelen	Leeftijd (0-91)	−0,012***	0,002	−6,662
	Geslacht			
	Man (0-1)	0,061	0,057	1,072
	Genderneutraal (0-1)	−0,374	0,532	−0,702
	Vrouw (0-1)	REF		
	Opleidingsniveau			
	Laag (0-1)	−0,486***	0,083	−5,839
	Middelbaar (0-1)	−0,368***	0,064	−5,796
	Hoog (0-1)	REF		
	2 × log likelihood	−12253,6680		
	AIC	12.276		

*p< 0,05; **p< 0,01; ***< 0,001

5.6 Melden

Tevens is aan de burgers gevraagd hoe waarschijnlijk het is dat ze in het hypothetische scenario het incident zouden melden en/of aangifte zouden doen op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). Gemiddeld genomen is dit

voor burgers waarschijnlijk (M = 7,98; SD = 2,86). Hoewel de verschillen tussen groepen klein zijn, blijkt uit tabel 5.9 dat de meldingsbereidheid voor burgers het hoogst is onder de groep waarbij 2.500 euro in bitcoin aan losgeld geëist werd, geadviseerd werd om te betalen, wel een back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (M = 8,341; SD = 2,642). De meldingsbereidheid is het laagst onder de groep waarbij 250 euro in bitcoin aan losgeld geëist werd, geadviseerd werd om wel te betalen, wel een back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (M = 7,501; SD = 3,073).

Tabel 5.9 Meldingsbereidheid per vignet voor burgers (n=4.082)

Groep	Vignet				Meldingsbereidheid (0-10)	
	Hoogte losgeld	Geadviseerd om te betalen	Back-up	Gedreigd met lekken	Gem.	Std. dev.
1	250 euro	Nee	Nee	Ja	7,919	2,760
2	250 euro	Nee	Ja	Ja	7,563	3,157
3	250 euro	Ja	Nee	Ja	8,075	2,778
4	250 euro	Ja	Ja	Ja	8,025	2,641
5	2.500 euro	Nee	Nee	Ja	7,966	3,031
6	2.500 euro	Nee	Ja	Ja	8,188	2,749
7	2.500 euro	Ja	Nee	Ja	8,339	2,576
8	2.500 euro	Ja	Ja	Ja	8,341	2,642
9	250 euro	Nee	Nee	Nee	7,953	2,867
10	250 euro	Nee	Ja	Nee	7,757	3,019
11	250 euro	Ja	Nee	Nee	8,208	2,712
12	250 euro	Ja	Ja	Nee	7,501	3,073
13	2.500 euro	Nee	Nee	Nee	7,785	2,928
14	2.500 euro	Nee	Ja	Nee	7,842	3,044
15	2.500 euro	Ja	Nee	Nee	8,201	2,738
16	2.500 euro	Ja	Ja	Nee	7,986	2,936

Met betrekking tot het melden van de hypothetische ransomware-aanval, zou de meerderheid van de burgers die het incident zou melden dit doen bij de politie (88,2%), gevolgd door de Fraudehelpdesk (46,2%) en een bank of financiële instelling (44,8%). Ook een aantal andere hulpbronnen zoals Senior Web en de werkgever werden aangedragen door de respondenten (tabel 5.10).

Tabel 5.10 Frequentie van instanties waar respondenten zouden melden in het hypothetische scenario (n=4.082)

	Contact met	
	n	%
Politie	3.599	88,2%
Bank of financiële instelling	1.828	44,8%
Verzekeringsmaatschappij	620	15,2%
Cybersecuritybedrijf/IT-leverancier/computerzaak/computerdeskundige/ internetprovider	801	19,6%
No More Ransom	443	10,8%
Slachtofferhulp	151	3,7%
Fraudehelpdesk	1.885	46,2%
Een andere organisatie		
– Senior Web	3	0,1%
– Consumentenbond	2	0,1%
– Werkgever	16	0,4%
– Weet ik niet/Dit zou ik uitzoeken, bijvoorbeeld via Google	28	0,7%

De respondenten is vervolgens gevraagd wat in dit hypothetische scenario redenen zouden zijn om wel of niet te melden bij de politie (tabel 5.11). De meest voorkomende redenen voor burgers om niet te melden waren dat het geen zin heeft, omdat de politie er toch niets aan zou doen (57,1%), dat het eerder een zaak is voor een andere instantie dan de politie (32,5%) en dat ze het zelf of met behulp van een andere partij zouden oplossen (25,9%). De meest voorkomende redenen voor burgers om wel te melden waren dat respondenten zouden willen dat de dader gepakt wordt (80,2%), om te voorkomen dat dit bij een ander gebeurt (68,4%) en omdat ze vinden dat het hun plicht is (53,3%).

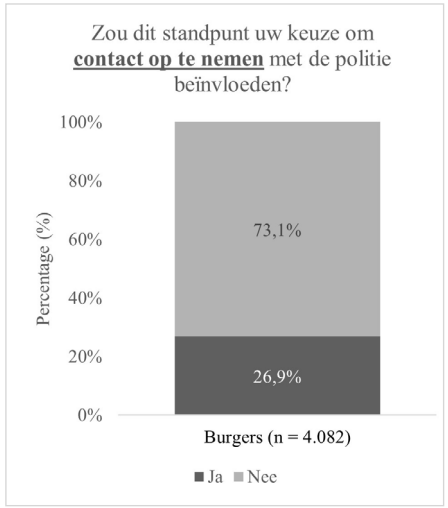
Tabel 5.11 Frequentie van reden(en) om (niet) te melden en/of aangifte te doen bij de politie onder burgers (n=4.082)

	n	%
Reden(en) om niet te melden *(meerdere antwoorden mogelijk)*	**483**	
Ik zou het zelf of met behulp van een andere partij oplossen	125	25,9%
Het is niet zo belangrijk	40	8,2%
Het kost te veel moeite	71	14,8%
Het heeft geen zin, de politie zou er toch niets aan doen	276	57,1%
De politie heeft niet de kennis om dit type delict aan te pakken	90	18,7%
Het is eerder een zaak voor een andere instantie dan de politie	157	32,5%
Ik heb weinig vertrouwen in de politie	84	17,4%

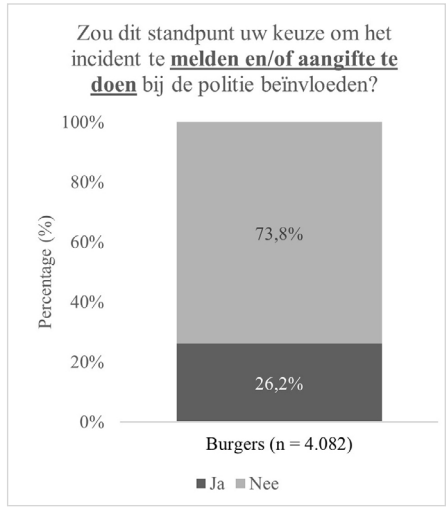
Tabel 5.11 Verder

	n	%
Ik zou bang zijn dat de dader wraak zal nemen	7	1,4%
Ik zou me schamen dat ik slachtoffer ben geworden	14	3%
Ik zou schamen dat ik het losgeld betaald heb	4	0,8%
Ik zou vinden dat het eigenlijk mijn eigen schuld is	26	5,3%
Anders, namelijk		
– Zou er niet aan denken/wist niet dat dit mogelijk is	1	0,2%
– Weet ik niet/geen idee waar ik het zou moeten melden	11	2,3%
– Zolang ik niet reageer/klik is er niets aan de hand	4	0,8%
Reden(en) om wel te melden *(meerdere antwoorden mogelijk)*	**3.599**	
Om te voorkomen dat dit opnieuw bij mij gebeurt	1.353	37,6%
Om te voorkomen dat dit bij een ander gebeurt	2.460	68,4%
Ik zou willen dat de dader gepakt wordt	2.885	80,2%
Om een veiligere (online) wereld te creëren	1.900	52,8%
Het is mijn plicht	1.919	53,3%
Om de schade vergoed te krijgen	647	18%
Anders, namelijk …		
– Voor advies/hulp	20	0,6%
– Attenderen op veiligheidsrisico's	1	0,02%
– T.b.v. statistieken	6	0,2%
– Hoe meer meldingen, hoe groter de kans dat er iets aan gedaan wordt	4	0,1%
– Geen idee bij welke organisatie anders	9	0,3%
– Omdat dit geadviseerd wordt	1	0,02%

Zoals eerder vermeld, zijn de respondenten het gemiddeld genomen (helemaal) eens met het advies van de politie dat slachtoffers het geëiste losgeld niet moeten betalen. Aan respondenten is gevraagd of dit standpunt de keuze om contact op te nemen met de politie en het incident te melden of aangifte te doen bij de politie zou beïnvloeden. Ongeveer een vierde van de respondenten geeft aan dat het hun keuze om contact op te nemen met de politie zou beïnvloeden (figuur 5.2). Daarnaast geeft ongeveer een vierde van de respondenten aan dat dit standpunt hun keuze om het ransomware-incident te melden/aangifte te doen bij de politie zou beïnvloeden (figuur 5.3).



Figuur 5.2 Invloed van standpunt politie om niet te betalen op keuze om contact op te nemen met de politie



Figuur 5.3 Invloed van standpunt politie om niet te betalen op keuze om te melden en/of aangifte te doen

Verklarende resulten

Om te onderzoeken of de waarschijnlijkheid van melden gerelateerd is aan de vignetfactoren is een Poisson regressie uitgevoerd. Het regressiemodel bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. Leeftijd, geslacht en opleidingsniveau zijn daarnaast als controlevariabelen aan het model toegevoegd. Zoals blijkt uit tabel 5.12, is er een positief significant verband tussen de hoogte van het losgeldbedrag en de waarschijnlijkheid van melden (B = 0,026, z = 2,302, p = 0,021). Burgers van wie 2.500 euro aan bitcoin is geëist, rapporteren een hogere waarschijnlijkheid van melden in vergelijking met burgers van wie 250 euro aan bitcoin is geëist. Daarnaast is er een positief significant verband tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de respondent heen en de waarschijnlijkheid van melden (B = 0,027, z = −2,400, p = 0,016). Burgers rapporteren een hogere waarschijnlijkheid van melden indien hen geadviseerd wordt om het losgeld te betalen. Daarentegen is er geen significant verband tussen dreigen met lekken (B = 0,020, z = −1,821, p = 0,06) en het hebben van een back-up (B = −0,017, z = −1,565, p = 0,118) en de waarschijnlijkheid van melden onder burgers.

Wanneer gekeken wordt naar de controlevariabelen blijkt er allereerst een positief significant verband te zijn tussen leeftijd en de waarschijnlijkheid van melden onder burgers (B = 0,003, z = 10,043, p = <0,001). Hoe ouder respondenten zijn, hoe hoger de waarschijnlijkheid van melden is. Daarnaast is er een significant verband tussen ge-

slacht en de waarschijnlijkheid van melden (B = −0,044, z = −3,952, p = < 0,001). De waarschijnlijkheid van melden is lager onder mannen dan onder vrouwen. Tot slot is opleidingsniveau significant gerelateerd aan de meldingsbereidheid. Burgers met een laag (B = −0,051, z = −3,199, p = 0,001) of middelbaar opleidingsniveau (B = −0,049, z = −3,850, p = < 0,001) rapporteren een lagere waarschijnlijkheid van melden in vergelijking met hoogopgeleiden.

Tabel 5.12 Poisson-regressie van de waarschijnlijkheid van melden onder burgers (n=4.082)

		B	S.E.	z
	(Intercept)	1,924***	0,022	87,112
Vignet factoren	Hoogte losgeld (0-1)	0,026*	0,011	2,302
	Gedreigd met lekken	0,020	0,011	1,821
	Back-up (0-1)	−0,017	0,011	−1,565
	Geadviseerd om te betalen (0-1)	0,027*	0,011	2,400
Controleva-riabelen	Leeftijd (0-91)	0,003***	0,000	10,043
	Geslacht			
	Man (0-1)	−0,044***	0,011	−3,952
	Genderneutraal (0-1)	0,048	0,099	0,483
	Vrouw (0-1)	REF		
	Opleidingsniveau			
	Laag (0-1)	−0,051**	0,016	−3,199
	Middelbaar (0-1)	−0,049***	0,013	−3,850
	Hoog (0-1)	REF		
	AIC	21.323		

*p< 0,05; **p< 0,01; ***< 0,001

5.7 Resumé

In dit hoofdstuk is stilgestaan bij de betalings- en meldingsbereidheid onder Nederlandse burgers die niet eerder slachtoffer zijn geworden van ransomware aan de hand van een hypothetisch scenario. Als het gaat om de verwachte eerste reactie van burgers in het hypothetische scenario, was de meest voorkomende emotie boosheid. Een deel van de respondenten zou zelf proberen om het probleem op te lossen, in de meeste gevallen door de verbinding met internet te verbreken. Een ander deel van de respondenten zou hulp zoeken, in de meeste gevallen van een organisatie of instantie, of een bekende, gevolgd door hulp via internet.

Met betrekking tot het contact opnemen met de daders, zou slechts 8% van de respondenten dit doen of iemand anders laten doen. In de meeste gevallen zouden respondenten dit doen om vast te stellen of het losgeldbericht echt is. Iets meer dan een kwart van de respondenten zou contact opnemen om te onderhandelen, wat neerkomt op 2,2% van de totale steekproef. De meerderheid hiervan zou onderhandelen om het losgeldbedrag te verlagen.

Als het gaat om de impact, verwacht de meerderheid van de respondenten emotionele of psychische gevolgen te ervaren, met name een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden. De meerderheid van de respondenten gaf daarnaast aan andere gevolgen te zullen ervaren, met name het besteden van tijd aan het oplossen van het incident. Iets meer dan de helft van de respondenten verwacht financiële gevolgen (buiten het eventueel betaalde losgeld), waarbij dit in de meeste gevallen naar schatting minder dan 1.000 euro zou zijn. Voor een groot deel van de respondenten zou het ransomware-incident tevens leiden tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In de meeste gevallen zouden respondenten (vaker) externe back-ups maken van bestanden en gegevens.

De betalingsbereidheid is laag in het hypothetische scenario, met als voornaamste reden dat respondenten er niet op zouden vertrouwen dat de toegang hersteld zou worden na betaling. De meest voorkomende reden om wel te betalen was dat respondenten de aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen. Uit de regressieanalyse blijkt bovendien dat een losgeldbedrag van 250 euro (ten opzichte van 2.500 euro), de dreiging van het lekken van data en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen gerelateerd is aan een significant hogere waarschijnlijkheid van betalen.

De meldingsbereidheid is hoog in het hypothetische scenario. De meerderheid van de burgers zou het incident melden bij de politie (88,2%), gevolgd door de Fraudehelpdesk (46,2%) en een bank of financiële instelling (44,8%). De voornaamste reden om te melden bij de politie is dat respondenten zouden willen dat de dader gepakt wordt. De voornaamste reden om niet te melden is dat het volgens respondenten geen zin zou hebben omdat de politie er toch niets aan zou doen. Respondenten zijn het eens met het algemene advies van de politie om het losgeld niet te betalen en bij ongeveer 41% zou het standpunt invloed hebben op de keuze om te betalen. Tegelijkertijd zou ditzelfde standpunt bij ongeveer 27% invloed hebben op de keuze om contact op te nemen met de politie en bij 26% om het incident te melden en/of aangifte te doen. Uit de regressieanalyse blijkt daarnaast dat een losgeldbedrag van 2.500 euro (ten opzichte van 250 euro) en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen gerelateerd is aan een significant hogere waarschijnlijkheid van melden.

5.8 Vergelijking deelstudie 1A en 2A

In voorgaande secties is stilgestaan bij de prevalentie, aard en impact van daadwerkelijk slachtofferschap van ransomware onder Nederlandse burgers (deelstudie 1A) en de betalings- en meldingsbereidheid aan de hand van een hypothetisch scenario onder Nederlandse burgers die niet eerder slachtoffer zijn geworden van ransomware (deelstudie 2A). In deze paragraaf worden de resultaten van beide deelstudies onder burgers vergeleken.

Bij zowel daadwerkelijk slachtofferschap als in het hypothetische scenario was de meest voorkomende emotie onder burgers boosheid. In beide deelstudies zouden de meeste respondenten daarnaast proberen om zelf het probleem op te lossen door de verbinding met internet te verbreken. Van de burgers die hulp heeft gezocht of zou zoeken, zou de grootste groep burgers in deelstudie 1 hulp zoeken van een bekende, terwijl de grootste groep in deelstudie 2 hulp zou zoeken van een organisatie, instantie of deskundige.

In beide deelstudies neemt een klein deel van de respondenten contact op met de daders. Waar 4,4% van de daadwerkelijke slachtoffers contact heeft opgenomen, zou 8% van de niet-slachtoffers (in het hypothetische scenario) dit doen. In beide deelstudies liggen hier bovendien andere motivaties aan ten grondslag. Waar de slachtoffers in de meeste gevallen contact hebben opgenomen om te informeren over de hoogte van het losgeld, zouden de niet-slachtoffers dit doen om vast te stellen of het losgeldbericht echt is. Opvallend is daarnaast dat geen enkele burger die slachtoffer is geworden heeft onderhandeld met de daders, terwijl 2,2% van de totale steekproef van niet-slachtoffers aangeeft dit wel te willen doen, met name om het losgeldbedrag te verlagen.

Op basis van het hypothetische scenario verwacht 80% van de niet-slachtoffers een of meerdere van de in de vragenlijst genoemde emotionele of psychische gevolgen te ervaren na een ransomware-aanval. Onder de daadwerkelijke slachtoffers was dit bij 44,8% van de respondenten het geval. De meest voorkomende (verwachte en daadwerkelijke) gevolgen komen overeen, namelijk een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden. Bij beide groepen is het meest voorkomende andere gevolg het besteden van tijd aan het oplossen van het incident. Waar 60,4% van de niet-slachtoffers financiële gevolgen verwacht, werd dit ervaren door 28,6% van de slachtoffers, waarbij het bij beide groepen in de meeste gevallen om minder dan 1.000 euro ging. Bij een groot deel van de slachtoffers en niet-slachtoffers leidt het incident bovendien tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. Waar de meeste niet-slachtoffers (vaker) externe back-ups zouden maken van bestanden en gegevens, is het grootste aandeel slachtoffers voorzichtiger geworden met welke websites ze bezoeken, wat ze downloaden en welke bijlagen ze openen.

De betalingsbereidheid is laag, zowel in het hypothetische scenario als onder de slachtoffers. Slechts 4,1% van de respondenten die daadwerkelijk slachtoffer is geworden heeft betaald, terwijl de waarschijnlijkheid van betalen in het hypothetische scenario 1,36 is op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). De meeste respondenten in beide groepen gaven als reden dat ze niet vertrouwen dat de toegang hersteld zou worden na betaling. Waar de meeste slachtoffers die wel betaalden de tegenovergestelde reden geven, namelijk dat ze er wel op vertrouwden dat toegang hersteld zou worden na betaling, geven de meeste niet-slachtoffers een andere motivatie. De meest voorkomende reden onder niet-slachtoffers om te betalen was dat respondenten de aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen. Uit de regressieanalyse blijkt bovendien dat een losgeldbedrag van 250 euro (ten opzichte van 2.500 euro) de dreiging van het lekken van data en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen gerelateerd is aan een significant hogere waarschijnlijkheid van betalen in het hypothetische scenario.

Hoewel de meldingsbereidheid hoog is onder respondenten in het hypothetische scenario, blijkt dit niet het geval onder de slachtoffers. Waar de waarschijnlijkheid van melden in het hypothetische scenario 7,98 is op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk) en 88,2% zou melden bij de politie, heeft 15,6% van de slachtoffers contact opgenomen met de politie en slechts 2,1% daadwerkelijk aangifte gedaan. Zowel de slachtoffers als niet-slachtoffers gaven als voornaamste reden om te melden dat ze zouden willen dat de dader gepakt wordt. Waar de meeste slachtoffers aangeven dat ze niet gemeld hebben omdat ze het zelf of met behulp van een andere partij hebben opgelost, zouden de niet-slachtoffers voornamelijk niet melden omdat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen.

Zowel de slachtoffers als de niet-slachtoffers zijn het eens met het advies van de politie om het losgeld niet te betalen. Dit standpunt heeft bij ongeveer 21% van de slachtoffers en 27% van de niet-slachtoffers invloed op de keuze om contact op te nemen met de politie. Het heeft daarnaast bij ongeveer 40% van de slachtoffers en 26% van de niet-slachtoffers invloed op de keuze om een melding en/of aangifte te doen. Uit de regressieanalyse blijkt daarnaast dat een losgeldbedrag van 2.500 euro (ten opzichte van 250 euro) en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen gerelateerd is aan een significant hogere waarschijnlijkheid van melden in het hypothetische scenario.

Samengenomen zijn de belangrijkste verschillen tussen deelstudie 1 (onder slachtoffers) en deelstudie 2 (respondenten die rapporteren naar aanleiding van een fictief scenario) met betrekking tot onderhandelen dat slachtoffers met name contact zouden opnemen om te informeren over de hoogte van het losgeld en niet-slachtoffers om vast te stellen of het losgeldbericht echt is. Daarnaast zou 2,2% van de niet-slachtoffers on-

derhandelen, terwijl geen enkel slachtoffer dat daadwerkelijk heeft gedaan. Met betrekking tot betalen was het belangrijkste verschil dat de motivatie om niet te betalen uiteenliep, waarbij slachtoffers met name betaalden omdat ze vertrouwden dat de toegang hersteld zou worden, terwijl niet-slachtoffers met name zouden betalen omdat ze de aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen. Met betrekking tot melden was het belangrijkste verschil dat de meldingsbereidheid hoog is onder niet-slachtoffers, terwijl slechts 15,6% van de slachtoffers contact heeft opgenomen met de politie en 2,1% aangifte heeft gedaan. Ook de belangrijkste beweegreden om niet te melden liep uiteen. Bij de slachtoffers was dit in de meeste gevallen omdat ze het zelf of met behulp van een andere partij hebben opgelost, terwijl de niet-slachtoffers voornamelijk niet zouden melden omdat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen.

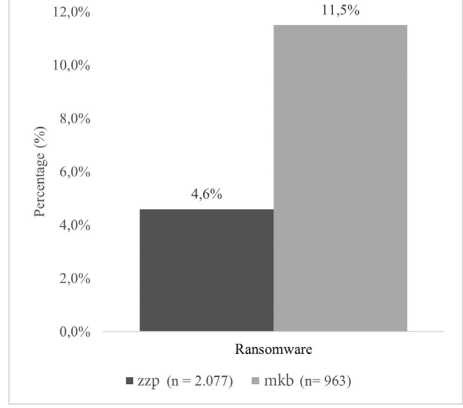
Deel II Resultaten ondernemers

6 Prevalentie, aard en impact van zelfgerapporteerd slachtofferschap van ransomware onder ondernemers

In dit hoofdstuk worden de resultaten van deelstudie 1B naar slachtofferschap van ransomware onder ondernemers besproken, waarbij wordt stilgestaan bij de prevalentie, aard en impact van slachtofferschap.[26]

6.1 Prevalentie

Aan het begin van de vragenlijst is aan alle ondernemers gevraagd om voor acht vormen van cybercriminaliteit aan te geven of hun onderneming dit (of een poging ertoe) ooit heeft meegemaakt. Van de 2.077 zzp'ers is 4,6% (n=96) ooit slachtoffer geworden van ransomware, van de 963 mkb'ers is 11,5% (n=111) ooit slachtoffer geworden van ransomware (figuur 6.1).



Figuur 6.1 Prevalentie van slachtofferschap van cybercriminaliteit onder zzp'ers en mkb'ers

26 De frequenties en percentages in tabellen tellen niet altijd op tot de totalen als gevolg van het afronden van getallen in verband met het wegen van de data. Daarnaast tellen sommige percentages niet op tot de totalen omdat respondenten meerdere antwoorden konden selecteren. Dit laatste is aangeduid in de tabellen.

De respondenten die gerapporteerd hebben slachtoffer te zijn geworden van ransomware, zijn doorverwezen naar deelstudie 1B, waarin vervolgvragen zijn gesteld over hun ervaringen. Het vervolg van de resultaten heeft betrekking op de groep respondenten die gerapporteerd heeft slachtoffer te zijn geworden van ransomware en de volledige vragenlijst heeft ingevuld (zzp = 88, mkb = 100).

6.2 Achtergrondkenmerken

Aan de ondernemers in deelstudie 1B is allereerst gevraagd hoeveel tijd ze doorgaans online spenderen voor hun bedrijf, en welke online mogelijkheden, verzekering en beveiligingsmaatregelen hun bedrijf had voordat ze slachtoffer van ransomware werden (tabel 6.1). De meeste zzp'ers zijn dagelijks (37,9%) of (bijna) continu online (24,1%). Het grootste deel heeft accounts of pagina's op sociale media (54,1%), slaat elektronisch bedrijfsgegevens of persoonlijke gegevens op (41,3%) of heeft financiële of boekhoudingsoftware (34%). Vrijwel alle zzp'ers zijn niet verzekerd tegen cybersecurity-incidenten (98,3%). Back-ups op een externe harde schijf, clouddienst of server (87,1%), het hebben van een up-to-date antivirusproduct (75%) en het direct uitvoeren van updates zodra deze beschikbaar zijn (62,2%), waren de meest voorkomende beveiligingsmaatregelen onder zzp'ers voordat ze slachtoffer werden.

De meeste mkb'ers zijn (bijna) continu (43,3%) of meerdere keren per dag (20,9%) online. Net als bij de zzp'ers heeft het grootste deel accounts of pagina's op sociale media (58,6%), financiële of boekhoudingsoftware (57,4%) en slaat elektronisch bedrijfsgegevens of persoonlijke gegevens op (50%). Een iets groter deel van de mkb'ers heeft een cybersecurityverzekering in vergelijking met de zzp'ers, maar ook de meerderheid van de mkb'ers is niet verzekerd tegen cybersecurity-incidenten (83,4%). Back-ups op een externe harde schijf, clouddienst of server (89,1%), het hebben van een up-to-date virusproduct (77,8%) en het hebben van firewalls die zowel het volledige IT-netwerk als individuele apparaten beschermen (69,7%) waren de meest voorkomende beveiligingsmaatregelen onder mkb'ers voordat ze slachtoffer werden.

Daarnaast is aan respondenten gevraagd of ze (eind)verantwoordelijk waren voor de cybersecurity binnen hun bedrijf. Bij 87,3% van de zzp'ers en 81,1% van de mkb'ers was dit het geval.

Tabel 6.1 Frequentie van tijd online, en online mogelijkheden, verzekering en beveiligingsmaatregelen voor slachtofferschap onder zzp'ers en mkb'ers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Tijd online voor bedrijf	**88**		**100**	
Minder dan 1 keer per maand	0	0%	3	3,1%
Minimaal 1 keer per maand, maar niet wekelijks	0	0%	0	0%
Minimaal 1 keer per week, maar niet dagelijks	8	9,5%	5	5,2%
Dagelijks	33	37,9%	16	15,8%
Meerdere keren per dag	17	19%	21	20,9%
Minstens ieder uur	8	9,5%	12	11,8%
Ik ben (bijna) continu online	21	24,1%	43	43,3%
Online mogelijkheden bedrijf *(meerdere antwoorden mogelijk)*	**88**		**100**	
Accounts of pagina's op sociale media	48	54,1%	58	58,6%
De mogelijkheid voor klanten om online te bestellen, te reserveren, te betalen voor producten of diensten, of een schenking te doen	9	10,4%	27	26,7%
De mogelijkheid voor klanten om online toegang te krijgen tot (enkele) diensten	8	8,6%	16	16,1%
Een online bankrekening waarnaar klanten betalingen kunnen overmaken	14	16,5%	32	32,6%
Een industrieel controlesysteem	1	0,9%	1	0,8%
Een Enterprise Resource Planning (ERP)-systeem	1	1,7%	18	17,6%
Financiële of boekhoudingssoftware	30	34%	57	57,4%
Het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs	36	41,3%	50	50%
Anders	10	11,2%	6	5,9%
Geen van de bovenstaande opties	10	11,1%	7	7,3%
Verzekering	**88**		**100**	
Specifieke verzekering voor cybersecurity	1	0,9%	3	3,5%
Cybersecurityverzekering onderdeel van bredere verzekeringspolis	0	0%	6	6,1%
Niet verzekerd tegen cybersecurity-incidenten	86	98,3%	83	83,4%
Weet ik niet	1	0,9%	7	7%

Tabel 6.1 Vervolg

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Beveiligingsmaatregelen voor slachtofferschap *(meerdere antwoorden mogelijk*	**88**		**100**	
Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	77	87,1%	89	89,1%
Wachtwoordbeleid dat zorgt voor sterke wachtwoorden	34	39,2%	39	39,5%
Up-to-date antivirusproduct	66	75%	78	77,8%
Firewall die zowel volledige IT-netwerk als individuele apparaten beschermt	48	54,9%	69	69,7%
Beveiligingssoftware die netwerken en apparaten scant op virussen of andere kwaadaardige software	52	58,6%	68	68,4%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	55	62,2%	62	61,9%
Monitoren van gebruikers- of netwerkactiviteiten	7	7,6%	18	17,7%
IT-administratie en toegangsrechten beperkt tot specifieke gebruikers	29	33,5%	45	44,9%
IT-administratie en toegangsrechten bijhouden	17	19,8%	37	37,6%
Specifieke regels voor veilig opslaan van bestanden met persoonsgegevens	11	12,9%	15	14,6%
Gevoelige bestanden en gegevens versleuteld	9	10,4%	13	13,2%
Veiligheidsrestricties op apparaten die eigendom zijn van het bedrijf	7	8,5%	11	11,3%
Toegang tot bedrijfsnetwerk alleen toegestaan op apparaten van het bedrijf	19	21,3%	20	20%
Gescheiden wifi-netwerken voor personeel en gasten	18	20,3%	32	32,2%
Tweestapsverificatie	18	20,8%	16	15,7%
Iemand (intern of extern) in dienst die verantwoordelijk is voor cybersecurity	8	8,6%	19	19,3%
Bedrijfscontinuïteitsplan opgesteld	2	2,4%	2	1,9%
Anders	0	0%	0	0%
Geen van bovenstaande	2	2,6%	2	2,2%

6.3 Frequentie, incidentie en type ransomware

Zoals genoemd heeft 4,6% van de zzp'ers gerapporteerd ooit slachtoffer te zijn geworden van ransomware. Van de slachtoffers is 6,8% in de afgelopen 12 maanden, 16,5% tussen 1-2 jaar geleden, 21,4% tussen 2-4 jaar geleden en iets meer dan de helft (55,3%) 5 of meer jaar geleden slachtoffer geworden. Het percentage slachtofferschap van ransomware in het afgelopen jaar binnen de gehele steekproef van zzp'ers is 0,3%. De meerderheid van de respondenten is 1 keer slachtoffer geworden (89,8%), een deel is 2 keer slachtoffer geworden (5,1%) en het kleinste deel is 3 keer (3,4%) of 4 keer of vaker (1,7%) slachtoffer geworden.[27] Bij meer dan een derde van de zzp'ers was sprake van cryptoware (versleuteling) (33,9%). Een kleiner deel van de respondenten is slachtoffer geworden

27 Respondenten die meerdere keren slachtoffer zijn geworden, is gevraagd om de vervolgvragen in te vullen over de laatste keer dat dit gebeurde.

van lockerware (vergrendeling) (29,3%), scareware met een bericht van een zogenaamde wetshandhavingsinstantie (17,2%) of weet het niet meer (6,9%) (tabel 6.2).
Van de mkb'ers heeft 11,5% gerapporteerd ooit slachtoffer te zijn geworden van ransomware. Van de slachtoffers is 8,8% in de afgelopen 12 maanden, 13,2% tussen 1-2 jaar geleden, 29,6% tussen 2-4 jaar geleden en ongeveer de helft (48,4%) 5 of meer jaar geleden slachtoffer geworden. Het percentage slachtofferschap van ransomware in het afgelopen jaar binnen de gehele steekproef van mkb'ers is 0,9%. Vergelijkbaar als bij de zzp'ers is de meerderheid van de mkb'ers 1 keer slachtoffer geworden (86,9%), gevolgd door 2 keer (12,3%) en 3 keer of vaker (0,8%). Bij meer dan een derde van de mkb'ers was sprake van cryptoware (versleuteling) (34,9%) of lockerware (vergrendeling) (33,3%). Een kleiner deel van de respondenten is slachtoffer geworden van scareware met een bericht van een zogenaamde wetshandhavingsinstantie (7,4%) of weet het niet meer (11,1%) (tabel 6.2).

Tabel 6.2 Frequentie van incidentie, jaartal en type ransomware onder ondernemers

	zzp (n=88)		**mkb (n=**100)	
	n	**%**	**n**	**%**
Incidentie	**88**		**100**	
1 keer	79	89,8%	87	86,9%
2 keer	5	5,1%	12	12,3%
3 keer	3	3,4%	0	0%
4 keer of vaker	1	1,7%	1	0,8%
Laatste keer slachtoffer	**88**		**100**	
Een jaar geleden of minder	6	6,8%	9	8,8%
1-2 jaar geleden	14	16,5%	13	13,2%
2-4 jaar geleden	19	21,4%	29	29,6%
5 of meer jaar geleden	49	55,3%	48	48,4%
Type ransomware	**88**		**100**	
Lockerware (vergrendeling)	26	29,3%	33	33,3%
Cryptoware (versleuteling)	30	33,9%	35	34,9%
Scareware wethandhavingsinstantie	15	17,2%	7	7,4%
Geen van de bovenstaande opties	11	12,7%	13	13,2%
Ik weet het niet meer	6	6,9%	11	11,1%

6.4 Aard van incident

Vervolgens is aan respondenten gevraagd hoe ze (met de kennis van nu) denken dat de ransomware op hun apparaat of systeem is gekomen (tabel 6.3). Ongeveer 1 op de 5 (20,9%) zzp'ers weet niet hoe hun systeem besmet is geraakt. Het grootste deel van de zzp'ers die dit wel weet, heeft geklikt op een link of heeft een bijlage geopend in een (phishing) e-mail (44,6%). Een kleiner deel heeft geklikt op een link, advertentie of

pop-up tijdens het surfen op internet (13,5%), heeft een malafide applicatie of malware geïnstalleerd (6,1%), had een kwetsbaarheid of beveiligingslek (7,9%) of er was een bedrijf gehackt waar hun gegevens bekend waren (5,2%). Daarnaast hebben twee respondenten in de open antwoorden aangegeven dat hun systeem vermoedelijk besmet is geraakt tijdens het surfen op internet of een bezoek aan een website, of door een fout van de provider.

Voor de mkb'ers geldt dat 15,6% van de respondenten niet weet hoe hun systeem besmet is geraakt. Ongeveer de helft van de mkb'ers die dit wel weet, heeft geklikt op een link of een bijlage geopend in een (phishing) e-email (54,5%). Bij een kleiner deel was sprake van een kwetsbaarheid of beveiligingslek (12,3%), is er geklikt op een link, advertentie of pop-up tijdens het surfen op internet (10,2%), was een bedrijf gehackt waar gegevens van de respondent bekend waren (5,2%) of is een kwaadaardige applicatie of software geïnstalleerd (1,4%). Blijkens de open antwoorden denken twee respondenten daarnaast dat hun systeem vermoedelijk besmet is geraakt tijdens het surfen op internet of een bezoek aan een website, of doordat ze gebeld zijn door iemand die zich voordeed als een helpdesk (bijvoorbeeld van Microsoft).

In de meeste gevallen stond er bij zzp'ers geen deadline vermeld in het losgeldbericht (48,6%) of kregen slachtoffers 1-3 dagen (27,4%) of minder dan 24 uur (16,9%) de tijd om te betalen. Bij een kleine meerderheid van de zzp'ers was er naast de vergrendeling of versleuteling bovendien geen sprake van een aanvullende dreiging (51,4%). Bij een kleiner deel van de respondenten was dit wel het geval, zoals dreigen met het verwijderen van de decryptiesleutel (16,6%) of het lekken van bestanden of gegevens (16,5%). Bij een deel van de respondenten was sprake van een andere dreiging, waaronder dreigen met het wissen of aanbrengen van schade aan bestanden (11,1%) of dreigen met aangifte, vervolging of boete (0,9%).

Ook bij de mkb'ers stond er in de meeste gevallen geen deadline vermeld in het losgeldbericht (51%) of kregen slachtoffers 1-3 dagen de tijd om te betalen (25,2%). In tegenstelling tot de zzp'ers kreeg een groter deel van de mkb'ers tussen 4-6 dagen (8,7%) of meer dan 7 dagen (9,1%) de tijd om te betalen en een kleiner deel minder dan 24 uur (6,1%). Net als bij zzp'ers was er bij een kleine meerderheid van de mkb'ers naast de vergrendeling of versleuteling bovendien geen sprake van een aanvullende dreiging (56,2%). Bij een kleiner deel van de respondenten was dit wel het geval, zoals dreigen met het verwijderen van de decryptiesleutel (18,8%) of het lekken van bestanden of gegevens (13,5%). Bij een deel van de mkb'ers was sprake van een andere dreiging, namelijk dreigen met het wissen of aanbrengen van schade aan bestanden (9%) en dreigen met het verhogen van de losgeldprijs als er pogingen werden gedaan om zelf de data te ontsleutelen (0,5%).

Tabel 6.3 Frequentie van wijze van besmetting, deadline, aard van de dreiging en aangetaste apparaten of systemen en data onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Wijze van besmetting	**88**		**100**	
Geklikt op link of bijlage geopend in een e-mail	39	44,6%	54	54,5%
Geklikt op een link, advertentie of pop-up op internet	12	13,5%	10	10,2%
Bedrijf waar gegevens bekend waren was gehackt	5	5,2%	5	5,2%
Kwetsbaarheid of beveiligingslek in gebruikte software of systeem	7	7,9%	12	12,3%
Kwaadaardige applicatie of software geïnstalleerd	5	6,1%	1	1,4%
Anders, namelijk …				
– Tijdens surfen op internet/bezoek aan een website	1	0,9%	1	0,5%
– Gebeld door zogenaamde helpdesk	-	-	1	0,5%
– Fout van provider	1	0,9%	-	-
Weet ik niet/onbekend	18	20,9%	15	15,6%
Deadline	**88**		**100**	
Minder dan 24 uur	15	16,9%	6	6,1%
1-3 dagen	24	27,4%	25	25,2%
4-6 dagen	4	4,3%	9	8,7%
7 of meer dagen	2	2,8%	9	9,1%
Dat stond niet in het losgeldbericht	43	48,6%	51	51%
Aard dreiging *(meerdere antwoorden mogelijk)*	**88**		**100**	
Er is gedreigd met het verwijderen van de decryptiesleutel/permanente blokkade	15	16,6%	19	18,8%
Er is gedreigd met het lekken van bestanden of gegevens	15	16,5%	13	13,5%
Er is gedreigd met boetes van de Autoriteit Persoonsgegevens	5	5,2%	3	3,2%
Er is gedreigd met het inlichten van concurrenten	1	0,9%	3	3,4%
Er is gedreigd met het inlichten van de pers	2	2,6%	1	0,8%
Er is gedreigd met een DDoS-aanval	1	0,9%	4	4,1%
Er is gedreigd met iets anders, namelijk …				
– Geen toegang tot/schade aan/wissen van bestanden	10	11,1%	9	9%
– Aangifte, vervolging of boete	1	0,9%	1	0,8%
– Openbaar maken van zogenaamde compromitterende beelden	1	0,9%	-	-
– Verhoging van prijs als er pogingen werden gedaan om zelf de data te ontsleutelen	-	-	1	0,5%
– Weet ik niet meer	2	1,8%	3	2,7%
Geen van bovenstaande	45	51,4%	56	56,2%

In veruit de meeste gevallen hadden zzp'ers door de ransomware geen toegang meer tot hun computer (82,9%). Er was daarnaast een kleinere groep respondenten bij wie an-

dere apparaten of systemen waren aangetast, zoals een telefoon, tablet, cloudopslag of NAS. De meest voorkomende bestanden of gegevens die aangetast waren, betroffen financiële gegevens en boekhouding (25,1%), gevolgd door persoonsgegevens (21,8%), data van klanten (21,8%) en productgegevens (19,1%).

Ook bij de mkb'ers had de meerderheid geen toegang meer tot hun computer(s) (80,8%). In tegenstelling tot de zzp'ers, waren daarnaast bij aanzienlijk meer mkb'ers de computerserver(s) (28,7%) en back-ups (11,3%) aangetast. De meest voorkomende bestanden of gegevens die aangetast waren betroffen voor mkb'ers, net als bij zzp'ers, de financiële gegevens en boekhouding (38,1%). In vergelijking met zzp'ers was bij de mkb'ers vaker sprake van aantasting van data van klanten (37,6%), productgegevens (36,6%) en persoonsgegevens (33,1%). Daarnaast heeft 24,9% van de zzp'ers en 10,5% van de mkb'ers gespecificeerd dat alles op hun apparaat of systeem ontoegankelijk was gemaakt (tabel 6.4).

Tabel 6.4 Frequentie van wijze van besmetting, deadline, aard van de dreiging en aangetaste apparaten of systemen en data onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Aangetaste apparaten of systemen *(meerdere antwoorden mogelijk)*	**88**		**100**	
Computer (desktop of laptop)	73	82,9%	80	80,8%
Mobiele telefoon of smartphone	1	0,9%	1	0,8%
Tablet	2	1,8%	2	2,3%
Computerserver(s)	4	5%	29	28,7%
Cloudopslag	1	0,9%	4	4%
Back-up(s)	5	6%	11	11,3%
Anders, namelijk …				
– NAS	1	0,9%	-	-
– Online accounts (bijv. sociale media, e-mail)	5	5,1%	1	0,8%
– Toegang tot browser/website	-	-	1	0,8%
– Software	-	-	-	-
– Er was (nog) niets aangetast, er werd alleen mee gedreigd	2	1,8%	-	-
Aangetaste data *(meerdere antwoorden mogelijk)*	**88**		**100**	
Persoonsgegevens	19	21,8%	33	33,1%
Data van klanten	19	21,8%	37	37,6%
Data van medewerkers	7	7,9%	16	15,9%
Productgegevens	17	19,1%	36	36,6%
Patenten en auteursrecht	1	0,9%	3	3,2%
Financiële gegevens en boekhouding	22	25,1%	38	38,1%
Weet ik niet	9	10,1%	8	7,6%

Tabel 6.4 Verder

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Anders, namelijk …				
– Pdf	1	0,9%	-	-
– Officebestanden (o.a. tekstbestanden)	4	4,3%	7	7,3%
– E-mails	4	5,1%	-	-
– Systeembestanden	1	0,9%	-	-
– Alles (alle bestanden/hele apparaat/besturingssysteem geblokkeerd)	22	24,9%	10	10,5%
– Overige bestanden gerelateerd aan bedrijfsvoering	1	1,7%	2	2,4%
– Er was (nog) niets aangetast, er werd alleen mee gedreigd	1	0,9%	-	-

6.5 Eerste reactie

Respondenten is vervolgens gevraagd wat hun eerste emotie en handeling(en) waren nadat ze waren geconfronteerd met het losgeldbedrag (tabel 6.5). De meest ervaren emoties betroffen bij zowel zzp'ers als mkb'ers boosheid (respectievelijk 68,2% en 63,7%), afkeer (respectievelijk 28,3% en 33,1%) en nervositeit (respectievelijk 15,8% en 28,4%).

Een deel van de zzp'ers heeft zelf geprobeerd om het probleem op te lossen. De meesten daarvan hebben de verbinding met internet verbroken (36,2%), geprobeerd data te herstellen vanaf een back-up (41,1%) of het apparaat teruggezet naar fabrieksinstellingen (21,6%). Een kleiner deel heeft iets anders geprobeerd, zoals een programma gebruiken om de ransomware te verwijderen of de data te ontsleutelen (17,3%), het apparaat opnieuw opstarten (13,8%) of het openen van bestanden door de bestandsextensie te veranderen (5,2%). Van deze respondenten heeft de meerderheid de volledige toegang teruggekregen (70,3%), een kleiner deel heeft gedeeltelijke toegang teruggekregen (18%) en het kleinste deel heeft geen toegang teruggekregen (11,7%). Een ander deel van de respondenten heeft niet zelf geprobeerd om het probleem op te lossen, maar heeft hulp gezocht. De grootste groep zocht hulp van een organisatie, instantie, ICT-deskundige, computerzaak of provider (32,7%), gevolgd door een bekende (23,4%), hulp via internet (14,5%) of hulp binnen het bedrijf (4,2%). Uit de open antwoorden blijkt daarnaast dat een kleine groep respondenten andere technische oplossingen heeft geprobeerd (5,5%), als eerste reactie heeft betaald (5,2%), het apparaat heeft weggedaan en een nieuw apparaat heeft gekocht (3,5%) of niets heeft gedaan (2,6%).

Bij de mkb'ers heeft ook een deel zelf geprobeerd om het probleem op te lossen. Anders dan bij de zzp'ers hebben de meeste respondenten geprobeerd data te herstellen vanaf een back-up (44,7%), gevolgd door het verbreken van de verbinding met internet

(42,7%), of geprobeerd om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen (13,2%). Een kleiner deel heeft iets anders geprobeerd, zoals het apparaat terugzetten naar fabrieksinstellingen (9,8%) of opnieuw opstarten (8,6%). Van deze respondenten heeft iets minder dan de helft de volledige toegang teruggekregen (43,5%), een kleiner deel heeft gedeeltelijke toegang teruggekregen (33,3%) en het kleinste deel heeft geen toegang teruggekregen (23,2%). Een ander deel van de respondenten heeft niet zelf geprobeerd om het probleem op te lossen, maar heeft hulp gezocht. Bijna de helft van de mkb'ers heeft hulp gezocht van een organisatie, instantie, ICT-deskundige, computerzaak of provider (45,5%), gevolgd door een bekende (19,5%), hulp binnen het bedrijf (8,5%) of hulp via internet (2,8%). Uit de open antwoorden blijkt daarnaast dat een kleine groep mkb'ers een nieuw apparaat heeft gekocht (5,5%), niets heeft gedaan (4,9%), het losgeld heeft betaald (4,5%) of andere technische oplossingen heeft geprobeerd (1,3%).

Tabel 6.5 Frequentie van eerste emotie, eerste handeling- en uitkomst onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Eerste emotie *(meerdere antwoorden mogelijk)*	**88**		**100**	
Boosheid	60	68,2%	63	63,7%
Afkeer	25	28,3%	33	33,1%
Angst	8	9,5%	9	9,3%
Nervositeit	14	15,8%	28	28,4%
Verdriet	6	6,9%	5	4,7%
Ontspanning	1	1,7%	4	4,2%
Blijheid	0	0%	1	1%
Anders, namelijk …				
– Geschrokken/ontzet	-	-	1	0,8%
– Lachwekkend	1	0,9%	-	-
– Onverschillig/neutraal	1	0,9%	1	1,4%
– Uitgedaagd	-	-	2	1,6%
– Bezorgd	1	0,9%	-	-
Geen van de bovenstaande opties	5	6%	3	2,9%
Weet ik niet	0	0%	2	2,2%
Eerste handeling *(meerdere antwoorden mogelijk)*				
Verbinding met internet verbroken	32	36,2%	43	42,7%
Apparaat opnieuw opgestart	12	13,8%	9	8,6%
Apparaat teruggezet naar fabrieksinstellingen	19	21,6%	10	9,8%
Hulp of advies gezocht binnen bedrijf	4	4,2%	8	8,5%
Hulp of advies gezocht op internet	14	15,4%	3	2,8%
Hulp of advies gezocht van een bekende	21	23,4%	19	19,5%

Tabel 6.5 Verder

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Hulp of advies gezocht van een organisatie, instantie, ICT-deskundige, computerzaak of provider	29	32,7%	45	45,5%
Bestanden of gegevens geprobeerd te herstellen vanaf een back-up	36	41,1%	45	44,7%
Geprobeerd om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen	15	17,3%	13	13,2%
Geprobeerd bestanden weer te openen door hun extensie terug te veranderen naar het originele formaat	5	5,2%	4	4%
Losgeld betaald	6	6,6%	4	4,5%
Niets gedaan	2	2,6%	5	4,9%
Iets anders gedaan, namelijk …				
– Een nieuw apparaat (computer/schijf) gekocht	3	3,5%	5	5,5%
– Andere technische oplossingen (bijv. formatteren, systeemherstel)	5	5,5%	1	1,3%
Uitkomst zelf geprobeerd op te lossen	**66**		**79**	
Volledige toegang terug	46	70,3%	34	43,5%
Gedeeltelijke toegang terug	12	18%	26	33,3%
Geen toegang terug	8	11,7%	18	23,2%

6.6 Onderhandelen

Soms is het mogelijk om contact op te nemen met de daders. Respondenten is gevraagd of, door wie, hoe en met welk doel er contact is opgenomen (tabel 6.6). De meerderheid van de zzp'ers (93,2%) heeft geen contact opgenomen met de daders. Een kleiner deel heeft een bekende contact laten opnemen (4,4%), zelf contact opgenomen (1,1%) of heeft iemand ingehuurd om contact op te nemen (1,1%). In de meeste gevallen gebeurde dit contact via e-mail (50%), gevolgd door een chatsysteem op een website of portaal van de daders (16,7%) of telefonisch contact (16,7%).

Ook de meerderheid van de mkb'ers (93,8%) heeft geen contact opgenomen met de daders. Een kleiner deel van de mkb'ers heeft iemand ingehuurd om contact op te nemen (3,8%) of zelf contact opgenomen (2,4%). Anders dan bij de zzp'ers, gebeurde dit contact in de meeste gevallen via een chatsysteem op een website of portaal van de daders (38,4%), gevolgd door via e-mail (34,8%) of sociale media (16,7%).

De redenen die zzp'ers noemden om contact op te nemen waren om vast te stellen welke data waren gestolen (33,3%), om hulp te vragen *na* het betalen (33,3%) of zo spoedig mogelijk weer aan het werk te kunnen (33,3%). Een kleiner deel heeft contact

opgenomen om vast te stellen of het losgeldbericht echt was (16,7%) of te informeren over de hoogte van het losgeld (16,7%).

Bij de mkb'ers speelden iets andere beweegredenen een rol. De drie meest genoemde redenen waren om vast te stellen of het losgeldbericht echt was (30,6%), om hulp te vragen *bij* het betalen (29,7%) en om te onderhandelen (26,7%). Terwijl geen enkele zzp'er heeft onderhandeld, hebben twee mkb'ers wel onderhandeld, met als doel om het losgeldbedrag te verlagen of langer de tijd te krijgen. Dit komt neer op 2% van de totale steekproef van mkb'ers. Bij een van de respondenten hebben de onderhandelingen geen verandering opgeleverd, de andere respondent weet niet wat de uitkomst van de onderhandelingen was.

Tabel 6.6 Frequentie van of, door wie en hoe er contact opgenomen is met de daders onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Contact opgenomen met daders	**88**		**100**	
Zelf (of collega heeft) contact opgenomen	1	1,1%	2	2,4%
Bekende heeft contact opgenomen	4	4,4%	0	0%
Ingehuurde partij heeft contact opgenomen	1	1,1%	4	3,8%
Geen contact opgenomen	82	93,2%	93	93,8%
Communicatiemiddel	**6**		**6**	
E-mail	3	50%	2	34,8%
Chatsysteem op een website of portaal	1	16,7%	2	38,4%
Telefonisch	1	16,7%	0	0%
Anders, namelijk …				
– Weet ik niet	1	16,7%	1	16,7%
– Sociale media	-	-	1	16,7%
Doel contact *(meerdere antwoorden mogelijk)*	**6**		**6**	
Om vast te stellen of het losgeldbericht echt was	1	16,7%	2	30,6%
Om te informeren over de hoogte van het losgeld (bijvoorbeeld omdat dit in het losgeldbericht niet vermeld stond)	1	16,7%	0	0%
Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline	0	0%	2	26,7%
Om vast te stellen welke bestanden of gegevens waren gestolen	2	33,3%	0	0%
Om hulp te vragen bij het betalen (bijvoorbeeld bij het aanschaffen van bitcoin)	0	0%	2	29,7%
Om hulp te vragen na het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens)	2	33,3%	2	26,3%
Om tijd te rekken	0	0%	0	0%
Anders, namelijk …			0	0%
– Om zo spoedig mogelijk weer aan het werk te kunnen	2	33,3%	-	-

6.7 Betalen

Iets meer dan een derde van de zzp'ers en mkb'ers heeft aan de hand van een bedrag en valutasoort aangeduid wat de hoogte van het geëiste losgeld was. Hiervan heeft 75% van de zzp'ers een bedrag aangeduid in euro's (in sommige gevallen omgerekend vanuit een andere koers), 9,4% in Amerikaanse dollars en 15,6% in bitcoin.[28] Van de mkb'ers heeft 85,3% een bedrag aangeduid in euro's, 8,8% in Amerikaanse dollars en 5,9% in bitcoin. Het andere deel van de respondenten kon zich de losgeldeis niet herinneren, vermeldde alleen een bedrag (zonder valutasoort) of stelde dat er nog geen concreet bedrag geëist was omdat ze eerst contact moesten opnemen met de daders en dat niet gedaan hebben.

De geëiste losgeldbedragen lopen sterk uiteen. Voor de zzp'ers was de gemiddelde losgeldeis 13.919 euro en 1.628,27 dollar. De mediaan van het geëiste losgeld was 1.148 euro en 400 dollar. Het meest voorkomende losgeldbedrag was 1000 euro en 400 dollar (tabel 6.7). Bij de mkb'ers was de gemiddelde losgeldeis 231.343,44 euro en 2.788,61 dollar, met een mediaan van 10.000 euro en 3.050 dollar. Het meestvoorkomende losgeldbedrag was voor deze groep 10.000 euro en 5.000 dollar (tabel 6.8). Het lijkt erop dat over het algemeen hogere losgeldbedragen geëist worden van midden- en kleinbedrijven in vergelijking met zzp'ers.

Tabel 6.7 Hoogte geëiste losgeld in verschillende valutasoorten onder zzp'ers[29]

	n	**Min.**	**Max.**	**Mediaan**	**Modus**	**Gem.**	**Std. dev.**
€ (euro)	24	500	200.000	1.148,04	1.000	13.919	39.604,10
$ (dollar)	3	400	5.000	400	400	1.628,27	2.488,11
Totaal	32						

Tabel 6.8 Hoogte geëiste losgeld in verschillende valutasoorten onder mkb'ers[30]

	n	**Min.**	**Max.**	**Mediaan**	**Modus**	**Gem.**	**Std. dev.**
€ (euro)	29	250	2.000.000	10.000	10.000	231.343,44	567.109,72
$ (dollar)	3	100	5.000	3.050	5.000	2.788,61	2.703,34
Totaal	34						

28 De hoogte van het losgeld in bitcoin wordt niet vermeld in tabel 6.7 en 6.8 omdat hierbij te veel onbekende factoren zijn. Zo varieerde de bitcoinkoers sterk in de tijd en is de precieze datum van het ransomware-incident onbekend, waardoor geen juiste inschatting gemaakt kan worden van de waarde.

29 In sommige gevallen moest het losgeld in bitcoin betaald worden, maar hebben respondenten aangeduid dat het om x euro of dollar in bitcoin ging.

30 In sommige gevallen moest het losgeld in bitcoin betaald worden, maar hebben respondenten aangeduid dat het om x euro of dollar in bitcoin ging.

De meerderheid (92,4%) van de zzp'ers heeft het geëiste losgeld niet betaald, terwijl een klein deel van de zzp'ers een gedeelte van (1,8%) of het volledige losgeldbedrag (5,8%) heeft betaald. Bij de 3 zzp'ers die het betaalde losgeldbedrag vermeld hebben, ging het om 250 euro, 2.000 euro en 400 dollar. Ook bij de mkb'ers heeft de meerderheid (93,9%) het losgeld niet betaald. Een klein deel van de mkb'ers heeft een deel (0,8%) of het volledige losgeld betaald (5,3%). Bij de 4 mkb'ers die het betaalde losgeldbedrag vermeld hebben, ging het om 1.903, 2.500 en 5.000 euro en 1 bitcoin.

De respondenten zijn vervolgens gevraagd naar de reden(en) waarom ze wel of niet betaald hebben (tabel 6.9). De belangrijkste redenen voor zzp'ers om het losgeld niet te betalen waren dat het onethisch is om criminelen te betalen (37%), dat respondenten niet vertrouwden dat de toegang hersteld zou worden na betaling (26,9%), en dat respondenten niet bang waren dat de daders data zouden lekken of dat er andere gevolgen zouden zijn voor het niet betalen (26,9%). De meest voorkomende redenen voor zzp'ers om wel te betalen waren dat respondenten de aangetaste bestanden, gegevens of apparaten niet wilden verliezen (44,6%), dat ze erop vertrouwden dat de toegang hersteld zou worden na betaling (33%) en dat het losgeldbedrag niet heel hoog was en ze het zich konden veroorloven (32%).

Anders dan bij de zzp'ers was de meest voorkomende reden voor mkb'ers om het losgeld niet te betalen dat ze back-ups hadden (56,5%). Vergelijkbaar met de zzp'ers werd tevens als reden genoemd dat het onethisch is om criminelen te betalen (35,6%), dat respondenten niet vertrouwden dat de toegang hersteld zou worden na betaling (29%) en dat respondenten niet bang waren dat de daders data zouden lekken of dat er andere gevolgen zouden zijn voor het niet betalen (15,9%). De meest voorkomende reden om wel te betalen was net als bij de zzp'ers dat respondenten de aangetaste bestanden, gegevens of apparaten niet wilden verliezen (73,1%). In tegenstelling tot bij de zzp'ers waren daarnaast andere redenen belangrijk, waaronder dat mkb'ers geadviseerd werd door IT- of cybersecurityspecialisten om te betalen (56,7%) en betalen goedkoper was dan geen zaken kunnen doen (43,6%) (tabel 6.9).

Tabel 6.9 Frequentie van reden(en) om (niet) te betalen onder zzp'ers en mkb'ers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Losgeld betaald	**88**		**100**	
Een deel van het losgeld betaald	2	1,8%	1	0,8%
Losgeld volledig betaald	5	5,8%	5	5,3%
Niet betaald	81	92,4%	93	93,9%
Reden(en) om niet te betalen *(meerdere antwoorden mogelijk)*	**81**		**93**	
Losgeldbedrag te hoog	7	9,2%	8	8,6%
Betalen duurder dan geen zaken kunnen doen	2	2,8%	2	2,4%

Tabel 6.9 Verder

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Geadviseerd door politie om niet te betalen	4	5,3%	10	11,2%
Geadviseerd door bekende om niet te betalen	7	8,5%	6	6%
Geadviseerd door IT- of cybersecurityspecialist om niet te betalen	14	16,9%	21	23%
Bedrijf had geen verzekering die kosten van losgeld dekte	5	6,5%	5	5%
Back-up(s) van data	36	44%	53	56,5%
Bestanden, gegevens of apparaten waren niet belangrijk	8	9,6%	9	9,4%
Vertrouwde er niet op dat de toegang hersteld zou worden na betaling	22	26,9%	27	29%
Niet bang voor lekken van data of andere gevolgen bij niet betalen	22	26,9%	15	15,9%
Onethisch om criminelen te betalen	30	37%	33	35,6%
Lukte niet om te betalen	1	0,9%	2	2,5%
Anders, namelijk …				
– Zelf (of met behulp van ander) opgelost	12	13,9%	5	5,3%
– Uit principe/laat me niet chanteren	1	0,9%	6	5,7%
– Wist dat het een valse dreiging was	2	2,6%	-	-
– Impact van aanval was beperkt	-	-	1	0,8%
Geen van de bovenstaande opties	2	2,8%	4	3,8%
Reden(en) om wel te betalen *(meerdere antwoorden mogelijk)*	**7**		**6**	
Losgeldbedrag niet heel hoog	2	32%	2	35,7%
Betalen goedkoper dan geen zaken kunnen doen	0	0%	3	43,6%
Geadviseerd door bekende om te betalen	0	0%	0	0%
Geadviseerd door IT- of cybersecurityspecialist om te betalen	1	12,1%	3	56,7%
Geen back-up(s)s van data	0	0%	1	16,4%
Bedrijf had verzekering die kosten van losgeld dekte	0	0%	0	0%
Wilde bestanden, gegevens of apparaten niet verliezen	3	44,6%	4	73,1%
Vertrouwde erop dat toegang hersteld zou worden na betaling	2	33%	2	26,5%
Bang voor lekken van data of andere gevolgen bij niet betalen	0	0%	1	13,4%
Anders, namelijk …	0	0%	0	0%
Geen van de bovenstaande opties	0	0%	0	0%

Zoals blijkt uit tabel 6.10 is bij de meerderheid van de zzp'ers die betaald heeft de toegang volledig hersteld (85,7%), terwijl bij een kleiner deel de toegang niet hersteld is (14,3%). Tegelijkertijd is het de meerderheid van de zzp'ers die niet betaald heeft ook gelukt om volledig (80,2%) of gedeeltelijk (13,6%) de toegang te herstellen. Slechts in 6,2% van de gevallen is de toegang niet hersteld nadat niet betaald is.

Ook bij de meerderheid van de mkb'ers die betaald heeft, is de toegang volledig hersteld (83,3%), terwijl bij een kleiner deel de toegang gedeeltelijk (16,6%) hersteld is. Bij geen

enkele respondent is de toegang niet hersteld. Tegelijkertijd is het de meerderheid van de mkb'ers die niet betaald heeft ook gelukt om volledig of gedeeltelijk de toegang te herstellen. In slechts 7,5% van de gevallen is de toegang niet hersteld na betaling, wat lager is dan bij de zzp'ers.

Aan respondenten is daarnaast gevraagd of ze het idee hadden dat hun bestanden of gegevens gedeeld zijn met of verkocht zijn aan anderen. De meerderheid van de zzp'ers geeft aan dat dit niet het geval is (71,6%), een kleiner deel geeft aan het niet te weten (24,2%) en de minderheid denkt dat dit wel het geval is (4,2%). Ook de meerderheid van de mkb'ers geeft aan dat dit niet het geval is (68%), terwijl een kleiner deel aangeeft het niet te weten (29,3%). De minderheid van de mkb'ers denkt dat dit wel het geval is (2,7%).

Tabel 6.10 Kruistabel van betalen afgezet tegen of toegang hersteld is onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	Niet betaald	**Betaald**	**Niet betaald**	**Betaald**
Toegang terug				
Volledig	65 (80,2%)	6 (85,7%)	66 (71%)	5 (83,3%)
Gedeeltelijk	11 (13,6%)	0 (0%)	20 (21,5%)	1 (16,6%)
Nee	5 (6,2%)	1 (14,3%)	7 (7,5)	0 (0%)
Totaal	81	7	93	6

6.8 Impact

Respondenten is gevraagd naar de impact van het ransomware-incident (tabel 6.11). De meerderheid van de zzp'ers en mkb'ers ervaarde geen emotionele of psychische gevolgen (respectievelijk 61,2% en 65,6%). Bij de ondernemers die dit wel ervaarden, betroffen de meest voorkomende gevolgen dat respondenten zich minder veilig voelden (zzp: 23,4%; mkb: 16,5%), minder vertrouwen hadden in mensen (zzp: 16,9%; mkb: 17,5%) of minder vertrouwen hadden in de eigen digitale vaardigheden (zzp: 10,4%; mkb: 12,4%). Een kleiner deel ervaarde andere gevolgen zoals, slaapproblemen, depressieve klachten of het opnieuw beleven van het voorval.

De meerderheid van de respondenten gaf daarnaast aan dat ze andere gevolgen hebben ervaren. Voor de zzp'ers betrof dit in de meeste gevallen kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (36%), verhindering in het uitvoeren van de dagelijkse werkzaamheden (29%) en het besteden van tijd aan het oplossen van het incident of inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders (25,4%). Ook voor de mkb'ers betrof dit in de meeste gevallen kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (65,6%), verhindering in het uitvoeren van de dagelijkse werkzaamheden (42,2%) en het besteden van tijd aan

het oplossen van het incident of inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders (32,3%).

Wat betreft de financiële impact gaf 30,4% van de zzp'ers aan geen financiële gevolgen te hebben ervaren en 9,3% het niet te weten. Bij de zzp'ers die wel financiële gevolgen hebben ervaren, was dit in de meeste gevallen minder dan 1.000 euro (40,5%). In geen enkel geval is de financiële schade (inclusief een eventuele losgeldbetaling) vergoed. Een kleiner deel van de mkb'ers gaf aan geen financiële gevolgen te hebben ervaren (15,9%) of gaf aan het niet te weten (10,1%). Bij de mkb'ers die wel financiële gevolgen hebben ervaren, was dit in de meeste gevallen minder dan 1.000 euro (34,7%) of tussen de 1.000 en 5.000 euro (25,5%). In vier gevallen is de financiële schade volledig of gedeeltelijk vergoed door een verzekeringsmaatschappij (tabel 6.11).

Tabel 6.11 Frequentie van emotionele, andere en financiële gevolgen onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Emotionele/psychische gevolgen *(meerdere antwoorden mogelijk)*	**88**		**100**	
Minder veilig voelen	21	23,4%	16	16,5%
Minder vertrouwen in mensen	15	16,9%	17	17,5%
Het voorval telkens opnieuw beleven	1	0,9%	1	1,3%
Slaapproblemen.	2	2,6%	1	1,3%
Angstklachten en/of paniekaanvallen	0	0%	1	1,4%
Depressieve klachten	2	2,5%	0	0%
Minder vertrouwen in eigen digitale vaardigheden	9	10,4%	12	12,4%
Anders, namelijk …				
– Gespannen/stress	-	-	1	1,3%
Geen van de bovenstaande opties	54	61,2%	65	65,6%
Weet ik niet	0	0%	1	0,8%
Andere gevolgen *(meerdere antwoorden mogelijk)*	**88**		**100**	
Verhinderd in uitvoeren van dagelijkse werkzaamheden	26	29%	42	42,4%
Verlies van inkomsten, waarde van aandelen of inkomen	5	5,9%	10	9,7%
Tijd besteed aan het oplossen van het incident of inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders	22	25,4%	32	32,3%
Kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	32	36%	56	56,6%
Bestanden of gegevens verloren	19	21,3%	24	24,5%
Boetes van regelgevers of wetgevers	0	0%	0	0%
Reputatieschade	0	0%	1	1,3%
Onderbreking van levering van goederen of diensten aan klanten, begunstigden, of gebruikers	7	7,6%	12	12,4%

Tabel 6.11 Verder

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders	1	0,9%	1	0,5%
Schadevergoeding, compensatie of korting verleend aan klanten	0	0%	0	0%
Anders, namelijk …				
– Cruciale zaken worden alleen nog op papier gedaan	1	0,9%	-	-
– Alerter/voorzichtiger geworden online	3	3,5%	1	1,4%
Geen van bovenstaande opties	27	30,4%	24	24,2%
Financiële gevolgen (m.u.v. betalen losgeld)	**88**		**100**	
Geen	27	30,4%	16	15,9%
Minder dan €1.000	36	40,5%	35	34,7%
€1.000 tot €5.000	8	8,8%	25	25,5%
€5.000 tot €10.000	7	7,6%	5	4,7%
€10.000 tot €50.000	2	2.6%	7	6,8%
€50.000 tot €100.000	1	0,9%	0	0%
€100.000 tot €250.000	0	0%	2	2,2%
Weet ik niet	8	9,3%	10	10,1%
Financiële schade vergoed (incl. betaalde losgeld)	**49**		**72**	
Volledig vergoed	0	0%	1	1,4%
Gedeeltelijk vergoed	0	0%	3	4,2%
Niet vergoed	49	100%	68	94,4%
Aangevraagd en nog geen beslissing ontvangen	0	0%	0	0%
Instantie die financiële schade heeft vergoed/mogelijk gaat vergoed			**4**	
Bank of financiële instelling	-	-	0	0%
Verzekeringsmaatschappij	-	-	4	100%
Andere instantie	-	-	0	0%

Daarnaast is aan respondenten gevraagd of het incident gevolgen heeft gehad voor het online gedrag of de beveiligingsmaatregelen, wat bij een groot deel van de respondenten het geval was (tabel 6.12). De grootste groep zzp'ers maakt (vaker) externe back-ups van bestanden en gegevens (49,3%), voert updates direct uit zodra deze beschikbaar zijn (28,9%) en laat beveiligingssoftware apparaten scannen op virussen of andere kwaadaardige software (24,4%). De grootste groep mkb'ers maakt (vaker) externe back-ups van bestanden en gegevens (51,2%), laat beveiligingssoftware apparaten scannen op virussen of andere kwaadaardige software (37,1%) en heeft een wachtwoordbeleid ingevoerd dat zorgt voor sterke wachtwoorden (23,3%).

Tabel 6.12 Frequentie van genomen beveiligingsmaatregelen na slachtofferschap onder ondernemers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**88**		**100**	
Ander besturingssysteem genomen	2	2,8%	7	6,8%
(Vaker) back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	43	49,3%	51	51,2%
Wachtwoordbeleid dat zorgt voor sterke wachtwoorden	18	20,5%	23	23,3%
(Ander) antivirusproduct aangeschaft	20	22,6%	19	19%
Firewall aangeschaft	17	19%	22	22,4%
Beveiligingssoftware netwerken en apparaten laten scannen op virussen of andere kwaadaardige software	21	24,4%	37	37,1%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	25	28,9%	17	17,3%
Monitoren van gebruikers- of netwerkactiviteiten	1	0,9%	6	6,3%
IT-administratie en toegangsrechten beperkt tot specifieke gebruikers	4	4,5%	6	5,8%
IT-administratie en toegangsrechten bijhouden	2	2,7%	9	9%
Specifieke regels opgesteld voor veilig opslaan van bestanden met persoonsgegevens	6	6,9%	6	6,5%
Andere standaardbrowser genomen	13	14,6%	4	4,2%
Gevoelige bestanden en gegevens versleuteld	5	6,1%	11	10,6%
Veiligheidsrestricties op apparaten die eigendom zijn van het bedrijf	4	4,4%	5	4,5%
Toegang tot bedrijfsnetwerk alleen toegestaan op apparaten van het bedrijf	6	7%	9	9,4%
Gescheiden wifi-netwerken voor personeel en gasten	3	3,5%	10	9,7%
Tweestapsverificatie	19	22,1%	15	14,7%
(Ander) iemand (intern of extern) in dienst die verantwoordelijk is voor cybersecurity	11	12,8%	10	10,3%
Bedrijfscontinuïteitsplan opgesteld	2	2,4%	1	0,8%
Anders, namelijk …				
– Nieuwe computer, los van internet, aangeschaft	1	0,9%	-	-
– Overgestapt op online cloudoplossing	1	0,9%	3	3%
– Meer cybersecurity awareness, o.a. m.b.t. phishing-e-mails	5	5,1%	4	3,9%
– Betere isolatie tussen servers	-	-	1	0,8%
– Gestopt met digitale administratie	1	0,9%	-	-
Geen van bovenstaande	11	12,7%	12	12,4%

6.9 Melden

Vervolgens is onderzocht in hoeverre ondernemers naar aanleiding van het ransomware-incident contact hebben gezocht met een aantal organisaties. Zzp'ers hebben het vaakst contact opgenomen met een cybersecuritybedrijf of IT-leverancier (45,6%), de Fraudehelpdesk (16,5%) of de politie (12,3%) voor advies, ondersteuning of om melding van het incident te maken (tabel 6.13). Gemiddeld genomen zijn respondenten over deze organisaties (op een schaal van 1 'zeer ontevreden' tot 5 'zeer tevreden') neutraal tot tevreden, met uitzondering van cybersecuritybedrijven of IT-leveranciers, waar slachtoffers tevreden tot zeer tevreden over zijn. Daarnaast zijn respondenten ontevreden tot neutraal over hun verzekeringsmaatschappij en No More Ransom, hoewel het om een lage respons gaat.

Tabel 6.13 Frequentie van contact met verschillende instanties en tevredenheid over deze instanties onder zzp'ers (*meerdere antwoorden mogelijk*) (n=88)

		Contact met		Tevredenheid
Instantie	**N**	**%**	**Gem.**	**Std. dev.**
Politie	11	12,3%	3,36	1,104
Bank of financiële instelling	4	4,5%	3,62	0,933
Verzekeringsmaatschappij	2	1,8%	2,52	0,836
Cybersecuritybedrijf/IT-leverancier/computerzaak	40	45,6%	4,41	1,036
Autoriteit Persoonsgegevens	4	4,4%	3,78	1,359
No More Ransom	5	5,2%	2,87	1,226
Slachtofferhulp	1	0,9%	-	-
Fraudehelpdesk	14	16,5%	3,85	1,017
Een andere organisatie, namelijk …				
– Accountant	1	0,9%	-	-
– Belastingdienst	1	0,9%	-	-
– Provider	1	0,9%	-	-

De meerderheid van de mkb'ers heeft contact opgenomen met een cybersecuritybedrijf of IT-leverancier (69,5%), meer dan bij de zzp'ers het geval was. De mkb'ers namen daarnaast het vaakst contact op met de politie (26,7%) en de Fraudehelpdesk (14,5%) (tabel 6.14). Gemiddeld genomen zijn respondenten over deze organisaties neutraal tot tevreden, met uitzondering van cybersecuritybedrijven of IT-leveranciers, waar mkb'ers tevreden tot zeer tevreden over zijn.

Tabel 6.14 Frequentie van contact met verschillende instanties en tevredenheid over deze instanties onder mkb'ers (*meerdere antwoorden mogelijk*) (n=100)

		Contact met		Tevredenheid
Instantie	**N**	**%**	**Gem.**	**Std. dev.**
Politie	27	26,7%	3,21	1,248
Bank of financiële instelling	14	14,3%	3,89	1,017
Verzekeringsmaatschappij	12	12%	3,13	1,046
Cybersecuritybedrijf/IT-leverancier/ computerzaak	69	69,5%	4,47	0,939
Autoriteit Persoonsgegevens	4	4,3%	3,37	0,552
No More Ransom	1	1%	-	-
Slachtofferhulp	0	0%	-	-
Fraudehelpdesk	14	14,5%	3,06	0,770
Een andere organisatie, namelijk …				
– Kamer van Koophandel	1	0,5%	-	-
– Juridisch specialist	1	0,5%	-	-

Iets meer dan de helft van de zzp'ers heeft contact opgenomen met de politie om aangifte te doen (56,8%), een kleiner deel om het incident te melden (43,2%) en hulp en/of informatie te krijgen (43,2%). Van de respondenten die contact met de politie hebben gezocht om melding en/of aangifte te doen, heeft 7,5% daadwerkelijk aangifte gedaan waarbij een proces-verbaal is ondertekend (tabel 6.15). Dit komt neer op een aangiftepercentage van 1,1% onder de 88 zzp'ers die slachtoffer zijn geworden.

Aanzienlijk meer mkb'ers hebben in vergelijking met de zzp'ers contact opgenomen met de politie om aangifte te doen (74,2%). Een kleiner deel nam contact op voor hulp en/of informatie (28,7%) en om het incident te melden (19,8%). Van de mkb'ers die contact met de politie hebben gezocht om melding en/of aangifte te doen, heeft 40,4% daadwerkelijk aangifte gedaan waarbij een proces-verbaal is ondertekend (tabel 6.15). Dit komt neer op een aangiftepercentage van 10% onder de 100 mkb'ers die slachtoffer zijn geworden.

Tabel 6.15 Frequentie van doel waarmee contact is opgenomen met de politie en aangiftepercentage na contact onder ondernemers

	zzp		mkb	
	n	**%**	**n**	**%**
Doel contact politie *(meerdere antwoorden mogelijk)*	**11**		**27**	
Voor hulp en/of informatie	5	43,2%	8	28,7%
Om aangifte te doen	6	56,8%	20	74,2%
Om het incident te melden	5	43,2%	5	19,8%
Aangifte gedaan (indien doel contact politie = melden of aangifte)	**11**		**25**	
Nee	10	92,5%	15	59,6%
Ja	1	7,5%	10	40,4%

De belangrijkste redenen voor zzp'ers om het ransomware-incident niet te melden en/of geen aangifte te doen bij de politie (tabel 6.16) waren dat respondenten het zelf of met behulp van een andere partij hebben opgelost (55,7%), het geen zin heeft om melding of aangifte te doen aangezien de politie er toch niets aan doet (18,7%) en dat het incident niet zo belangrijk is (6,7%). De meest voorkomende redenen voor zzp'ers om wel te melden en/of aangifte te doen waren om te voorkomen dat dit bij een ander gebeurt (34,9%), dat het hun plicht is (21,9%) en dat respondenten wilden dat de dader gepakt wordt (14,9%).

De belangrijkste redenen voor mkb'ers om het incident niet te melden en/of geen aangifte te doen bij de politie waren dat respondenten het zelf of met behulp van een andere partij hebben opgelost (49,3%), het geen zin heeft om melding of aangifte te doen aangezien de politie er toch niets aan doet (23,8%) en dat het te veel tijd/moeite kost (3,5%). De meest voorkomende redenen voor mkb'ers om wel te melden en/of aangifte te doen waren dat respondenten wilden dat de dader gepakt wordt (22,4%), om te voorkomen dat dit bij een ander gebeurt (16,2%) en dat het hun plicht is (15,7%).

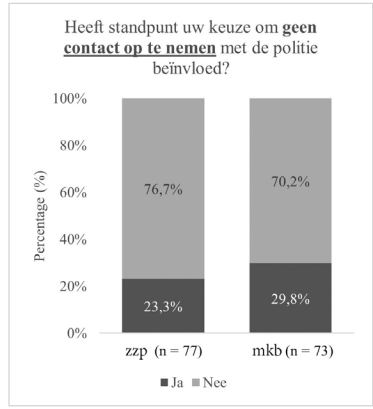
Tabel 6.16 Frequentie van belangrijkste reden om (niet) te melden en/of aangifte te doen bij de politie onder zzp'ers en mkb'ers

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Belangrijkste reden om niet te melden	**75**		**75**	
Mijn bedrijf heeft het zelf of met behulp van een andere partij opgelost	41	55,7%	37	49,3%
Het is niet zo belangrijk	0	0%	2	3,1%
Het kost te veel tijd/moeite	5	6,7%	3	3,5%
Het heeft geen zin, de politie zal er toch niets aan doen	14	18,7%	18	23,8%
De politie heeft niet de kennis om dit type delict aan te pakken	3	4%	2	2,5%
Het is eerder een zaak voor een andere instantie dan de politie	0	0%	1	1,7%
Weinig vertrouwen in de politie	4	5,3%	1	0,7%
Bang dat de dader wraak zal nemen	0	0%	1	1,1%
De politie wilde de melding/aangifte niet opnemen	1	1,3%	2	3%
Ik schaam me dat mijn bedrijf slachtoffer is geworden	2	2,7%	1	1,8%
Ik schaam me dat mijn bedrijf het losgeld betaald heeft	0	0%	0	0%
Ik vind dat het eigenlijk mijn/onze eigen schuld is	4	5,3%	2	2,4%
Het lukt niet om digitaal aangifte/melding te doen	0	0%	0	0%
Bang voor reputatieschade	0	0%	1	1,1%
Anders, namelijk …				
– Niet aan gedacht	1	1,3%	2	2,7%
– Geen/beperkte schade of een lage impact	-	-	2	2,7%

Tabel 6.16 Verder

	zzp (n=88)		**mkb** (n=100)	
	n	**%**	**n**	**%**
Belangrijkste reden om wel te melden	**11**		**25**	
Om te voorkomen dat dit opnieuw bij mijn bedrijf gebeurt	1	7,5%	0	0%
Om te voorkomen dat dit bij een ander gebeurt	4	34,9%	4	16,2%
Ik wil dat de dader gepakt wordt	2	14,9%	6	22,4%
Om een veiligere (online) wereld te creëren	1	13,9%	4	14,9%
Het is de plicht van mijn bedrijf	2	21,9%	4	15,7%
Om de schade vergoed te krijgen	0	0%	3	12,9%
Anders, namelijk …				
– Ik wist niet wat ik moest doen	1	6,9%	-	-
– Indekken van risico's	-	-	2	2,2%
– Voor het geval er persoonsgegevens gestolen zouden zijn	-	-	2	2,2%

Naast bovenstaande redenen, is ook aandacht besteed aan het feit dat de politie adviseert om het losgeld niet te betalen. Respondenten is gevraagd in hoeverre zij het eens zijn (op een schaal van 1 'helemaal mee oneens' tot 5 'helemaal mee eens') met de stelling 'De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?' Zowel zzp'ers (M = 4,57, SD = 0,844) als mkb'ers (M = 4,57, SD = 0,946) zijn het gemiddeld (helemaal) eens. Slachtoffers is vervolgens gevraagd of dit standpunt hun beslissing om contact op te nemen met de politie voor advies, ondersteuning of om melding van het incident te maken heeft beïnvloed. Zoals te zien is in figuur 6.2 heeft bij 23,3% van de zzp'ers en 29,8% van de mkb'ers die *geen* contact hebben opgenomen met de politie, het standpunt van de politie hieraan bijgedragen.[31]



Figuur 6.2 Invloed van standpunt politie om niet te betalen op keuze om geen contact op te nemen met de politie

31 In tegenstelling tot bij de burgers heeft een fout in de routing ertoe geleid dat de ondernemers niet gevraagd is of het standpunt van de politie invloed heeft gehad op hun keuze om geen melding en/of aangifte te doen.

6.10 Resumé

In dit hoofdstuk is stilgestaan bij de prevalentie, aard en impact van slachtofferschap van ransomware onder Nederlandse zzp'ers en mkb'ers. Uit de resultaten blijkt dat 4,6% van de zzp'ers en 11,5% van de mkb'ers ooit en respectievelijk 0,3% en 0,9% in het afgelopen jaar slachtoffer is geworden van ransomware, waarvan de meerderheid eenmalig slachtoffer is geworden. Bij de meeste slachtoffers vond het incident meer dan 5 jaar geleden plaats.

Als het gaat om de aard van het delict was er in de meeste gevallen bij zowel zzp'ers als mkb'ers sprake van lockerware (vergrendeling van (onderdelen van) het systeem) of cryptoware (versleuteling). Bij de meeste respondenten betrof dit aantasting van de computer, en aantasting van financiële gegevens of boekhouding. De meeste zzp'ers en mkb'ers denken dat de ransomware op hun apparaat of systeem is gekomen door het klikken op een link of bijlage in een e-mail. Bij een kleine meerderheid van de respondenten was naast de vergrendeling of versleuteling geen sprake van een aanvullende dreiging. Bij de respondenten bij wie dit wel het geval was, ging het met name om het dreigen met het verwijderen van de decryptiesleutel of het lekken van bestanden of gegevens. Wanneer er een deadline in het losgeldbericht stond vermeld, kregen zzp'ers meestal minder dan 24 uur of tussen de 1 en 3 dagen de tijd om te betalen, terwijl de meeste mkb'ers tussen de 1 en 3 dagen of tussen de 4 en 6 dagen de tijd kregen om te betalen.

Als het gaat om de eerste emotie en reactie van slachtoffers, was bij zowel zzp'ers als mkb'ers de meest voorkomende emotie boosheid. Een deel van de respondenten heeft zelf geprobeerd om het probleem op te lossen. De meeste zzp'ers deden dit door de verbinding met internet te verbreken, de meeste mkb'ers door data proberen te herstellen vanaf een back-up. Bij de meerderheid van de respondenten die het zelf heeft gepoogd op te lossen, is het gelukt om de toegang tot het apparaat of systeem te herstellen. Een ander deel van de respondenten heeft niet zelf geprobeerd om het probleem op te lossen, maar heeft hulp gezocht. In de meeste gevallen betrof dit bij beide groepen hulp van een organisatie, instantie, ICT-deskundige, computerzaak of provider.

Slechts 6,6% van de zzp'ers en 6,2% van de mkb'ers heeft zelf contact opgenomen of iemand anders contact laten opnemen met de daders, voornamelijk via e-mail (zzp'ers) of een chatsysteem op een website of portaal (mkb'ers). De zzp'ers namen in de meeste gevallen contact op om vast te stellen welke data waren gestolen, om hulp te vragen na het betalen of om zo spoedig mogelijk weer aan het werk te kunnen. De meeste mkb'ers namen contact op om vast te stellen of het losgeldbericht echt was, om hulp te vragen bij het betalen of om te onderhandelen. Terwijl geen enkele zzp'er heeft onderhandeld, hebben enkele mkb'ers onderhandeld om het losgeldbedrag te verlagen of langer de tijd te krijgen. Dit komt neer op 2% van de totale steekproef. Bij een van de respondenten

heeft dit geen verandering opgeleverd, de andere respondent weet niet wat de uitkomst van de onderhandelingen was.

Ook is onderzocht in hoeverre en met welke overwegingen ondernemers het losgeld betalen. Bij de zzp'ers werd gemiddeld 13.919 euro aan losgeld gevraagd, met een mediaan van 1.149 euro. Bij de mkb'ers was het gemiddeld geëiste losgeld hoger met 231.343 euro en een mediaan van 10.000 euro. Van de zzp'ers heeft ongeveer 92% het geëiste losgeld niet betaald, met als voornaamste reden dat respondenten het onethisch vonden om criminelen te betalen. De meeste zzp'ers die wel betaald hebben, gaven als reden dat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen. De gemiddelde betaling was 1.250 euro. Van de mkb'ers heeft ongeveer 94% het geëiste losgeld niet betaald, met als voornaamste reden dat ze een back-up hadden. De meeste mkb'ers die wel betaald hebben, gaven net als de zzp'ers als reden dat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen. De gemiddelde betaling was 3.134 euro. Bij de meerderheid van de zzp'ers en mkb'ers is de toegang gedeeltelijk of volledig hersteld, ongeacht of ze het losgeld betaald hebben. De meeste respondenten hadden bovendien niet het idee dat hun data gelekt of verkocht zijn.

Als het gaat om de impact, ervaarde ongeveer 40% van de zzp'ers en 35% van de mkb'ers emotionele of psychische gevolgen, met name een minder veilig gevoel en minder vertrouwen in andere mensen. De meerderheid van de respondenten gaf daarnaast aan andere gevolgen te hebben ervaren. Voor zowel de zzp'ers als mkb'ers betrof dit met name kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk, of verhindering in de uitvoering van dagelijkse werkzaamheden. Ongeveer 60% van de zzp'ers en 74% van de mkb'ers heeft financiële gevolgen ervaren (buiten het eventuele losgeld), waarbij dit in de meeste gevallen minder dan 1.000 euro was. Bij geen enkele zzp'er en slechts 5,6% van de mkb'ers is de financiële schade (gedeeltelijk) vergoed, door een verzekeringsmaatschappij. Voor een groot deel van de respondenten heeft het ransomware-incident tevens geleid tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In de meeste gevallen zijn zzp'ers en mkb'ers (vaker) externe back-ups van bestanden en gegevens gaan maken.

Tot slot is aan respondenten gevraagd met welke organisaties ze contact hebben opgenomen voor advies, ondersteuning of om melding van het incident te maken. De meeste zzp'ers namen contact op met een cybersecuritybedrijf of IT-leverancier (45,6%), gevolgd door de Fraudehelpdesk (16,5%) en de politie (12,3%). In verhouding nam een groter deel mkb'ers contact op met een cybersecuritybedrijf of IT-leverancier (69,5%) of de politie (26,7%), en minder met de Fraudehelpdesk (14,5%). Van alle respondenten heeft 1,1% van de zzp'ers en 10% van de mkb'ers een daadwerkelijke aangifte gedaan bij de politie waarbij een proces-verbaal is ondertekend. De meest voorkomende reden om het incident niet te melden bij de politie was voor beide groepen dat respondenten het zelf of met behulp van een andere partij hebben opgelost. De meest voorkomende reden voor zzp'ers om wel te melden was dat respondenten wilden voor-

komen dat het bij een ander gebeurt, terwijl dit bij mkb'ers was omdat respondenten wilden dat de dader gepakt wordt. Hoewel respondenten het eens zijn met het algemene advies van de politie om het losgeld niet te betalen, heeft ditzelfde standpunt er bij ongeveer 23% van de zzp'ers en 30% van de mkb'ers toe geleid dat ze geen contact hebben opgenomen met de politie.

7 Factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap van ransomware onder ondernemers

In dit hoofdstuk worden de resultaten beschreven van het onderzoek onder ondernemers naar de factoren die bijdragen aan de betalings- en meldingsbereidheid na hypothetisch slachtofferschap (deelstudie 2B).[32] Ondernemers werd gevraagd om zich de hypothetische situatie voor te stellen waarin hun bedrijf getroffen was door ransomware en de respondent een beslissing moet nemen over het wel of niet betalen van losgeld en het melden van het incident, aan de hand van een vignet (zie paragraaf 3.1.2.2). In paragraaf 7.8 worden de resultaten van deelstudie 1B en 2B vergeleken.

7.1 Achtergrondkenmerken

Aan de respondenten is allereerst gevraagd hoeveel tijd ze doorgaans online spenderen voor hun bedrijf, en welke online mogelijkheden, verzekering en beveiligingsmaatregelen hun bedrijf heeft (tabel 7.1). De meeste zzp'ers zijn dagelijks (28,5%) of (bijna) continu online (22,5%). Het grootste deel heeft accounts of pagina's op sociale media (50,3%), heeft een online bankrekening (42,8%) of heeft financiële of boekhoudsoftware (41,1%). Een groot deel van de zzp'ers is niet verzekerd tegen cybersecurity-incidenten (80%). Back-ups op een externe harde schijf, clouddienst of server (82,1%), het hebben van een up-to-date virusproduct (70,4%) en het direct uitvoeren van updates zodra deze beschikbaar zijn (63,8%), waren de meest voorkomende beveiligingsmaatregelen onder zzp'ers.

De meeste mkb'ers zijn meerdere keren per dag (28%) of (bijna) continu (27,7%) online. Het grootste deel heeft financiële of boekhoudsoftware (69,5%), accounts of pagina's op sociale media (67,6%), en slaat elektronisch bedrijfsgegevens of persoonlijke gegevens op (53,6%). In vergelijking met de zzp'ers heeft een iets groter deel van de mkb'ers een cybersecurityverzekering, maar ook is 64,7% van de mkb'ers niet verzekerd tegen cybersecurity-incidenten. Back-ups op een externe harde schijf, clouddienst of

32 De frequenties en percentages in tabellen tellen niet altijd op tot de totalen als gevolg van het afronden van getallen in verband met het wegen van de data. Daarnaast tellen sommige percentages niet op tot de totalen omdat respondenten meerdere antwoorden konden selecteren. Dit laatste is aangeduid in de tabellen.

server (88,3%), het hebben van een up-to-date virusproduct (78%) en het direct uitvoeren van updates zodra deze beschikbaar zijn (72,6%), zijn, net als bij zzp'ers, de meest voorkomende beveiligingsmaatregelen onder mkb'ers.

Daarnaast is aan respondenten gevraagd of ze (eind)verantwoordelijk waren voor de cybersecurity binnen hun bedrijf. Bij 88,5% van de zzp'ers en 78,1% van de mkb'ers was dit het geval.

Tabel 7.1 Frequentie van tijd online, online mogelijkheden, verzekering en beveiligingsmaatregelen onder zzp'ers en mkb'ers

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Tijd online voor bedrijf	**1.769**		**732**	
Minder dan 1 keer per maand	60	3,4%	6	0,8%
Minimaal 1 keer per maand, maar niet wekelijks	63	3,6%	3	0,4%
Minimaal 1 keer per week, maar niet dagelijks	224	12,7%	29	3,9%
Dagelijks	504	28,5%	195	26,7%
Meerdere keren per dag	353	20%	205	28%
Minstens ieder uur	165	9,3%	91	12,4%
Ik ben (bijna) continu online	399	22,5%	202	27,7%
Online mogelijkheden bedrijf *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Accounts of pagina's op sociale media	889	50,3%	495	67,6%
De mogelijkheid voor klanten om online te bestellen, te reserveren, te betalen voor producten of diensten, of een schenking te doen	333	18,8%	239	32,6%
De mogelijkheid voor klanten om online toegang te krijgen tot (enkele) diensten	230	13%	152	20,7%
Een online bankrekening waarnaar klanten betalingen kunnen overmaken	756	42,8%	312	42,6%
Een industrieel controlesysteem	17	1%	16	2,2%
Een Enterprise Resource Planning (ERP)-systeem	56	3,2%	90	12,3%
Financiële of boekhoudsoftware	727	41,1%	509	69,5%
Het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs	636	36%	393	53,6%
Anders	103	5,8%	23	3,2%
Geen van de bovenstaande opties	272	15,4%	39	5,4%
Verzekering	**1.769**		**732**	
Specifieke verzekering voor cybersecurity	54	3%	45	6,2%
Cybersecurityverzekering onderdeel van bredere verzekeringspolis	106	6%	96	13,1%
Niet verzekerd tegen cybersecurity-incidenten	1.415	80%	474	64,7%
Weet ik niet	194	10,9%	117	16%

Tabel 7.1 Verder

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	1.452	82,1%	647	88,4%
Wachtwoordbeleid dat zorgt voor sterke wachtwoorden	858	48,5%	413	56,4%
Up-to-date antivirusproduct	1.246	70,4%	571	78%
Firewall die zowel volledige IT-netwerk als individuele apparaten beschermt	848	47,9%	455	62,1%
Beveiligingssoftware die netwerken en apparaten scant op virussen of andere kwaadaardige software	855	48,3%	438	59,9%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	1.129	63,8%	532	72,6%
Monitoren van gebruikers- of netwerkactiviteiten	138	7,8%	130	17,7%
IT-administratie en toegangsrechten beperkt tot specifieke gebruikers	505	28,5%	392	53,5%
IT-administratie en toegangsrechten bijhouden	304	17,2%	272	37,2%
Specifieke regels voor veilig opslaan van bestanden met persoonsgegevens	229	12,9%	194	26,5%
Gevoelige bestanden en gegevens versleuteld	280	15,8%	156	21,4%
Veiligheidsrestricties op apparaten die eigendom zijn van het bedrijf	108	6,1%	141	19,2%
Toegang tot bedrijfsnetwerk alleen toegestaan op apparaten van het bedrijf	244	13,8%	191	26,1%
Gescheiden wifi-netwerken voor personeel en gasten	268	15,2%	300	41%
Tweestapsverificatie	677	38,3%	338	46,1%
Iemand (intern of extern) in dienst die verantwoordelijk is voor cybersecurity	90	5,1%	165	22,5%
Bedrijfscontinuïteitsplan opgesteld	37	2,1%	40	5,5%
Anders	11	0,6%	2	0,3%
Geen van bovenstaande	87	4,9%	24	3,3%

7.2 Eerste reactie

Respondenten is na vertoning van het vignet allereerst gevraagd wat hun eerste emotie en handeling(en) zouden zijn nadat ze geconfronteerd zouden zijn met het losgeldbericht (tabel 7.2). De meest ervaren emoties zouden bij zowel zzp'ers als mkb'ers boosheid (respectievelijk 78% en 76,9%), nervositeit (respectievelijk 44,5% en 40,4%) en afkeer (respectievelijk 37,8% en 37%) zijn. Een klein deel van de respondenten heeft daarnaast in de open antwoorden aangegeven dat ze zich dom of stom zouden voelen, kwaad zouden zijn op zichzelf of zich zouden schamen of geïrriteerd zouden zijn.

Een deel van de zzp'ers en mkb'ers zou zelf proberen om het probleem op te lossen (tabel 7.2). De meeste zzp'ers zouden de verbinding met internet verbreken (42,4%),

proberen data te herstellen vanaf een back-up (38,1%) of proberen om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen (19,9%). De meeste mkb'ers zouden tevens de verbinding met internet verbreken (41,8%) of proberen data te herstellen vanaf een back-up (33,8%), of zouden het apparaat opnieuw opstarten (15,2%). Een deel van de ondernemers zou (ook) hulp zoeken. De meerderheid van de zzp'ers en mkb'ers zou hulp zoeken van een organisatie, instantie, IT-leverancier, systeembeheerder, automatiseringsbedrijf of deskundige (respectievelijk 64,4% en 75,3%) (waaronder ook de politie), gevolgd door een bekende of collega (respectievelijk 32,5% en 29,3%) en hulp via internet (respectievelijk 24,8% en 16,9%).

Tabel 7.2 Frequentie van eerste emotie, eerste handeling- en uitkomst onder ondernemers

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Eerste emotie *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Boosheid	1.379	78%	563	76,9%
Afkeer	668	37,8%	271	37%
Angst	418	23,6%	129	17,6%
Nervositeit	787	44,5%	296	40,4%
Verdriet	305	17,3%	91	12,4%
Ontspanning	40	2,3%	17	2,3%
Blijheid	2	0,1%	0	0%
Anders, namelijk …				
– Verrast/verbaasd/ongeloof	2	0,1%	1	0,1%
– Dom/stom voelen/kwaad op zelf/schaamte	7	0,4%	3	0,4%
– Machteloos/hulpeloos	7	0,4%	2	0,3%
– Geschrokken/ontzet	2	0,1%	1	0,2%
– Geïrriteerd/gefrustreerd/verontwaardigd	11	0,7%	12	1,7%
– Lachwekkend	5	0,3%	-	-
– Onverschillig/neutraal/gelaten	10	0,6%	1	0,1%
– Bezorgd	1	0,05%	2	0,2%
– Gespannen/gestrest	2	0,1%	1	0,1%
– Vermoeid	2	0,1%	-	-
– Agressief/moordneigingen	2	0,1%	3	0,4%
– Teleurstelling	5	0,3%	-	-
Geen van de bovenstaande opties	61	3,4%	32	4,4%

Tabel 7.2 Verder

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Eerste handeling *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Verbinding met internet of stroom verbreken	750	42,4%	306	41,8%
Apparaat opnieuw opstarten	282	16%	111	15,2%
Apparaat terugzetten naar fabrieksinstellingen	305	17,2%	103	14%
Hulp of advies zoeken op internet	439	24,8%	124	16,9%
Hulp of advies zoeken van een bekende/collega	575	32,5%	214	29,3%
Hulp of advies zoeken van een organisatie, instantie, IT-leverancier, systeembeheerder, automatiseringsbedrijf, deskundige	1142	64,6%	551	75,3%
Proberen bestanden of gegevens te herstellen vanaf een back-up	673	38,1%	248	33,8%
Proberen om een programma of code te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen	352	19,9%	101	13,7%
Proberen om bestanden weer te openen door hun extensie terug te veranderen naar het originele formaat	94	5,3%	23	3,1%
Ik zou niks doen	52	3%	15	2%
Ik zou iets anders doen, namelijk …				
– Een nieuw apparaat (hardware/software) gekocht	10	0,6%	2	0,3%
– Andere technische oplossingen (bijv. 2e onafhankelijke systeem opstarten, systeem ontkoppelen, formatteren, reset)	5	0,3%	4	0,5%
– Nieuwe omgeving opbouwen/opnieuw beginnen	5	0,3%	1	0,1%
– Risicoanalyse uitvoeren	3	0,2%	-	-
– Contact met hoofdkantoor/partners	1	0,1%	2	0,3%
– Onderzoeken of dreiging legitiem is	3	0,2%	-	-
– Hardware vernietigen	1	0,1%	-	-
– Bericht verwijderen	3	0,2%	-	-
– Klanten informeren	1	0,1%	-	-
– Weet ik niet	1	0,1%	1	0,1%

7.3 Onderhandelen

Respondenten is daarnaast gevraagd of, door wie, en met welk doel ze contact zouden opnemen met de daders (tabel 7.3). De meerderheid van de zzp'ers (87,6%) en mkb'ers (82,6%) zou geen contact opnemen met de daders. Een kleiner deel zou iemand inhuren om contact op te nemen (respectievelijk 7% en 11,8%), zou zelf contact opnemen (respectievelijk 3,8% en 4,1%) of zou een bekende contact laten opnemen (respectievelijk 1,6% en 1,5%).

De voornaamste redenen die zzp'ers noemen om contact op te nemen, waren om vast te stellen of het losgeldbericht echt is (48,9%), om tijd te rekken (47,3%) of om te onderhandelen (39,4%). Bij mkb'ers waren de meest voorkomende redenen om vast te stellen of het losgeldbericht echt is (50,2%), om te onderhandelen (36,2%) of om vast te stellen welke bestanden of gegevens door de daders zijn gestolen (36,1%). In de hele steekproef zou 4,9% van de zzp'ers en 6,3% van de mkb'ers onderhandelen. De meerderheid van de zzp'ers en mkb'ers zou dit doen om het losgeldbedrag te verlagen. Opvallend is dat een klein deel van met name de zzp'ers contact zou opnemen of zou onderhandelen om de identiteit van de daders te achterhalen of informatie te verzamelen die de politie kan helpen in de opsporing.

Tabel 7.3 Frequentie van of, door wie en hoe er contact opgenomen zou worden met de daders

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Contact opnemen met daders	**1.769**		**732**	
Ikzelf of een collega zou contact opnemen	68	3,8%	30	4,1%
Bekende contact laten opnemen	28	1,6%	11	1,5%
Ingehuurde partij contact laten opnemen	123	7%	86	11,8%
Geen contact opnemen	1.550	87,6%	605	82,6%
Doel *(meerdere antwoorden mogelijk)*	219		127	
Om vast te stellen of het losgeldbericht echt is	107	48,9%	64	50,2%
Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline	86	39,4%	46	36,2%
Om vast te stellen welke bestanden of gegevens zijn gestolen	64	29,3%	46	36,1%
Om hulp te vragen bij het betalen (bijvoorbeeld bij het aanschaffen van bitcoin)	34	15,4%	21	16,5%
Om hulp te vragen na het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens)	40	18,1%	24	18,9%
Om tijd te rekken	104	47,3%	42	32,8%
Anders, namelijk …				
– T.b.v. achterhalen identiteit/ter ondersteuning opsporing politie	12	5,5%	3	0,4%
– Om frustratie te uiten/te laten weten niet te gaan betalen	6	2,7%	10	1,4%
– Inschatting maken van hoe professioneel ze zijn/ernst dreiging	2	0,9%	-	-
– Om na te gaan of ze zich na betaling aan de afspraken houden (bijv. omtrent niet lekken)	1	0,5%	-	-
– Om meer informatie te krijgen/mogelijkheden te bespreken	-	-	1	0,1%

Tabel 7.3 Verder

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Doel onderhandelingen *(meerdere antwoorden mogelijk)*	**86**		**46**	
Om het losgeldbedrag te verlagen	63	73,5%	33	71,6%
Om langer de tijd te krijgen/tijd te rekken	52	60,4%	28	61,7%
Om een andere reden, namelijk …	16	18,8%	9	19,3%
– Informatie inwinnen/t.b.v. achterhalen identiteit/ter ondersteuning opsporing politie	7	8,1%	-	-
– Inschatting maken van ernst dreiging (wat hebben de daders?)	2	2,3%	1	2,2%
– Nieuwsgierigheid	-	-	1	2,2%
– Om na te gaan of ze te vertrouwen zijn/of ze zich na betaling aan de afspraken houden	2	2,3%	3	6,5%
– Beslag maken op tijd om slachtofferschap bij anderen te voorkomen	-	-	2	4,3%
– Om probleem te verhelpen	2	2,3%	2	4,3%
– Informeren wat er aan de hand is	1	1,2%	-	-
– Is een vereiste van de verzekering	-	-	1	2,2%
– Akkoord bereiken over niet betalen	-	-	-	-

7.4 Impact

Respondenten is gevraagd wat (naar verwachting) de impact van het ransomware-incident zou zijn (tabel 7.4). De meeste zzp'ers en mkb'ers verwachten zich minder veilig te voelen (respectievelijk 53,1% en 41,3%), gevolgd door het hebben van minder vertrouwen in de eigen digitale vaardigheden (respectievelijk 43,3% en 36,2%), en minder vertrouwen in mensen (respectievelijk 34,2% en 32,8%). Een kleiner deel denkt andere gevolgen te ervaren, zoals slaapproblemen, depressieve klachten of het opnieuw beleven van het voorval.

De meerderheid van de ondernemers gaf daarnaast aan dat ze naar verwachting andere gevolgen zouden ervaren (tabel 7.4). Voor de zzp'ers betrof dit in de meeste gevallen kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (54,3%), verhindering in het uitvoeren van de dagelijkse werkzaamheden (45,2%), en het verliezen van bestanden of gegevens (45,2%).

Voor de mkb'ers betrof dit in de meeste gevallen kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk (65,7%), verhindering in het uitvoeren van de dagelijkse werkzaamheden (57,2%), en het besteden van tijd aan het oplossen van het incident of inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders (55,5%). Opvallend is dat in vergelijking met de zzp'ers een groter deel van de

mkb'ers verwacht tijd of kosten te moeten besteden aan het oplossen van het incident of de reparatie(s), en onderbreking van levering van goederen of diensten verwacht.

Wat betreft de financiële impact (buiten het eventueel betaalde losgeld), gaf de minderheid van de zzp'ers (6,7%) en mkb'ers (4,1%) aan dat ze naar verwachting geen financiele gevolgen zouden ervaren. Daarnaast gaf 24,9% van de zzp'ers en 22,8% van de mkb'ers aan het niet te weten. Bij de zzp'ers die wel financiële gevolgen denken te ervaren, was dit in de meeste gevallen tussen de 1.000 en 5.000 euro (27,8%) of minder dan 1.000 euro (20,4%). Bij de mkb'ers was dit in de meeste gevallen tussen de 1.000 en 5.000 euro (24,6%) of tussen de 5.000 en 10.000 euro (15,9%) (tabel 7.4).

Tabel 7.4 Frequentie van emotionele, andere en financiële gevolgen onder ondernemers

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Emotionele/psychische gevolgen *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Minder veilig voelen	939	53,1%	303	41,3%
Minder vertrouwen in mensen	605	34,2%	240	32,8%
Het voorval telkens opnieuw beleven	179	10,1%	56	7,6%
Slaapproblemen	394	22,3%	112	15,3%
Angstklachten en/of paniekaanvallen	171	9,7%	52	7,2%
Depressieve klachten	127	7,2%	35	4,7%
Minder vertrouwen in eigen digitale vaardigheden	767	43,3%	265	36,2%
Andere emotionele of psychische gevolgen, namelijk …				
– Gespannen/stress/piekeren/zorgen	13	0,7%	3	0,4%
– Gevoel van schaamte/falen/onbekwaamheid/schuldgevoelens/boos op zichzelf	11	0,6%	2	0,3%
– Agressie/boosheid	26	1,5%	23	3,1%
– Buikpijn	1	0,1%	-	-
– Gebrek aan focus/gevoel van onrust	2	0,1%	-	-
– Vermoeidheid	1	0,1%	-	-
– Minder vertrouwen in overheid/politie	1	0,1%	-	-
– Meer angst/wantrouwen online	1	0,1%	1	0,1%
Geen van de bovenstaande opties	287	16,2%	150	20,5%
Weet ik niet	153	8,6%	82	11,2%
Andere gevolgen *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Verhinderd in uitvoeren van dagelijkse werkzaamheden	800	45,2%	418	57,2%
Verlies van inkomsten, waarde van aandelen of inkomen	597	33,7%	258	35,3%
Tijd besteden aan het oplossen van het incident of inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders	799	45,2%	406	55,5%

Tabel 7.4 Verder

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Kosten maken vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk	960	54,3%	481	65,7%
Bestanden of gegevens verliezen	800	45,2%	317	43,3%
Boetes van regelgevers of wetgevers	141	8%	76	10,4%
Reputatieschade	347	19,6%	149	20,4%
Onderbreking van levering van goederen of diensten aan klanten, begunstigden, of gebruikers	499	28,2%	263	36%
Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders	302	17%	158	21,5%
Schadevergoeding, compensatie of korting verlenen aan klanten	56	3,1%	25	3,4%
Anders, namelijk …				
– Risico op bekendmaking van (privacygevoelige) gegevens (van klanten)	2	0,1%	1	0,1%
– Faillissement	-	-	1	0,1%
– Alerter/voorzichtiger geworden online	1	0,1%	-	-
Geen van bovenstaande opties	244	13,8%	61	8,4%
Financiële gevolgen (m.u.v. betalen losgeld)	**1.769**		**732**	
Geen	119	6,7%	30	4,1%
Minder dan €1.000	361	20,4%	82	11,2%
€1.000 tot €5.000	491	27,8%	180	24,6%
€5.000 tot €10.000	180	10,2%	117	15,9%
€10.000 tot €50.000	129	7,3%	106	14,5%
€50.000 tot €100.000	27	1,6%	29	3,9%
€100.000 tot €250.000	13	0,7%	13	1,7%
€250.000 tot €500.0001	1	0,0%	4	0,5%
€500.000 of meer	8	0,5%	6	0,8%
Weet ik niet	440	24,9%	167	22,8%

Daarnaast is aan respondenten gevraagd of het incident gevolgen zou hebben voor het online gedrag of de beveiligingsmaatregelen, wat bij 69,8% van de zzp'ers en 70,1% van de mkb'ers het geval was. Zoals blijkt uit tabel 7.5 zou de grootste groep zzp'ers die beveiligingsmaatregelen zou nemen (vaker) externe back-ups van bestanden en gegevens maken (60%), een wachtwoordbeleid invoeren dat zorgt voor sterke wachtwoorden (26,3%) en een firewall aanschaffen (25,3%). De grootste groep mkb'ers die maatregelen zou nemen, zou (vaker) externe back-ups van bestanden en gegevens maken (49,5%), een wachtwoordbeleid invoeren dat zorgt voor sterke wachtwoorden (27,6%) en beveiligingssoftware op apparaten laten scannen op virussen of andere kwaadaardige software (24,4%).

Tabel 7.5 Frequentie van genomen beveiligingsmaatregelen na slachtofferschap onder zzp'ers en mkb'ers

	zzp		mkb	
	n	**%**	**n**	**%**
Beveiligingsmaatregelen *(meerdere antwoorden mogelijk)*	**1.235**		**513**	
Ander besturingssysteem nemen	83	6,8%	35	6,7%
(Vaker) back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server	741	60%	254	49,5%
Wachtwoordbeleid dat zorgt voor sterke wachtwoorden	325	26,3%	142	27,6%
(Ander) antivirusproduct aanschaffen	209	16,9%	63	12,3%
Firewall aanschaffen	312	25,3%	113	22%
Beveiligingssoftware op netwerken en apparaten laten scannen op virussen of andere kwaadaardige software	293	23,7%	125	24,4%
Updates van besturingssystemen, apps en/of software direct uitvoeren zodra beschikbaar	78	6,3%	61	11,8%
Monitoren van gebruikers- of netwerkactiviteiten	208	16,8%	58	11,3%
IT-administratie en toegangsrechten beperken tot specifieke gebruikers	117	9,5%	54	10,6%
IT-administratie en toegangsrechten bijhouden	84	6,8%	41	7,9%
Specifieke regels opstellen voor veilig opslaan van bestanden met persoonsgegevens	119	9,7%	56	11%
Andere standaardbrowser nemen	63	5,1%	19	3,7%
Gevoelige bestanden en gegevens versleutelen	284	23%	93	18,1%
Veiligheidsrestricties op apparaten die eigendom zijn van het bedrijf	108	8,7%	63	12,2%
Toegang tot bedrijfsnetwerk alleen toegestaan op apparaten van het bedrijf	128	10,4%	72	14%
Gescheiden wifi-netwerken voor personeel en gasten	109	8,9%	63	12,2%
Tweestapsverificatie	242	19,6%	95	18,5%
Iemand (intern of extern) in dienst nemen die verantwoordelijk is voor cybersecurity	177	14,4%	100	19,5%
Bedrijfscontinuïteitsplan opstellen	87	7%	65	12,7%
Anders, namelijk …				
– Afhankelijk van advies specialist/expert/IT-leverancier	45	3,6%	22	4,3%
– Afhankelijk van analyse hoe het incident is gebeurd, daarop maatregelen treffen	14	1,1%	7	1,4%
– Nieuwe computer aanschaffen	1	0,1%	-	-
– Meer cybersecurity awareness, o.a. m.b.t. phishing-e-mails, sterke wachtwoorden	5	0,4%	2	0,4%
– Meer offline werken	2	0,2%	-	-
– Periodieke controle/onderhoud door expert	1	0,1%	-	-
– Overstappen van provider/leverancier	-	-	3	0,6%
– Inloggegevens veranderen	2	0,2%	-	-
– Ik weet het (nog) niet	21	1,7%	7	1,4%
Geen van bovenstaande	96	7,8%	33	6,5%

7.5 Betalen

Na het vignet is aan respondenten gevraagd hoe waarschijnlijk het is dat ze in het hypothetische scenario het losgeld zouden betalen op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). Gemiddeld genomen is dit voor zowel zzp'ers (*M* = 1,11; *SD* = 1,890) als mkb'ers (*M* = 1,19; *SD* = 1,984) niet waarschijnlijk. Zoals blijkt uit tabel 7.6 is de betalingsbereidheid van zzp'ers het hoogst in de groep waarbij 1% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om te betalen, geen back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (*M* = 1,902; *SD* = 2,634). De betalingsbereidheid is het laagst in de groep waarbij 1% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om niet te betalen, wel een back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (*M* = 0,578; *SD* = 1,265).

Tabel 7.6 Betalingsbereidheid per vignet voor zzp'ers (n=1.769)

Groep	**Vignet**				**Betalingsbereidheid (0-10)**	
	Hoogte losgeld	**Geadviseerd om te betalen**	**Back-up**	**Gedreigd met lekken**	**Gem.**	**Std. dev.**
1	1% van jaaromzet	Nee	Nee	Ja	0,956	1,779
2	1% van jaaromzet	Nee	Ja	Ja	0,881	1,696
3	1% van jaaromzet	Ja	Nee	Ja	1,582	2,321
4	1% van jaaromzet	Ja	Ja	Ja	1,334	2,157
5	25% van jaaromzet	Nee	Nee	Ja	1,149	1,825
6	25% van jaaromzet	Nee	Ja	Ja	0,885	1,724
7	25% van jaaromzet	Ja	Nee	Ja	1,106	2,099
8	25% van jaaromzet	Ja	Ja	Ja	1,070	1,748
9	1% van jaaromzet	Nee	Nee	Nee	0,953	1,584
10	1% van jaaromzet	Nee	Ja	Nee	0,578	1,265
11	1% van jaaromzet	Ja	Nee	Nee	1,902	2,634
12	1% van jaaromzet	Ja	Ja	Nee	1,303	1,945
13	25% van jaaromzet	Nee	Nee	Nee	0,968	1,695
14	25% van jaaromzet	Nee	Ja	Nee	0,591	1,257
15	25% van jaaromzet	Ja	Nee	Nee	1,426	2,097
16	25% van jaaromzet	Ja	Ja	Nee	1,030	1,559

Blijkens tabel 7.7 is bij mkb'ers de betalingsbereidheid het hoogst onder de groep waarbij 1% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om te betalen, wel een back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (*M* = 2,337; *SD* = 2,720). De betalingsbereidheid is het laagst onder de groep waarbij 25% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om niet te betalen, wel een back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (*M* = 0,268; *SD* = 0,736).

Tabel 7.7 Betalingsbereidheid per vignet voor mkb'ers (n=732)

Groep	Vignet				Betalingsbereidheid (0-10)	
	Hoogte losgeld	Geadviseerd om te betalen	Back-up	Gedreigd met lekken	Gem.	Std. dev.
1	1% van jaaromzet	Nee	Nee	Ja	1,594	2,301
2	1% van jaaromzet	Nee	Ja	Ja	1,143	1,730
3	1% van jaaromzet	Ja	Nee	Ja	1,766	2,634
4	1% van jaaromzet	Ja	Ja	Ja	2,337	2,720
5	25% van jaaromzet	Nee	Nee	Ja	0,662	1,392
6	25% van jaaromzet	Nee	Ja	Ja	0,268	0,736
7	25% van jaaromzet	Ja	Nee	Ja	1,202	1,927
8	25% van jaaromzet	Ja	Ja	Ja	1,369	1,716
9	1% van jaaromzet	Nee	Nee	Nee	1,578	2,199
10	1% van jaaromzet	Nee	Ja	Nee	0,916	1,840
11	1% van jaaromzet	Ja	Nee	Nee	1,545	2,413
12	1% van jaaromzet	Ja	Ja	Nee	1,068	1,894
13	25% van jaaromzet	Nee	Nee	Nee	0,517	1,290
14	25% van jaaromzet	Nee	Ja	Nee	0,762	1,682
15	25% van jaaromzet	Ja	Nee	Nee	1,176	1,805
16	25% van jaaromzet	Ja	Ja	Nee	1,187	1,984

De respondenten is vervolgens gevraagd wat in dit hypothetische scenario redenen zouden zijn om wel of niet het losgeld te betalen (tabel 7.8). De meest voorkomende redenen voor zzp'ers en mkb'ers om het losgeld niet te betalen waren dat het onethisch is om criminelen te betalen (respectievelijk 60,9% en 58,2%), dat ze er niet op zouden vertrouwen dat de toegang hersteld zou worden na betaling (respectievelijk 48,4% en 46,9%) en dat respondenten niet bang zouden zijn dat de daders data zouden lekken of dat er andere gevolgen zouden zijn voor het niet betalen (respectievelijk 24,4% en 23,9%). De meest voorkomende reden om wel te betalen was dat betalen goedkoper zou zijn dan geen zaken kunnen doen (respectievelijk 10,8% en 13,4%), bij zzp'ers gevolgd door dat het losgeldbedrag niet heel hoog was (10,2%) en bij mkb'ers gevolgd door het vertrouwen dat toegang hersteld zou worden na betaling (10%).

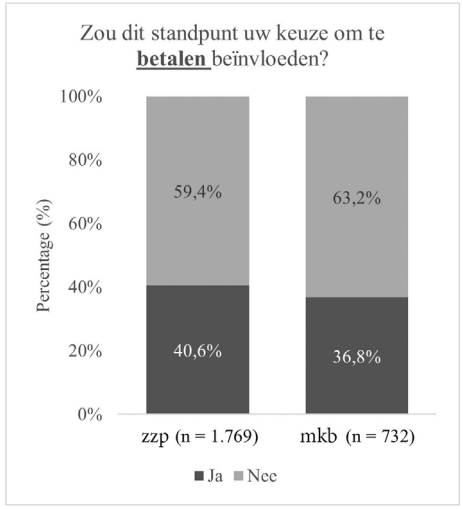
Tabel 7.8 Frequentie van reden(en) om (niet) te betalen onder zzp'ers en mkb'ers

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Redenen om niet te betalen *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Losgeldbedrag te hoog	407	23%	160	21,9%
Betalen zou duurder zijn dan geen zaken kunnen doen	273	15,4%	91	12,4%
Zou bestanden, gegevens of apparaten niet belangrijk vinden	256	14,4%	93	12,7%
Zou er niet op vertrouwen dat toegang hersteld zou worden na betaling	855	48,4%	343	46,9%

Tabel 7.8 Verder

	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Niet bang voor lekken van data of andere gevolgen bij niet betalen	431	24,4%	175	23,9%
Onethisch om criminelen te betalen	1.078	60,9%	426	58,2%
Zou niet weten hoe ik de betaling zou moeten doen	219	12,4%	95	13%
Anders, namelijk …	123	7%		
– Ik zou het zelf (of met behulp van een ander) oplossen, bijv. met een back-up	32	1,8%	14	2%
– Uit principe/laat me niet chanteren/houdt criminaliteit in stand	31	1,8%	17	2,4%
– Ik zou denken dat het een valse/ongeloofwaardige dreiging is	3	0,2%	-	-
– Impact van aanval zou beperkt zijn/bedrijfscontinuïteit niet in gevaar	5	0,3%	2	0,3%
– Bang om opnieuw geraakt te worden of dat meer geld geëist wordt	9	0,5%	9	1,3%
– Opvolging advies expert(s)	3	0,2%	1	0,2%
– Niet bevoegd om te beslissen	-	-	2	0,3%
– Ik zou eerst contact opnemen met de daders	1	0,1%	-	-
– Zou er niet op vertrouwen dat gestolen data niet gelekt of verkocht zouden worden na betaling	2	0,1%	-	-
– Ik zou eerst om extern advies vragen	2	0,1%	-	-
– Justitie adviseert om niet te betalen	-	-	1	0,1%
– Ik weet het (nog) niet	2	0,1%	1	0,1%
Geen van de bovenstaande opties	96	5,5%	27	3,7%
Ik zou het losgeld wel betalen	16	0,9%	13	1,8%
Redenen om wel te betalen *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Losgeldbedrag niet heel hoog	178	10,2%	48	6,5%
Betalen zou goedkoper zijn dan geen zaken kunnen doen	192	10,8%	98	13,4%
Zou bestanden, gegevens of apparaten niet willen verliezen	196	11,1%	73	9,9%
Zou erop vertrouwen dat toegang hersteld zou worden na betaling	125	7,1%	73	10%
Bang voor lekken van data of andere gevolgen bij niet betalen	115	6,5%	54	7,4%
Anders, namelijk …				
– Als expert(s) dit zou(den) adviseren	12	0,7%	7	0,9%
– Dit is het belang van klanten/om te voorkomen dat vertrouwelijke informatie openbaar wordt	1	0,1%	2	0,2%
– Als er geen andere mogelijkheid is/dit het einde van het bedrijf zou betekenen	5	0,3%	3	0,5%
– Vanuit angst/paniek	1	0,1%	-	-
– Dit is de snelste of makkelijkste optie	1	0,1%	-	-
– Ik weet het (nog) niet, hangt af van andere maatregelen (bijv. of back-up werkt)	5	0,3%	6	0,9%
Geen van de bovenstaande opties	146	8,3%	35	4,7%
Ik zou het losgeld niet betalen	1.127	63,7%	464	63,3%

De Nederlandse politie neemt het standpunt in dat slachtoffers het geëiste losgeld niet zouden moeten betalen. Zowel de zzp'ers (M = 4,54; SD = 0,800) als mkb'ers (M = 4,59; SD = 0,773) zijn het gemiddeld genomen (helemaal) eens met dit standpunt. Aan respondenten is bovendien gevraagd of dit standpunt de keuze om te betalen zou beïnvloeden. Minder dan de helft van de zzp'ers (40,6%) en mkb'ers (36,8%) geeft aan dat dit standpunt invloed zou hebben op hun keuze om te betalen (figuur 7.1).



Figuur 7.1 Invloed van standpunt politie om niet te betalen op keuze om te betalen

Verklarende resultaten

Om te onderzoeken of de waarschijnlijkheid van betalen gerelateerd is aan situationele factoren is een negatieve binomiale regressie uitgevoerd. Regressiemodel 1 gericht op de zzp'ers bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. De sector van de organisatie is daarnaast als controlevariabele aan het model toegevoegd. Zoals blijkt uit tabel 7.9, is er een negatief significant verband tussen het hebben van een back-up en de waarschijnlijkheid van betalen (B = −0,262, z = −2,895, p = 0,004). Dit betekent, met andere woorden, dat zzp'ers die geen back-up hebben een hogere waarschijnlijkheid van betalen hebben gerapporteerd in vergelijking met burgers die wel een back-up hebben. Er is daarnaast een positieve significante relatie tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de ondernemer heen en de waarschijnlijkheid van betalen (B = 0,424, z = 4,695, p = < 0,001). Zzp'ers rapporteren een hogere waarschijnlijkheid van betalen indien hen geadviseerd wordt om het losgeld te betalen. Er is geen significant verband tussen de hoogte van het geëiste losgeldbedrag (B = −0,116, z = −1,283, p = 0,200) en dreigen met lekken (B = 0,071, z = 0,791, p = 0,429) en de waarschijnlijkheid van betalen onder zzp'ers. Bovendien is er een significant verband tussen de sectoren landbouw/visserij (B = −1,312, z = −3,849, p = < 0,001) en handel, logistiek en horeca (B = −0,330, z = −2,476, p = 0,013) en de waarschijnlijkheid van betalen. In de sectoren landbouw/visserij en handel, logistiek en horeca is de waarschijnlijkheid van betalen lager in vergelijking met de sector financiële en zakelijke dienstverlening.

Regressiemodel 2 gericht op de mkb'ers bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. De grootte en sector van de organisatie zijn daarnaast als controlevariabelen aan het model toegevoegd. Zoals blijkt uit tabel 7.9, is er net als in model 1 (zzp'ers) geen significant verband tussen het dreigen met lekken (B = 0,095, z = 0,696, p = 0,486) en de waarschijnlijkheid van betalen onder mkb'ers. In tegenstelling tot model 1, is er geen significant verband tussen het hebben van een back-up en de waarschijnlijkheid van betalen (B = −0,126, z = −0,923, p = 0,356). Er is wel een negatief significant verband tussen de hoogte van het geëiste losgeldbedrag en de waarschijnlijkheid van betalen (B = −0,685, z = −4,944, p = < 0,001). Mkb'ers van wie 25% van de jaaromzet in bitcoin werd geëist, rapporteren een lagere waarschijnlijkheid van betalen ten opzichte van mkb'ers van wie 1% van de jaaromzet in bitcoin werd geëist. Dit betekent, met andere woorden, dat mkb'ers een hogere waarschijnlijkheid van betalen rapporteren indien het losgeldbedrag lager is. Er is ook een positief significant verband tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de ondernemer heen en de waarschijnlijkheid van betalen (B = 0,474, z = 3,465, p = < 0,001). Mkb'ers rapporteren een hogere waarschijnlijkheid van betalen indien hen geadviseerd wordt om het losgeld te betalen. Bovendien betreffen de bedrijfsgroottes klein (B = 0,502, z = 3,067, p = 0,002) en midden (B = 0,745, z = 2,030, p = 0,042) significante variabelen. Kleine- en middelgrote bedrijven rapporteren een hogere waarschijnlijkheid van betalen in vergelijking met microbedrijven. Tot slot is er een significant verband tussen de sector handel, logistiek en horeca en de waarschijnlijkheid van betalen (B = −0,406, z = −2,178, p = 0,029). In de sector handel, logistiek en horeca is de waarschijnlijkheid van betalen lager in vergelijking met de sector financiële en zakelijke dienstverlening.

Tabel 7.9 Negatieve binomiale regressie van de waarschijnlijkheid van betalen onder zzp'ers en mkb'ers

		Model 1: zzp (n=1.762)			**Model 2: mkb** (n=724)		
		B	**S.E.**	**z**	**B**	**S.E.**	**z**
	(Intercept)	0,168***	0,119	1,418	0,264***	0,209	1,261
Vignet factoren	Hoogte losgeld (0-1)	−0,116	0,090	−1,283	-0,685***	0,138	−4,944
	Gedreigd met lekken	0,071	0,090	0,791	0,095	0,137	0,696
	Back-up (0-1)	−0,262**	0,091	−2,895	−0,126	137	−0,923
	Geadviseerd om te betalen (0-1)	0,424***	0,090	4,695	0,474***	0,137	3,465
	Grootte bedrijf						
	Micro (0-1)	-	-	-	REF		
	Klein (0-1)	-	-	-	0,502**	0,164	3,067
	Midden (0-1)	-	-	-	0,745*	0,367	2,030
Controle-variabelen	*Sector*						
	Financiële en zakelijke dienstverlening (0-1)	REF			REF		
	Landbouw/visserij (0-1)	−1,312***	0,341	−3,849	−0,200	0,291	−0,687
	Industrie, bouw en nutsbedrijven (0-1)	−0,216	0,137	−1,579	−0,151	0,238	−0,635
	Handel en logistiek, horeca (0-1)	−0,330*	0,133	−2,476	−0,406*	0,187	−2,178
	Overheid, onderwijs, zorg en overig (0-1)	−0,205	0,112	−1,833	−0,169	0,201	−0,842
	2 × log-likelihood	−4842,5350			−2052,24		
	AIC	4862,5			2076,2		

*p< 0,05, **p< 0,01, ***p< 0,001

7.6 Melden

Vervolgens is aan de ondernemers gevraagd hoe waarschijnlijk het is dat ze in het hypothetische scenario het incident zouden melden en/of aangifte zouden doen op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). Gemiddeld genomen is dit voor zowel zzp'ers (M = 8,87; SD = 2,344) als mkb'ers (M = 9,07; SD = 2,104) waarschijnlijk. Hoewel de verschillen tussen groepen klein zijn, blijkt uit tabel 7.10 dat de meldingsbereidheid voor zzp'ers het hoogst is onder de groep waarbij 25% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om niet te betalen, geen back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (M = 9,191; SD = 1,605). Voor de zzp'ers is de meldingsbereidheid het laagst onder de groep waarbij 1% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om wel te betalen, geen

back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (M = 8,515; SD = 2,846).

Tabel 7.10 Meldingsbereidheid per vignet voor zzp'ers (n=1.769)

Groep	**Vignet**				**Meldingsbereidheid (0-10)**	
	Hoogte losgeld	**Geadviseerd om te betalen**	**Back-up**	**Gedreigd met lekken**	**Gem.**	**Std. dev.**
1	1% van jaaromzet	Nee	Nee	Ja	8,861	2,471
2	1% van jaaromzet	Nee	Ja	Ja	8,814	2,473
3	1% van jaaromzet	Ja	Nee	Ja	8,515	2,846
4	1% van jaaromzet	Ja	Ja	Ja	8,605	2,647
5	25% van jaaromzet	Nee	Nee	Ja	9,051	2,168
6	25% van jaaromzet	Nee	Ja	Ja	8,787	2,621
7	25% van jaaromzet	Ja	Nee	Ja	8,842	2,458
8	25% van jaaromzet	Ja	Ja	Ja	8,843	2,468
9	1% van jaaromzet	Nee	Nee	Nee	8,924	2,301
10	1% van jaaromzet	Nee	Ja	Nee	8,968	2,114
11	1% van jaaromzet	Ja	Nee	Nee	8,889	2,146
12	1% van jaaromzet	Ja	Ja	Nee	8,809	2,308
13	25% van jaaromzet	Nee	Nee	Nee	9,191	1,605
14	25% van jaaromzet	Nee	Ja	Nee	8,786	2,204
15	25% van jaaromzet	Ja	Nee	Nee	9,005	2,307
16	25% van jaaromzet	Ja	Ja	Nee	8,937	2,169

Ook de bij mkb'ers zijn de verschillen tussen de groepen klein. De meldingsbereidheid (tabel 7.11) is bij de mkb'ers het hoogst onder de groep waarbij 25% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om te betalen, geen back-up beschikbaar was en niet gedreigd werd met het lekken van gestolen data (M = 9,785; SD = 0,681). De meldingsbereidheid is het laagst onder de groep waarbij 25% van de jaaromzet aan losgeld geëist werd, geadviseerd werd om wel te betalen, geen back-up beschikbaar was en wel gedreigd werd met het lekken van gestolen data (M = 8,385; SD = 2,569).

Tabel 7.11 Meldingsbereidheid per vignet voor mkb'ers (n=732)

Groep	Vignet				Meldingsbereidheid	
	Hoogte losgeld	Geadviseerd om te betalen	Back-up	Gedreigd met lekken	Gem.	Std. dev.
1	1% van jaaromzet	Nee	Nee	Ja	9,498	1,025
2	1% van jaaromzet	Nee	Ja	Ja	9,196	2,211
3	1% van jaaromzet	Ja	Nee	Ja	8,820	2,697
4	1% van jaaromzet	Ja	Ja	Ja	9,149	1,490
5	25% van jaaromzet	Nee	Nee	Ja	8,787	2,649
6	25% van jaaromzet	Nee	Ja	Ja	9,201	2,273
7	25% van jaaromzet	Ja	Nee	Ja	8,385	2,569
8	25% van jaaromzet	Ja	Ja	Ja	8,873	2,387
9	1% van jaaromzet	Nee	Nee	Nee	9,055	1,755
10	1% van jaaromzet	Nee	Ja	Nee	8,648	2,478
11	1% van jaaromzet	Ja	Nee	Nee	9,349	1,829
12	1% van jaaromzet	Ja	Ja	Nee	9,232	1,845
13	25% van jaaromzet	Nee	Nee	Nee	8,504	2,800
14	25% van jaaromzet	Nee	Ja	Nee	9,261	1,966
15	25% van jaaromzet	Ja	Nee	Nee	9,785	0,681
16	25% van jaaromzet	Ja	Ja	Nee	9,287	1,627

Met betrekking tot het melden van de hypothetische ransomware-aanval, zou de meerderheid van de zzp'ers en mkb'ers het incident melden bij de politie (respectievelijk 92,5% en 92%), gevolgd door een bank of financiële instelling (respectievelijk 47,6% en 50,1%) (tabel 7.12). Opvallend is dat een groter deel van de mkb'ers melding zou maken bij een cybersecuritybedrijf/IT-leverancier of verzekeringsmaatschappij in vergelijking met de zzp'ers. Een groter deel van de zzp'ers zou daarentegen melding maken bij de Fraudehelpdesk. Respondenten hebben daarnaast een aantal andere hulpbronnen vermeld waar ze een melding zouden maken, zoals een beroepsvereniging of brancheorganisatie of een juridisch loket (tabel 5.10).

Tabel 7.12 Frequentie van instanties waar respondenten zouden melden in het hypothetische scenario

	zzp (n=1.769)		mkb (n=732)	
	n	%	n	%
Contact met *(meerdere antwoorden mogelijk)*	**1.769**		**732**	
Politie	1.637	92,5%	674	92%
Bank of financiële instelling	842	47,6%	367	50,1%
Verzekeringsmaatschappij	479	27,1%	311	42,5%
Cybersecuritybedrijf/IT-leverancier/internetprovider/ systeembeheerder	542	30,7%	361	49,3%
No More Ransom	218	12,3%	69	9,5%
Autoriteit Persoonsgegevens	436	24,7%	183	25%
Slachtofferhulp	44	2,5%	18	2,5%
Fraudehelpdesk	802	45,3%	270	36,9%
Een andere organisatie				
– Accountant	1	0,1%	2	0,2%
– Advocaat/juridisch loket	2	0,1%	-	-
– Belastingdienst	1	0,1%	-	-
– Beroepsvereniging/brancheorganisatie/vakbond	7	0,4%	3	0,4%
– Consumentenbond	1	0,1%	-	-
– Media	1	0,1%	-	-
– DIVD	1	0,1%	-	-
– NCSC	1	0,1%	1	0,1%
– Kamer van koophandel	1	0,1%	-	-
– Boekhouder	1	0,1%	4	0,5%
– Private recherche			1	0,1%
– Weet ik niet/dit zou ik uitzoeken, bijvoorbeeld via Google	8	0,4%	4	0,5%

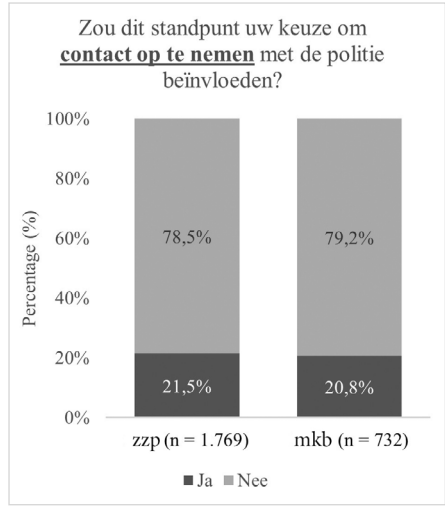
De respondenten is vervolgens gevraagd wat in dit hypothetische scenario redenen zouden zijn om wel of niet te melden bij de politie (tabel 7.13). De meest voorkomende redenen voor zzp'ers en mkb'ers om niet te melden waren dat het geen zin heeft omdat de politie er toch niets aan zou doen (respectievelijk 46,6% en 45,8%), dat het eerder een zaak is voor een andere instantie dan de politie (respectievelijk 21,3% en 20,6%) en dat ondernemers het zelf of met behulp van een andere partij zouden oplossen (respectievelijk 19,6% en 25%). De meest voorkomende redenen voor zzp'ers en mkb'ers om in het hypothetische scenario wel te melden waren omdat ze zouden willen dat de dader gepakt wordt (respectievelijk 79,8% en 82,1%), om te voorkomen dat dit bij een ander gebeurt (respectievelijk 68,4% en 67,4%) en omdat het hun plicht is (respectievelijk 63,3% en 68,3%).

Tabel 7.13 Frequentie van reden(en) om (niet) te melden en/of aangifte te doen bij de politie onder zzp'ers en mkb'ers

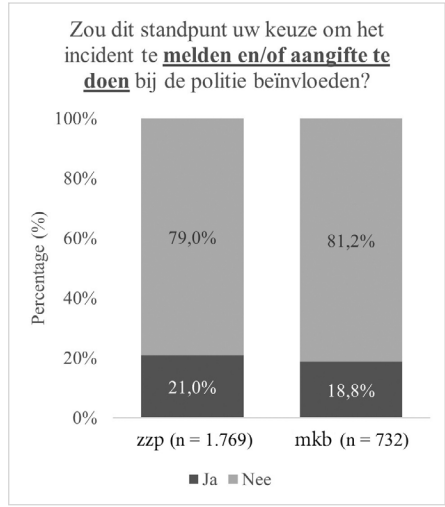
	zzp (n=1.769)		**mkb** (n=732)	
	n	**%**	**n**	**%**
Redenen om niet te melden *(meerdere antwoorden mogelijk)*	**133**		**59**	
Mijn bedrijf zou het zelf of met behulp van een andere partij oplossen	26	19,6%	15	25%
Het is niet zo belangrijk	17	12,4%	3	4,3%
Het kost te veel moeite	23	17,1%	10	17,1%
Het heeft geen zin, de politie zou er toch niets aan doen	62	46,6%	27	45,8%
De politie heeft niet de kennis om dit type delict aan te pakken	23	17,3%	13	21,4%
Het is eerder een zaak voor een andere instantie dan de politie	28	21,3%	12	20,6%
Ik heb weinig vertrouwen in de politie	12	9,1%	6	9,9%
Ik zou bang zijn dat de dader wraak zal nemen	2	1,2%	2	4%
Ik zou me schamen dat mijn bedrijf slachtoffer is geworden	2	1,7%	1	0,9%
Ik zou schamen dat mijn bedrijf het losgeld betaald heeft	2	1,8%	1	0,9%
Ik zou vinden dat het eigenlijk mijn/onze eigen schuld is	4	3,3%	4	6,2%
Ik zou bang zijn voor reputatieschade	6	4,5%	2	3,1%
Anders, namelijk …			8	13,8%
– Zou er niet aan denken	-	-	1	0,9%
– De politie heeft er niks aan	-	-	1	0,9%
Redenen om wel te melden *(meerdere antwoorden mogelijk)*	**1.636**		**674**	
Om te voorkomen dat dit opnieuw bij mijn bedrijf gebeurt	636	38,8%	293	43,5%
Om te voorkomen dat dit bij een ander gebeurt	1.118	68,4%	454	67,4%
Ik zou willen dat de dader gepakt wordt	1.305	79,8%	553	82,1%
Om een veiligere (online) wereld te creëren	943	57,6%	387	57,4%
Het is mijn plicht	1.037	63,3%	460	68,3%
Om de schade vergoed te krijgen	344	21%	183	27,2%
Anders namelijk …				
– Voor advies/hulp	11	0,7%	-	-
– Attenderen op veiligheidsrisico's	-		1	0,1%
– Het gaat om een strafrechtelijk feit	1	0,1%	-	-
– T.b.v. statistieken	7	0,4%	-	-
– I.v.m. financiële compensatie	-		1	0,1%
– Informeren waar het fout is gegaan	1	0,1%	-	-

Zoals eerder vermeld, zijn de ondernemers het gemiddeld genomen (helemaal) eens met het advies van de politie dat slachtoffers het geëiste losgeld niet moeten betalen. Aan respondenten is gevraagd of dit standpunt de keuze om contact op te nemen met de politie en het incident te melden/aangifte te doen bij de politie zou beïnvloeden.

Ongeveer een vijfde van de respondenten geeft aan dat het hun keuze om contact op te nemen met de politie zou beïnvloeden (figuur 7.2). Daarnaast geeft ongeveer een vijfde van de respondenten aan dat dit standpunt hun keuze om het ransomware-incident te melden/aangifte te doen bij de politie zou beïnvloeden (figuur 7.3).



Figuur 7.2 Invloed van standpunt politie om niet te betalen op keuze om contact op te nemen met de politie



Figuur 7.3 Invloed van standpunt politie om niet te betalen op keuze om te melden en/of aangifte te doen

Verklarende resultaten

Om te onderzoeken of de waarschijnlijkheid van melden gerelateerd is aan situationele factoren is een negatief binomiale regressie uitgevoerd. Regressiemodel 1 gericht op de zzp'ers bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. De sector van de organisatie is daarnaast als controlevariabele aan het model toegevoegd. Zoals blijkt uit tabel 7.14 is er geen significant verband tussen de hoogte van het geëiste losgeldbedrag ($B = 0{,}017$, $z = -1{,}041$, $p = 0{,}298$), dreigen met lekken ($B = -0{,}016$, $z = -{,}974$, $p = 0{,}330$), het hebben van een back-up ($B = -0{,}009$, $z = -0{,}583$, $p = 0{,}560$) en geadviseerd worden om te betalen ($B = -0{,}012$, $z = -0{,}771$, $p = 0{,}441$) en de waarschijnlijkheid van melden onder zzp'ers.
Regressiemodel 2 gericht op de mkb'ers bevat de verklarende factoren hoogte van het losgeld, dreigen met lekken, het hebben van een back-up en advies om te betalen. De grootte en sector van de organisatie zijn daarnaast als controlevariabelen aan het model toegevoegd. Zoals blijkt uit tabel 7.14 is er ook in dit model geen significant verband tussen de hoogte van het geëiste losgeldbedrag ($B = -0{,}018$, $z = -0{,}732$, $p = 0{,}464$), dreigen met lekken ($B = -0{,}016$, $z = -0{,}631$, $p = 0{,}528$), het hebben van een back-up ($B = 0{,}013$, $z = 0{,}512$, $p = 0{,}609$) en geadviseerd worden om te betalen ($B = 0{,}000$, $z = 0{,}008$, $p = 0{,}994$) en de waarschijnlijkheid van melden onder mkb'ers.

Tabel 7.14 Negatief binomiale regressie van de waarschijnlijkheid van melden onder zzp'ers en mkb'ers

		Model 1: zzp (n=1.762)			**Model 2: mkb** (n=724)		
		B	**S.E.**	**z**	**B**	**S.E.**	**z**
	(Intercept)	2,200***	0,021	103,819	2,208***	0,038	57,635
Vignet factoren	Hoogte losgeld (0-1)	0,017	0,016	1,041	−0,018	0,025	−0,732
	Gedreigd met lekken	−0,016	0,016	−0,974	−0,016	0,025	−0,631
	Back-up (0-1)	−0,009	0,016	−0,583	0,013	0,025	0,512
	Geadviseerd om te betalen (0-1)	−0,012	0,016	−0,771	0,000	0,025	0,008
	Grootte bedrijf						
	Micro (0-1)	-	-	-	REF		
	Klein (0-1)	-	-	-	0,018	0,030	0,587
	Midden (0-1)	-	-	-	0,068	0,069	0,976
Controle-variabelen	*Sector*						
	Financiële en zakelijke dienstverlening (0-1)	REF			REF		
	Landbouw/visserij (0-1)	−0,098	0,051	−01,917	−0,005	0,053	−0,093
	Industrie, bouw en nutsbedrijven (0-1)	−0,044	0,025	−01,781	0,036	0,043	0,828
	Handel en logistiek, horeca (0-1)	−0,021	0,024	−0,886	−0,021	0,034	−0,612
	Overheid, onderwijs, zorg en overig (0-1)	0,017	0,020	0,861	0,019	0,037	0,532
	2 x log likelihood	−8597,734			−3439,738		
	AIC	8617,7			3463,7		

*p< 0,05, **p< 0,01, ***p< 0,001

7.7 Resumé

In dit hoofdstuk is aan de hand van een hypothetisch scenario stilgestaan bij de betalings- en meldingsbereidheid onder Nederlandse zzp'ers en mkb'ers die niet eerder slachtoffer zijn geworden van ransomware. Als het gaat om de verwachte eerste reactie in het hypothetische scenario, was de meest voorkomende emotie boosheid onder zowel zzp'ers als mkb'ers. Een deel van de respondenten zou zelf proberen om het probleem op te lossen, in de meeste gevallen zouden zowel zzp'ers als mkb'ers de verbinding met internet verbreken. Een ander deel van de respondenten zou hulp zoeken, in de meeste gevallen van een organisatie of instantie, gevolgd door een bekende of collega en hulp via internet.

Met betrekking tot het contact opnemen met de daders zou 12,4% van de zzp'ers en 17,4% van de mkb'ers dit doen of iemand anders laten doen. In de meeste gevallen zouden respondenten dit doen om vast te stellen of het losgeldbericht echt is. Ongeveer 40% van de zzp'ers en 36% van de mkb'ers zou contact opnemen om te onderhandelen, wat neerkomt op respectievelijk 4,9% en 6,3% van de totale steekproef. De meerderheid hiervan zou onderhandelen om het losgeldbedrag te verlagen.

Als het gaat om de impact verwacht de meerderheid van beide groepen emotionele of psychische gevolgen te ervaren, met name een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden. De meerderheid van de zzp'ers en mkb'ers gaf daarnaast aan dat zij ook andere gevolgen zouden ervaren, met name kosten vanwege reparatie of herstel. De meerderheid van de respondenten verwachtte financiële gevolgen (buiten het eventuele betaalde losgeld). Bij zzp'ers was dit in de meeste gevallen naar verwachting minder dan 1.000 euro of tussen de 1.000 en 5.000 euro. Mkb'ers schatten de kosten hoger in, met in de meeste gevallen een schatting tussen de 1.000 en 5.000 euro of tussen de 5.000 en 10.000 euro. Een groot deel van de respondenten rapporteert tevens dat het ransomware-incident bij hen zou leiden tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In de meeste gevallen zouden zzp'ers en mkb'ers (vaker) externe back-ups maken van bestanden en gegevens.

De betalingsbereidheid is laag in het hypothetische scenario, met als voornaamste reden dat zzp'ers en mkb'ers het onethisch vinden om criminelen te betalen. De meest voorkomende reden bij beide groepen om wel te betalen is dat het betalen van het losgeld goedkoper zou zijn dan geen zaken kunnen doen. Uit de regressieanalyse blijkt bovendien dat het niet hebben van een back-up en geadviseerd worden om te betalen (door een (cybersecurity)organisatie en de mensen om de respondenten heen), gerelateerd is aan een significant hogere waarschijnlijkheid van betalen onder zzp'ers. Bij de mkb'ers is een losgeldbedrag van 1% van de jaaromzet (ten opzichte van 25% van de jaaromzet) en geadviseerd worden om te betalen (door een (cybersecurity)organisatie en de mensen om de respondenten heen) gerelateerd aan een significant hogere waarschijnlijkheid van betalen.

De meldingsbereidheid is hoog in het hypothetische scenario. De meerderheid van de zzp'ers en mkb'ers heeft aangegeven dat zij het incident zouden melden bij de politie (respectievelijk 92,5% en 92%), gevolgd door een bank of financiële instelling (respectievelijk 47,6% en 50,1%). Een groter deel van de mkb'ers zou melding maken bij een cybersecuritybedrijf of IT-leverancier of verzekeringsmaatschappij, terwijl een groter deel van de zzp'ers melding zou maken bij de Fraudehelpdesk. De voornaamste reden om te melden is dat respondenten willen dat de dader gepakt wordt. De voornaamste reden om niet te melden is dat het volgens respondenten geen zin heeft omdat de politie er toch niets aan zou doen. Zowel zzp'ers als mkb'ers zijn het eens met het algemene advies van de politie om het losgeld niet te betalen en bij ongeveer 41% van de zzp'ers en 37% van de mkb'ers zou het standpunt invloed hebben op de keuze om te betalen.

Tegelijkertijd zou ditzelfde standpunt bij ongeveer een vijfde van de zzp'ers en mkb'ers invloed hebben op de keuze om contact op te nemen met de politie en bij een vijfde invloed hebben op de keuze om het incident te melden en/of aangifte te doen. Uit de regressieanalyse blijkt dat er geen significant verband is tussen de hoogte van het geëiste losgeldbedrag, dreigen met lekken, het hebben van een back-up en geadviseerd worden om te betalen en de waarschijnlijkheid van melden onder zzp'ers en mkb'ers.

7.8 Vergelijking deelstudie 1B en 2B

In het voorgaande is stilgestaan bij de prevalentie, aard en impact van slachtofferschap van ransomware onder Nederlandse ondernemers (deelstudie 1B) en de betalings- en meldingsbereidheid aan de hand van een hypothetisch scenario onder Nederlandse ondernemers die niet eerder slachtoffer zijn geworden van ransomware (deelstudie 2B). In deze paragraaf worden de resultaten van beide deelstudies onder ondernemers vergeleken.

Bij zowel daadwerkelijk slachtofferschap als in het hypothetische scenario was de meest voorkomende emotie onder ondernemers boosheid. In beide deelstudies zouden de meeste zzp'ers proberen om zelf het probleem op te lossen door de verbinding met internet te verbreken. Onder mkb'ers verschilt dit tussen slachtoffers en niet-slachtoffers. Waar de meeste niet-slachtoffers zouden proberen om het probleem op te lossen door de verbinding met internet te verbreken, hebben de meeste mkb'ers die daadwerkelijk slachtoffer zijn geworden geprobeerd de data te herstellen vanaf een back-up. In beide deelstudies hebben de meeste zzp'ers en mkb'ers die hulp (zouden) zoeken dit gedaan bij een organisatie of instantie.

In beide deelstudies neemt een klein deel van de respondenten contact op met de daders. Waar onder de daadwerkelijke slachtoffers 6,6% en 6,2% van respectievelijk de zzp'ers en mkb'ers contact op zou nemen, zou 12,4% en 17,4% van respectievelijk de zzp'ers en mkb'ers onder de niet-slachtoffers (in het hypothetische scenario) dit doen. In beide deelstudies liggen hier bovendien andere motivaties aan ten grondslag. Waar de slachtoffers in de meeste gevallen contact hebben opgenomen om vast te stellen welke data waren gestolen of vast te stellen of het losgeldbericht echt is, zouden de niet-slachtoffers dit met name doen om vast te stellen of het losgeldbericht echt is. Opvallend is daarnaast dat geen enkele zzp'er die slachtoffer is geworden zou onderhandelen met de daders, terwijl 4,9% van de totale steekproef van zzp'ers die geen slachtoffer is geworden dit wel zou doen, met name om het losgeldbedrag te verlagen. Bij de mkb'ers heeft slechts 2% van de slachtoffers onderhandeld, terwijl 6,3% van de totale steekproef van mkb'ers die geen slachtoffer is geworden zou onderhandelen, met name om het losgeldbedrag te verlagen.

Als het gaat om de impact, verwacht 75,2% van de zzp'ers en 68,3% van de mkb'ers die niet eerder slachtoffer zijn geworden op basis van het hypothetische scenario emotionele of psychische gevolgen te ervaren na een ransomware-aanval. Onder de daadwerkelijke slachtoffers was dit bij 38,8% en 33,6% van respectievelijk de zzp'ers en mkb'ers het geval. De meest voorkomende (verwachte en daadwerkelijke) gevolgen komen overeen, namelijk een minder veilig gevoel, gevolgd door minder vertrouwen in andere mensen onder slachtoffers en minder vertrouwen in de eigen digitale vaardigheden onder niet-slachtoffers. Bij beide groepen is het meest voorkomende andere gevolg kosten vanwege reparatie of herstel. Waar 68,4% van de zzp'ers en 73,1% van de mkb'ers onder de niet-slachtoffers financiële gevolgen verwacht, was dit bij 60,3% van de zzp'ers en 74% van de mkb'ers onder de slachtoffers het geval, hoewel de meeste niet-slachtoffers de financiële kosten wat hoger hebben ingeschat dan dat bij de slachtoffers het geval was. Bij een groot deel van de slachtoffers en niet-slachtoffers leidt het incident bovendien tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In beide deelstudies gaat het bij de meeste zzp'ers en mkb'ers om het (vaker) maken van externe back-ups van bestanden en gegevens.

De betalingsbereidheid is laag, zowel in het hypothetische scenario als onder de slachtoffers. Slechts 7,6% van de zzp'ers en 6,1% van de mkb'ers die slachtoffer is geworden heeft het losgeld betaald, terwijl de gemiddelde waarschijnlijkheid van betalen in het hypothetische scenario respectievelijk 1,11 is voor zzp'ers en 1,19 is voor mkb'ers op een schaal van 0 (helemaal niet waarschijnlijk) tot 10 (zeer waarschijnlijk). De meeste zzp'ers in beide deelstudies geven als reden om niet te betalen dat het onethisch is om criminelen te betalen. Waar de meeste mkb'ers die geen slachtoffer zijn geworden dit ook als reden aanhaalden, gaven de mkb'ers die wel slachtoffer zijn geworden als voornaamste reden om niet te betalen dat ze een back-up hadden. De meest voorkomende reden onder zowel zzp'ers als mkb'ers die slachtoffer zijn geworden om wel te betalen was dat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen. Bij de niet-slachtoffers was de voornaamste reden om te betalen daarentegen dat het betalen van het losgeld goedkoper zou zijn dan geen zaken kunnen doen. Uit de regressieanalyse blijkt bovendien dat het niet hebben van een back-up en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen, leidt tot een hogere waarschijnlijkheid van betalen onder zzp'ers. Bij de mkb'ers is een losgeldbedrag van 1% van de jaaromzet (ten opzichte van 25% van de jaaromzet) en geadviseerd worden door een (cybersecurity)organisatie en de mensen om de respondenten heen om te betalen gerelateerd aan een significant hogere waarschijnlijkheid van betalen in het hypothetische scenario.

Hoewel de meldingsbereidheid hoog is onder respondenten in het hypothetische scenario, blijkt dit niet het geval onder de slachtoffers. Waar ongeveer 92% van de ondernemers in het hypothetische scenario het incident zou melden bij de politie, heeft 12,3% en 26,7% van respectievelijk de zzp'ers en mkb'ers die slachtoffer zijn geworden contact opgenomen met de politie en slechts respectievelijk 1,1% en 10% daadwerkelijk aangifte gedaan. Waar de zzp'ers die slachtoffer zijn geworden als voornaamste reden om te melden gaven dat ze wilden voorkomen dat het bij een ander gebeurt, was

dit bij mkb'ers omdat ze wilden dat de dader gepakt wordt. De meeste niet-slachtoffers gaven als voornaamste reden dat ze zouden willen dat de dader gepakt wordt. Waar de meeste slachtoffers die niet gemeld hebben als voornaamste reden gaven dat ze het zelf of met behulp van een andere partij hebben opgelost, gaven de niet-slachtoffers als voornaamste reden dat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen. Zowel de slachtoffers als de niet-slachtoffers zijn het eens met het advies van de politie om het losgeld niet te betalen. Dit standpunt heeft bij 23% en 30% van respectievelijk de zzp'ers en mkb'ers die slachtoffer zijn geworden en een vijfde van de niet-slachtoffers invloed op de keuze om contact op te nemen met de politie. Uit de regressieanalyse blijkt dat de hoogte van het geëiste losgeldbedrag, dreigen met lekken, het hebben van een back-up en geadviseerd worden om te betalen niet significant samenhangen met de waarschijnlijkheid van melden onder zzp'ers en mkb'ers in het hypothetische scenario.

Samengenomen zijn de belangrijkste verschillen tussen deelstudie 1 (onder slachtoffers) en deelstudie 2 (respondenten die rapporteren naar aanleiding van een fictief scenario) met betrekking tot onderhandelen dat een wat groter deel van de niet-slachtoffers contact zou opnemen met de daders in vergelijking met de slachtoffers. Hier liggen bovendien andere beweegredenen aan ten grondslag. Waar een deel van de slachtoffers met name contact zou opnemen om vast te stellen welke data waren gestolen, zouden niet-slachtoffers dit voornamelijk doen om vast te stellen of het losgeldbericht echt is. Daarnaast zou ongeveer 5% tot 6,5% van de niet-slachtoffers onderhandelen, terwijl geen enkele zzp'er en slechts 2% van de mkb'ers die slachtoffer zijn geworden dat daadwerkelijk heeft gedaan. Met betrekking tot betalen was het belangrijkste verschil dat de motivatie om niet te betalen onder mkb'ers uiteenloopt, waarbij slachtoffers met name niet betaalden omdat ze een back-up hadden en niet-slachtoffers omdat het onethisch zou zijn om criminelen te betalen. Met betrekking tot melden was het belangrijkste verschil dat de meldingsbereidheid hoog is onder niet-slachtoffers, terwijl slechts tussen 12% tot 27% van de ondernemers contact heeft opgenomen met de politie en tussen 1 en 10% aangifte heeft gedaan. Ook de belangrijkste beweegreden om wel of niet te melden liep uiteen. De belangrijkste reden om wel te melden was in de meeste gevallen onder zzp'ers dat ze wilden voorkomen dat het bij een ander gebeurt en bij de niet-slachtoffers (zowel zzp'ers als mkb'ers) omdat ze zouden willen dat de dader gepakt wordt. De belangrijkste reden om niet te melden, was in de meeste gevallen onder slachtoffers dat ze het zelf of met behulp van een andere partij hebben opgelost, terwijl de niet-slachtoffers voornamelijk niet zouden melden omdat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen.

Deel III Resultaten experts

8 Advisering van slachtoffers vanuit publieke en private organisaties

Om de onderzoeksvragen in deelstudie 3 over de advisering van slachtoffers vanuit verschillende publieke en private organisaties te beantwoorden, zijn tien interviews gehouden met experts werkzaam bij de politie, in de cybersecurity-industrie, in de wetenschap en bij Slachtofferhulp Nederland (zie paragraaf 3.2). Het doel van deze interviews was enerzijds om meer inzicht te krijgen in hoe verschillende organisaties slachtoffers adviseren te handelen bij een ransomware-incident, en anderzijds in hoeverre slachtoffers zich aan deze adviezen houden. Bovendien zijn de belangrijkste resultaten uit de deelstudies 1 en 2 voorgelegd aan de experts en is hun gevraagd hierop te reflecteren.

In dit hoofdstuk wordt allereerst geschetst hoe verschillende publieke en private organisaties slachtoffers van ransomware ondersteunen en adviseren te handelen, in hoeverre slachtoffers van ransomware deze adviezen opvolgen en hoe zich dit verhoudt tot de resultaten uit deelstudie 1 en 2 (paragraaf 8.1 en 8.2).[33] Daarnaast wordt beschreven wat de sterke en verbeterpunten zijn in deze ondersteuning van slachtoffers (paragraaf 8.3).[34]

8.1 Hulpbronnen en voorzieningen

Voor slachtoffers van ransomware zijn verschillende hulpbronnen en voorzieningen beschikbaar. Allereerst wordt op verschillende websites (zie bijv. Consumentenbond, n.d.; Digital Trust Center, n.d.-b; Fraudehelpdesk, n.d.; NCSC, n.d.; No More Ransom, n.d.-b) meer informatie gegeven over wat ransomware is en wat slachtoffers kunnen doen als ze getroffen zijn door ransomware. Dit varieert van praktische tips, zoals het verbreken van de netwerkverbinding, tot partijen waar slachtoffers contact mee op kunnen nemen, zoals de politie, een verzekeringsbedrijf, een cybersecuritybedrijf of computerdeskundige. No More Ransom biedt bovendien decryptors voor sommige ransomwarevarianten, waarmee slachtoffers zelf data kunnen ontsleutelen (No More Ransom, n.d.-a).

33 Omdat de resultaten van deelstudie 1 en 2 zijn voorgelegd aan de experts tijdens de interviews, volgt de vergelijking tussen deelstudie 1, 2 en 3 niet aan het einde van het hoofdstuk, zoals in voorgaande hoofdstukken het geval was, maar is dit geïntegreerd in paragraaf 8.2.

34 Omwille van de leesbaarheid zijn eventuele dubbele woorden verwijderd uit de citaten die in dit hoofdstuk verwerkt zijn.

Er zijn daarnaast partijen waar slachtoffers contact mee kunnen opnemen of melding kunnen doen van het incident. Deze partijen vervullen verschillende rollen, in verschillende fasen van het incident. Nadat slachtoffers voor het eerst geconfronteerd zijn met de versleuteling van hun gegevens als gevolg van de ransomware kunnen zij bijvoorbeeld contact opnemen met hun verzekering (indien van toepassing) voor incidenten- en juridische ondersteuning, of met een cybersecuritybedrijf of computerdeskundige voor ondersteuning bij herstel van de data of systemen. In deze fase of nadat een eerste beeld gevormd is van de omvang en ernst van het incident, kunnen slachtoffers het incident melden bij de politie voor informatievoorziening of andere ondersteuning, of de Fraudehelpdesk, tevens voor informatievoorziening of om doorverwezen te worden naar de juiste instantie(s). Organisaties die zijn getroffen door ransomware zijn daarnaast verplicht om een melding te maken bij de Autoriteit Persoonsgegevens indien sprake is van een datalek. Na het hoogtepunt van de crisis en eventueel herstel van de data of systemen kunnen slachtoffers bovendien een aangifte doen bij de politie of contact opnemen met Slachtofferhulp Nederland voor traumaverwerking of juridische ondersteuning.

Er kunnen dus diverse partijen een rol spelen bij de advisering van slachtoffers. In het vervolg van dit hoofdstuk zal dieper worden ingegaan op twee partijen die een belangrijke rol spelen in de advisering en ondersteuning van slachtoffers: cybersecuritybedrijven en de politie. In de volgende paragraaf beschrijven we hoe slachtoffers met deze partijen in contact komen en hoe de dienstverlening eruitziet, waarna dieper ingegaan wordt op hoe deze partijen slachtoffers van ransomware adviseren en ondersteunen als het gaat om onderhandelen, betalen en melden. Daarnaast wordt stilgestaan bij sterke en verbeterpunten in de ondersteuning van slachtoffers van ransomware.

8.1.1 *Cybersecuritybedrijven*

Vier respondenten hebben inzicht gegeven in de ondersteuning en advisering van slachtoffers van ransomware vanuit de cybersecuritysector. Eén respondent is werkzaam bij een belangenorganisatie voor de cybersecuritysector en drie experts zijn werkzaam bij verschillende cybersecuritybedrijven die dienstverlening verzorgen aan organisaties in Nederland en het buitenland. Onderdeel van de dienstverlening is onder andere monitoring, pentesting,[35] en *incident response*.[36] De focus in de interviews lag met name op dit laatste onderdeel.

Het varieert welk type organisatie klant is bij de cybersecuritybedrijven. Hoewel het vooral lijkt te gaan om grote organisaties van enkele honderden tot (tienduizenden)

35 Penetratietest, het controleren van computersystemen op kwetsbaarheden.
36 Het proces waarmee een organisatie omgaat met een incident na de gevolgen van een incident (Digital Trust Center, n.d.-a).

medewerkers, merken enkele experts op dat ze ook kleine of middelgrote organisaties hebben bijgestaan. Twee respondenten denken dat grotere organisaties sneller geneigd zijn om een cybersecuritybedrijf in te schakelen in verband met de grote impact van het incident en de kosten die verbonden zijn aan *incident response*. Volgens een respondent hebben dergelijke organisaties ook vaker een cyberverzekering, waarbij er contracten zijn met *incident response*-partijen. De respondenten schatten dat tussen de 40% en 60% van de incidenten waarvoor ze ingehuurd worden een ransomware-aanval betreft.

De ondersteuning van slachtoffers van ransomware door cybersecuritybedrijven bestaat uit verschillende facetten. Zoals een respondent beschrijft, is het doel om de getroffen organisatie 'zo snel mogelijk *up and running* te krijgen'. Volgens de cybersecurityexperts is de eerste stap vervolgens om in gesprek met het slachtoffer te verifiëren om wat voor type cyberincident het gaat, in kaart te brengen wat er gebeurd is en wat de ernst van het incident is. Er vindt forensische analyse plaats, waarbij onder andere onderzocht wordt hoe de daders binnen zijn gekomen, of er achterdeuren zijn geplaatst en of er data gestolen zijn. Ook wordt onderzoek gedaan naar de criminele groepering achter de aanval. Over sommige groeperingen hebben de cybersecuritybedrijven zelf al informatie of er is publieke informatie over beschikbaar. Aan de hand hiervan wordt meer inzicht verkregen in de modus operandi, maar bijvoorbeeld ook of er een mogelijkheid is om te onderhandelen over de hoogte van het losgeld (zie paragraaf 8.2.1).

De dienstverlening bestaat echter vaak uit meer dan alleen het herstellen van de systemen. Meerdere respondenten beschrijven dat het stressniveau en de onzekerheid zo hoog zijn dat klanten op hen leunen. Onderdeel van de dienstverlening kan dan ook zijn dat ze aan het slachtoffer uitleggen wat er gebeurd is en wat deze de komende tijd kan verwachten:

> *Dus die eerste week is het vooral zorgen dat je mensen bewust maakt van 'hé weet dat dit een marathon gaat zijn' en iemand zei laatst: 'het is een estafettemarathon'. Dus het is ook niet zo dat iedereen dezelfde tijd heel erg druk is (…) Maar het is wel een marathon, geen sprint. (R6, Cybersecurity)*

Ook kunnen ze met het slachtoffer stilstaan bij de communicatiestrategie, zowel intern als extern (bij eventuele media-aandacht) en zorgen dat er aandacht is voor fysiek en mentaal welzijn van medewerkers tijdens de crisis.

8.1.2 *Politie*

Vier van de experts zijn in verschillende functies werkzaam bij de politie en hebben kennis en ervaring met slachtofferschap van ransomware. Het varieert volgens deze respondenten welk type slachtoffer contact opneemt met de politie. Waar de cybersecuritybedrijven vooral te maken hebben met organisaties, kloppen bij de politie zowel

particulieren als ondernemers aan, hoewel een van de respondenten het beeld heeft dat de aangiftebereidheid lager is onder particulieren. De organisaties variëren van mkb tot grote organisaties, hoewel een respondent het vermoeden heeft dat kleinere bedrijven sneller contact opnemen met de politie, omdat ze 'iets meer met de handen in het haar zitten', en niet weten wat ze moeten doen. Daarentegen zullen veel middenbedrijven en grote organisaties zich volgens deze respondent eerst wenden tot een cybersecuritybedrijf.

Er zijn grofweg twee manieren waarop slachtoffers van ransomware bij de politie in beeld komen: 1) reactief, waarbij het slachtoffer contact met de politie opneemt; en 2) proactief, waarbij de politie zelf met het slachtoffer in contact komt.

Het slachtoffer kan op verschillende manieren zelf contact opnemen met de politie. Ten eerste kan het slachtoffer bellen (0900-8844). Ten tweede kan het slachtoffer langsgaan op een politiebureau. In dat geval wordt het slachtoffer geholpen door een basisteam. In het kader hiervan is er een vragenlijst gericht op ransomware ontwikkeld die het basisteam helpt om bij een melding van een slachtoffer de juiste vragen te stellen en de juiste informatie op te halen. Dit gaat bijvoorbeeld om technische indicatoren, hoeveel losgeld er is gevraagd, of het losgeld betaald is en of er schade is.[37] Het basisteam kan vervolgens met het cybercrimeteam contact opnemen voor ondersteuning. In dit verband benoemt een van de respondenten dat slachtoffers vaak geadviseerd wordt om niet zomaar langs te komen op het bureau, maar een afspraak te maken en aan te geven dat het om een technisch incident gaat, zodat er een digitaal specialist of iemand van het cybercrimeteam aanwezig kan zijn bij de afspraak. Voor particulieren is er daarnaast een derde optie om online aangifte te doen van ransomware.[38] Een van de respondenten merkt wel op dat het bij veel van de online aangiftes in werkelijkheid om andere typen cybercriminaliteit lijkt te gaan, zoals phishing of identiteitsfraude.

Daarnaast probeert de politie ook proactief met (potentiële) slachtoffers in contact te komen, om korte lijnen te hebben en te kijken of de politie ergens van betekenis kan zijn. Ten eerste houdt de politie *leak pages* van ransomwaregroeperingen en mediaberichtgeving in de gaten. Indien het om een Nederlandse organisatie gaat, wordt de juiste politie-eenheid geïnformeerd en gemotiveerd om contact met het slachtoffer op te nemen, hoewel een van de respondenten erbij vermeld dat dit niet altijd gebeurt. Daarnaast worden politiemedewerkers soms benaderd vanuit private partijen zoals cybersecuritybedrijven dat er er een slachtoffer is of dat er mogelijk een slachtoffer gaat vallen. Ook in dat geval wordt dit doorgezet naar de relevante politie-eenheid.

37 Zie ook https://www.politie.nl/binaries/content/assets/politie/onderwerpen/ransomware/checklist-aangifte-ransomwarebesmetting.pdf.

38 Indien het incident minder dan een jaar geleden is. Voor incidenten langer dan een jaar geleden wordt particulieren aangeraden om 0900-8844 te bellen.

De timing van het contact varieert. Sommige slachtoffers nemen aan het begin van het incident contact op, in sommige gevallen omdat ze niet weten wat ze moeten doen, maar meestal om de politie op de hoogte te houden. Daarnaast klopt een deel van de slachtoffers aan als het incident voorbij is. In dit verband kan er een onderscheid gemaakt worden tussen een melding of signaal, en een aangifte. Een melding of signaal is vooral bedoeld als kennisgeving dat een incident heeft plaatsgevonden en om informatie te delen met de politie die op dat moment cruciaal is. Een aangifte vindt meestal na afronding van het incident plaats en bevat meer informatie, zoals bijvoorbeeld een (forensisch) rapport. Vaak zijn dan pas ook de volledige schade en omvang van het incident duidelijk. Een melding of signaal in de beginfase leidt niet in alle gevallen tot een aangifte na afloop van het incident, beschrijft een van de respondenten. Daarom worden hier tegenwoordig bij een eerste signaal afspraken over gemaakt. Indien er uiteindelijk geen aangifte wordt gedaan, heeft de politie in dat geval de mogelijkheid om informatie te vorderen.

8.2 Advisering en ondersteuning van slachtoffers

In deze paragraaf wordt beschreven hoe cybersecuritybedrijven en de politie slachtoffers van ransomware adviseren en ondersteunen als het gaat om onderhandelen, betalen en melden. Daarnaast wordt beschreven hoe zich dit verhoudt tot de resultaten uit deelstudies 1 en 2 over daadwerkelijk en hypothetisch slachtofferschap van ransomware onder burgers en ondernemers. De belangrijkste uitkomsten uit deelstudie 1 en 2 met betrekking tot het onderhandelen, betalen en melden zijn voorgelegd aan de experts voor duiding.

8.2.1 *Communicatie/onderhandelen*

De experts maken een onderscheid tussen enerzijds *contact leggen* met de daders, en anderzijds *onderhandelen* over de hoogte van het losgeld.

8.2.1.1 *Contact leggen met daders*

Drie van de cybersecurity-experts geven aan dat vrijwel altijd vanuit hun organisaties geadviseerd wordt om contact op te nemen met de daders. De respondenten beschrijven dat dit in eerste instantie niet zozeer wordt gedaan om te onderhandelen over de losgeldeis, maar vooral om zoveel mogelijk informatie in te winnen, bijvoorbeeld of en welke data gestolen zijn. Dit kan bijvoorbeeld helpen bij het bepalen van de ernst of impact van het incident en het gefundeerd nemen van besluiten in het kader van vraagstukken zoals of het losgeld betaald moet worden, wat men moet met eventueel gestolen data, welke juridische gevolgen het heeft en welke communicatiestrategie passend is.

> *Voor veel organisaties is die hele aanval een soort van zwart gat (…) We liggen stil, we moeten nu weer herstellen, we zetten back-ups terug. Klaar. Ja, dat is te kort door de*

bocht. En de belangrijke stappen die wij in het begin zetten met de onderhandeling is echt beeld krijgen bij (…) welke informatie kunnen we allemaal loskrijgen om te zorgen dat zo'n board goede besluiten kan nemen? Dus in het begin is het ook helemaal geen onderhandeling. Het gaat eigenlijk puur over gesprek met, en band opbouwen met, om de informatie te verkrijgen die nodig is. (R6, Cybersecurity)

Contact opnemen met de daders kan daarnaast ook ingezet worden om tijd te winnen en om op de achtergrond te proberen om de systemen te herstellen.

Er wordt echter niet in alle gevallen contact opgenomen met de daders of onderhandeld. Een respondent beschrijft dat er slachtoffers zijn die vanuit principiële overwegingen niet onderhandelen. Daarnaast adviseert een cybersecuritybedrijf waar een van de respondenten werkzaam is volgens de respondent aan klanten om nooit contact op te nemen, te onderhandelen met daders of het losgeld te betalen omdat het betaalde losgeld door de ransomwaregroepering gebruikt kan worden voor nieuwe aanvallen. Zij assisteren zodoende ook niet in onderhandelingen. Wel is er vanuit dit bedrijf begrip voor de situatie waarin het slachtoffer niet anders kan en worden slachtoffers die overwegen om het losgeld te betalen, geadviseerd om contact op te nemen met een externe partner die de onderhandeling en eventuele betaling doet. In dit geval is het cybersecuritybedrijf dus geen onderdeel van het onderhandelingsproces, maar wordt het wel op de hoogte gehouden van eventuele informatie die door de daders in de communicatie wordt gegeven over de aanval, of als er overgegaan wordt tot betalen en er systemen ontsleuteld worden.

De politie-experts geven aan dat de politie geen actieve rol speelt in de communicatie of onderhandeling met daders, mede ingegeven door het standpunt van de politie om geen losgeld te betalen en hiermee criminaliteit te faciliteren (zie paragraaf 8.2.2). Onderhandelingen zullen volgens de respondenten altijd via een cybersecuritybedrijf of het slachtoffer zelf verlopen. Sommige politie-experts zien wel het belang in van contact opnemen met de daders, ongeacht of men overgaat tot betalen, bijvoorbeeld om tijd te rekken en om meer informatie te verkrijgen, wat tactisch ook voordelen heeft voor de opsporing vanuit de politie.

8.2.1.2 *Onderhandelen over de hoogte van het losgeld.*

Een tweede stap in het communicatieproces is vervolgens om te onderhandelen over de hoogte van het losgeld. Volgens cybersecurityexperts lukt het in de meeste gevallen om de losgeldeis te verlagen. Een complicerende factor kan wel zijn dat onderhandelingen met dezelfde ransomwaregroepering niet automatisch vergelijkbaar zullen verlopen, gezien men met verschillende *affiliates*[39] te maken kan hebben. Een van de respondenten duidt dit aan als het verschil tussen *affiliates* die snel geld willen verdienen en dus openstaan voor onderhandelingen, versus *affiliates* die beter snappen wat ze hebben geraakt en wat de impact is en als gevolg minder bereid zijn de prijs te verlagen.

39 *Affiliates* betreffen externe partners die de ransomware niet zelf ontwikkelen, maar kunnen 'huren' tegen een vergoeding of door een deel van de losgeldopbrengsten af te staan, en die de vervolgstappen in het delict uitvoeren, waaronder het versleutelen van de data.

8.2.1.3 *Vergelijking met deelstudie 1 & 2*

Hoewel meerdere respondenten in deelstudie 3 aangeven dat vaak geadviseerd wordt om contact op te nemen met de daders, is de bereidheid om contact op te nemen met de daders in zowel deelstudie 1 als deelstudie 2 laag. Wel valt op dat de intentie om contact op te nemen in deze deelstudies onder niet-slachtoffers hoger is dan onder slachtoffers, en iets hoger is onder ondernemers dan onder burgers. Waar het voornaamste motief voor burgers om contact op te nemen in deelstudie 1 was om te informeren over de hoogte van het losgeld, was dit bij de ondernemers om vast te stellen welke data zijn gestolen. Het voornaamste motief voor zowel burgers als ondernemers in deelstudie 2 was om vast te stellen of het losgeldbericht echt is. Hoewel in deelstudie 3 niet aan bod kwam dat slachtoffers contact opnemen met de daders om te informeren over de hoogte van het losgeld of vast te stellen of het losgeldbericht echt is, kwam wel naar voren dat het gebruikt wordt om vast te stellen welke data zijn gestolen.

Een opvallende uitkomst is bovendien dat de bereidheid om te onderhandelen laag is in deelstudie 1 en 2, terwijl uit deelstudie 3 blijkt dat dit regelmatig wordt gedaan en door cybersecuritybedrijven ook (vrijwel) altijd geadviseerd wordt. Waar een relatief klein percentage van de niet-slachtoffers in deelstudie 2 zou onderhandelen in een hypothetisch scenario, heeft in werkelijkheid geen enkele burger of zzp'er en slechts een paar van van de mkb'ers die slachtoffer werd in deelstudie 1 dit gedaan.

Experts dragen verschillende mogelijke verklaringen aan voor dit verschil. Ten eerste dat onderhandelen minder gebruikelijk is onder burgers, gezien bij dit type ransomware vaak sprake is van een vast prijsmodel en er geen mogelijkheid is tot onderhandelen. Dit type ransomware kenmerkt zich als 'veel slachtoffers voor weinig geld'. Ten tweede dat de zzp'ers en mkb'ers wellicht minder kennis en expertise in huis hebben om in te schatten wat er gebeurd is en wat de impact is. Dit beïnvloedt mogelijk de keuze om contact op te nemen met de daders. Ten derde dat het voor een kleine onderneming wellicht makkelijker is om te herstellen of de verliezen te accepteren, in vergelijking met grotere organisaties waar meer 'kapot' is en daardoor de druk hoger is om te betalen en dus te onderhandelen. Ook de belangen van medewerkers of klanten kunnen in deze beslissing een rol spelen. Een respondent beschrijft in dit verband dat hoe groter de ernst van het incident is, hoe groter de kans op onderhandelen is. Tot slot wijzen experts erop dat contact opnemen met een ransomwaregroepering geen vanzelfsprekendheid is. Dit vereist bijvoorbeeld enige affiniteit met ICT, begrip van hoe het dark web werkt, en verstand van gesprekstechnieken, iets wat bij de gemiddelde burger, zzp'er of mkb'er mogelijk niet aanwezig is.

Dus je moet snappen hoe het werkt en hoe je de stappen zet om op een veilige manier dat gesprek te kunnen voeren. Maar daarnaast, het is ook een vak. Dus op het moment dat jij zelf geraakt bent en je business ligt plat en je bent een bakker met een aantal vestigingen en je kunt niks. Ja, weet je, het stoom komt uit je oren, je bent boos, verdrietig, snapt er geen hout van. Ja, diep onder, dik onder stress. Niet het beste moment om een goede gespreksvoering te doen en goede besluiten te nemen. Dus je hebt daar ook een stukje ondersteuning en begeleiding bij nodig. Dus als je de weg al zou kunnen vinden en al zou weten hoe je dat gesprek moet aanknopen, het goede gesprek daarin voeren is dan de volgende uitdaging. (R6, Cybersecurity)

Organisaties die voornemens zijn te onderhandelen, zullen dan ook vaak de hulp inschakelen van een cybersecuritybedrijf. Niet elk slachtoffer heeft echter de middelen om een dergelijk bedrijf in te huren.

8.2.2 ***Betalen***

8.2.2.1 *Niet betalen, tenzij …*

Als het gaat om advisering met betrekking tot het betalen van het losgeld, hebben vrijwel alle partijen de uitgangspositie dat het beter is om het geëiste losgeld niet te betalen. Dit standpunt kent echter verschillende onderbouwingen.
De politie[40] motiveert het standpunt dat slachtoffers het losgeld niet moeten betalen vanuit het idee dat het ransomwarebusinessmodel in stand wordt gehouden:

Dat zit hem vooral erin omdat we ook zien (…) dat heel veel geld weer teruggaat naar volgende slachtoffers, dus wordt gebruikt voor de financiering van [het maken van] nieuwe slachtoffers. En het beeld is wel dat winstgevendheid waarschijnlijk het belangrijkste aspect is van ransomware waarom het er zoveel is. Dus als je die winstgevendheid kan verkleinen, hè, dus er wordt bijvoorbeeld minder betaald, er wordt minder vaak betaald, ja, dan kun je dat natuurlijk verlagen, zeg maar die winstgevendheid. En daardoor misschien ransomware. Dus daarom is dat politiestandpunt zo fel. Maar ja, het is wel zo dat als een slachtoffer aanklopt bij de politie, dat er ook begrip is voor de situatie van het slachtoffer. (R4, Politie)

Daarnaast benoemt een van de politie-experts dat betalen geen zaligmakende oplossing is omdat het herstel ook na het ontvangen van de decryptiesleutel tijd en moeite kost. '*Maar het is bijvoorbeeld niet zo dat je dan ja letterlijk het slotje van je netwerk afdoet en je aan de slag bent*' (R8). En hoewel onderdeel van het businessmodel van de daders is dat ze hun afspraken nakomen als het gaat om het aanbieden van een decryptiemogelijkheid na betaling, komen daders niet altijd hun afspraken na als het gaat om de gestolen data. Zo heeft de politie bij meerdere ransomwaregroeperingen geobser-

40 En in het verlengde daarvan andere partijen die dit advies hebben overgenomen, zoals Slachtofferhulp Nederland.

veerd dat gestolen data niet verwijderd worden na betaling, waardoor het risico blijft bestaan dat deze op een later moment nog gelekt of doorverkocht worden.

Dus [het slachtoffer] houdt heel erg vast, dat bedrijf, aan nou ja op het moment dat ik betaal, is die garantie er [dat data niet verkocht worden]. Ja, die garantie is er alleen maar in woord en wij hebben zeg maar ook wel kunnen zien dat dat wel gewoon door wordt verkocht [...] Op het moment dat je data gestolen is, dan is het ook gewoon weg en is er geen enkele mogelijkheid om dat meer tegen te houden. (R9, Politie).

De politie-experts geven echter wel aan dat er meer nuance achter het standpunt schuilgaat om niet te betalen, en dat er vanuit de politie begrip is voor de afweging om te betalen als het slachtoffer geen andere mogelijkheid ziet. Een van de respondenten stelt in dat kader wel dat het dan nog belangrijker is dat het slachtoffer deze informatie met de politie deelt.

Kijk, op het moment dat je ervoor kiest om wel te betalen, want dat is niet verboden, deel dan de informatie al helemaal met ons. Want dat is, ja, dat is echt cruciaal. En we zien ook in onze internationale onderzoeken dat we gewoon echt daarmee veel beter in staat zijn om de schade en de omvang en geld terug te vorderen en zo, dus ja, dat is echt wel erg belangrijk. (R8, Politie)

Ook in de cybersecuritysector is de uitgangspositie om niet te betalen. Meerdere respondenten benoemen echter tegelijkertijd dat ze situaties hebben meegemaakt waarbij betalen de enige optie was. In dergelijke gevallen wordt het uitgangspunt om zo min mogelijk betalen. Vanuit deze overweging wordt ook onderhandeld over de hoogte van het losgeld. De betalingspercentages variëren volgens de respondenten. Waar de ene respondent aanduidt dat in net geen 20% van de ransomware-incidenten het losgeld betaald is, wijzen andere respondenten op betalingspercentages van 30% tot 50% en schat een andere respondent dat vrijwel al hun klanten overgaan tot het betalen van het losgeld.

8.2.2.2 *Motieven van slachtoffers om (niet) te betalen*

Een van de respondenten omschrijft de keuze om te betalen als een kosten-batenafweging die mede afhangt van het cyberweerbaarheidsniveau bij aanvang van de aanval, maar ook van de complexiteit en de ernst van het incident. Verschillende motieven liggen volgens de experts ten grondslag aan de keuze om te betalen. Ten eerste wordt door politie en cybersecurityexperts benoemd dat slachtoffers overgaan tot betaling als de bedrijfscontinuïteit (te erg of te lang) verstoord is, of als niet betalen het einde van het bedrijf of faillissement betekent. Dit hangt mede af van het feit of slachtoffers backups beschikbaar hebben en deze niet geraakt zijn in de ransomware-aanval. Ten tweede is een belangrijke reden om over te gaan tot betaling van het losgeld om te voorkomen dat gevoelige data gepubliceerd worden, bijvoorbeeld op een *leak page*. Hierbij benoemen cybersecurityexperts dat het feit dat er data zijn gestolen door de daders de door-

slag kan geven om het losgeld te betalen, zelfs in gevallen waarin men kan herstellen met back-ups.

> *Dus de bescherming van informatie, van klanten en van je personeel, waarvan men niet wil dat die op het darkweb gaan rondslingeren. Dus dat is een, dat is een overweging. En ja, een andere overweging is ook van ja, zeker als het, als tijd een rol begint te spelen, en dat zie je met name ook bij organisaties die wat meer op productie gericht zijn in plaats van op data gericht zijn, dat elke dag (…) dat ze stilstaan, dat dat gewoon in de klauwen begint te lopen. Dus dat kunnen zeker hele goede redenen zijn om alsnog, om wel te betalen. (R2, Belangenorganisatie cybersecurity)*

> *Maar het risico wat je dan loopt, is dat je niet betaalt en natuurlijk eigenlijk altijd wel die data op dark web wordt gezet. Wat weer verkocht kan worden en weer gebruikt kan worden in de toekomst voor een andere malafide handeling. (R7, Cybersecurity)*

Enkele politie-experts denken daarnaast dat voor een kleine groep het 'sneller up and running zijn' of het versnellen van het proces een doorslaggevende factor is, terwijl er in dergelijke gevallen wel back-ups beschikbaar zijn.

Omgekeerd is een belangrijk motief om niet te betalen dat het slachtoffer kan herstellen van back-ups. Bovendien kan een rol spelen dat slachtoffers vanuit principiële overweging niet willen betalen of het onethisch vinden. Meerdere respondenten plaatsen hierbij wel de kanttekening dat het altijd makkelijk is om het betalen van losgeld onethisch te vinden, totdat je geen mogelijkheid hebt om te herstellen na een ransomware incident.

> *Want het is ook ethisch ingewikkeld om wel te betalen aan criminelen. En zeker omdat de criminelen hierin ook steeds, ze voelen zich onaantastbaar dus ze worden steeds een beetje rijker en steeds een beetje, daardoor ook steeds meer mag. Dat is niet wat je wil promoten. (…) Dus daar de balans in vinden tussen: in hoeverre is ethisch een belangrijke drijfveer, ja, absoluut, maar soms blijkt er gewoon geen andere oplossing te zijn. (R6, Cybersecurity).*

Daarnaast kan ook van belang zijn welke data gestolen zijn omdat niet alle data even essentieel of privacygevoelig zijn.

Sommige experts constateren dat de betalingsbereidheid de afgelopen jaren lijkt te zijn afgenomen. Volgens deze respondenten zijn slachtoffers sneller geneigd om bestanden te herstellen vanaf een back-up of op een andere wijze, of weigeren ze te betalen. Steeds meer organisaties lijken principieel tegen betalen te zijn en willen geen onderdeel uitmaken van het ransomwareverdienmodel. Aan de andere kant vermoedt een van de experts van de politie dat in de maatschappij het betalen van losgeld steeds meer is genormaliseerd. Hij stelt:

> *Ik denk wel echt dat helaas het feit dat we zo lang dat dit al speelt en dat het in het nieuws is (…), dat het wel toch veiliger is geworden om te betalen. En het is belangrijk dat we (…) met elkaar over ransomware en slachtofferschap praten. (…) Ik wil niet elke keer discussies hebben over wel of niet betalen, maar we moeten wel met z'n allen kritisch zijn op de situatie zoals die voorligt. Dat het echt een soort last-ditch effort [een laatste poging] zou kunnen zijn en dat het niet een kwestie is van oh ja, weet je, ja, het is een soort van cost of doing business en we moeten onze IT-systemen updaten en nou dit betalen we en dan gaan we over tot de orde van de dag. (R8, Politie)*

Tussen het bereiken van overeenstemming over het doen van en de hoogte van de losgeldbetaling en de uiteindelijke decryptie vinden nog een aantal handelingen plaats, aldus de cybersecurityexperts. Een respondent beschrijft dat het cybersecuritybedrijf de losgeldeis in euro's op de rekening krijgt van het slachtoffer. Het cybersecuritybedrijf betaalt vervolgens aan een bitcoinbroker, en deze broker verhandelt de bitcoins met de groepering. Vervolgens ontvangt het cybersecuritybedrijf van de ransomwaregroeperingen de decryptiesleutel(s). Bovendien beschrijft een respondent dat het vanuit juridisch oogpunt van belang is om te onderzoeken of het niet gaat om betaling aan een partij die op een sanctielijst staat.[41, 42] Als het slachtoffer eenmaal betaald heeft en de decryptiesleutel is ontvangen, zijn er dagen nodig voor het herstel. Een respondent beschrijft bijvoorbeeld dat vaak 'het nodige kapot is' als gevolg van de aanval, en andere respondenten duiden erop dat alles (i.e. infrastructuur en softwareapplicaties) schoongemaakt moet worden, bijvoorbeeld van eventuele *backdoors* die een cybersecurityrisico inhouden.[43] Slachtoffers worden bovendien geadviseerd om maatregelen te nemen om de beveiliging te verbeteren. Een respondent beschrijft dat hier een bepaald '*opportunity window*' voor is.

> *Als je daar te lang mee wacht, of laten we zeggen twee weken nadat de crisis voorbij is, dan zie je dat extreem wegnemen, die kansen, om dat nog voor mekaar te krijgen. Want ja, alles werkt weer en iedereen gaat wat, valt gewoon weer in de naïeve wereld waar ze al inzaten (…) Maar het is heel bijzonder om te zien soms dat als het dan een paar weken na dat incident is, dat die bereidheid om te investeren in cybersecurity wel echt, ja, gewoon terugvalt. Wat gek is, want ze zitten dan gewoon weer op hetzelfde punt als waardoor het probleem in eerste instantie is ontstaan. (R3, Cybersecurity)*

41 Op de sanctielijst staan personen, organisaties, regimes of landen waartegen sancties gelden, zoals financiële sancties of handelsbeperkingen. Het niet naleven van de sanctielijst is strafbaar.

42 Recentelijk heeft de EU zes individuen gesanctioneerd die verantwoordelijk zijn voor cyberaanvallen, waaronder ransomware-aanvallen. Als gevolg zijn de tegoeden van deze individuen in de EU bevroren, is inreizen niet toegestaan en is samenwerken en (indirect) zakendoen met deze individuen verboden voor burgers en bedrijven in de EU (Rijksoverheid, 2024).

43 Een backdoor wordt door cybercriminelen geplaatst op een systeem om op een later moment toegang te verkrijgen en hiermee dus de beveiliging te omzeilen.

8.2.2.3 *Vergelijking met deelstudie 1 & 2*

De bereidheid om het losgeld te betalen is relatief laag in zowel deelstudie 1 als deelstudie 2. Deze resultaten contrasteren met de resultaten van deelstudie 3 als het gaat om het betalingspercentage. Hoewel altijd het uitgangspunt is om niet te betalen, en dit ook actief wordt uitgedragen door bijvoorbeeld de politie, geven cybersecurityexperts aan dat een groter aandeel van de slachtoffers betaalt. Een mogelijke verklaring die door de experts in deelstudie 3 is aangedragen, is dat de doelgroepen uit deelstudie 1 en 2 wellicht minder snel een cyberverzekering hebben dan de organisaties die bij de cybersecuritybedrijven aankloppen, en daardoor minder geneigd zijn te betalen. Uit deelstudie 1 en 2 blijkt ook dat een minderheid van de zzp'ers en mkb'ers verzekerd is voor cyberincidenten. Daarnaast wijzen de experts erop dat deze doelgroepen mogelijk een minder grote impact ervaren of dat de lagere betalingsbereidheid het gevolg is van de tevens lage onderhandelingsbereidheid onder deze doelgroep.

Waar het voornaamste motief voor burgers om te betalen in deelstudie 1 was dat ze erop vertrouwden dat de toegang hersteld zou worden na betaling, was dat in deelstudie 2 omdat ze aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen. Het voornaamste motief voor ondernemers om te betalen was onder slachtoffers dat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen en onder niet-slachtoffers dat het betalen van het losgeld goedkoper zou zijn dan geen zaken kunnen doen. Zowel de burgers in deelstudie 1 als 2 zouden niet betalen omdat ze vertrouwden dat de toegang hersteld zou worden na betaling. De ondernemers in deelstudie 1 en 2 zouden niet betalen omdat het onethisch is om te betalen of omdat ze een back-up hadden. In grote lijnen komen deze uitkomsten overeen met deelstudie 3. Door experts werd bijvoorbeeld genoemd dat slachtoffers overgaan tot betaling als de bedrijfscontinuïteit (te erg of te lang) verstoord is, wat mede afhankelijk is van de beschikbaarheid van back-ups. Daarnaast is volgens experts een belangrijke reden om niet te betalen dat slachtoffers kunnen herstellen van een back-up, en speelt bij sommige slachtoffers dat ze uit principe niet betalen. In tegenstelling tot deelstudie 1 en 2, lijkt in deelstudie 3 de dreiging van het lekken van data een grotere rol te spelen in de keuze om wel of niet te betalen. De dreiging van lekken kan een rol spelen in de beslissing om te betalen, maar kan volgens experts ook afhangen van hoe gevoelig de gestolen data zijn. Aan de andere kant benoemt een andere expert dat door organisaties in eerste instantie vaak luchtig gedacht wordt over gestolen data. Ook dat zou bij de respondenten in deelstudie 1 en 2 een rol kunnen spelen in hun beslissingsprocessen.

In deelstudie 2 kwam bovendien naar voren dat de betalingsbereidheid voor burgers gerelateerd is aan de hoogte van het losgeld, dreigen met lekken en advies om te betalen, voor zzp'ers gerelateerd is aan het niet hebben van een back-up en advies om te betalen en voor mkb'ers gerelateerd is aan de hoogte van het losgeld en advies om te betalen. Met betrekking tot het advies om te betalen wijzen meerdere respondenten erop dat dit een logisch verband is, gezien slachtoffers in crisis zitten na een ransomware-incident en ze varen op de expertise en het advies van de *incident response*-partij

die ze inhuren. Zoals in deelstudie 3 ook aan bod kwam, wordt echter alleen geadviseerd om te betalen indien men geen andere oplossing ziet. Een politie-expert benadrukt dat het wel belangrijk is dat alle partijen die zich bezighouden met ransomware hierin de dialoog blijven aangaan waarom geadviseerd wordt om te betalen en of er mogelijkheden tot iets anders zijn. Om de betalingsbereidheid te verlagen, wijzen experts daarnaast op oplossingen als ondersteuning of subsidie vanuit de overheid om te herstellen van een aanval zonder het losgeld te betalen, meer informatievoorziening over preventieve maatregelen of veranderingen in de verzekeringssector.

8.2.3 ***Melden***

8.2.3.1 *De rol van de politie*

Het advies om een melding of aangifte te doen bij de politie wordt door de politie gemotiveerd vanuit het idee dat ze er niet alleen zijn 'om boeven te vangen', zoals vaak gedacht wordt, maar ook voor interventies aan de voorkant.

> *Dat is wel ook wat wij ook proberen aan te geven van doe vooral aangifte (…) Maar, en dat klinkt misschien wat paradoxaal (…) verwacht niet dat we een dag later met dertien mensen aan jouw zaak gaan werken. Maar we zijn continu met ransomware bezig en afhankelijk van wat dus de situatie is of welk, ja, of er een lopend onderzoek is of het is een ja, een grote organisatie met een bepaald belang die geraakt wordt, ja, dan wordt daar echt wel naar gekeken (R8, Politie).*

Een melding of aangifte is belangrijk voor prioritering, het beschermen van de maatschappij en het voorkomen van toekomstige slachtoffers.

> *Op het moment dat het niet gemeld wordt bij de politie, kan het ook zijn dat wij de verkeerde prioriteiten stellen, omdat we het niet zo vaak zien. Als het nooit wordt gemeld (…) gaan we er ook geen aandacht aan besteden, want we weten niet dat het gebeurt. (R10, Politie)*

Tegelijkertijd kan de politie bij een melding ook iets betekenen voor slachtoffers. Hierbij kan gedacht worden aan het delen van kennis over de ransomwaregroepering, maar soms ook het aanbieden van decryptiemogelijkheden, speciale bevoegdheden zoals het tappen van de infrastructuur van slachtoffers of gestolen data van de servers van de groepering halen, en in enkele gevallen het traceren van het betaalde losgeld. Voorbeelden van politieacties zijn het neerhalen van de website van Lockbit en het beschikbaar stellen van een decryptor, het terughalen van het losgeld dat betaald werd door de Universiteit Maastricht en het verkrijgen van decryptiesleutels van de Deadbolt-ransomware door een truc met de betaling.

Een van de politie-experts benadrukt dat de cybersecuritybedrijven een belangrijke rol spelen in de keuze om de politie erbij te betrekken. De cybersecurityexperts duiden

aan dat altijd aan slachtoffers geadviseerd wordt om melding van het ransomware-incident te doen bij de politie, hoewel een van de respondenten benoemt dat het een zoektocht is naar het juiste moment om de melding te doen. De eerste prioriteit van de cybersecuritybedrijven is immers het herstel van de klant, terwijl dit voor de politie opsporing is. Het advies om melding te doen wordt door cybersecuritybedrijven op verschillende wijzen naar slachtoffers toe gemotiveerd. Aan de ene kant wordt het vanuit een maatschappelijk, altruïstisch oogpunt gemotiveerd. Hierbij kan gedacht worden aan het veiliger maken van de maatschappij, het verhogen van de cyberweerbaarheid en voorkomen dat het een ander overkomt. Slachtoffers wordt ook gewezen op het feit dat het delen van informatie de politie helpt om inzage te geven in hoe vaak ransomware voorkomt, prioriteiten te stellen en bovendien helpt om op nationaal en internationaal vlak 'puzzelstukjes' bij elkaar te leggen in de aanpak van ransomware. Een van de respondenten wijst hierbij op het voorbeeld van Lockbit, waarbij dankzij informatieverstrekking en internationale samenwerking recentelijk een *affiliate* is opgepakt en de website van de ransomwaregroepering is overgenomen door de politie. Aan de andere kant wijst een van de respondenten erop dat ze slachtoffers ook uitleggen dat het voor het slachtoffer wellicht ook nog iets kan opleveren als de politie een onderzoek start en noemt hierbij de Universiteit van Maastricht als voorbeeld.

Een deel van de cybersecurityexperts heeft het beeld dat de meeste slachtoffers het advies opvolgen om melding bij de politie te doen, hoewel een van de respondenten de kanttekening plaatst dat ze er vanuit het cybersecuritybedrijf op moeten aandringen omdat klanten er niet altijd aan denken om voor slachtofferschap van cybercrime aangifte te doen. Een andere respondent denkt echter dat niet altijd aangifte wordt gedaan ondanks dat dit door hen wordt geadviseerd.

8.2.3.2 *Motieven van slachtoffers om (niet) te melden bij de politie*

Volgens de experts is een belangrijke reden voor slachtoffers om het ransomware-incident te melden ten eerste dat ze dit doen vanuit maatschappelijk oogpunt. Ze zien het bijvoorbeeld als hun plicht of als goed burgerschap, willen informatie delen met de politie of willen de maatschappij veiliger maken. Ten tweede doen een aantal slachtoffers melding omdat ze niet weten wat ze moeten doen en/of hopen dat de politie nog iets kan betekenen op korte of lange termijn. Ten derde is aangifte soms vereist in het kader van de verzekering. Tot slot denken sommige slachtoffers dat melden verplicht is.

De belangrijkste motieven om geen melding te maken zijn daarentegen ten eerste dat voor slachtoffers onvoldoende duidelijk is wat het hun kan opleveren, ze het nut er niet van inzien of het gevoel hebben dat de politie niks doet. Een van de respondenten beschrijft dat in het kader hiervan meer aan informatievoorziening gedaan kan worden:

> *Ik [het slachtoffer] zit op dat moment in crisis. Ik heb er nog nooit van tevoren over nagedacht en nu komen deze externen, zoals wij, die zeggen jij moet aangifte doen van dit en dat. Maar dat is te veel voor mij om over na te denken (…) Wat gaat het mij opleveren als ik aangifte doe? Want ik heb genoeg te doen om mijn organisatie te redden op dat moment, dus daar ben ik liefst zelf helemaal niet mee bezig als het niet belangrijk genoeg is. Dus dat moet veel toegankelijker worden. (R3, Cybersecurity)*

Ten tweede is een motivatie om niet te melden dat slachtoffers het incident geheim willen houden:

> *'Veel van deze slachtoffers, ook vanwege schaamte, reputatie, angst voor [Autoriteit Persoonsgegevens], nou, noem allemaal maar op, maken een bewuste keuze om het zoveel mogelijk onder de pet te houden' (R2, Belangenorgainsatie cybersecurity).*

In het kader hiervan beschrijft een van de experts van de politie dat veel slachtoffers ook niet genoemd willen worden in een rechtszaak als er vanuit de politie onderzoek wordt gedaan of een verdachte wordt aangehouden, om naamsbekendheid te voorkomen. Een manier om de meldingsbereidheid te verhogen zou volgens een van de experts dan ook kunnen zijn om afgeschermde aangiftes mogelijk te maken, waarbij voor slachtoffers op voorhand duidelijk is dat hun naam niet bekend wordt gemaakt.

Ten derde vermoeden de politie-experts dat het standpunt van de politie om het losgeld niet te betalen, slachtoffers niet motiveert en misschien zelfs weerhoudt om het incident te melden. Een van de respondenten beschrijft dit als 'een lastig schouwspel', waarbij de politie enerzijds adviseert om niet te betalen, maar anderzijds wel vraagt om het te melden als je toch overgaat tot betalen.

> *Daar is natuurlijk heel lastig dat als jij het gevoel hebt van ik moet betalen en de politie is zo fel tegen, dat je dan misschien toch bang bent dat de politie daar jou verantwoordelijk voor houdt of dat het vervelende consequenties voor je gaat hebben. (R4, Politie).*

Ten vierde is het volgens experts niet gemakkelijk om aangifte te doen, en weerhoudt de tijd en moeite die het kost slachtoffers mogelijk hiervan. Ten vijfde kan een rol spelen dat slachtoffers zichzelf niet dusdandig als 'slachtoffer' identificeren, normaliseren dat het er nou eenmaal bij hoort, of er geen verder gevolg aan willen geven als een coping mechanisme. Tot slot zouden onbekendheid met voorzieningen een rol kunnen spelen.

8.2.3.3 *Vergelijking met deelstudie 1 & 2*

Hoewel in deelstudie 2 de meldingsbereidheid in het hypothetische scenario hoog is, blijkt dit niet het geval onder de respondenten in deelstudie 1 die slachtoffer zijn geworden van ransomware. Zowel de meldingsbereidheid als de aangiftebereidheid is het laagst onder zzp'ers en het hoogste onder mkb'ers. Dit contrasteert met de inschatting van de cybersecurityexperts in deelstudie 3 dat in veel gevallen wel melding wordt ge-

maakt bij de politie, maar lijkt wel overeen te komen met het beeld dat de politie van de meldingsbereidheid heeft. Het verschil in meldingsbereidheid tussen burgers, zzp'ers en mkb'ers zou volgens een van de politie-experts mogelijk verklaard kunnen worden vanuit het feit dat mkb'ers een grotere impact ervaren, en daardoor ook sneller geneigd zijn om het incident te melden.

Onder de niet-slachtoffers was bij zowel burgers als ondernemers de voornaamste reden om te melden bij de politie dat ze zouden willen dat de dader gepakt wordt. Onder de slachtoffers was de voornaamste reden van burgers om te melden tevens dat ze wilden dat de dader gepakt wordt, terwijl de ondernemers wilden voorkomen dat het bij een ander gebeurt. Dit laatste is in overeenstemming met de motieven die in deelstudie 3 naar voren kwamen, waaronder vanuit maatschappelijk oogpunt en omdat slachtoffers hopen dat de politie iets kan betekenen. Een van de politie-experts plaats bij deze uitkomst wel de kanttekening dat hij hoopt dat men in de toekomst niet zozeer contact opneemt met de politie omdat ze willen dat de dader gepakt wordt, wat complex is voor cyberdelicten, maar dat men dat doet omdat de politie op andere wijzen kan helpen en vanuit maatschappelijk belang.

De voornaamste reden om niet te melden was bij alle groepen slachtoffers dat ze het zelf of met behulp van een andere partij hebben opgelost, terwijl dit onder niet-slachtoffers zou zijn omdat het geen zin heeft daar de politie er toch niets aan zou doen. Dit is in overeenstemming met de uitkomsten van deelstudie 3, waaruit blijkt dat voor slachtoffers onvoldoende duidelijk is wat melden hun kan opleveren, ze het nut er niet van inzien, of het gevoel hebben dat de politie niks doet.

Daarnaast kwam uit de resultaten naar voren dat zowel de slachtoffers als niet-slachtoffers het eens zijn met het standpunt van de politie om het losgeld niet te betalen. Tegelijkertijd geeft 20% tot 30% van de respondenten die slachtoffer zijn geworden van ransomware aan dat dit standpunt van de politie hen ervan heeft weerhouden om contact op te nemen met de politie. Dit is in overeenstemming met de inzichten van de politie-experts in deelstudie 3. Een van de politie-experts reflecteert dat dit impliceert dat het advies mogelijk averechts werkt, omdat het slachtoffers niet gaat weerhouden om te betalen op het moment dat ze die optie overwegen, maar ze wel weerhoudt om het te melden bij de politie. In dat kader stelt de expert dat de nadruk vanuit de politie wellicht minder moet liggen op het wel of niet betalen, maar op andere dingen, zoals het belang van melden bij de politie. Een andere expert oppert dat mogelijk nog beter benadrukt kan worden dat het betalen van het losgeld niet tot een oordeel leidt vanuit de politie, en dat ook bij betaling een melding bij de politie van belang is.

8.3 Sterke- en verbeterpunten in de ondersteuning van slachtoffers

Met respondenten is ook gesproken over wat goed gaat en waar nog ruimte voor verbetering is in de ondersteuning van slachtoffers van ransomware. Meerdere respon-

denten hebben benoemd dat de onderlinge samenwerking en informatiedeling tussen partijen verbeterd is. Respondenten wijzen bijvoorbeeld op Project Melissa, een samenwerkingsverband tussen publieke en private partijen (o.a. Openbaar Ministerie, NCSC, Cyberveilig Nederland en cybersecuritybedrijven) waarbij informatie wordt uitgewisseld over ransomware-aanvallen (NCSC, 2023). Die uitwisseling van informatie gebeurt op verschillende wijzen. Zo worden de betrokken cybersecuritybedrijven gevraagd om maandelijks anoniem informatie aan te leveren, onder andere over of er ransomware-aanvallen geweest zijn bij klanten, of er betaald is, en in welke sector het was. Daarnaast zijn er meerdere keren per jaar bijeenkomsten waarin informatie gedeeld wordt over wat er op dat moment speelt of wat nieuwe ontwikkelingen zijn in het landschap. Een keer per jaar staat bovendien een onderwerp centraal, zoals onderhandelingen. Het delen van informatie heeft er recentelijk nog toe geleid dat slachtofferschap van de Cactus-ransomware voorkomen werd bij organisaties in binnen- en buitenland (Digital Trust Center, 2024).

Meerdere respondenten wijzen er tegelijkertijd op dat er nog ruimte voor verbetering is in de samenwerking op het gebied van ransomware.

> *Een vangnet is zo sterk als de grootste maas. En ik denk dat we nu nog heel vaak als diverse partijen te wijd, te ver van elkaar georganiseerd zijn, waardoor mensen letterlijk door de maas van het net heen glippen. (R1, Slachtofferhulp)*

> *Ik denk dat het voor in zijn algemeenheid echt wel fijn zou zijn dat we meer als maatschappij tegen de crimineel optrekken, zeg maar. Dus zowel vanuit het slachtoffer als vanuit incident response als vanuit NCSC, politie, Autoriteit Persoonsgegevens hè, de hele keten die erbij hoort, zeg maar. Dat dat een hoop zou kunnen helpen. Ja, wij tegen de crimineel, zeg maar, of tegen het probleem, in plaats van ieder zijn eigen dingetje en daarvoor strijden. (R8, Politie)*

Daarnaast wijzen enkele respondenten erop dat een goede ontwikkeling is dat er meer aandacht is gekomen voor de impact van slachtofferschap van cybercriminaliteit. Deze respondenten noemen als voorbeeld een initiatief bij de politie in Oost-Nederland, waarbij de politie ook ter plaatse komt bij meldingen van gedigitaliseerde criminaliteit. Tot voor kort gebeurde dit alleen voor traditionele vormen van criminaliteit. De politie biedt hiermee een luisterend oor en emotionele steun, iets waar slachtoffers van cybercriminaliteit veel behoefte aan hebben volgens een van de respondenten. Een van de respondenten denkt daarnaast dat het de drempel verlaagt voor het slachtoffer om contact op te nemen met de politie. Een van cybersecurityexperts wijst er ook op dat er in de afgelopen jaren meer aandacht is gekomen voor de impact van cybercriminaliteit binnen Slachtofferhulp Nederland. Zij hebben bijvoorbeeld korte lijntjes met Slachtofferhulp Nederland zodat ze een slachtoffer van ransomware kunnen doorverwijzen als er geen hulpbronnen zijn binnen de getroffen organisatie of in de omgeving. De dienstverlening van Slachtofferhulp Nederland is niet toegespitst op slachtoffers van ransom-

ware of cybercriminaliteit. Wel is volgens een respondent van Slachtofferhulp Nederland het reguliere dienstverleningsaanbod beschikbaar, waaronder psychosociale ondersteuning (i.e. werken aan stressreductie) of juridische dienstverlening (ondersteuning bij het strafproces als een verdachte is aangehouden).

Tegelijkertijd wijzen respondenten erop dat er nog winst te behalen valt in de positie en ondersteuning van het slachtoffer. Ten eerste stellen meerdere respondenten dat slachtoffers van ransomware nog onvoldoende als slachtoffer gezien worden. Er heerst onder slachtoffers veel schaamte en angst voor oordelen vanuit de maatschappij, mede vanwege *victim blaming*. Een respondent vermoedt dat met een verandering hierin veel van de andere problemen rondom informatiedeling verdwijnen. Ten tweede blijft de impact van een ransomware-incident, ondanks ontwikkelingen in de keten, nog onderbelicht. Er mag meer ondersteuning komen voor de fysieke en mentale gevolgen. Dit kan vanuit de overheid, maar volgens een respondent is hier ook een rol weggelegd voor de cybersecuritysector. Dergelijke nazorg zou bovendien ook tot nieuwe inzichten kunnen leiden voor preventie, aldus twee respondenten. Een andere respondent stelt dat het in dit verband een goede ontwikkeling zou zijn om de ervaringen van slachtoffers van ransomware (bijv. hoe ze omgegaan zijn met het ransomware-incident en hoe men kan voorkomen dat ze in dezelfde situatie komen) meer te delen, omdat dit mogelijk meer impact heeft in de maatschappij dan informatievoorziening vanuit de overheid.

Er is daarnaast nog ruimte voor verbetering in de ondersteuning vanuit de politie. Ten eerste blijkt uit vrijwel alle interviews dat onvoldoende duidelijk is wat de rol van de politie is en wat de politie kan betekenen bij slachtofferschap van ransomware. Twee respondenten wijzen erop dat de politie in het kader hiervan meer aan informatievoorziening kan doen.

> *Ja en ik denk dat wel belangrijk is om dan wel heel duidelijk aan te geven waarom. Waarom is die aangifte van belang? (…) Met allerlei andere landen kunnen we dit aanpakken, maar daar hebben we wel informatie voor nodig. Op het moment dat wij geen informatie hebben, hebben we ook niks om op te sporen (…) Wel degelijk gebeurt er iets, alleen niet met individuele basis en dat is belangrijk, om dat verschil uit te leggen denk ik aan de maatschappij. (R9, Politie)*

Hierbij is het van belang om aan verwachtingsmanagement te doen van wat wel en niet mogelijk is vanuit de politie. Daarnaast denken enkele respondenten dat de politie meer kan communiceren over concrete acties, zoals bij Lockbit of Deadbolt gebeurde. Meerdere politie-experts plaatsen hierbij wel de kanttekening dat men hierbij altijd een balans moet zoeken omdat ze geen informatie willen vrijgeven die in het voordeel van de ransomwaregroepering werkt. Ten tweede kunnen de processen verbeterd worden. Hoewel de politie hier wel al mee bezig is, wijzen politie-experts erop dat het proces van melding of aangifte verbeterd kan worden. Zo is het momenteel nog niet mogelijk

voor bedrijven om online aangifte te doen en kan de online aangifte in het algemeen verbeterd worden omdat slachtoffers soms ten onrechte melding maken van een ander delict dan ransomware. Uit andere expertinterviews bleek bovendien dat de tijd en moeite die aangifte doen (ook op het bureau) kost, een drempel is om contact op te nemen met de politie. En ook in de terugkoppeling aan slachtoffers na een melding is ruimte voor verbetering volgens een respondent, hoewel dit wel al gebeurd, bijvoorbeeld als er een decryptor beschikbaar komt. Tot slot wijzen enkele respondenten erop dat een meldplicht de informatiepositie van de politie zou kunnen verbeteren. Een van deze respondenten denkt bovendien dat een dergelijke meldplicht ook invloed zou kunnen hebben op de betalingsbereidheid.

> *Sowieso zou ik een meldplicht heel erg fijn vinden, waarbij technische informatie gedeeld wordt en ook metadata (…) Als je gewoon weet als land, hé, deze sectoren worden geraakt op deze varianten en ja, zo vaak wordt er betaald en dit wordt er betaald en dit zijn aanvullende gegevens over die betaling (…) Ja, dat zou het echt de aanpak en de prioritering denk ik, echt wel wezenlijk kunnen veranderen (…) En zeker ook als bijeffect hebben op het moment dat je betaalt, dat je dan ja meldplicht hebt, zeg maar net als met de Autoriteit Persoonsgegevens met bijvoorbeeld (…) een boete of iets in de richting of een soort afdwingmiddel, nou, dan denk ik dat men misschien ook net iets wat harder nadenkt alvorens te gaan betalen. Maar hoe dan ook, het belangrijkste is dat we daarmee dus veel meer concrete informatie krijgen om onderzoek te kunnen doen. (R8, Politie)*

9 Conclusie en discussie

In de afgelopen jaren zijn ransomware-aanvallen in hoeveelheid en professionalisering toegenomen, met een financiële, fysieke, of maatschappelijke impact als gevolg. Tot op heden is er echter nog weinig bekend over de prevalentie van slachtofferschap van ransomware onder burgers en ondernemers en welke beslissingen zij nemen omtrent onderhandelen, betalen en melden als ze slachtoffer worden. Het huidige onderzoek heeft dan ook als doel om meer inzicht te verkrijgen in slachtofferschap van ransomware onder Nederlandse burgers, zzp'ers en mkb'ers, en aanknopingspunten te bieden voor de aanpak. Aan de hand van drie deelstudies is de volgende probleemstelling beantwoord:

> *Hoe vaak worden Nederlandse burgers en bedrijven slachtoffer van ransomware, hoe reageren zij met betrekking tot onderhandelen, betalen en melden en hoe verhoudt dit zich tot de adviezen van publieke en private organisaties die slachtoffers van ransomware ondersteunen?*

In deelstudie 1 is meer inzicht verkregen in de prevalentie van slachtofferschap van ransomware onder burgers (n=20.659), zzp'ers (n=2.077) en mkb'ers (n=1.963). Daarnaast is meer inzicht verkregen in de aard en impact van slachtofferschap aan de hand van een vragenlijst onder burgers (n=856), zzp'ers (n=88) en mkb'ers (n=100) die slachtoffer van ransomware zijn geworden. In deelstudie 2 is meer inzicht verkregen in de factoren die bijdragen aan de bereidheid tot het betalen van losgeld en het melden van het incident aan de hand van een vragenlijst met een vignetexperiment (fictief ransomwarescenario) onder burgers (n=4.082), zzp'ers (n=1.769) en mkb'ers (n=732) die *niet* eerder slachtoffer zijn geworden van ransomware. In deelstudie 3 is aan de hand van expertinterviews (n=10) meer inzicht verkregen in de hoe politie, cybersecurityexperts en andere organisaties slachtoffers adviseren te handelen in het geval van ransomware, en in hoeverre slachtoffers deze adviezen opvolgen.

In paragraaf 9.1 worden de resultaten van het onderzoek besproken met betrekking tot de prevalentie, aard en impact van slachtofferschap van ransomware (paragraaf 9.1.1), onderhandelen (paragraaf 9.1.2), betalen (paragraaf 9.1.3), en melden (paragraaf 9.1.4) en wordt een antwoord gegeven op de deelvragen per thema. In paragraaf 9.2 wordt stilgestaan bij de belangrijkste conclusies en implicaties (paragraaf 9.2.1) en beperkingen van het onderzoek (paragraaf 9.2.2).

9.1 Conclusies

9.1.1 *Prevalentie, aard en impact van slachtofferschap van ransomware*

In deelstudie 1 is allereerst onderzocht hoeveel respondenten slachtoffer zijn geworden van ransomware. Uit de resultaten blijkt dat 4,5% van de burgers, 4,6% van de zzp'ers en 11,5% van de mkb'ers ooit slachtoffer is geworden van ransomware, waarvan de meerderheid eenmalig slachtoffer is geworden. Bij de meeste slachtoffers vond het incident meer dan 5 jaar geleden plaats. Van de slachtoffers is 5,6% van de burgers, 6,8% van de zzp'ers en 8,8% van de mkb'ers slachtoffer geworden in de afgelopen 12 maanden, wat neerkomt op respectievelijk 0,2%, 0,3% en 0,9% van de totale steekproef. Voor burgers komt dit overeen met de in de literatuur gerapporteerde prevalentiecijfers tussen de 0,2% en 4,8% over een periode van één jaar (Bergmann et al., 2018; Cartwright et al., 2023; CBS, 2019; Conradie, 2023; Ortloff et al., 2021; Simoiu et al., 2019; Van de Weijer & Leukfeldt, 2023; Voce & Morgan, 2023; Yilmaz et al., 2022). Voor zzp'ers is dit lager dan de in de literatuur beschreven prevalentie tussen de 0,7% en 6% over een periode van één jaar onder ondernemers (CBS, 2023; European Commission, 2022; Matthijsse et al., 2024; Van de Weijer & Leukfeldt, 2023; Voce & Morgan, 2021).

In deelstudie 1 is daarnaast meer inzicht verkregen in de aard van slachtofferschap aan de hand van een vragenlijst onder burgers, zzp'ers en mkb'ers die slachtoffer zijn geworden. Als het gaat om de aard van het delict was er bij burgers in de meeste gevallen sprake van lockerware (vergrendeling van (onderdelen van) het systeem), gevolgd door scareware (met een bericht van een zogenaamde wetshandhavingsinstantie). Bij de zzp'ers en mkb'ers was in de meeste gevallen sprake van lockerware of cryptoware (versleuteling). Bij de burgers betrof dit in de meeste gevallen aantasting van de computer en aantasting van bestanden met emotionele waarde, zoals foto's of video's. Voor de ondernemers betrof dit in de meeste gevallen aantasting van de computer en aantasting van financiële gegevens of boekhouding. De meeste burgers denken dat de ransomware op hun apparaat of systeem is gekomen door het klikken op een link, advertentie of pop-up tijdens surfen op internet, terwijl de meeste ondernemers denken dat dit gebeurd is door het klikken op een link of bijlage in een e-mail. Bij de meerderheid van de burgers, zzp'ers en mkb'ers was naast de vergrendeling of versleuteling geen sprake van een aanvullende dreiging. Bij de respondenten bij wie dit wel het geval was, ging het met name om het dreigen met het verwijderen van de decryptiesleutel (i.e. permanente blokkade) of het lekken van bestanden of gegevens. Wanneer er een deadline in het losgeldbericht stond vermeld, kregen de burgers en zzp'ers meestal minder dan 24 uur of tussen de 1 en 3 dagen de tijd om te betalen, terwijl de meeste mkb'ers tussen de 1 en 3 dagen of tussen de 4 en 6 dagen de tijd kregen om te betalen.

Vervolgens is in deelstudie 1 onderzocht welke impact slachtoffers ervaren. Tevens is middels een vignet (een fictief ransomwarescenario) de impact onderzocht onder burgers, zzp'ers en mkb'ers die niet eerder slachtoffer zijn geworden in deelstudie 2. Bij

zowel de respondenten die eerder slachtoffer zijn geworden als de respondenten die niet eerder slachtoffer zijn geworden was de meest voorkomende emotie onder alle groepen boosheid. Een deel van de respondenten in beide deelstudies heeft geprobeerd of zou zelf proberen het probleem op te lossen. De meeste burgers en zzp'ers die zowel wel als niet eerder slachtoffer zijn geworden zouden dit doen door de verbinding met internet te verbreken. De mkb'ers die niet eerder slachtoffer zijn geworden zouden hetzelfde doen, terwijl de meeste mkb'ers die wel slachtoffer zijn geworden geprobeerd hebben te herstellen vanaf een back-up. Bij de meerderheid van de daadwerkelijke slachtoffers die het zelf hebben gepoogd op te lossen, is het gelukt om de toegang tot het apparaat of systeem te herstellen. Een ander deel van de respondenten die wel en niet eerder slachtoffer is geworden, heeft hulp gezocht of zou hulp zoeken om het probleem op te lossen. De grootste groep burgers die slachtoffer is geworden en hulp heeft gezocht, heeft dit gedaan bij een bekende, terwijl de grootste groep burgers die geen slachtoffer is geworden, hulp zou zoeken van een organisatie of instantie. De grootste groep zzp'ers en mkb'ers die hulp heeft gezocht of zou zoeken, heeft dit gedaan of zou dit doen zouden dit doen bij een organisatie, instantie, ICT-deskundige, computerzaak of provider.

Hoewel ongeveer 80% van de burgers, 75% van de zzp'ers en 68% van de mkb'ers die niet eerder slachtoffer van ransomware zijn geworden, zouden verwachten emotionele of psychische gevolgen te ervaren, waren deze aantallen bij de daadwerkelijke slachtoffers lager, hoewel nog steeds aanzienlijk. Onder de slachtoffers heeft ongeveer 45% van de burgers, 39% van de zzp'ers en 34% van de mkb'ers emotionele of psychische gevolgen ervaren. Het is onduidelijk waar het verschil tussen de verwachte en daadwerkelijke emotionele impact door veroorzaakt wordt. De meest voorkomende verwachte en daadwerkelijke gevolgen kwamen overeen. Onder burgers ging dit in de meeste gevallen om een minder veilig gevoel en minder vertrouwen in de eigen digitale vaardigheden, terwijl het bij de meeste ondernemers ging om een minder veilig gevoel, gevolgd door minder vertrouwen in andere mensen (onder slachtoffers) en minder vertrouwen in de eigen digitale vaardigheden (onder niet-slachtoffers). Dit is in overeenstemming met eerder onderzoek naar ransomware (Northwave, 2022) en cybercriminaliteit (Akkermans et al., 2023; Button et al., 2021; Leukfeldt et al., 2018). Ook in enkele expertinterviews werd benoemd dat er meer aandacht en ondersteuning mag komen voor de fysieke of mentale impact van ransomware.

Bij burgers was het meest voorkomende (verwachte) andere gevolg onder zowel slachtoffers als niet-slachtoffers het besteden van tijd aan het oplossen van het incident. Voor ondernemers die wel en niet eerder slachtoffer zijn geworden, ging het met name om kosten vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk, wat ook in de literatuur genoemd wordt (Brennenraedts et al., 2022; CBS, 2023; Meurs et al., 2022b). Waar ongeveer 60% van de burgers die niet eerder slachtoffer zijn geworden financiële gevolgen verwachtte, werd dit ervaren door ongeveer 29% van de burgers die wel slachtoffer zijn geworden, waarbij het bij beide groepen in de meeste gevallen om

minder dan 1.000 euro ging. Waar ongeveer 68% van de zzp'ers en 73% van de mkb'ers financiële gevolgen verwachtten, was dit daadwerkelijk het geval bij 60% van de zzp'ers en 74% van de mkb'ers die slachtoffer zijn geworden. De meeste ondernemers die geen slachtoffer zijn geworden, schatten de kosten enigszins hoger in dan de door slachtoffers gerapporteerde kosten. In de meeste gevallen waren de verwachte kosten tussen de 1.000 en 5.000 euro ten opzichte van minder dan 1.000 euro aan daadwerkelijke schade. Bij slechts 4,3% van de burgers, 0% van de zzp'ers en 5,6% van de mkb'ers die slachtoffer van ransomware zijn geworden, is de financiële schade (gedeeltelijk) vergoed door een verzekeringsmaatschappij, bank of andere instantie.

Voor een groot deel van de respondenten die wel en niet eerder slachtoffer zijn geworden, heeft het ransomware-incident geleid of zou het leiden tot veranderingen in online gedrag of genomen beveiligingsmaatregelen. In de meeste gevallen zouden de burgers die niet eerder slachtoffer zijn geworden (vaker) externe back-ups maken van bestanden en gegevens, terwijl de grootste groep burgers die wel slachtoffer zijn geworden voorzichter is geworden met welke websites ze bezoeken, wat ze downloaden en welke bijlagen ze openen. De meeste ondernemers die wel en niet eerder slachtoffer zijn geworden, zouden (vaker) externe back-ups van bestanden en gegevens (gaan) maken.

9.1.2 *Onderhandelen*

In deelstudie 1 is ook meer inzicht verkregen in de mate waarin slachtoffers van ransomware onderhandelen met daders, welke beweegreden(en) hierbij een rol spelen en wat de uitkomst van de onderhandeling was. Dit is daarnaast onderzocht in deelstudie 2 onder burgers en ondernemers die niet eerder slachtoffer zijn geworden. Ook is het onderwerp aan bod gekomen in de expertinterviews in deelstudie 3.

Slechts een klein deel van de respondenten die wel en niet eerder slachtoffer zijn geworden, heeft contact opgenomen of zou contact opnemen met de daders, hoewel de aantallen onder daadwerkelijke slachtoffers wat lager zijn dan in het hypothetische scenario. Waar 8,0% van de burgers, 12,4% van de zzp'ers en 17,4% van de mkb'ers die niet eerder slachtoffer zijn geworden contact zou opnemen, heeft 4,4% van de burgers, 6,6% van de zzp'ers en 6,2% van de mkb'ers die slachtoffer zijn geworden contact opgenomen of iemand anders contact laten opnemen met de criminelen. Dit gebeurde voornamelijk via e-mail of een chatsysteem op een website of portaal. Er liggen bovendien andere motivaties aan het contact ten grondslag voor de slachtoffers en niet-slachtoffers. Waar zowel de burgers als ondernemers die niet eerder slachtoffer zijn geworden contact zouden opnemen om vast te stellen of het losgeldbericht echt is, hebben de burgers die slachtoffer zijn geworden contact opgenomen om te informeren over de hoogte van het losgeld en de ondernemers die slachtoffer zijn geworden om vast te stellen welke data waren gestolen.

De resultaten met betrekking tot het onderhandelen lopen uiteen tussen de respondenten die wel en niet slachtoffer zijn geworden. Terwijl 27,4% van de burgers, 40,0% van de zzp'ers en 36,0% van de mkb'ers die niet eerder slachtoffer zijn geworden contact zou opnemen om te onderhandelen (respectievelijk 2,2%, 4,9% en 6,3% van de totale steekproef), heeft in werkelijkheid geen enkele burger of zzp'er en slechts een enkele mkb'er (2% van de totale steekproef) die slachtoffer is geworden van ransomware onderhandeld. De mkb'ers deden dit om het losgeldbedrag te verlagen of langer de tijd te krijgen. Bij een van de respondenten heeft dit geen verandering opgeleverd, de andere respondent weet niet wat de uitkomst van de onderhandelingen was.

Een opvallende uitkomst is bovendien dat de bereidheid om contact op te nemen laag is onder de respondenten van de vragenlijsten, terwijl uit de expertinterviews blijkt dat dit door cybersecuritybedrijven (vrijwel) altijd geadviseerd wordt. Een deel van de experts wijst bijvoorbeeld op voordelen als het rekken van tijd, het inwinnen van informatie of het krijgen van een beter inzicht in de ernst en impact van het incident, wat vervolgbeslissingen kan beïnvloeden. In de literatuur wordt er daarnaast op gewezen dat het behulpzaam kan zijn om te controleren of het communicatiekanaal nog actief is (Caporusso et al., 2019) en dat het in sommige gevallen zelfs nodig is om informatie te ontvangen over de hoogte van het losgeld (Meurs et al., 2022b), wat tevens de beslissing om te betalen kan beïnvloeden. Hoewel in expertinterviews niet aan bod kwam dat slachtoffers contact opnamen met cybercriminelen om te informeren over de hoogte van het losgeld of vast te stellen of het losgeldbericht echt is zoals in de vragenlijsten onder slachtoffers en niet-slachtoffers het geval was, kwam in de interviews wel naar voren dat contact wordt opgenomen om vast te stellen welke data zijn gestolen. Ook van onderhandelen lijkt slechts in een enkel geval sprake te zijn in de vragenlijsten, terwijl onderhandelingen regelmatig leiden tot een verlaging van het losgeldbedrag, aldus de experts.

De resultaten wijzen daarmee op aanzienlijke verschillen tussen het gedrag van de daadwerkelijke slachtoffers en het verwachte gedrag van niet-slachtoffers enerzijds en het advies van experts anderzijds. Ten eerste zou dit erop kunnen wijzen dat burgers en zzp'ers (en in iets mindere mate mkb'ers) onvoldoende inzicht hebben in wat contact of onderhandeling ze zou kunnen opleveren. Ten tweede is een mogelijkheid dat deze doelgroep door gebrekkige kennis of voorzieningen niet in staat is om contact op te nemen of onderhandelingen te doen, wat volgens een van de experts geen vanzelfsprekendheid is. Ook in eerder onderzoek wordt gewezen op de complexiteit van het onderhandelingsproces, wat onder andere kalmte, kennis van de criminele groepering en onderhandelingstactieken vereist (Boticiu & Teichmann, 2024). De resultaten lijken dit te bevestigen, aangezien bij de meeste respondenten die contact hebben opgenomen, dit gedaan is door een bekende (in het geval van burgers en zzp'ers) of een ingehuurde partij (in het geval van mkb'ers). Het feit dat alleen enkele mkb'ers onderhandeld hebben, is in dit verband wellicht een logisch gevolg van het feit dat zij een partij hebben ingehuurd. Ten derde kan het gebrek aan contact of onderhandelingen het gevolg zijn

van het expliciete advies van sommige partijen, waaronder de politie en No More Ransom, om niet in te gaan op losgeldeisen. Een kanttekening bij de resultaten is dat het niet bij alle typen ransomware mogelijk is om contact op te nemen met de daders, wat voor de klanten van de cybersecurityexperts wel het geval was. Uit de resultaten blijkt niet of respondenten uit de vragenlijsten deze optie geboden werd, wat de resultaten beïnvloed zou kunnen hebben.

9.1.3 *Betalen*

In deelstudie 1 onder burgers en ondernemers die slachtoffer zijn geworden van ransomware, deelstudie 2 onder burgers en ondernemers die geen slachtoffer zijn geworden en deelstudie 3 onder experts is ook stilgestaan bij de mate waarin slachtoffers van ransomware bereid zijn het losgeld te betalen en welke beweegreden(en) en situationele factoren hierbij een rol spelen.

Aan de respondenten die slachtoffer zijn geworden van ransomware is gevraagd hoeveel losgeld van hen geëist werd. Dit was het laagst onder burgers en het hoogst onder mkb'ers. Gemiddeld werd bij de burgers 3.676 euro aan losgeld gevraagd, met een mediaan van 500 euro. Bij de zzp'ers werd gemiddeld 13.919 euro aan losgeld gevraagd, met een mediaan van 1.149 euro. Bij de mkb'ers was het gemiddeld geëiste losgeld het hoogst met 231.343 euro en een mediaan van 10.000 euro.

Zowel bij de respondenten die eerder slachtoffer zijn geworden als bij de respondenten die niet eerder slachtoffer zijn geworden is de betalingsbereidheid laag. Gemiddeld genomen was het voor de burgers en ondernemers die geen slachtoffer zijn geworden niet waarschijnlijk dat ze zouden betalen. Ook een klein deel van de daadwerkelijke slachtoffers, 4,1% van de burgers, 7,6% van de zzp'ers en 6,1% van de mkb'ers, heeft aangegeven het geëiste losgeld te hebben betaald. De gemiddelde losgeldbetaling onder slachtoffers was voor burgers 700 euro, voor zzp'ers 1.250 euro en voor mkb'ers 3.134 euro. Bij alle drie de groepen is bij de meerderheid van de respondenten de toegang gedeeltelijk of volledig hersteld, ongeacht of ze het losgeld betaald hebben. De meeste respondenten hadden bovendien niet het idee dat hun data gelekt of verkocht zijn.

Uit de interviews blijkt dat de experts de betalingsbereidheid hoger inschatten. De experts duiden dit verschil vanuit het idee dat de doelgroepen in de vragenlijsten minder snel een cyberverzekering hebben, minder impact ervaren (en daardoor minder geneigd zijn om te betalen), of als gevolg van de lage onderhandelingsbereidheid onder deze doelgroepen. De uitkomsten zijn in overeenstemming met eerder onderzoek waaruit gebleken is dat tussen 0,7% en 25% van de burgers het losgeld heeft betaald na slachtofferschap (Cartwright et al., 2023; CBS, 2019; Ortloff et al., 2021; Simoiu et al., 2019; Yilmaz et al., 2022), maar niet in overeenstemming met eerder onderzoek waaruit blijkt dat tussen de 14% en 32,2% van de organisaties het losgeld betaalt (CBS, 2023; Meurs et al., 2022b; Project Melissa, 2024; Voce & Morgan, 2021). Een kanttekening

hierbij is dat sommige van de eerdere onderzoeken ook gericht zijn op grote organisaties, of gebaseerd zijn op slachtoffers die bekend zijn bij de politie of cybersecuritysector, wat de resultaten kan hebben beïnvloed. De resultaten bevestigen bovendien niet het beeld in de literatuur dat mkb'ers meer geneigd zijn om het losgeld te betalen in vergelijking met niet-mkb-eigenaren en werknemers (Voce & Morgan, 2021), en dat mkb'ers vaker betalen dan zzp'ers (CBS, 2023). Een mogelijke verklaring voor dit verschil zou kunnen zijn dat sommige slachtoffers in de steekproef langer geleden slachtoffer zijn geworden, toen het ransomwarelandschap er nog anders uitzag. Zo blijkt uit de resultaten dat een aanzienlijk deel van de respondenten slachtoffer is geworden van lockerware of scareware, waarbij het mogelijk makkelijker was om te herstellen zonder betaling in vergelijking met de cryptoware. Uit eerder onderzoek is bovendien gebleken dat ransomwaregroeperingen in de afgelopen jaren zijn geprofessionaliseerd (Matthijsse et al., 2023), wat ook zou kunnen betekenen dat het moeilijker is geworden om te herstellen zonder betaling. Ook het dreigen met lekken van gestolen data kwam in het verleden minder voor. Uit de resultaten van de vragenlijsten blijken de betalingspercentages echter niet wezenlijk lager te zijn onder slachtoffers die langer geleden slachtoffer zijn geworden dan onder recente slachtoffers. Daarnaast zijn er geen grote verschillen in betalingspercentages gevonden tussen de verschillende typen ransomware waar respondenten slachtoffer van zijn geworden. Tot slot kan deze lagere betalingsbereidheid ook het gevolg zijn van ontwikkelingen in de maatschappij, zoals een beter begrip van de impact van het betalen van losgeld, de advisering vanuit verschillende instanties om het losgeld niet te betalen, verbeterde beveiligingsmaatregelen en initiatieven zoals No More Ransom.

De voornaamste redenen om te betalen lopen uiteen, maar zijn in overeenstemming met eerder onderzoek (Connolly & Borrion, 2022; Simoiu et al., 2019; Voce & Morgan, 2021). Onder de niet-slachtoffers zouden burgers betalen omdat ze de aangetaste bestanden, gegevens of apparaten niet zouden willen verliezen, terwijl de ondernemers het losgeld zouden betalen omdat dit goedkoper zou zijn dan geen zaken kunnen doen. De ondernemers die slachtoffer zijn geworden en die betaald hebben, deden dit voornamelijk omdat ze de aangetaste bestanden, gegevens of apparaten niet wilden verliezen. Daarentegen hadden de burgers die slachtoffer zijn geworden als voornaamste reden om te betalen dat ze erop vertrouwden dat toegang herstel zou worden na betaling.

De voornaamste reden om niet te betalen loopt meer uiteen tussen de steekproeven. Zowel de burgers die wel en geen slachtoffer zijn van ransomware hebben niet betaald of zouden niet betalen omdat ze niet vertrouwden dat de toegang hersteld zou worden na betaling. De zzp'ers die wel en niet slachtoffer zijn geworden waren het vaakst van mening dat betalen onethisch is. Waar de grootste groep mkb'ers die geen slachtoffer is dit ook als reden aanhaalde, gaven de mkb'ers die slachtoffer zijn geworden als voornaamste reden om niet te betalen dat ze een back-up hadden. Dergelijke motieven kwamen in de literatuur ook naar voren (Cartwright et al., 2023; Connolly & Borrion,

2022; Matthijsse et al., 2023; Voce & Morgan, 2021, 2022; Yilmaz et al., 2021). Deze uitkomsten komen gedeeltelijk overeen met de uitkomsten van de interviews waarin door experts beschreven werd dat slachtoffers overgaan tot betaling als de bedrijfscontinuïteit (te erg of te lang) verstoord is, wat mede afhankelijk is van de beschikbaarheid van back-ups.

Er is daarnaast in deelstudie 2 onder niet-slachtoffers gekeken naar situationele factoren die bijdragen aan de betalingsbereidheid. De resultaten lopen uiteen tussen groepen. Er is een significant verband tussen de hoogte van het losgeld en de betalingsbereidheid van burgers en mkb'ers, maar niet voor zzp'ers. Burgers van wie in een fictief ransomwarescenario 2.500 euro in bitcoin en mkb'ers van wie 25% van de jaaromzet werd geëist aan losgeld, rapporteerden een lagere waarschijnlijkheid van betalen dan respondenten van wie 250 euro in bitcoin of 1% van de jaaromzet werd geëist. Dit is in overeenstemming met het onderzoek van Voce en Morgan (2021) waarin gesteld werd dat de betaalbaarheid van de losgeldeis een rol speelt, maar in tegenstelling tot een onderzoek van Matthijsse et al. (2024) waarin de hoogte van het losgeld niet gerelateerd was aan de betalingsbereidheid. Het hebben van een back-up was bij zzp'ers gerelateerd aan een significant lagere waarschijnlijkheid van betalen, maar er was geen sprake van een significant verband bij de burgers en mkb'ers, in tegenstelling tot eerder onderzoek (Cartwright et al., 2023; Connolly & Borrion, 2022; Matthijsse et al., 2023; 2024; Meurs et al., 2022b; Voce & Morgan, 2021).

Er is daarnaast een significant verband tussen de dreiging met het lekken van data en de betalingsbereidheid onder burgers, maar niet bij de ondernemers. Burgers bij wie gedreigd werd met het lekken van data rapporteerden een hogere waarschijnlijkheid van betalen. Het uitblijven van een significant verband bij ondernemers is opvallend omdat uit de expertinterviews en eerder onderzoek (Cartwright et al., 2023; Matthijsse et al., 2023; Meurs et al., 2022b) is gebleken dat angst voor het lekken van gestolen data een belangrijk motief kan zijn om het losgeld te betalen. Dit verschil zou erop kunnen duiden dat de impact van gestolen data onderschat wordt door respondenten, of dat respondenten de kans dat gestolen data gelekt of verkocht worden onderschatten. Zo blijkt uit de vragenlijst onder slachtoffers dat veel respondenten (mogelijk ten onrechte) denken dat hun data niet gelekt of verkocht gaan worden. Ook een cybersecurity-expert wijst er in een interview op dat in eerste instantie vaak te luchtig gedacht wordt door slachtoffers over het feit dat data gestolen zijn. Tegelijkertijd hebben verschillende experts erop gewezen dat betaling van het losgeld geen garantie is dat gestolen data niet alsnog gelekt of doorverkocht worden. Zo heeft de politie bij meerdere ransomwaregroeperingen geobserveerd dat gestolen data niet verwijderd worden na betaling, waardoor het risico blijft bestaan dat deze op een later moment nog gelekt of doorverkocht worden. Deze overweging zou ook bij respondenten kunnen hebben meegewogen in hun keuze om al dan niet het losgeld te betalen.

Bovendien is er bij burgers en ondernemers sprake van een significant verband tussen geadviseerd worden om te betalen en de waarschijnlijkheid van betalen. Respondenten die geadviseerd werd om te betalen, rapporteerden een hogere waarschijnlijkheid van betalen, in overeenstemming met eerder onderzoek (Connolly & Borrion, 2022; Matthijsse et al., 2024; Voce & Morgan, 2021).

Als het gaat om achtergrondkenmerken is er voor burgers een significant verband tussen leeftijd en opleidingsniveau en de waarschijnlijkheid van betalen. Hoe jonger respondenten zijn, hoe hoger de waarschijnlijkheid van betalen is. Onder laag- of middelbaar opgeleiden is de waarschijnlijkheid van betalen lager in vergelijking met hoogopgeleiden. Voor de mkb'ers is er een significant verband tussen de bedrijfsgrootte en de waarschijnlijkheid van betalen. Kleine en middelgrote bedrijven rapporteren een hogere waarschijnlijkheid van betalen in vergelijking met microbedrijven. Tot slot is er een significant verband tussen sector en betalingsbereidheid onder zzp'ers en mkb'ers. Zzp'ers in de sectoren landbouw en visserij, en handel, logistiek en horeca rapporteren een lagere waarschijnlijkheid van betalen dan in de sector financiële en zakelijke dienstverlening. Ook mkb'ers in de sector handel, logistiek en horeca rapporteren een lagere waarschijnlijkheid van betalen in vergelijking met de sector financiële en zakelijke dienstverlening.

9.1.4 *Melden*

Tot slot is in deelstudie 1 onder burgers en ondernemers die slachtoffer zijn geworden van ransomware, deelstudie 2 onder burgers en ondernemers die geen slachtoffer zijn geworden en deelstudie 3 onder experts meer inzicht verkregen in de mate waarin slachtoffers van ransomware bereid zijn het incident te melden, bij welke partijen dit gebeurt en welke beweegreden(en) en situationele factoren hierbij een rol spelen.

Hoewel de meldingsbereidheid bij de politie of een andere organisatie hoog is onder niet-slachtoffers in het hypothetische scenario, blijkt dit niet het geval onder de respondenten die daadwerkelijk slachtoffer zijn geworden. Burgers en ondernemers die niet eerder slachtoffer zijn geworden, achten het gemiddeld genomen waarschijnlijk dat ze het incident melden, waarvan de meeste respondenten het incident zouden melden bij de politie. Aan de respondenten die daadwerkelijk slachtoffer zijn geworden, is tevens gevraagd met welke organisaties ze contact hebben opgenomen voor advies, ondersteuning of om melding van het incident te maken. In overeenstemming met de literatuur (CBS, 2023; Connolly & Borrion, 2022; Simoiu et al., 2019, 2019; Voce & Morgan, 2022; Yilmaz et al., 2022) bleken slachtoffers van ransomware meer geneigd om advies of ondersteuning te zoeken bij een organisatie anders dan de politie. De meeste burgers en ondernemers die slachtoffer zijn geworden namen contact op met een cybersecuritybedrijf of IT-leverancier, gevolgd door de politie of Fraudehelpdesk.

In tegenstelling tot de respondenten die geen slachtoffer zijn geworden, heeft slechts 15,6% van de burgers, 12,3% van de zzp'ers en 26,7% van de mkb'ers die slachtoffer zijn geworden contact opgenomen met de politie. Hierbij was het aangiftepercentage respectievelijk 2,1%, 1,1% en 10% van de totale steekproef. Deze percentages zijn laag in vergelijking met de inschatting van de cybersecurityexperts in de interviews dat in veel gevallen wel melding wordt gemaakt bij de politie, maar ze lijken wel overeen te komen met het beeld dat de politie van de meldingsbereidheid heeft. Het percentage slachtoffers dat contact opneemt met de politie komt in grote lijnen overeen met eerder onderzoek waarin gesproken wordt van een meldingspercentage tussen de 9 en 23% (CBS, 2023; European Commission, 2022; Simoiu et al., 2019; Van de Weijer et al., 2020; Voce & Morgan, 2022). Dat meer mkb'ers die slachtoffer zijn geworden contact opnemen en melden in vergelijking met zzp'ers en burgers, zou verklaard kunnen worden vanuit het feit dat mkb'ers mogelijk een grotere impact ervaren, en daardoor ook sneller geneigd zijn om het incident te melden. Daarnaast zou dit het gevolg kunnen zijn van het feit dat deze groep wellicht sneller een cybersecuritybedrijf inschakelt voor hulp. Uit de expertinterviews blijkt namelijk dat deze bedrijven in veel gevallen adviseren om melding van het incident te maken bij de politie. Tot slot is deze groep vaker verzekerd tegen cyberincidenten dan burgers en zzp'ers, en is het doen van een aangifte soms een vereiste van de verzekeraar.

De meest voorkomende reden om het incident niet te melden bij de politie was voor zowel de burgers en ondernemers die slachtoffer zijn geworden dat ze het probleem zelf of met behulp van een andere partij hebben opgelost. Daarentegen gaven de burgers en ondernemers die geen slachtoffer zijn geworden als voornaamste reden dat het volgens hen geen zin zou hebben en de politie er toch niets aan zou doen. Dit is in overeenstemming met de uitkomsten van de expertinterviews, waaruit bleek dat het voor slachtoffers onvoldoende duidelijk is wat melden hun kan opleveren, dat ze het nut er niet van inzien, of het gevoel hebben dat de politie niets doet. Dit beeld komt ook terug in de literatuur over aangiftebereidheid van cybercriminaliteit (Conradie, 2023; Cybbar & CSD, 2023; Van de Weijer et al., 2020; Veenstra et al., 2015; Voce & Morgan, 2022; Wanamaker, 2019).

De meest voorkomende reden om wel te melden was bij de burgers en mkb'ers die wel en niet slachtoffer zijn geworden van ransomware dat ze wilden dat de dader gepakt wordt. Ook de meeste zzp'ers die geen slachtoffer zijn geworden, gaven als voornaamste reden dat ze wilden dat de dader gepakt wordt, terwijl de meest voorkomende reden voor zzp'ers die slachtoffer zijn geworden was omdat ze wilden voorkomen dat het bij een ander gebeurt, zoals ook in het onderzoek van Voce en Morgan (2022) aan bod komt. Deze motieven zijn in overeenstemming met de uitkomsten van de expertinterviews, waarin experts beschreven dat slachtoffers melden vanuit maatschappelijk oogpunt en omdat zij hopen dat de politie iets kan betekenen. Dat respondenten in de vragenlijsten hebben aangegeven dat ze hopen dat de dader gepakt wordt, is een opvallende uitkomst omdat dit – hoewel niet onmogelijk – niet altijd gemakkelijk is bij een

internationaal delict als ransomware, aldus ook de politie-experts. Ook dit zou erop kunnen duiden dat voor slachtoffers niet altijd helder is wat ze wel en niet kunnen verwachten van de politie.

Aan respondenten is ook gevraagd hoe ze aankijken tegen het standpunt en advies van de politie om het losgeld niet te betalen. In de expertinterviews werd door politiemedewerkers benoemd dat het standpunt van de politie om niet te betalen slachtoffers mogelijk weerhoudt om het ransomware-incident te melden bij de politie. De resultaten van het huidige onderzoek wijzen erop dat hoewel zowel de slachtoffers als niet-slachtoffers het met dit standpunt eens zijn, ditzelfde standpunt er bij ongeveer 21% van de burgers, 23% van de zzp'ers en 30% van de mkb'ers die slachtoffer zijn geworden toe heeft geleid dat ze geen contact hebben opgenomen met de politie. Ook bij ongeveer 27% van de burgers, 22% van de zzp'ers en 21% van de mkb'ers die geen slachtoffer zijn geworden, was dit het geval. Het heeft er bovendien bij 40% van de burgers die slachtoffer zijn geworden toe geleid dat ze na contact met de politie uiteindelijk geen melding en/of aangifte hebben gedaan. Ook bij ongeveer 26% van de burgers, 21% van de zzp'ers en 19% van de mkb'ers die geen slachtoffer zijn geworden, zou het standpunt de keuze om melding en/of aangifte te doen beïnvloeden, ongeacht of ze voornemens waren contact met de politie op te nemen.

Tot slot is in deelstudie 2 onder niet-slachtoffers gekeken naar situationele factoren die bijdragen aan de meldingsbereidheid. Er is een significant verband tussen de hoogte van het losgeld en de waarschijnlijkheid van melden voor burgers, maar niet voor ondernemers. Burgers van wie 2.500 euro aan bitcoin in losgeld is geëist, rapporteren een hogere waarschijnlijkheid van melden dan burgers van wie 250 euro aan bitcoin werd geëist. Daarnaast is er een positief significant verband tussen geadviseerd worden om te betalen door een (cybersecurity)organisatie en de mensen om de respondent heen en de waarschijnlijkheid van melden voor burgers, maar niet voor ondernemers. Burgers rapporteren een hogere waarschijnlijkheid van melden indien ze geadviseerd wordt om het losgeld te betalen. Er is geen significant verband gevonden tussen dreigen met lekken of het hebben van een back-up en de waarschijnlijkheid van melden onder burgers en ondernemers. Als het gaat om achtergrondkenmerken waren voor burgers leeftijd, geslacht en opleidingsniveau significante factoren. Burgers die ouder, hoogopgeleid of vrouw zijn, rapporteerden een hogere waarschijnlijkheid van melden.

9.2 Discussie

In deze paragraaf wordt stilgestaan bij de belangrijkste conclusies en implicaties van het onderzoek voor het voorkomen en mitigeren van (de gevolgen van) ransomware, evenals voor de rol van de politie en andere publieke of private partijen. Deze implicaties richten zich op drie onderwerpen: 1) het verlagen van de betalingsbereidheid, 2) verbetering in de positie en ondersteuning van slachtoffers en 3) verbetering in de in-

formatiepositie van de politie en het verhogen van de meldingsbereidheid. Vervolgens wordt stilgestaan bij de beperkingen van het onderzoek.

9.2.1 *Implicaties*

9.2.1.1 *Het verlagen van de betalingsbereidheid*

Belangrijkste implicaties
- Cybersecuritymaatregelen zijn van belang, niet alleen om slachtofferschap te voorkomen, maar ook in het kader van herstel en de beslissing om het losgeld te betalen.
- De informatievoorziening vanuit publieke partijen omtrent de effecten van het betalen van het losgeld voor het slachtoffer en de maatschappij kan verbeterd worden.
- Samenwerking tussen de politie en cybersecuritysector is van belang om de betalingsbereidheid te verlagen.
- Er is meer onderzoek nodig naar interventies om de betalingsbereidheid te verlagen, zoals een slachtofferfonds.

Het huidige onderzoek heeft geleid tot een beter begrip van de beweegredenen en factoren die een rol spelen in de beslissing om het geëiste losgeld te betalen na een ransomware-aanval. De resultaten illustreren het belang van het nemen van cybersecuritymaatregelen. Zo blijkt uit het onderzoek dat niet alle respondenten voldoende beveiligingsmaatregelen namen, en bleek slechts een hele kleine groep ondernemers een bedrijfscontinuïteitsplan te hebben voordat ze slachtoffer werden. Bovendien is gebleken dat belangrijke beweegredenen om het losgeld te betalen onder andere waren dat respondenten bestanden of gegevens niet wilden verliezen, terwijl de beschikbaarheid van back-ups een van de redenen was om het losgeld juist niet te betalen. Ook een te ernstige of lange verstoring van de bedrijfscontinuïteit hing bij ondernemers samen met een hogere betalingsbereidheid, iets wat ook mede afhankelijk is van maatregelen als het maken van goede, gescheiden back-ups.

Ten tweede hebben de resultaten ook implicaties voor de partijen die zich bezighouden met de aanpak van ransomware. Er is ruimte voor verbetering in de informatievoorziening omtrent losgeldbetalingen. Door onder andere de overheid, politie en Slachtofferhulp Nederland wordt geadviseerd om nooit het losgeld te betalen, wat wordt gemotiveerd vanuit de overweging dat losgeldbetalingen het ransomwarebusinessmodel in stand houden. De vraag is echter of voor burgers en ondernemers voldoende duidelijk is wat de gedachtegang achter dit advies is en wat de gevolgen zijn van het betalen van het losgeld voor het slachtoffer en de maatschappij. Zo blijkt uit het huidige onderzoek dat een beweegreden om het losgeld te betalen voor slachtoffers is om te voorkomen dat hun gestolen data gelekt of verkocht worden, terwijl de politie erop wijst dat betalen niet garandeert dat de data ook echt door de daders verwijderd worden zoals ze beloven. Door een verbeterde informatievoorziening door publieke partijen over de effecten van het betalen van het losgeld voor het slachtoffer en de maatschappij, kan de

kosten-batenoverweging om te betalen mogelijk beïnvloed worden zodat minder slachtoffers betalen.

Ten derde illustreren de resultaten dat samenwerking tussen de cybersecuritysector en de politie omtrent het verlagen van de betalingsbereidheid van belang is. Slachtoffers zijn meer geneigd om contact op te nemen met een cybersecuritybedrijf, IT-leverancier of andere deskundige dan met andere partijen zoals de politie. De cybersecurityexperts schatten dat 40-60% van de incidenten waar ze mee te maken krijgen om ransomware gaat. In het vignetexperiment was de waarschijnlijkheid van betalen voor zowel de burgers, zzp'ers als mkb'ers bovendien gerelateerd aan geadviseerd worden om te betalen door een cybersecuritybedrijf en de mensen om de respondent heen. Dit ligt in lijn met de verwachting dat slachtoffers leunen op hun advies en expertise. Hoewel cybersecuritybedrijven alleen zullen adviseren om te betalen als er geen alternatieven zijn, hebben ze desalniettemin een sleutelpositie. Het is dus belangrijk dat met verschillende partijen wordt samengewerkt om slachtoffers goed te adviseren en beleid te ontwikkelen om losgeldbetalingen te voorkomen. Tot slot kan gedacht worden aan andere interventies om de betalingsbereidheid te verlagen, zoals een subsidie die het nemen van beveiligingsmaatregelen stimuleert, veranderingen in verzekeringseisen, of een fonds om na slachtofferschap te herstellen van een ransomware-aanval als het losgeld niet betaald wordt (zie bijvoorbeeld ook Mott et al., 2023; Nieuwesteeg et al., 2022; Nieuwesteeg & Faure, 2023). Meer onderzoek is nodig om te achterhalen of dergelijke initiatieven een effect hebben op de betalingsbereidheid.

9.2.1.2 *Verbetering in de positie en ondersteuning van slachtoffers*

Belangrijkste implicaties
- De informatievoorziening kan verbeterd worden omtrent de acties die slachtoffers kunnen ondernemen als ze slachtoffer worden en organisaties waarbij ze terechtkunnen. Er is meer onderzoek nodig naar effectieve manieren om de informatievoorziening te verbeteren en meer uniform te maken.
- Er moet meer aandacht komen voor de fysieke en mentale gevolgen van slachtofferschap van ransomware, waarbij handvatten aan slachtoffers worden geboden door partijen die slachtoffers bijstaan om hiermee om te gaan of de juiste hulp te vinden.

Een andere implicatie van het huidige onderzoek is dat er ruimte is voor verbetering in de positie en ondersteuning van slachtoffers van ransomware. Een ransomware-aanval is een ingrijpende gebeurtenis. Ondernemers en burgers worden geacht onder hoge tijdsdruk stappen te ondernemen of beslissingen te nemen, terwijl ze niet altijd de juiste kennis of middelen hebben om dit te doen. Hoewel voor slachtoffers verschillende hulpbronnen- en voorzieningen beschikbaar zijn op internet en bij verschillende organisaties, zijn deze voorzieningen versnipperd. Voor slachtoffers is niet altijd duidelijk wat ze zelf aan actie(s) kunnen ondernemen als ze slachtoffer worden en bij welke

organisaties ze terechtkunnen in elke fase van het incident en met welk doel. Vervolgonderzoek moet uitwijzen wat een effectieve manier is om deze informatievoorziening te verbeteren en meer uniform te maken en slachtoffers zo handelingsperspectief te geven. Hierbij zou bijvoorbeeld gedacht kunnen worden aan inhoudelijke afstemming tussen partijen die online al informatie of hulp aanbieden omtrent ransomware, waarbij de inhoud zoveel mogelijk overeen moet komen en slachtoffers steeds naar dezelfde website/partij worden doorverwezen. Dit wordt momenteel bijvoorbeeld al toegepast binnen het thema online fraude door de werkgroep integrale aanpak online fraude. Een voorbeeld hierbij is een website voor slachtoffers van ransomware, opgezet door de verschillende partijen die zich bezighouden met de aanpak van ransomware, waarop adviezen worden gegeven van wat slachtoffers vooraf, tijdens en na een aanval kunnen doen en bij welke organisaties ze terechtkunnen, vergezeld van een campagne om deze website bekendheid te geven. Daarnaast zouden er interventies ingezet kunnen worden om burgers en ondernemers te helpen bij het nemen van maatregelen. Hoewel het huidige onderzoek al meer inzicht heeft verschaft in de reacties van slachtoffers op een ransomware-aanval, is bovendien meer inzicht nodig in wat slachtoffers precies doen tijdens en na een ransomware-aanval, wat het ze heeft opgeleverd, maar bijvoorbeeld ook hoe het proces van contact opnemen of onderhandelen in zijn werk gaat, wat nu vooral lijkt te gebeuren onder grotere organisaties.

Daarnaast is de impact van ransomware een onderbelicht thema. Een aanzienlijk deel van de slachtoffers ervaarde emotionele of psychische gevolgen, waaronder een minder veilig gevoel, minder vertrouwen in de eigen digitale vaardigheden of in andere mensen. De experts wijzen tevens op stress en onzekerheid. Deze emoties en gevoelens kunnen bovendien de betalings- en meldingsbereidheid beïnvloeden. Er moet meer aandacht komen voor de fysieke en mentale gevolgen van slachtofferschap van ransomware op de korte en lange termijn, waarbij slachtoffers handvatten worden geboden om hiermee om te gaan. Er is niet alleen een belangrijke rol weggelegd voor Slachtofferhulp Nederland om hier invulling aan te geven, maar ook voor andere partijen die slachtoffers ondersteunen om actief bij de impact stil te staan en door te verwijzen naar Slachtofferhulp Nederland indien nodig. In het huidige onderzoek is middels de vragenlijsten bovendien alleen inzicht verkregen in de emotionele impact van burgers en eigenaren van bedrijven. Meer inzicht is bij ondernemers nodig in de emotionele impact in alle lagen van de organisatie in de verschillende fasen van het incident. Er is daarnaast meer onderzoek nodig naar mogelijke verklaringen voor de verschillen in ervaren impact tussen burgers die in de privésfeer slachtoffer zijn geworden en ondernemers die in bedrijfsverband slachtoffer zijn geworden, evenals de discrepantie tussen de daadwerkelijke emotionele impact onder slachtoffers en de verwachte impact onder niet-slachtoffers.

9.2.1.3 *Verbetering in de informatiepositie van de politie en het verhogen van de meldingsbereidheid*

Belangrijkste implicaties

- Samenwerking en informatie-uitwisseling tussen de politie en andere partijen die zich bezighouden met ransomware is van belang voor de informatiepositie van de politie en moet zich blijven ontwikkelen.
- De meldingsbereidheid na slachtofferschap van ransomware is laag. Er zijn verschillende aanknopingspunten om de meldingsbereidheid te verhogen, zoals verbeterde informatievoorziening vanuit de politie over de mogelijkheden, het belang en de (realistische) gevolgen van een melding of aangifte, of het stimuleren van melden door andere partijen zoals cybersecuritybedrijven of verzekeringsmaatschappijen.
- Het advies van de politie om het losgeld niet te betalen weerhoudt een deel van de slachtoffers ervan om contact op te nemen met de politie. Verder onderzoek is nodig naar het effect van dit advies en wat dit betekent voor de communicatiestrategie van de politie.

Tot slot maken de uitkomsten van het onderzoek duidelijk dat er ruimte voor verbetering is in de informatiepositie van de politie en, in het verlengde daarvan, de meldingsbereidheid onder slachtoffers. Een goede ontwikkeling is dat er meer informatie uitgewisseld wordt tussen publieke- en private partijen zoals de politie, het OM en de cybersecuritysector, bijvoorbeeld in Project Melissa. De samenwerking en informatie-uitwisseling kan echter nog verder verbeterd worden. Zo wijzen experts erop dat niet alle cybersecuritybedrijven informatie uitwisselen met de politie, dat er geen informatiedeling is tussen de Autoriteit Persoonsgegevens en de politie (terwijl sommige slachtoffers mogelijk alleen melding maken van een datalek bij de autoriteit) en dat verschillende partijen in het algemeen nog te ver uit elkaar liggen. De samenwerking moet zich dus blijven ontwikkelen, waarbij ook aandacht uitgaat naar de juridische mogelijkheden voor informatiedeling, en tevens geëvalueerd wordt wat het effect van dergelijke initiatieven is op het verkrijgen van een beter inzicht in ransomware en het voorkomen van slachtofferschap.

Uit het huidige onderzoek blijkt bovendien dat de intentie om melding te maken bij de politie hoog is, maar dat de daadwerkelijke meldings- of aangiftebereidheid na slachtofferschap van ransomware laag is. Slachtoffers zoeken eerder advies of ondersteuning bij een andere organisatie, zoals een cybersecuritybedrijf of de Fraudehelpdesk. Hoewel uit het huidige onderzoek blijkt met welke partijen slachtoffers contact (zouden) opnemen en vanuit welke overwegingen, is er meer onderzoek nodig naar hoe slachtoffers bij deze partijen terechtkomen. Zo is bijvoorbeeld onduidelijk of slachtoffers al bekend waren met deze partijen, een bekende ze dit heeft aangeraden of dat ze het internet hebben geraadpleegd. Dergelijke inzichten zouden implicaties kunnen hebben voor de informatievoorziening naar slachtoffers toe. Daarnaast blijkt uit de resultaten

dat slachtoffers onvoldoende het nut inzien van een melding of aangifte bij de politie. Ze denken bijvoorbeeld dat de politie niets voor ze kan betekenen, terwijl de politie wel degelijk ondersteuning kan bieden, bijvoorbeeld door middel van het delen van kennis of het aanbieden van decryptiemogelijkheden. Ook kan schaamte en angst voor oordelen of reputatieschade een rol spelen.

De meldingsbereidheid zou op verschillende wijzen verhoogd kunnen worden. Ten eerste zou meer aan informatievoorziening gedaan kunnen worden over wat het belang van een melding of aangifte is voor zowel het slachtoffer als de maatschappij, bijvoorbeeld door informatievoorziening op de website van de politie, door het delen van 'succesverhalen' van politieacties of middels campagnes. Er is bovendien een belangrijke rol weggelegd voor andere partijen waar slachtoffers contact mee opnemen zoals cybersecuritybedrijven, de Fraudehelpdesk of verzekeringsmaatschappijen om melding of aangifte bij de politie te stimuleren. Een gezamenlijke boodschap is hierbij van belang. Tegelijkertijd is het zaak voor de politie om aan verwachtingsmanagement te doen naar het slachtoffer toe over wat wel en niet mogelijk is. Zo blijkt uit de resultaten dat sommige slachtoffers een melding hebben gemaakt bij de politie omdat ze wilden dat de dader gepakt wordt, terwijl de politie voor ransomware niet altijd in deze behoefte kan voorzien. Ook dit benadrukt het belang van goede informatievoorziening. Ten tweede kan een verbetering in processen volgens experts mogelijk een bijdrage leveren aan het verhogen van de meldingsbereidheid. Hierbij kan gedacht worden aan het verbeteren van de online aangifte voor burgers, het invoeren van online aangifte voor bedrijven, of meer persoonlijk contact, maar ook de terugkoppeling naar slachtoffers na een melding. Ten derde zou er een meldplicht ingevoerd kunnen worden. Een dergelijke meldplicht is recentelijk ingevoerd in Duitsland, en ook in het Verenigd Koninkrijk zou overwogen worden om het voor alle slachtoffers verplicht te maken om een ransomware-incident te melden bij de overheid (Martin, 2024). Toekomstig onderzoek moet uitwijzen wat de (juridische) mogelijkheden zijn voor het invoeren van een meldplicht in Nederland, en de mogelijke voor- en nadelen. Zo zou een dergelijke meldplicht gevolgen kunnen hebben voor hoe snel slachtoffers kunnen herstellen na een ransomware-incident, en moet rekening gehouden worden met capaciteitsbeperkingen bij de politie.

Een belangrijke uitkomst is, tot slot, dat het standpunt van de politie om het losgeld niet te betalen, een deel van de slachtoffers ervan weerhoudt om contact op te nemen met de politie. Dit roept de vraag op of dit advies effectief is. Er is meer onderzoek nodig naar de mate waarin het advies slachtoffers daadwerkelijk weerhoudt van het betalen van het losgeld. Vervolgens kan inzichtelijk gemaakt worden hoe zich dit verhoudt tot de uitkomst van het huidige onderzoek dat het sommige slachtoffers weerhoudt van het melden bij de politie, en wat dit betekent voor de communicatiestrategie van de politie.

9.2.2 *Beperkingen*

Hoewel het huidige onderzoek tot nieuwe inzichten heeft geleid, zijn er ook beperkingen waar rekening mee gehouden moet worden in de interpretatie van de resultaten.

Ten eerste zijn de data in deelstudie 1 en 2 verzameld onder deelnemers in een burger- en ondernemerspanel. Deze keuze is gemaakt omdat het doel was om onder een grote, representatieve groep Nederlandse burgers en ondernemers inzicht te krijgen in de prevalentie van ransomware. Een consequentie van deze keuze is dat er geen inzicht is verkregen in de ervaringen van grote organisaties (> 250 medewerkers), daar de grote meerderheid van de ondernemers in de panels zzp'ers of mkb'ers betrof. Het zou kunnen dat het beslissingsgedrag van grote organisaties anders is dan dat van zzp'ers en mkb'ers. Zo zijn er bijvoorbeeld indicaties in de expertinterviews dat grote organisaties sneller een cybersecuritybedrijf zullen inschakelen, wat weer gevolgen kan hebben voor de onderhandelings-, betalings- en meldingsbereidheid. Vervolgonderzoek zou zich op deze doelgroep kunnen richten.

Ten tweede zijn veel van de respondenten in deelstudie 1 langer dan 12 maanden geleden slachtoffer geworden. Voor meer dan de helft van de burgers en de zzp'ers en iets minder dan de helft van de mkb'ers was het incident 5 of meer jaar geleden. Er zou dus sprake kunnen zijn van een zogeheten *recall bias* als gevolg van het niet volledig of juist herinneren van kenmerken van het incident. Enkele respondenten gaven bijvoorbeeld in open antwoorden aan dat ze zich de precieze losgeldeis niet konden herinneren. Daarnaast ontwikkelt het ransomware-ecosysteem zich snel, waardoor de ervaringen van een slachtoffer van 5 jaar geleden niet representatief hoeven te zijn voor de ervaringen van een slachtoffer nu. Denk hierbij aan de *leak pages* van ransomwaregroeperingen die een ontwikkeling van de afgelopen paar jaar zijn. In dit verband zou longitudinaal onderzoek naar slachtofferschap gedaan kunnen worden, niet alleen om veranderingen in de modus operandi en ervaringen met slachtofferschap te kunnen meten, maar bijvoorbeeld ook om te zien wat de gevolgen van interventies zijn voor de prevalentie, het beslissingsgedrag en de impact.

Ten derde is in deelstudie 2 gebruikgemaakt van een vignetexperiment met een fictief ransomwarescenario. Voorafgaand aan de dataverzameling is een poweranalyse uitgevoerd om het aantal manipulaties in het vignet te bepalen. Deze werd gebaseerd op de geschatte steekproefgrootte van de kleinste groep, in dit geval de mkb'ers. Aangezien de nettosteekproefgrootte (n=732) kleiner was dan de oorspronkelijke schatting (n=1.150), was het vermogen om kleine effectgroottes te detecteren ook lager dan verwacht. Gezien de statistische significantie van de resultaten zijn we echter van mening dat de steekproefgrootte geen significante invloed had. Dit is bovendien niet van toepassing op de steekproeven onder burgers en zzp'ers die hoger uitvielen dan 1.150 respondenten.

Ten vierde roept de vergelijking tussen deelstudie 1 en 2 de vraag op in hoeverre beslissingsgedrag in het vignetexperiment daadwerkelijk keuzegedrag tijdens een echt ransomware-incident benadert. Hoewel de betalingsbereidheid zowel onder slachtoffers als in het vignetexperiment relatief laag is en dus overeen lijkt te komen, lopen de resultaten tussen beide deelstudies voor de meldingsbereidheid sterk uiteen, vergelijkbaar met de studie van Van de Weijer et al. (2020). Waar de meldingsbereidheid in het hypothetisch scenario hoog is, heeft minder dan 30% van de slachtoffers contact opgenomen met de politie en heeft een nog kleiner deel van de respondenten aangifte gedaan. Er is gebruikgemaakt van een vignetexperiment omdat dit gezien wordt als een nuttige methode voor onderzoek naar gevoelige onderwerpen (zoals slachtofferschap van ransomware) waarbij experimenteel onderzoek minder geschikt is vanwege ethische bezwaren (Aguinis & Bradley, 2014) en als een goed alternatief voor directe enquêtevragen, waardoor het realisme en de validiteit worden vergroot en de sociale wenselijkheidsbias wordt verminderd (Wason et al., 2022). Over het algemeen lijken vignetten een geschikte methode voor onderzoek naar een gevoelig onderwerp als ransomware, waarbij slachtoffers mogelijk minder bereid zijn om te melden dat ze slachtoffer zijn geworden of zijn afgeperst om losgeld te betalen. Om effectief te zijn, moeten vignetten echter zo realistisch mogelijk zijn (Aguinis & Bradley, 2014; Baguley et al., 2022) omdat onrealistische scenario's alleen illustreren welk gedrag of welke uitkomsten *kunnen* voorkomen, maar niet noodzakelijkerwijs wat er in een echte situatie *zal* gebeuren (Aguinis & Bradley, 2014). In een poging om zowel de immersie als het realisme van het vignet te verhogen, kregen respondenten een losgeldbericht en een losgeldwebsite te zien die zijn nagebootst van die van ransomwaregroeperingen. Daarnaast is gebruikgemaakt van een lopende timer om het gevoel van urgentie te verhogen en is gepoogd de ernst van het incident duidelijk te maken door te vermelden dat alle data en systemen ontoegankelijk zijn gemaakt. Hierdoor benaderde het vignet meer de ervaringen van ransomwareslachtofferschap in een natuurlijke omgeving, wat meer valide antwoorden opleverde (Aguinis & Bradley, 2014). Er is echter een mogelijkheid dat het vignet de respondenten nog steeds niet volledig onderdompelde, of dat ze de behoefte voelden om een sociaal wenselijk antwoord te geven. Bovendien is slachtofferschap van ransomware een *high stake*-scenario dat slechts tot bepaalde hoogte na te bootsen is in een vignetexperiment (Aguinis & Bradley, 2014). Hoewel respondenten een indruk kregen van de belangen die op het spel staan (zoals de kosten van het losgeld of het dreigende verlies van gegevens) en het gevoel van urgentie door een lopende timer, was op elk moment voor respondenten duidelijk dat het om een hypothetisch scenario ging. Daardoor is het denkbaar dat het vignet niet dezelfde context creëerde als in het 'echte leven' en dus niet dezelfde respons opleverde als in een natuurlijke omgeving (Aguinis & Bradley, 2014). Zodoende kunnen de uitkomsten uit het vignetexperiment alleen geïnterpreteerd worden als voorgenomen betalings- en meldingsgedrag, en niet als daadwerkelijk beslissingsgedrag.

Tot slot zijn in deelstudie 3 interviews gehouden met experts in de cybersecuritysector om meer inzicht te verkrijgen in adviezen met betrekking tot onderhandelen, betalen

en melden. Een beperking is dat deze respondenten vooral zicht hebben op grote(re) organisaties die slachtoffer zijn geworden, en in mindere mate op kleine of middelgrote organisaties, hoewel twee respondenten deze organisaties wel hebben bijgestaan. Het is mogelijk dat grote organisaties die slachtoffers zijn geworden andere beslissingen nemen als het gaat om onderhandelen, betalen of melden in vergelijking met zzp'ers of kleine en middelgrote organisaties.

Ondanks de beperkingen heeft het huidige onderzoek tot belangrijke inzichten geleid. Door verschillende methoden van onderzoek (i.e. slachtoffervragenlijsten, vignetexperiment en expertinterviews) te combineren is meer inzicht verkregen in slachtofferschap van ransomware. Dit heeft geleid tot een betere inschatting van de prevalentie van slachtofferschap van ransomware onder een representatieve groep respondenten, evenals meer inzicht in de aard en impact. Daarnaast is meer inzicht verkregen in de hulpbehoeften van slachtoffers en hun beslissingsprocessen, bijvoorbeeld als het gaat om onderhandelen, betalen en melden. Het onderzoek is bovendien onder verschillende doelgroepen uitgevoerd, namelijk burgers, zzp'ers en mkb'ers, slachtoffers en niet-slachtoffers. Hierdoor was het niet alleen mogelijk om het gedrag van verschillende typen slachtoffers te vergelijken, maar ook de vergelijking te maken tussen daadwerkelijk gedrag en de intentie tot gedrag. Dergelijke inzichten zijn van belang in de ontwikkeling van beleid om slachtofferschap van ransomware te voorkomen, de gevolgen ervan te mitigeren en slachtoffers adequate ondersteuning te bieden.

Literatuur

Aguinis, H. & Bradley, K. J. (2014). Best Practice Recommendations for Designing and Implementing Experimental Vignette Methodology Studies. *Organizational Research Methods*, *17*(4), 351–371. https://doi.org/10.1177/1094428114547952.

Akbanov, M., Vassilakis, V. G. & Logothetis, M. D. (2019). WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms. *Journal of Telecommunications and Information Technology*, *1*, 113–124. https://doi.org/10.26636/jtit.2019.130218.

Akkermans, M., Arends, J., Derksen, E. & Reep, C. (2023). *Online veiligheid en criminaliteit 2022*. CBS. https://www.cbs.nl/-/media/_pdf/2023/19/online-veiligheid-en-criminaliteit-2022.pdf.

Al-rimy, B. A. S., Maarof, M. A. & Shaid, S. Z. M. (2018). Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions. *Computers & Security*, *74*, 144–166. https://doi.org/10.1016/j.cose.2018.01.001.

Arief, B., Periam, A., Cetin, O. & Hernandez-Castro, J. (2020). Using eyetracker to find ways to mitigate ransomware. *ICISSP 2020 - Proceedings of the 6th International Conference on Information Systems Security and Privacy*, 448–456. https://doi.org/10.5220/0008956004480456.

Atzmüller, C. & Steiner, P. M. (2010). Experimental vignette studies in survey research. *Methodology*, *6*(3), 128–138. https://doi.org/10.1027/1614-2241/a000014.

Baguley, T., Dunham, G. & Steer, O. (2022). Statistical modelling of vignette data in psychology. *British Journal of Psychology*, *113*, 1143–1163. https://doi.org/10.1111/bjop.12577.

Bambenek, J. C. & Bashir, M. (2020). Ethics, Economics, and Ransomware: How Human Decisions Grow the Threat. In I. Corradini, E. Nardelli, & T. Ahram (Eds.), *Advances in Human Factors in Cybersecurity* (Vol. 1219, pp. 17–22). Springer International Publishing. https://doi.org/10.1007/978-3-030-52581-1_3.

Bergmann, M. C., Dreißigacker, A., Von Skarczinski, B. & Wollinger, G. R. (2018). Cyber-Dependent Crime Victimization: The Same Risk for Everyone? *Cyberpsychology, Behavior, and Social Networking*, *21*(2), 84–90. https://doi.org/10.1089/cyber.2016.0727.

Boticiu, S. & Teichmann, F. (2024). How does one negotiate with ransomware attackers? *International Cybersecurity Law Review*, *5*(1), 55–65. https://doi.org/10.1365/s43439-023-00106-w.

Brennenraedts, R., van der Vorst, T., Kats, J., Rieback, M., Vos, A., Jelicic, N., Jansen, R., Blom, T. & van Sambeek, N. (2022). *Verkenning risicofactoren ransomware-aanvallen*. Dialogic.

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R. & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 1–11. https://doi.org/10.1016/j.tele.2021.101675.

Caporusso, N., Chea, S. & Abukhaled, R. (2019). A Game-Theoretical Model of Ransomware. *Advances in Intelligent Systems and Computing. Proceedings of the AHFE 2018 International Conference on Human Factors in Cybersecurity*, *782*, 69–78. https://doi.org/10.1007/978-3-319-94782-2_7.

Cartwright, A., Cartwright, E., Xue, L. & Hernandez-Castro, J. (2023). An investigation of individual willingness to pay ransomware. *Journal of Financial Crime*, *30*(3), 728–741. https://doi.org/10.1108/JFC-02-2022-0055.

CBS. (n.d.). *Ontwikkelingen zzp*. Retrieved 2 July 2024, from https://www.cbs.nl/nl-nl/dossier/dossier-zzp/ontwikkelingen-zzp.

CBS. (2019). *Digitale Veiligheid & Criminaliteit 2018*. Centraal Bureau voor de Statistiek.

CBS. (2022). *Online Veiligheid en Criminaliteit 2022 [Vragenlijst]*.

CBS. (2023). *Cybersecuritymonitor 2022*. CBS. https://www.cbs.nl/-/media/_pdf/2023/31/cybersecuritymonitor_2022.pdf.

Cialdini, R. B. (2006). *The Psychology of Persuasion*. Harper Business.

Cohen, J. (1988). *Statistical Power Analysis for the Behavioral Sciences Second Edition*. Lawrence Erlbaum Associates.

Connolly, L. Y. & Borrion, H. (2022). Reducing Ransomware Crime: Analysis of Victims' Payment Decisions. *Computers & Security*, *119*, 1–14. https://doi.org/10.1016/j.cose.2022.102760.

Conradie, M. (2023). *Cybersecurity onderzoek Alert Online 2023*.

Consumentenbond. (n.d.). *Ransomware (gijzel-software) voorkomen en verwijderen*. Retrieved 7 May 2024, from https://www.consumentenbond.nl/veilig-internetten/ransomware-cryptoware-gijzelsoftware.

Conti, M., Gangwal, A. & Ruj, S. (2018). On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security*, *79*, 162–189. https://doi.org/10.1016/j.cose.2018.08.008.

Cybbar & CSD. (2023). *Cybercrime against businesses in the EU: Challenges to Reporting [Policy Brief]* (pp. 1–4).

CyberEdge Group (2022). *2022 Cyberthreat Defense Report* (pp. 1–66). CyberEdge Group. https://cyber-edge.com/cyberthreat-defense-report-2022/.

Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G. & Benedetto, L. (2019). A Cyber-Kill-Chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277–305. https://doi.org/10.1007/s11416-019-00338-7.

Digital Trust Center. (n.d.-a). *Incident response plan*. Retrieved 30 April 2024, from https://www.digitaltrustcenter.nl/informatie-advies/incident-response-plan#:~:text=Wat%20is%20incident%20response%3F,plaatsvindt%3A%20een%20Incident%20Response%20Plan.

Digital Trust Center. (n.d.-b). *Wat te doen bij een ransomware-aanval?* Retrieved 7 May 2024, from https://www.digitaltrustcenter.nl/informatie-advies/ransomware/wat-te-doen-bij-een-ransomware-aanval.

Digital Trust Center. (2024, April 25). *Samenwerkingsverband Melissa vindt diverse Nederlandse slachtoffers van ransomwaregroepering Cactus*. https://www.digitaltrustcenter.nl/nieuws/samenwerkingsverband-melissa-vindt-diverse-nederlandse-slachtoffers-van-ransomwaregroepering.

ENISA. (2021). *ENISA Threat Landscape 2021*. https://doi.org/10.2824/324797.

European Commission. (2022). *Flash Eurobarometer 496—SMEs and cybercrime*. https://doi.org/10.2837/89101.

Europol. (2021). *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Europol. https://doi.org/10.2813/113799.

Europol. (2023). *IOCTA, internet organised crime threat assessment 2023.* Publications Office. https://data.europa.eu/doi/10.2813/587536.

Eurostat. (2022). *Number of persons employed by enterprise size class, 2019 [Infographic]*. https://ec.europa.eu/eurostat/cache/infographs/sbs_2022/#small.

Evers, J. (2015). *Kwalitatieve analyse: Kunst én kunde*. Boom Lemma Uitgevers.

FBI. (2021). *Internet Crime Report* (pp. 1–33). FBI.

Ferbrache, D. (1992). *A Pathology of Computer Viruses*. Springer-Verlag.

Fraudehelpdesk. (n.d.). *Uw computerbestanden worden gegijzeld*. Retrieved 7 May 2024, from https://www.fraudehelpdesk.nl/ondernemers-fraude/uw-computerbestanden-worden-gegijzeld/#:~:text=Gijzelsoftware%2C%20ook%20wel%20ransomware%20genoemd,het%20Engels%20'ransom'.

Gottfredson, M. R. & Hindelang, M. J. (1979). A Study of the Behavior of Law. *American Sociological Review*, *44*(1), 3. https://doi.org/10.2307/2094813.

Grauer, K., Jardine, E., Leosz, E. & Updegrave, H. (2023). *The 2023 Crypto Crime Report*. Chainalysis. https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

Grauer, K., Kueshner, W. & Updegrave, H. (2022). *The 2022 Crypto Crime Report: Original data and research into cryptocurrency-based crime* (pp. 1–140). Chainalysis. https://go.chainalysis.com/2022-Crypto-Crime-Report.html.

Green, J. A. (2021). Too many zeros and/or highly skewed? A tutorial on modelling health behaviour as count data with Poisson and negative binomial regression. *Health Psychology and Behavioral Medicine*, *9*(1), 436–455. https://doi.org/10.1080/21642850.2021.1920416.

Hadlington, L. (2017). *Exploring the Psychological Mechanisms used in Ransomware Splash Screens* (pp. 1–20). De Montfort University Leicester.

Hilbe, J. M. (2011). *Negative Binomial Regression*. Cambridge University Press. https://doi.org/10.1017/CBO9780511973420.

Ipsos I&O. (n.d.-a). *I&O Research Ondernemerspanel*. I&O Research Panel. Retrieved 14 April 2023, from https://www.ioresearch.nl/onderzoeksmethoden/io-research-ondernemerspanel/.

Ipsos I&O. (n.d.-b). *I&O Research Panel*. I&O Research Panel. Retrieved 15 December 2022, from https://www.ioresearch.nl/onderzoeksmethoden/io-research-panel/.

Johns, E. (2021). *Cyber Security Breaches Survey 2021*. Department for Digital, Culture, Media & Sport.

Kaspersky. (2021). *Consumer appetite versus action: The state of data privacy amid growing digital dependency* (pp. 1–13).

Keane, O. (1990). Legal Issues. *Virus Bulletin*, 8–10.

Keshavarzi, M. & Ghaffary, H. R. (2020). I2CE3: A dedicated and separated attack chain for ransomware offenses as the most infamous cyber extortion. *Computer Science Review*, *36*, 2–18. https://doi.org/10.1016/j.cosrev.2020.100233.

Knebel, S., Schultz, M. D. & Seele, P. (2021). Cyberattacks as "state of exception" reconceptualizing cybersecurity from prevention to surviving and accommodating. *Journal of Information, Communication and Ethics in Society*, 1–19. https://doi.org/10.1108/JICES-01-2021-0015.

Leukfeldt, R., Notté, R. & Malsch, M. (2018). *Slachtofferschap van online criminaliteit: Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit*. NSCR.

Martin, A. (2024, May 21). Exclusive: UK to propose mandatory reporting for ransomware attacks and licensing regime for all payments. *The Record*. https://therecord.media/uk-proposal-mandatory-reporting-ransomware-attacks.

Matthijsse, S. R., Moneva, A., Van 't Hoff-de Goede, M. S. & Leukfeldt, E. R. (2024). Examining ransomware payment decision-making among small and medium-sized enterprises. European Journal of Criminology, 0(0), 1–21. https://doi.org/10.1177/14773708241285671.

Matthijsse, S. R., van 't Hoff-de Goede, M. S. & Leukfeldt, E. R. (2023). Your files have been encrypted: A crime script analysis of ransomware attacks. *Trends in Organized Crime*. https://doi.org/10.1007/s12117-023-09496-z.

Meland, P. H., Bayoumy, Y. F. F. & Sindre, G. (2020). The Ransomware-as-a-Service economy within the darknet. *Computers & Security*, *92*, 1–9. https://doi.org/10.1016/j.cose.2020.101762.

Meurs, T. & Holterman, L. (2023). *Data-exfiltratie bij een ransomware-aanval*. Cyberveilig Nederland, NCSC, Politie, Openbaar Ministeria, Data Expert, Fox-IT, Deloitte, Tesorion, Kennedy van der Laan, Computest, Northwave, Trellix & NFIR.

Meurs, T., Junger, M., Tews, E. & Abhishta, A. (2022a). NAS-ransomware: Hoe ransomware-aanvallen tegen NAS-apparaten verschillen van reguliere ransomware-aanvallen. *Tijdschrift voor Veiligheid*, *21*(3–4), 69–88. https://doi.org/10.5553/TvV/.000044.

Meurs, T., Junger, M., Tews, E. & Abhishta, A. (2022b). *Ransomware: How attacker's effort, victim characteristics and context influence ransom requested, payment and financial loss*. 2022 APWG Symposium on Electronic Crime Research (eCrime).

Mott, G., Turner, S., Nurse, J. R. C., MacColl, J., Sullivan, J., Cartwright, A. & Cartwright, E. (2023). Between a rock and a hard(ening) place: Cyber insurance in the ransomware era. *Computers & Security*, *128*. https://doi.org/10.1016/j.cose.2023.103162.

NCSC. (n.d.). *Ransomware*. Retrieved 7 May 2024, from https://www.ncsc.nl/wat-kun-je-zelf-doen/dreiging/ransomware.

NCSC. (2023, October 3). *Melissa: Samenwerkingsverband ransomwarebestrijding*. https://www.ncsc.nl/actueel/nieuws/2023/oktober/3/melissa-samenwerkingsverband-ransomwarebestrijding.

NCTV. (2021). *Cybersecuritybeeld Nederland* (pp. 1–66). Nationaal Coördinator Terrorismebestrijding en Veiligheid. https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021.

NCTV. (2022). *Cybersecuritybeeld Nederland 2022* (pp. 1–50). NCTV. https://www.nctv.nl/documenten/publicaties/2022/07/04/cybersecuritybeeld-nederland-2022.

Nieuwesteeg, B. & Faure, M. (2023). The Uneasy Case for a Ransom Tax. *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2022.45.

Nieuwesteeg, B., van der Sluijs, A., Ferwerda, H., van der Donck, M., Oldengarm, P. & Leukfeldt, R. (2022). *Nederlands Cyber Security Lab Labsessie #4 Hoe kunnen we organisaties helpen om geen losgeld meer te betalen?*.

No More Ransom. (n.d.-a). *Ontsleuteltools*. Retrieved 7 May 2024, from https://www.nomoreransom.org/nl/decryption-tools.html.

No More Ransom. (n.d.-b). *Veelgestelde vragen over ransomware*. Retrieved 7 May 2024, from https://www.nomoreransom.org/nl/ransomware-qa.html#payment.

Northwave. (2022). *After the crisis comes the blow: The mental impact of ransomware attacks*.

Ortloff, A. M., Vossen, M. & Tiefenau, C. (2021). Replicating a study of ransomware in Germany. *ACM International Conference Proceeding Series*, 151–164. https://doi.org/10.1145/3481357.3481508.

Project Melissa. (2024). *Jaarbeeld Ransomware 2023*. https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2024/februari/22/jaarbeeld-ransomware-2023/Jaarbeeld_Ransomware_2023_jan_dec.pdf.

Rijksoverheid. (2024, June 24). *EU sanctioneert voor het eerst cybercriminele kopstukken*. https://www.rijksoverheid.nl/ministeries/ministerie-van-buitenlandse-zaken/nieuws/2024/06/24/eu-sancties-cybercriminele-kopstukken.

Sajjan, R. S. & Ghorpade, V. R. (2017). Ransomware Attacks: Radical Menace for Cloud Computing. *International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, 1640–1646.

Saldaña, J. (2013). *The coding manual for qualitative researchers* (2nd ed). SAGE.

Simoiu, C., Gates, C., Bonneau, J. & Goel, S. (2019). 'I was told to buy a software or lose my computer. I ignored it': A study of ransomware. *USENIX Symposium on Usable Privacy and Security (SOUPS)*, 155–174.

Skogan, W. G. (1984). Reporting Crimes to the Police: The Status of World Research. *Journal of Research in Crime and Delinquency*, *21*(2), 113–137.

Sophos. (2021). *The State of Ransomware 2021* (pp. 1–18).

Tarling, R. & Morris, K. (2010). Reporting Crime to the Police. *British Journal of Criminology*, *50*(3), 474–490.

Van de Weijer, S. G. A., Leukfeldt, E. R. & Van der Zee, S. (2020). *Slachtoffer van online criminaliteit, wat nu? Een onderzoek naar de aangiftebereidheid onder burgers en ondernemers*. Sdu Uitgevers. https://www.politieenwetenschap.nl/publicatie/politiewetenschap/2020/slachtoffer-van-onlinecriminaliteit-wat-nu-356/.

Van de Weijer, S. G. A. & Leukfeldt, R. (2023). *Cybercriminaliteit tijdens de coronacrisis: Aard, omvang en impact van cyberrisico's voor burgers en het mkb*. NSCR/De Haagse Hogeschool.

Van de Weijer, S. G. A., Leukfeldt, R. & Bernasco, W. (2019). Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology*, *16*(4), 486–508. https://doi.org/10.1177/1477370818773610.

Veenstra, S., Zuurveen, R. & Stol, W. (2015). *Cybercrime onder bedrijven Een onderzoek naar slachtofferschap van cybercrime onder het Midden-en Kleinbedrijf en Zelfstandigen Zonder Personeel in Nederland*. NHL Hogeschool/Politieacademie/Open Universiteit. https://cybersciencecenter.nl/media/1054/2015-05-13-cybercrime-onder-bedrijven-def.pdf.

Voce, I. & Morgan, A. (2021). Ransomware victimisation among Australian computer users. *Statistical Bulletin*, *35*, 1–17.

Voce, I. & Morgan, A. (2022). Help-seeking among Australian ransomware victims. *Statistical Bulletin*, *38*, 1–13. https://doi.org/10.52922/sb78504.

Voce, I. & Morgan, A. (2023). *Cybercrime in Australia 2023* (43). Australian Institute of Criminology. https://doi.org/10.52922/sr77031.

Wanamaker, K. A. (2019). *Profile of Canadian businesses who report cybercrime to police: The 2017 Canadian Survey of Cyber Security and Cybercrime*. Public Safety Canada.

Wason, K. D., Polonsky, M. J. & Hyman, M. R. (2022). Designing vignette studies in marketing. *Australasian Marketing Journal*, *10*(3), 41–58.

Whelan, C., Bright, D. & Martin, J. (2023). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology*, 26338076231199793. https://doi.org/10.1177/26338076231199793.

Yilmaz, Y., Cetin, O., Arief, B. & Hernandez-Castro, J. (2021). Investigating the impact of ransomware splash screens. *Journal of Information Security and Applications*, *61*, 1–13. https://doi.org/10.1016/j.jisa.2021.102934.

Yilmaz, Y., Cetin, O., Grigore, C., Arief, B. & Hernandez-Castro, J. (2022). Personality Types and Ransomware Victimisation. *Digital Threats: Research and Practice*. https://doi.org/10.1145/3568994.

Young, A. L. & Yung, M. (2017). On Ransomware and Envisioning the Enemy of Tomorrow. *Computer*, *50*(11), 82–85.

Bijlage 1 Vragenlijst 1A

Inleiding en informed consent
Bedankt dat u wilt deelnemen aan dit onderzoek van de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Dit onderzoek gaat over online criminaliteit. Wij willen aan u vragen of u online criminaliteit heeft meegemaakt en welke gevolgen u heeft ervaren.

Waarom hebben wij uw ervaringen nodig?
Pas wanneer we weten hoeveel mensen slachtoffer worden en wat er precies gebeurd is, kunnen we iets doen aan online criminaliteit. We willen u daarom vragen zo eerlijk mogelijk over uw eventuele ervaringen te vertellen.

Privacy en anonimiteit
Dit vragenlijstonderzoek is gemaakt door onderzoekers van de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving en wordt uitgevoerd door I&O Research. Uw antwoorden worden uitsluitend gebruikt voor het doel van het onderzoek en verwerkt volgens de privacyverklaring van I&O Research.[44] Er zijn maatregelen genomen om ervoor te zorgen dat uw antwoorden niet naar u te herleiden zijn. Dat betekent bijvoorbeeld dat I&O Research uw antwoorden verstuurt aan de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving op een manier dat deze niet naar u te zijn herleiden. In een publicatie zullen anonieme gegevens worden gebruikt.

Ik verklaar dat:
- Ik weet dat het onderzoek wordt uitgevoerd zoals beschreven in bovenstaande toelichting. Ik heb dit gelezen en begrijp de informatie.
- Ik genoeg tijd heb gehad om te beslissen of ik wil deelnemen.
- Ik weet dat meedoen vrijwillig is en dat ik op ieder moment kan beslissen om toch niet mee te doen of te stoppen met het onderzoek. Daarvoor hoef ik geen reden te geven. Ik begrijp dat het intrekken van mijn toestemming geen gevolgen heeft voor de verwerking van mijn persoonsgegevens in de periode voorafgaand aan het intrekken van de toestemming.
- Ik toestemming geef voor het verzamelen, bewaren en gebruiken van mijn ingevulde gegevens voor de beantwoording van de onderzoeksvraag in dit onderzoek.

44 Zie https://www.iopanel.nl/privacy.

- Ik weet dat de gegevens die de onderzoekers bewaren geanonimiseerd zijn en niet rechtstreeks te herleiden zijn naar mijn persoon.
- Ik weet dat onderzoeksgegevens na het onderzoek nog 10 jaar worden bewaard en daarna worden vernietigd.

Door de knop 'ja' aan te klikken stemt u in met deelname aan het onderzoek en gaat u ermee akkoord dat I&O Research en de Haagse Hogeschool uw gegevens verwerken voor dit onderzoek.

Stemt u ermee in dat wij uw antwoorden voor dit onderzoek gebruiken? [Verplichte vraag]
☐ Ja [door naar Q1a]
☐ Nee [Einde vragenlijst]

Q1a. Screeningsvraag 1a
Welke van de volgende vormen van online criminaliteit of een poging daartoe heeft u ooit meegemaakt?

Phishing: u ontving een e-mail of ander bericht dat van een legitieme instantie leek te komen, maar waarschijnlijk van een oplichter was om uw (inlog)gegevens te achterhalen.
☐ Ja
☐ Nee

Vriend-in-nood-fraude: u ontving bijvoorbeeld via WhatsApp-berichten van iemand die zich voordeed als een bekende en om geld vroeg (bijvoorbeeld vanwege een zogenaamd noodgeval).
☐ Ja
☐ Nee

Voorschotfraude: u moest een voorschot betalen om een groot bedrag te ontvangen (bijvoorbeeld vanwege een erfenis, investering of loterij).
☐ Ja
☐ Nee

Ransomware: uw bestanden, gegevens of appara(a)t(en) werden geblokkeerd of versleuteld en er werd om losgeld gevraagd om hier weer toegang tot te krijgen.
☐ Ja
☐ Nee

Datingfraude: u werd door iemand die u heeft ontmoet via een datingsite of sociale media gevraagd om geld over te maken (bijvoorbeeld zogenaamd om u te bezoeken of vanwege een noodgeval).
☐ Ja
☐ Nee

Aankoopfraude: u heeft via internet een product of dienst aangeschaft dat nooit geleverd is.
☐ Ja
☐ Nee

Helpdeskfraude: u heeft iemand die zich voordeed als een medewerker van een helpdesk toegang gegeven tot uw computer, waarna er geld afhandig is gemaakt.
☐ Ja
☐ Nee

Identiteitsfraude: er is zonder uw toestemming gebruikgemaakt van uw persoonlijke of financiële gegevens (bijvoorbeeld om producten te kopen of documenten aan te vragen op uw naam).
☐ Ja
☐ Nee

Bij elke vorm moet een meer uitgebreide toelichting zichtbaar zijn als pop-up.

Phishing
Phishing is een vorm van online oplichting waarbij criminelen e-mails of websites van legitieme instanties namaken om slachtoffers te misleiden, om zodoende (inlog)gegevens te achterhalen en toegang te krijgen tot online accounts.

Vriend-in-nood-fraude
Bij Vriend-in-nood-fraude sturen criminelen bijvoorbeeld via WhatsApp berichten, waarbij zij doen alsof zij een bekende van het slachtoffer zijn en zij een nieuw telefoonnummer hebben. Als het slachtoffer eenmaal overtuigd is dat de berichten van deze vriend of familielid komen, vragen de criminelen om geld (bijvoorbeeld vanwege een noodgeval). Slachtoffers maken geld over in de overtuiging dat zij hun vriend of familielid helpen.

Voorschotfraude
De kern van voorschotfraude is dat slachtoffers via e-mail of sociale media worden gevraagd om een voorschot te betalen om vervolgens een groot bedrag te ontvangen. Het gaat dan bijvoorbeeld om een zogenaamde erfenis, investering of loterij.

Ransomware
Wanneer je slachtoffer bent van ransomware, ook wel gijzelsoftware genoemd, blokkeren of versleutelen criminelen je bestanden, gegevens of appara(a)t(en) en geven die pas weer vrij als losgeld wordt betaald.

Datingfraude
Slachtoffers van datingfraude worden opgelicht door iemand die zij hebben ontmoet via bijvoorbeeld een datingsite of sociale media. Na het aangaan van de relatie vraagt de oplichter het slachtoffer om geld over te maken, bijvoorbeeld om het slachtoffer te bezoeken of vanwege een noodgeval.

Helpdeskfraude
Bij helpdeskfraude hebben slachtoffers telefonisch contact met iemand die zich voordoet als een medewerker van een helpdesk van een softwarebedrijf, zoals Microsoft. De oplichters overtuigen slachtoffers hen toegang te geven tot hun computer en maken hen uiteindelijk geld afhandig.

Aankoopfraude
Slachtoffers van aankoopfraude kopen via internet een product of dienst en hebben ten minste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is, omdat de verkoper hen heeft opgelicht.

Identiteitsfraude
Identiteitsfraude houdt in dat iemand zonder uw toestemming uw persoonlijke of financiële gegevens gebruikt om er zelf geld aan te verdienen. Iemand koopt bijvoorbeeld producten op uw naam of vraagt officiële documenten aan op uw naam. Meestal is identiteitsfraude een gevolg van diefstal van identiteitsgegevens, maar het kan ook zijn dat u zelf de identiteitsgegevens heeft verstrekt.

[Indien ransomware = ja, ga naar Q1b. Indien ransomware = nee, einde onderzoek]

Q1b. Screeningsvraag 1b
U heeft aangegeven dat uw bestanden, gegevens of apparaten ooit geblokkeerd of versleuteld zijn door criminelen en dat er om losgeld is gevraagd om hier weer toegang tot te krijgen. Klopt het dat u dit is overkomen?
☐ Ja [door naar Q2]
☐ Nee [Einde onderzoek]

Q2. Screeningsvraag 2
Welke van de volgende scenario's is op u van toepassing?
☐ Ik ben zelf slachtoffer geworden [door naar Q3]
☐ De organisatie waar ik werk is slachtoffer geworden en daardoor waren mijn gegevens, bestanden en/of apparaten versleuteld [Einde onderzoek]

Wat u is overkomen noemen wij ransomware. We zouden u graag vragen stellen over wat er is gebeurd en de gevolgen die u heeft ervaren. We willen u vragen zo eerlijk mogelijk over uw ervaring te vertellen.

We stellen u eerst enkele algemene vragen.

Blok 1: Achtergrondkenmerken

Q1. Tijd online
Hoeveel tijd spendeert u doorgaans online voor privédoeleinden?
☐ Minder dan 1 keer per maand
☐ Minimaal 1 keer per maand, maar niet wekelijks
☐ Minimaal 1 keer per week, maar niet dagelijks
☐ Dagelijks
☐ Meerdere keren per dag
☐ Minstens ieder uur (tijdens de uren dat ik wakker ben)
☐ Ik ben (bijna) continu online (tijdens de uren dat ik wakker ben)

Q2. Cybersecuritymaatregelen
Welke van de volgende beveiligingsmaatregelen nam u voordat u slachtoffer werd? (Meerdere antwoorden mogelijk)
☐ Ik maakte back-ups van mijn bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Ik had unieke wachtwoorden ingesteld voor al mijn apparaten en accounts
☐ Ik deelde mijn persoonlijk wachtwoorden niet met anderen
☐ Ik had een up-to-date antivirusproduct
☐ Ik had een firewall
☐ Ik liet beveiligingssoftware mijn apparaten scannen op virussen of andere kwaadaardige software
☐ Ik voerde updates van besturingssystemen, apps en/of software direct uit zodra ze beschikbaar zijn
☐ Ik was voorzichtig met welke websites ik bezoek, wat ik download en welke bijlagen ik open
☐ Ik maakte gebruik van een VPN-verbinding
☐ Ik gebruikte browserextensies die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Ik had mijn persoonlijke bestanden en gegevens versleuteld
☐ Ik had tweestapsverificatie ingesteld (2 stappen in plaats van 1 stap om in te loggen)
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Pop-up 2h: Een VPN (Virtual Private Network)-verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
Pop-up 2i: Een browserextensie is software die een browser extra functionaliteit beidt, zoals het managen van cookies of advertenties tijdens het surfen op internet

---

Blok 2: Omstandigheden
We zullen u nu vragen stellen over wat er is gebeurd toen u slachtoffer werd van ransomware.

We willen hier nogmaals benadrukken dat alle antwoorden geanonimiseerd worden en niet terug te herleiden zijn naar u.

Q3. Slachtofferschap – frequentie
Hoe vaak bent u slachtoffer geworden van ransomware?
☐ 1 keer [door naar Q4]
☐ 2 keer [Onderstaande melding weergeven voordat men doorgaat naar Q4:]
☐ 3 keer [Onderstaande melding weergeven voordat men doorgaat naar Q4:]
☐ 4 keer of vaker [Onderstaande melding weergeven voordat men doorgaat naar Q4:]

U heeft aangegeven dat u meerdere keren slachtoffer bent geworden van ransomware. Wilt u de vervolgvragen in dit onderzoek alstublieft alleen beantwoorden over de laatste keer dat dit gebeurde?

Q4. Slachtofferschap – wanneer
Wanneer bent u (voor het laatst) slachtoffer geworden van ransomware?
☐ Een jaar geleden of minder
☐ Tussen 1 en 2 jaar geleden
☐ Tussen de 2 en 4 jaar geleden
☐ 5 of meer jaar geleden

Q5. Type ransomware
Had de ransomware-aanval een van de volgende kenmerken?
☐ Ik zag een scherm, pop-up of bericht waarin stond dat mijn apparaat was vergrendeld (*locked*).
☐ Ik zag een scherm, pop-up of bericht waarin stond dat mijn gegevens of bestanden versleuteld (*encrypted*) waren.
☐ Ik zag een bericht, zogenaamd van een wetshandhavingsinstantie (bijv. FBI, ministerie van Justitie), dat me informeerde dat ik betrapt was op het uitvoeren van een illegale of ongewenste activiteit online.
☐ Geen van bovenstaande
☐ Ik weet het niet meer

Q6. Type apparaat
Welke apparaten of systemen waren geblokkeerd of versleuteld? (Meerdere antwoorden mogelijk)
☐ Computer (desktop of laptop)
☐ Mobiele telefoon of smartphone
☐ Tablet
☐ Computerserver(s)
☐ Cloudopslag (bijvoorbeeld iCloud, OneDrive)
☐ Back-up(s)
☐ Anders, namelijk … [open antwoord]

Q7. Type data
Welk type bestanden of gegevens waren geblokkeerd of versleuteld? Als uw apparaat geheel geblokkeerd of versleuteld was, vragen we u aan te geven welke type bestanden op dit apparaat waren opgeslagen. (Meerdere antwoorden mogelijk)
☐ Persoonsgegevens (bijv. informatie over naam, adres, inloggegevens, kopie paspoort)
☐ Bestanden met emotionele waarde (bijv. foto's/video's)
☐ Bestanden voor studie of werk
☐ Financiële gegevens en boekhouding
☐ Anders, namelijk … [open antwoord]
☐ Weet ik niet

Q8. Besmetting
Met de kennis die u nu heeft, hoe denkt u dat de ransomware op uw apparaat of systeem is gekomen?
☐ Ik klikte op een link of opende een bijlage in een e-mail
☐ Ik klikte op een link, advertentie of pop-up tijdens het surfen op internet
☐ Een bedrijf waar mijn gegevens bekend waren was gehackt
☐ Er zat een kwetsbaarheid of beveiligingslek in software of een systeem dat ik gebruikte
☐ Ik had een applicatie of software geïnstalleerd die kwaadaardig bleek te zijn
☐ Anders, namelijk … [open antwoord]
☐ Weet ik niet

Q9. Eerste emotie
Op enig moment hebben de criminelen u om geld gevraagd om weer toegang te krijgen tot uw bestanden, gegevens of apparaten. Dit noemen we een losgeldbericht.
Wat voelde u toen u geconfronteerd werd met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik voelde me boos
☐ Ik voelde afkeer
☐ Ik voelde me bang

☐ Ik voelde me nerveus
☐ Ik voelde me verdrietig
☐ Ik voelde me ontspannen
☐ Ik voelde me blij
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q10. Eerste reactie
Welke van de volgende dingen heeft u gedaan toen u werd geconfronteerd met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik heb de verbinding met internet verbroken [door naar Q11]
☐ Ik heb mijn apparaat opnieuw opgestart [Door naar Q11]
☐ Ik heb mijn apparaat teruggezet naar fabrieksinstellingen [door naar Q11]
☐ Ik heb hulp of advies gezocht op internet [door naar Q12]
☐ Ik heb hulp of advies gezocht van een bekende [door naar Q12]
☐ Ik heb hulp of advies gezocht van een organisatie of instantie [door naar Q12]
☐ Ik heb mijn bestanden of gegevens geprobeerd te herstellen vanaf een back-up [door naar Q11]
☐ Ik heb geprobeerd om een programma te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen [door naar Q11]
☐ Ik heb geprobeerd mijn bestanden weer te openen door hun extensie terug te veranderen naar hun originele formaat [door naar Q11]
☐ Ik heb het losgeld betaald [door naar Q12]
☐ Ik heb niks gedaan [door naar Q12]
☐ Ik heb iets anders gedaan, namelijk … [door naar Q11]

Bij antwoordoptie 10g pop-up met nadere toelichting: *Een bestandsextensie is een toevoeging aan het einde van een bestandsnaam die aanduidt om wat voor soort bestand het gaat, zoals .docx of .jpg.*

Q11. Eerste reactie – gevolg
U heeft zelf geprobeerd om uw bestanden, gegevens of apparaten terug te krijgen. Is dat gelukt?
☐ Ja, volledig
☐ Ja, gedeeltelijk
☐ Nee

Blok 3: Afpersing
We zullen u nu enkele vragen stellen over het losgeldbericht en hoe u gereageerd heeft.

Bij woord 'losgeldbericht' pop-up met nadere toelichting:

> *Als u slachtoffer bent geworden van ransomware zal u in de meeste gevallen geïnformeerd worden via* **een losgeldbericht** *op uw scherm of een tekstbestand op uw apparaat. Het losgeldbericht bevat meestal informatie over hoe u moet betalen en wat er gebeurt als u dat niet doet.*

Q12. Hoogte losgeld
Hoeveel losgeld werd van u geëist?
Noteer het bedrag en de valutasoort (bijv. euro's, dollars, bitcoin). Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐[Open antwoord – tekst]

[Vraag is verplicht]

Q13. Deadline
Hoelang had u de tijd om het losgeld te betalen?
Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐ Minder dan 24 uur
☐ 1-3 dagen
☐ 4-6 dagen
☐ 7 of meer dagen
☐ Dat stond niet in het losgeldbericht

Q14. Contact met daders
Heeft u of iemand anders contact opgenomen met de daders?
☐ Ja, ik heb zelf contact opgenomen met de daders [door naar Q15]
☐ Ja, een bekende heeft namens mij contact opgenomen met de daders [door naar Q15]
☐ Ja, ik heb iemand ingehuurd om namens mij contact op te nemen met de daders [door naar Q15]
☐ Nee, ik heb geen contact opgenomen met de daders [door naar Q19]

Q15. Contact – hoe
Hoe heeft u (of iemand namens u) contact opgenomen met de daders?
☐ Via e-mail
☐ Via een chatsysteem op een website of portaal van de daders
☐ Telefonisch
☐ Via een ander communicatiemiddel, namelijk …[open antwoord]

Q16. Contact – doel
Met welk doel heeft u (of iemand namens u) contact opgenomen met de daders? (Meerdere antwoorden mogelijk)
☐ Om vast te stellen of het losgeldbericht echt was [door naar Q19]
☐ Om te informeren over de hoogte van het losgeld (bijvoorbeeld omdat dit in het losgeldbericht niet vermeld stond) [door naar Q19]
☐ Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline [door naar Q17]
☐ Om vast te stellen welke bestanden of gegevens door de criminelen waren gestolen [door naar Q19]
☐ Om hulp te vragen bij het betalen (bijvoorbeeld bij het aanschaffen van bitcoin) [door naar Q19]
☐ Om hulp te vragen na het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens) [door naar Q19]
☐ Om tijd te rekken [door naar Q19]
☐ Anders, namelijk … [open antwoord] [door naar Q19]

Q17. Onderhandelen – doel
U heeft aangegeven dat er is onderhandeld met de daders. Met welk doel is er onderhandeld? (Meerdere antwoorden mogelijk)
☐ Om het losgeldbedrag te verlagen [door naar Q18]
☐ Om langer de tijd te krijgen [door naar Q18]
☐ Om een andere reden, namelijk … [open antwoord] [door naar Q18]
☐ Er is niet onderhandeld [door naar Q19]

Q18. Onderhandelen – resultaat
Wat was de uitkomst van de onderhandeling? (Meerdere antwoorden mogelijk)
☐ Het losgeldbedrag is verlaagd
☐ De deadline is verlengd
☐ Geen verandering
☐ Anders, namelijk …[open antwoord]

Q19. Aanvullende dreiging
Hebben de daders op enig moment gedreigd met een van de volgende dingen? (Meerdere antwoorden mogelijk)
☐ Er is gedreigd met het verwijderen van de decryptiesleutel
☐ Er is gedreigd met het lekken van mijn bestanden of gegevens
☐ Er is gedreigd met een DDoS-aanval
☐ Er is gedreigd met iets anders, namelijk … [open antwoord]
☐ Geen van bovenstaande

Bij antwoordoptie 19a pop-up met nadere toelichting: *Met een decryptiesleutel kunnen ontoegankelijk gemaakte bestanden ontsleuteld worden.*

Bij antwoordoptie 19c pop-up met nadere toelichting: *Een Distributed Denial of Service (DDoS)-aanval is een poging van cybercriminelen om ontzettend veel verzoeken naar een netwerk of website te versturen waardoor deze onbereikbaar wordt voor gebruikers. Dit is te vergelijken met een digitale file.*

Q20. Losgeld – betaald
Heeft u het gevraagde losgeld betaald?
☐ Ja, ik heb een deel van het gevraagde bedrag betaald [door naar Q21]
☐ Ja, ik heb het volledige bedrag betaald [door naar Q21]
☐ Nee, ik heb niet betaald [door naar Q25]

Q21. Hoogte losgeld – betaald
Hoeveel losgeld heeft u betaald?
Noteer het bedrag en de valutasoort (bijv. euro's, dollars, bitcoin). Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐[Open antwoord – tekst]
☐ Zeg ik liever niet

Q22. Reden – betaald
Wat was de reden dat u betaald heeft? (Meerdere opties mogelijk)
☐ Het gevraagde bedrag was niet heel hoog en ik kon het makkelijk betalen
☐ Een bekende adviseerde om het losgeld te betalen
☐ Een IT- of cybersecurityspecialist adviseerde om het losgeld te betalen
☐ Ik had geen back-ups van de bestanden en gegevens die ontoegankelijk waren
☐ De geblokkeerde of versleutelde bestanden, gegevens of apparaten waren belangrijk, ik wilde deze niet verliezen
☐ Ik vertrouwde erop dat ik na betaling weer toegang tot mijn apparaten, bestanden en gegevens zou krijgen
☐ Ik was bang dat de criminelen de bestanden of gegevens zouden lekken (met anderen delen) of dat er andere vervelende gevolgen zouden zijn als ik niet betaalde
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties

[door naar Q24]

Q23. Reden – niet betaald
Wat was de reden dat u niet betaald heeft? (Meerdere opties mogelijk)
☐ Het gevraagde bedrag was te hoog en ik kon dit niet betalen
☐ De politie adviseerde om het losgeld niet te betalen
☐ Een bekende adviseerde om het losgeld niet te betalen
☐ Een IT- of cybersecurityspecialist adviseerde om het losgeld niet te betalen
☐ Ik had back-ups van de bestanden of gegevens die ontoegankelijk waren
☐ De versleutelde bestanden, gegevens of apparaten waren niet belangrijk

☐ Ik vertrouwde er niet op dat ik na betaling weer toegang tot mijn apparaten, bestanden en gegevens zou krijgen
☐ Ik was niet bang dat de criminelen de bestanden of gegevens zouden lekken (met andere delen) of dat er andere vervelende gevolgen zouden zijn als ik niet betaalde
☐ Het is onethisch om criminelen te betalen
☐ Het lukte me niet om de betaling te doen
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties

[door naar Q24]

Q24. Toegang – terug
Heeft u weer toegang tot uw bestanden, gegevens of apparaten gekregen?
☐ Ja, volledig
☐ Ja, gedeeltelijk
☐ Nee

Q25. Data – gelekt
Heeft u het idee dat uw bestanden of gegevens zijn gedeeld met of verkocht zijn aan anderen?
☐ Ja
☐ Nee
☐ Weet ik niet

Blok 4: Gevolgen
De volgende vragen gaan over de gevolgen die u heeft ervaren.

Q26. Gevolgen – emotioneel
Heeft dit incident een of meer van de volgende (tijdelijke) emotionele of psychische gevolgen gehad voor u? (Meerdere antwoorden mogelijk). Ik …
☐ … voel(de) me minder veilig
☐ … had minder vertrouwen in mensen
☐ … beleefde het voorval telkens opnieuw
☐ … had slaapproblemen
☐ … had angstklachten en/of paniekaanvallen
☐ … had of heb depressieve klachten
☐ … had of heb minder vertrouwen in mijn eigen digitale vaardigheden
☐ … ervaarde andere emotionele of psychische gevolgen, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q27. Gevolgen
Heeft dit incident een of meer andere gevolgen gehad voor u? (Meerdere antwoorden mogelijk)
☐ Ik heb tijd besteed aan het oplossen van het incident
☐ Ik heb kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk
☐ Ik heb bestanden of gegevens verloren
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q28. Kosten
In sommige gevallen leidt ransomware tot meer financiële gevolgen dan alleen de kosten van het losgeld, zoals kosten voor reparatie of herstel. Hoe hoog zou u de kosten van het incident schatten bovenop het gevraagde losgeld?
☐ Geen
☐ Minder dan € 1.000
☐ € 1.000 tot € 5.000
☐ € 5.000 tot € 10.000
☐ € 10.000 tot € 50.000
☐ € 50.000 of meer
☐ Weet ik niet

Q29. Geld – terug
Is de financiële schade (inclusief de eventuele kosten van het losgeld) vergoed (bijvoorbeeld via een verzekering)?
☐ Ja, de financiële schade is volledig vergoed [door naar Q30]
☐ Ja, een gedeelte van de financiële schade is vergoed [door naar Q30]
☐ Nee, de financiële schade is niet vergoed [door naar Q31]
☐ Ik heb dit aangevraagd en nog geen beslissing ontvangen [door naar Q30]
☐ Er was geen financiële schade [door naar Q31]

Q30. Geld terug – wie
Door welke instantie is de financiële schade (inclusief de eventuele kosten van het losgeld) vergoed of bij welke instantie heeft u een aanvraag gedaan voor een vergoeding?
☐ Bank of financiële instelling
☐ Verzekeringsmaatschappij
☐ Anders, namelijk …

Q31. Gedragsverandering
Welke gevolgen heeft het incident gehad voor uw online gedrag of uw beveiligingsmaatregelen? (Meerdere antwoorden mogelijk)

☐ Ik heb een ander besturingssysteem genomen
☐ Ik maak (vaker) back-ups van mijn bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Ik heb unieke wachtwoorden ingesteld voor al mijn apparaten en accounts
☐ Ik deel mijn persoonlijk wachtwoorden niet (meer) met anderen
☐ Ik heb een antivirusproduct aangeschaft
☐ Ik heb een firewall aangeschaft
☐ Ik laat beveiligingssoftware mijn apparaten scannen op virussen of andere kwaadaardige software
☐ Ik voer updates van besturingssystemen, apps en/of software direct uit zodra ze beschikbaar zijn
☐ Ik heb een ander standaardbrowser genomen
☐ Ik ben voorzichtiger met welke websites ik bezoek, wat ik download en welke bijlagen ik open
☐ Ik heb een VPN-verbinding aangeschaft
☐ Ik heb browserextensies geïnstalleerd die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Ik heb mijn persoonlijke bestanden en gegevens versleuteld
☐ Ik heb tweestapsverificatie ingesteld (2 stappen in plaats van 1 stap om in te loggen)
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Pop-up 31j: Een VPN (Virtual Private Network)-verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
Pop-up 31k: Een browserextensie is software die een browser extra functionaliteit biedt, zoals het managen van cookies of advertenties tijdens het surfen op internet

---

Blok 5: Contact met anderen
We willen u nu vragen stellen over de partijen waarmee u contact heeft opgenomen naar aanleiding van het ransomware-incident.

Q32. Contact – derden
Heeft u met volgende partijen contact opgenomen naar aanleiding van het ransomware-incident voor advies, ondersteuning of om melding te maken van het incident? (Meerdere antwoorden mogelijk)

De politie
☐ Ja
☐ Nee

Uw bank of financiële instelling
☐ Ja
☐ Nee

Uw verzekeringsmaatschappij
☐ Ja
☐ Nee

Een cybersecuritybedrijf of IT-leverancier
☐ Ja
☐ Nee

No More Ransom
☐ Ja
☐ Nee

Slachtofferhulp
☐ Ja
☐ Nee

Fraudehelpdesk
☐ Ja
☐ Nee

Andere organisatie, namelijk … [open antwoord]
☐ Ja
☐ Nee

Pop-up met nadere toelichting bij 'No More Ransom': No More Ransom is een initiatief van het Team High-Tech Crime van de Nationale Politie, het European Cybercrime Centre van Europol, Kaspersky en McAfee. Het heeft tot doel slachtoffers van ransomware te helpen bij het herstellen van hun versleutelde gegevens zonder dat zij de criminelen hiervoor betalen, onder andere door het aanbieden van ontsleuteltools.

[Routing: bij elke 'ja' bij Q32b t/m Q32h, door naar Q33]
[Routing: Bij Q32a 'ja' door naar Q34]
[Routing: indien 'nee' bij Q32a t/m Q38f, door naar Q38]

Q33. Contact – elke organisatie
Hoe tevreden bent u over het contact dat u met [organisatie Q32b t/m Q32h] heeft gehad?

Zeer ontevreden				Zeer tevreden
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

[Door naar Q39, tenzij (ook) contact gehad met politie, dan door naar Q34]

Q34. Contact politie – doel
Met welk doel nam u contact op met de politie? (Meerdere antwoorden mogelijk)
☐ Voor hulp en/of informatie [door naar Q37]
☐ Om aangifte te doen [door naar Q35]
☐ Ik wilde geen aangifte doen, ik wilde alleen het incident melden [door naar Q35]

Pop-up met nadere toelichting:
U kunt een melding doen als u wilt dat de politie op de hoogte is van wat u is overkomen, zonder dat er een onderzoek wordt ingesteld of de dader wordt vervolgd. De politie kan de situatie in de gaten houden.
Bij een aangifte verzoekt u de politie om een onderzoek te starten. U heeft dan een document (proces-verbaal) getekend en een aangifteboekje mee naar huis gekregen.

Q35. Aangifte
Is er een aangifte gedaan bij de politie, waarbij een proces-verbaal is ondertekend?
☐ Ja
☐ Nee

[Door naar Q36]

Q36. Reden melding politie
Wat is de reden dat u het incident gemeld heeft en/of aangifte heeft gedaan bij de politie? (Meerdere antwoorden mogelijk)
☐ Om te voorkomen dat dit opnieuw bij mij gebeurt
☐ Om te voorkomen dat de dader dit opnieuw bij een ander kan doen
☐ Ik wil dat de dader gepakt wordt
☐ Om een veiligere (online) wereld te creëren
☐ Het is mijn plicht om aangifte/melding te doen
☐ Om de schade vergoed te krijgen
☐ Anders, namelijk … [open antwoord]

[Door naar Q38]

Q37. Reden van geen melding politie
Wat is de reden dat u het incident niet gemeld heeft en/of geen aangifte heeft gedaan bij de politie? (Meerdere antwoorden mogelijk)

☐ Ik heb het zelf of met behulp van een andere partij opgelost
☐ Het is niet zo belangrijk
☐ Het kost te veel moeite
☐ Het heeft geen zin, de politie zal er toch niets aan doen
☐ De politie heeft niet de kennis om dit type delict aan te pakken
☐ Het is eerder een zaak voor een andere instantie dan de politie
☐ Ik heb weinig vertrouwen in de politie
☐ Ik wilde melding/aangifte doen, maar de politie wilde mijn melding/aangifte niet opnemen
☐ Ik heb de schade al vergoed gekregen (het losgeld en/of overige kosten)
☐ Ik ben bang dat de dader wraak zal nemen
☐ Ik schaam me dat ik slachtoffer ben geworden van het delict
☐ Ik schaam me dat ik het losgeld betaald heb
☐ Ik vind dat het eigenlijk mijn eigen schuld is
☐ Het lukt niet om digitaal een melding/aangifte te doen
☐ Anders, namelijk … [open antwoord]

[Door naar Q38]

Q38. Politie – tevredenheid
Hoe tevreden bent u over het contact dat u met de politie heeft gehad?

Zeer ontevreden				Zeer tevreden
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q39. Standpunt politie
De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?

Helemaal oneens				helemaal mee eens
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q40. Standpunt politie – contact
[Alleen voor respondenten die bij Q32a 'nee' hebben ingevuld]
Heeft dit standpunt eraan bijgedragen dat u geen contact heeft gezocht met de politie?
☐ Ja
☐ Nee

Q41. Standpunt politie – melding
[Alleen voor respondenten die bij Q34 optie 2 of 3 hebben ingevuld]
Heeft dit standpunt eraan bijgedragen dat u uiteindelijk geen melding of aangifte heeft gedaan bij de politie?

☐ Ja
☐ Nee

Q42. Overig
Zijn er nog belangrijke zaken die u wilt delen over het ransomware-incident of het contact met de instanties?
[Open antwoord – tekst]

Afsluiting
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname aan dit onderzoek.

Wilt u verder praten over of melding maken van wat u is overkomen? Dan kunt u contact opnemen met een van de volgende instanties:
Politie Nederland[45]
No More Ransom[46]
Slachtofferhulp Nederland[47]
Fraudehelpdesk[48]

---

45 Zie https://www.politie.nl/
46 Zie https://www.nomoreransom.org/nl/index.html
47 Zie https://www.slachtofferhulp.nl/gebeurtenissen/fraude/malware-en-ransomware/)
48 Zie https://www.fraudehelpdesk.nl/ondernemers-fraude/uw-computerbestanden-worden-gegijzeld/

Bijlage 2 Vragenlijst 2A

Inleiding
In deze vragenlijst gaan we in op een specifieke vorm van online criminaliteit: ransomware. Ransomware wordt ook wel gijzelsoftware genoemd. Hierbij blokkeren of versleutelen criminelen uw bestanden, gegevens of appara(a)t(en) waardoor die niet meer te gebruiken zijn. U kunt daardoor bijvoorbeeld niet meer bij foto's en video's. Criminelen vragen losgeld om de bestanden te ontsleutelen.

In deze vragenlijst zullen we vragen stellen over wat u zou doen als u slachtoffer zou worden van ransomware. U hoeft geen slachtoffer te zijn geweest van ransomware om de vragenlijst in te vullen. Er zijn geen goede of foute antwoorden, we willen graag uw mening weten.

Blok 1: Achtergrondkenmerken
We stellen u eerst enkele algemene vragen.

Q1. Tijd online
Hoeveel tijd spendeert u doorgaans online voor privédoeleinden?
☐ Minder dan 1 keer per maand
☐ Minimaal 1 keer per maand, maar niet wekelijks
☐ Minimaal 1 keer per week, maar niet dagelijks
☐ Dagelijks
☐ Meerdere keren per dag
☐ Minstens ieder uur (tijdens de uren dat ik wakker ben)
☐ Ik ben (bijna) continu online (tijdens de uren dat ik wakker ben)

Q2. Cybersecuritymaatregelen
Welke van de volgende beveiligingsmaatregelen neemt u? (Meerdere antwoorden mogelijk)
☐ Ik maak back-ups van mijn bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Ik heb unieke wachtwoorden ingesteld voor al mijn apparaten en accounts
☐ Ik deel mijn persoonlijk wachtwoorden niet met anderen
☐ Ik heb een up-to-date antivirusproduct
☐ Ik heb een firewall

☐ Ik laat beveiligingssoftware mijn apparaten scannen op virussen of andere kwaadaardige software
☐ Ik voer updates van besturingssystemen, apps en/of software direct uit zodra ze beschikbaar zijn
☐ Ik ben voorzichtig met welke websites ik bezoek, wat ik download en welke bijlagen ik open
☐ Ik maak gebruik van een VPN-verbinding
☐ Ik gebruik browser extensies die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Ik heb mijn persoonlijke bestanden en gegevens versleuteld
☐ Ik heb tweestapsverificatie ingesteld (2 stappen in plaats van 1 stap om in te loggen)
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

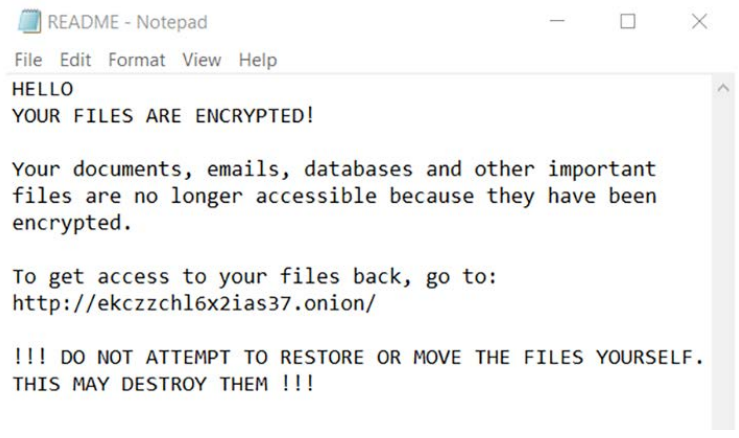
Pop-up 2h: Een VPN (Virtual Private Network)-verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
Pop-up 2i: Een browserextensie is software die een browser extra functionaliteit biedt, zoals het managen van cookies of advertenties tijdens het surfen op internet

---

Blok 2: Vignet
Er volgt een scenario waarbij iemand getroffen wordt door ransomware.

Probeert u zich voor te stellen dat dit u overkomt en u diegene bent die een beslissing moet nemen over het wel of niet betalen van losgeld en het melden van het incident. We willen graag weten wat u in dat geval zou doen. Er zijn geen goede of foute antwoorden, we willen graag uw mening weten.

De volgende boodschap staat op uw computer:



Door de criminelen wordt u doorgestuurd naar een gepersonaliseerde website waarop het volgende bericht te zien is:

Al uw data en systemen zijn ontoegankelijk gemaakt, inclusief bestanden van emotionele waarde. Er is **wel een/geen** back-up van deze gegevens beschikbaar. U heeft een (cybersecurity)organisatie ingeschakeld voor hulp. De mensen om u heen en deze organisatie adviseren u om **wel/niet** het losgeld te betalen.

Q8. Controlevraag 1
Hoeveel losgeld wordt er door de cybercriminelen geëist?
☐ 250 euro in bitcoin
☐ 2.500 euro in bitcoin

Voordat men door kan naar 'Q9' pop-up met volgende tekst: Door de criminelen wordt **250 euro**/**2.500 euro** in bitcoin aan losgeld geëist [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q9. Controlevraag 2
Hebben de criminelen gedreigd met het lekken van vertrouwelijke data?
☐ Ja
☐ Nee

Voordat men door kan naar 'Q10' pop-up met volgende tekst: Door de criminelen is **wel/niet gedreigd met het lekken van vertrouwelijke data**, waaronder documenten, foto's en video's [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q10. Controlevraag 3
Is er een back-up van de versleutelde gegevens beschikbaar?
☐ Ja
☐ Nee

Voordat men door kan naar 'Q11' pop-up met volgende tekst: Er is een **wel een/geen back-up** van de versleutelde gegevens **beschikbaar.** [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q11. Controlevraag 4
Is geadviseerd te betalen door de mensen om u heen en de ingehuurde (cybersecurity) organisatie?
☐ Ja
☐ Nee

Voordat men door kan naar 'Q12' pop-up met volgende tekst: De mensen om u heen en de ingehuurde (cybersecurity)organisatie adviseren om **wel/niet** te betalen. [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

We zullen u nu wat vragen stellen over het scenario.

Q12. Eerste emotie
Wat zou u voelen als u geconfronteerd zou worden met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik zou me boos voelen
☐ Ik zou afkeer voelen
☐ Ik zou me bang voelen
☐ Ik zou me nerveus voelen
☐ Ik zou me verdrietig voelen
☐ Ik zou me ontspannen voelen
☐ Ik zou me blij voelen
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q13. Eerste reactie
Welke van de volgende dingen zou u doen als u geconfronteerd zou worden met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik zou de verbinding met internet verbreken
☐ Ik zou mijn apparaat opnieuw opstarten
☐ Ik zou mijn apparaat terugzetten naar fabrieksinstellingen
☐ Ik zou hulp of advies zoeken op internet
☐ Ik zou hulp of advies zoeken van een bekende
☐ Ik zou hulp of advies zoeken van een organisatie of instantie
☐ Ik zou proberen mijn bestanden of gegevens te herstellen vanaf een back-up
☐ Ik zou proberen een programma te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen
☐ Ik zou proberen de bestanden weer te openen door hun extensie terug te veranderen naar hun originele formaat
☐ Ik zou niks doen
☐ Ik zou iets anders doen, namelijk …

Bij antwoordoptie 13g pop-up met nadere toelichting: *Een bestandsextensie is een toevoeging aan het einde van een bestandsnaam die aanduidt om wat voor soort bestand het gaat, zoals .docx of .jpg.*

Q14. Waarschijnlijkheid van betalen
Hoe waarschijnlijk is het dat u ervoor kiest om in deze situatie het losgeld te betalen?
Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q15. Reden van betalen
Wat is de reden dat u het losgeld zou betalen? (Meerdere antwoorden mogelijk)
☐ Het gevraagde bedrag is niet heel hoog en zou ik kunnen betalen
☐ Ik zou de geblokkeerde of versleutelde bestanden, gegevens of apparaten niet willen verliezen
☐ Ik zou erop vertrouwen dat ik na betaling weer toegang tot mijn apparaten, bestanden en gegevens zou krijgen
☐ Ik zou bang zijn dat de criminelen de bestanden of gegevens zouden lekken (met anderen delen) of dat er andere vervelende gevolgen zouden zijn als ik niet betaal
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties
☐ Ik zou het losgeld **niet** betalen

Q16. Reden van niet betalen
Wat is de reden dat u het losgeld **niet** zou betalen? (Meerdere antwoorden mogelijk)
☐ Het gevraagde bedrag is te hoog en zou ik niet kunnen betalen
☐ De versleutelde bestanden, gegevens of apparaten zou ik niet belangrijk vinden
☐ Ik zou er niet op vertrouwen dat ik na betaling weer toegang tot mijn apparaten, bestanden en gegevens zou krijgen

☐ Ik zou niet bang zijn dat de criminelen de bestanden of gegevens zouden lekken (met andere delen) of dat er andere vervelende gevolgen zouden zijn als ik niet betaal
☐ Het is onethisch om criminelen te betalen
☐ Ik zou niet weten hoe ik de betaling zou moeten doen
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties
☐ Ik zou het losgeld **wel** betalen

Q17. Waarschijnlijkheid van melden
Hoe waarschijnlijk is het dat u ervoor kiest om in deze situatie het incident te melden en/of aangifte te doen?
Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q18. Melden – partij
Bij welke van de volgende organisaties zou u het incident melden? (Meerdere antwoorden mogelijk)
☐ De politie
☐ Uw bank of financiële instelling
☐ Uw verzekeringsmaatschappij
☐ No More Ransom
☐ Een cybersecuritybedrijf of IT-leverancier
☐ Slachtofferhulp
☐ Fraudehelpdesk
☐ Andere organisatie, namelijk …

Pop-up met nadere toelichting bij 'No More Ransom': No More Ransom is een initiatief van het Team High-Tech Crime van de Nationale Politie, het European Cybercrime Centre van Europol, Kapersky en McAfee. Het heeft tot doel slachtoffers van ransomware te helpen bij het herstellen van hun versleutelde gegevens zonder dat zij de criminelen hiervoor betalen, onder andere door het aanbieden van ontsleuteltools.

[Indien 'ja' bij politie, door naar Q19. Indien 'nee' bij politie, door naar Q20]

Q19. Reden van melding bij politie
Wat is de reden dat u het incident zou melden en/of aangifte zou doen bij de politie? (Meerdere antwoorden mogelijk)
☐ Om te voorkomen dat dit opnieuw bij mij gebeurt
☐ Om te voorkomen dat de dader dit opnieuw bij een ander kan doen
☐ Ik zou willen dat de dader gepakt wordt

☐ Om een veiligere (online) wereld te creëren
☐ Het is mijn plicht om aangifte/melding te doen
☐ Om de schade vergoed te krijgen
☐ Anders, namelijk … [open antwoord]

[Door naar Q21]

Q20. Reden van geen melding bij politie
Wat is de reden dat u het incident niet zou melden en/of geen aangifte zou doen bij de politie? (Meerdere antwoorden mogelijk)
☐ Ik zou het zelf of met behulp van een andere partij oplossen
☐ Het is niet zo belangrijk
☐ Het kost te veel moeite
☐ Het heeft geen zin, de politie zou er toch niets aan doen
☐ De politie heeft niet de kennis om dit type delict aan te pakken
☐ Het is eerder een zaak voor een andere instantie dan de politie
☐ Ik heb weinig vertrouwen in de politie
☐ Ik zou bang zijn dat de dader wraak zal nemen
☐ Ik zou me schamen dat ik slachtoffer ben geworden van het delict
☐ Ik zou me schamen dat ik het losgeld betaald heb
☐ Ik zou vinden dat het eigenlijk mijn eigen schuld is
☐ Anders, namelijk … [open antwoord]

[Door naar Q21]

Q21. Standpunt van politie
De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?

Helemaal oneens				helemaal mee eens
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q22. Standpunt politie – betalen
Zou dit standpunt uw keuze om te **betalen** beïnvloeden?
☐ Ja
☐ Nee

Q23. Standpunt politie – contact
Zou dit standpunt uw keuze om **contact op te nemen** met de politie beïnvloeden?
☐ Ja
☐ Nee

Q24. Standpunt politie – melden
Zou dit standpunt uw keuze om het incident te **melden en/of aangifte te doen** bij de politie beïnvloeden?
☐ Ja
☐ Nee

Q25. Contact met daders
Zou u in dit scenario contact opnemen met de daders?
☐ Ja, ik zou zelf contact opnemen met de daders [door naar Q26]
☐ Ja, ik zou een bekende namens mij contact laten opnemen met de daders [door naar Q26]
☐ Ja, ik zou iemand inhuren om namens mij contact op te nemen met de daders [door naar Q26]
☐ Nee, ik zou geen contact opnemen met de daders [door naar Q28]

Q26. Contact – doel
Met welk doel zou u (of iemand namens u) contact opnemen met de daders? (Meerdere antwoorden mogelijk)
☐ Om vast te stellen of het losgeldbericht echt is [door naar Q28]
☐ Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline [door naar Q27]
☐ Om vast te stellen welke bestanden of gegevens door de criminelen zijn gestolen [door naar Q28]
☐ Om hulp te vragen **bij** het betalen (bijvoorbeeld bij het aanschaffen van bitcoin) [door naar Q28]
☐ Om hulp te vragen **na** het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens) [door naar Q28]
☐ Om tijd te rekken [door naar Q28]
☐ Anders, namelijk … [open antwoord] [door naar Q28]

Q27. Onderhandelen – doel
U heeft aangegeven dat u in deze situatie zou onderhandelen met de daders. Met welk doel zou u onderhandelen? (Meerdere antwoorden mogelijk)
☐ Om het losgeldbedrag te verlagen
☐ Om langer de tijd te krijgen
☐ Om een andere reden, namelijk … [open antwoord]
☐ Ik zou niet onderhandelen

Q28. Perceptie gevolgen – emotioneel
Stel u wordt geconfronteerd met het losgeldbericht. Wat zouden voor u de (tijdelijke) emotionele of psychische gevolgen zijn? Ik zou … (Meerdere antwoorden mogelijk)
☐ … me minder veilig voelen
☐ … minder vertrouwen in mensen hebben

☐ … het voorval telkens opnieuw beleven
☐ … slaapproblemen hebben
☐ … angstklachten en/of paniekaanvallen hebben
☐ … depressieve klachten hebben
☐ … minder vertrouwen hebben in mijn eigen digitale vaardigheden
☐ … andere emotionele of psychische gevolgen ervaren, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q29. Perceptie gevolgen
Welke andere gevolgen zou het incident voor u hebben? (Meerdere antwoorden mogelijk)
☐ Ik zou tijd besteden aan het oplossen van het incident
☐ Ik zou kosten hebben gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk
☐ Ik zou bestanden of gegevens zijn verloren
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q30. Perceptie kosten
In sommige gevallen leidt ransomware tot meer financiële gevolgen dan alleen de kosten van het losgeld, zoals kosten voor reparatie of herstel. Hoe hoog zou u in deze situatie de kosten van het incident schatten bovenop het gevraagde losgeld?
☐ Geen
☐ Minder dan €1.000
☐ €1.000 tot €5.000
☐ €5.000 tot €10.000
☐ €10.000 tot €50.000
☐ €50.000 of meer
☐ Weet ik niet

Q31. Cybersecuritymaatregelen
Denkt u dat u in deze situatie aanvullende beveiligingsmaatregelen zou nemen naar aanleiding van het incident? (Meerdere antwoorden mogelijk)
☐ Ja [door naar Q32]
☐ Nee [door naar Q33]

Q32. Cybersecuritymaatregelen
Welke van de volgende beveiligingsmaatregelen zou u nemen naar aanleiding van het incident? (Meerdere antwoorden mogelijk)
☐ Ik zou een ander besturingssysteem nemen
☐ Ik zou (vaker) back-ups maken van mijn bestanden en gegevens op een externe harde schijf, cloudopslag of server

☐ Ik zou unieke wachtwoorden instellen voor al mijn apparaten en accounts
☐ Ik zou mijn persoonlijke wachtwoorden niet (meer) delen met anderen
☐ Ik zou een antivirusproduct aanschaffen
☐ Ik zou een firewall aanschaffen
☐ Ik zou beveiligingssoftware mijn apparaten laten scannen op virussen of andere kwaadaardige software
☐ Ik zou updates van besturingssystemen, apps en/of software direct uitvoeren zodra ze beschikbaar zijn
☐ Ik zou een ander standaardbrowser nemen
☐ Ik zou voorzichtiger zijn met welke websites ik bezoek, wat ik download en welke bijlagen ik open
☐ Ik zou een VPN-verbinding aanschaffen
☐ Ik zou browserextensies installeren die mij helpen om veilig te surfen, zoals software om advertenties of pop-ups te blokkeren
☐ Ik zou mijn persoonlijke bestanden en gegevens versleutelen
☐ Ik zou tweestapsverificatie instellen (2 stappen in plaats van 1 stap om in te loggen)
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Pop-up 32j: Een VPN (Virtual Private Network)-verbinding geeft een gebruiker beveiligde en anonieme toegang tot een netwerk en maakt daarmee de internetverbinding veiliger.
Pop-up 32k: Een browserextensie is software die een browser extra functionaliteit biedt, zoals het managen van cookies of advertenties tijdens het surfen op internet.

Blok 3: Slachtofferschap
We stellen u tot slot enkele vragen over slachtofferschap van ransomware.

Q33. Gepercipieerde kwetsbaarheid – ander
Hoe groot schat u de gemiddelde kans dat een inwoner van Nederland slachtoffer zou worden van ransomware?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q34. Gepercipieerde kwetsbaarheid – zelf
Hoe groot schat u de gemiddelde kans dat u slachtoffer zou worden van ransomware?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q36. Slachtoffer – ander
Kent u iemand die ooit slachtoffer is geworden van ransomware waarbij bestanden, gegevens of apparaten geblokkeerd of versleuteld zijn door criminelen en er om losgeld is gevraagd om hier weer toegang tot te krijgen?
☐ Ja
☐ Nee

Tot slot
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname in dit onderzoek.

Bijlage 3 **Vragenlijst 1B**

Inleiding en informed consent
Bedankt dat u wilt deelnemen aan dit onderzoek van de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving. Dit onderzoek gaat over online criminaliteit. Wij willen aan u vragen of uw bedrijf online criminaliteit heeft meegemaakt en welke gevolgen u heeft ervaren.

Waarom hebben wij uw ervaringen nodig?
Pas wanneer we weten hoeveel ondernemers slachtoffer worden en wat er precies gebeurd is, kunnen we iets doen aan online criminaliteit. We willen u daarom vragen zo eerlijk mogelijk over uw eventuele ervaringen te vertellen.

Privacy en anonimiteit
Dit vragenlijstonderzoek is gemaakt door onderzoekers van de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving en wordt uitgevoerd door I&O Research. Uw antwoorden worden uitsluitend gebruikt voor het doel van het onderzoek en verwerkt volgens de privacyverklaring van I&O Research.[49] Er zijn maatregelen genomen om ervoor te zorgen dat uw antwoorden niet naar u te herleiden zijn. Dat betekent bijvoorbeeld dat I&O Research uw antwoorden verstuurt aan de Haagse Hogeschool en het Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving op een manier dat deze niet naar u of uw bedrijf te zijn herleiden. In een publicatie zullen anonieme gegevens worden gebruikt.

Ik verklaar dat:
- Ik weet dat het onderzoek wordt uitgevoerd zoals beschreven in bovenstaande toelichting. Ik heb dit gelezen en begrijp de informatie.
- Ik genoeg tijd heb gehad om te beslissen of ik wil deelnemen.
- Ik weet dat meedoen vrijwillig is en dat ik op ieder moment kan beslissen om toch niet mee te doen of te stoppen met het onderzoek. Daarvoor hoef ik geen reden te geven. Ik begrijp dat het intrekken van mijn toestemming geen gevolgen heeft voor de verwerking van mijn persoonsgegevens in de periode voorafgaand aan het intrekken van de toestemming.
- Ik toestemming geef voor het verzamelen, bewaren en gebruiken van mijn ingevulde gegevens voor de beantwoording van de onderzoeksvraag in dit onderzoek.

49 Zie https://www.iopanel.nl/privacy.

- Ik weet dat de gegevens die de onderzoekers bewaren geanonimiseerd zijn en niet rechtstreeks te herleiden zijn naar mijn persoon.
- Ik weet dat onderzoeksgegevens na het onderzoek nog 10 jaar worden bewaard en daarna worden vernietigd.

Door de knop 'ja' aan te klikken stemt u in met deelname aan het onderzoek en gaat u ermee akkoord dat I&O Research en de Haagse Hogeschool uw gegevens verwerken voor dit onderzoek.

Stemt u ermee in dat wij uw antwoorden voor dit onderzoek gebruiken? [Verplichte vraag]
☐ Ja [door naar Q1a]
☐ Nee [Einde vragenlijst]

Q1a. Screeningsvraag 1a
Welke van de volgende vormen van online criminaliteit of een poging daartoe heeft uw bedrijf ooit meegemaakt?

Phishing
Een medewerker van uw bedrijf ontving een e-mail of ander bericht dat van een legitieme instantie leek te komen, maar waarschijnlijk van een oplichter was om (inlog) gegevens te achterhalen.
☐ Ja
☐ Nee

CEO-fraude
Een medewerker van uw bedrijf ontving een opdracht van iemand die zich voordeed als CEO of directeur om een groot bedrag over te boeken.
☐ Ja
☐ Nee

Voorschotfraude
Uw bedrijf moest een voorschot betalen om een groot bedrag te ontvangen (bijvoorbeeld vanwege een erfenis, investering of loterij).
☐ Ja
☐ Nee

Ransomware
De bestanden, gegevens of appara(a)t(en) van uw bedrijf werden geblokkeerd of versleuteld en er werd om losgeld gevraagd om hier weer toegang tot te krijgen.
☐ Ja
☐ Nee

Advertentiefraude
Uw bedrijf heeft betaald voor het plaatsen van advertenties die niet of nauwelijks vertoond zijn of waarvoor geen opdracht is verleend.
☐ Ja
☐ Nee

Aankoopfraude
Uw bedrijf heeft via internet een product of dienst aangeschaft dat nooit geleverd is.
☐ Ja
☐ Nee

Helpdeskfraude
Uw bedrijf heeft iemand die zich voordeed als een medewerker van een helpdesk toegang gegeven tot uw computer, waarna er geld afhandig is gemaakt.
☐ Ja
☐ Nee

Identiteitsfraude
Er is zonder toestemming gebruikgemaakt van persoonlijke of financiële gegevens van uw bedrijf (bijvoorbeeld om producten te kopen of kredieten aan te vragen op naam van uw bedrijf).
☐ Ja
☐ Nee

Bij elke vorm moet een meer uitgebreide toelichting zichtbaar zijn als pop-up.

Phishing
Phishing is een vorm van online oplichting, waarbij criminelen e-mails of websites van legitieme instanties namaken om slachtoffers te misleiden, om zodoende (inlog)gegevens te achterhalen en toegang te krijgen tot online accounts.

CEO-fraude
Bij CEO-fraude ontvangt een medewerker van een bedrijf via e-mail of telefonisch een opdracht van iemand die zich voordoet als CEO of directeur om een groot bedrag over te boeken, bijvoorbeeld vanwege een factuur.

Voorschotfraude
De kern van voorschotfraude is dat slachtoffers via e-mail of sociale media wordt gevraagd om een voorschot te betalen om vervolgens een groot bedrag te ontvangen. Het gaat dan bijvoorbeeld om een zogenaamde erfenis, investering of loterij.

Ransomware
Wanneer je slachtoffer bent van ransomware, ook wel gijzelsoftware genoemd, blokkeren of versleutelen criminelen je bestanden, gegevens of appara(a)t(en) en geven die pas weer vrij als losgeld wordt betaald.

Advertentiefraude
Bij advertentiefraude worden er kosten in rekening gebracht voor het plaatsen van advertenties die niet of nauwelijks vertoond zijn of waarvoor geen opdracht is gegeven.

Helpdeskfraude
Bij helpdeskfraude hebben slachtoffers telefonisch contact met iemand die zich voordoet als een medewerker van een helpdesk van een softwarebedrijf, zoals Microsoft. De oplichters overtuigen slachtoffers hun toegang te geven tot hun computer en maken hen uiteindelijk geld afhandig.

Aankoopfraude
Slachtoffers van aankoopfraude kopen via internet een product of dienst en hebben ten minste een deel daarvan betaald, waarna het product of de dienst nooit geleverd is omdat de verkoper hen heeft opgelicht.

Identiteitsfraude
Identiteitsfraude houdt in dat iemand zonder uw toestemming de persoonlijke of financiële gegevens van uw bedrijf gebruikt om er zelf geld aan te verdienen. Iemand koopt bijvoorbeeld producten of vraagt kredieten aan op naam van het bedrijf. Meestal is identiteitsfraude een gevolg van diefstal van identiteitsgegevens, maar het kan ook zijn dat u zelf de identiteitsgegevens heeft verstrekt.

[Indien ransomware = ja, ga naar Q1b. Indien ransomware = nee, einde onderzoek]

Q1b. Screeningsvraag 1b (check)
U heeft aangegeven dat de bestanden, gegevens of apparaten van uw bedrijf ooit geblokkeerd of versleuteld zijn door criminelen en dat er om losgeld is gevraagd om hier weer toegang tot te krijgen. Klopt het dat uw bedrijf dit is overkomen?
☐ Ja [door naar vragenlijst voor slachtoffers, volgende pagina]
☐ Nee [door naar vragenlijst niet-slachtoffers, bijlage 5]

Wat u is overkomen noemen wij ransomware. We zouden u graag vragen stellen over wat er is gebeurd en de gevolgen die u heeft ervaren. We willen u vragen zo eerlijk mogelijk over uw ervaring te vertellen.

We stellen u eerst enkele algemene vragen over uw bedrijf.

Blok 1: Achtergrondkenmerken

Q1. Tijd online
Hoeveel tijd spendeert u doorgaans online voor uw bedrijf?
☐ Minder dan 1 keer per maand
☐ Minimaal 1 keer per maand, maar niet wekelijks
☐ Minimaal 1 keer per week, maar niet dagelijks
☐ Dagelijks
☐ Meerdere keren per dag
☐ Minstens ieder uur (tijdens de uren dat ik aan het werk ben)
☐ Ik ben (bijna) continu online (tijdens de uren dat ik aan het werk ben)

Q2. Activiteiten
Welke van de volgende mogelijkheden had of gebruikte uw bedrijf voordat uw bedrijf slachtoffer werd van ransomware? (Meerdere antwoorden mogelijk)
☐ Accounts of pagina's op sociale media (zoals Facebook of Twitter)
☐ De mogelijkheid voor klanten om online te bestellen, te reserveren, te betalen voor producten of diensten, of een schenking te doen
☐ De mogelijkheid voor klanten om online toegang te krijgen tot (enkele) van uw diensten
☐ Een online bankrekening waarnaar klanten betalingen kunnen overmaken
☐ Een industrieel controlesysteem
☐ Een Enterprise Resource Planning (ERP)-systeem
☐ Financiële of boekhoudsoftware
☐ Het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs
☐ Anders, namelijk … [open]
☐ Geen van bovenstaande
☐ Weet ik niet

Q3. Verzekering
Er zijn algemene verzekeringspolissen die dekking bieden voor de gevolgen van een cyberaanval. Er zijn ook specifieke verzekeringspolissen voor dit doeleinde. Welke van de volgende gevallen omschrijft het beste uw situatie voordat uw bedrijf slachtoffer werd van ransomware?
☐ Mijn bedrijf had een specifieke verzekering voor cybersecurity
☐ De cybersecurityverzekering van mijn bedrijf was onderdeel van een bredere verzekeringspolis
☐ Mijn bedrijf was niet verzekerd tegen cybersecurity-incidenten
☐ Weet ik niet

Q4. Jaaromzet
Wat is de jaaromzet van uw bedrijf, in euro's?
☐ Minder dan € 100.000
☐ € 100.000 tot € 500.000
☐ € 500.000 tot € 1.000.000
☐ € 1.000.000 tot € 2.500.000
☐ € 2.500.000 tot € 5.000.000
☐ Meer dan € 5.000.000
☐ Zeg ik liever niet
☐ Weet ik niet

Q5. Cybersecuritymaatregelen
Welke van de volgende beveiligingsmaatregelen nam uw bedrijf voordat uw bedrijf slachtoffer werd? (Meerdere antwoorden mogelijk)
☐ Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen
☐ Up-to-date antivirusproduct
☐ Firewalls die zowel uw volledige IT-netwerk beschermen, als individuele apparaten beschermen
☐ Beveiligingssoftware die netwerken en apparaten scant op virussen of andere kwaadaardige software
☐ Monitoring van gebruikers- of netwerkactiviteiten
☐ Uitvoeren van updates van besturingssystemen, apps en/of software wanneer beschikbaar
☐ IT-administratie en toegangsrechten waren beperkt tot specifieke gebruikers
☐ IT-administratie en toegangsrechten werden goed bijgehouden en waren bijgewerkt
☐ Specifieke regels voor het veilig opslaan van bestanden met persoonsgegevens
☐ Versleuteling van gevoelige bestanden en gegevens
☐ Veiligheidsrestricties van apparaten die eigendom waren van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)
☐ Toegang tot het bedrijfsnetwerk was alleen toegestaan op apparaten die eigendom waren van het bedrijf
☐ Gescheiden wifi-netwerken voor personeel en gasten
☐ Tweestapsverificatie (2 stappen in plaats van 1 stap om in te loggen)
☐ Iemand (intern of extern) in dienst die verantwoordelijk was voor cybersecurity
☐ Een bedrijfscontinuïteitsplan
☐ Geen van bovenstaande
☐ Anders, namelijk … [open]
☐ Weet ik niet

Q6. Verantwoordelijkheid voor cybersecurity
Was u (eind)verantwoordelijk voor de cybersecurity binnen uw bedrijf voordat uw bedrijf slachtoffer werd van ransomware?
☐ Ja
☐ Nee

Blok 2: Omstandigheden
We zullen u nu vragen stellen over wat er is gebeurd toen uw bedrijf slachtoffer werd van ransomware.
We willen hier nogmaals benadrukken dat alle antwoorden geanonimiseerd worden en niet terug te herleiden zijn naar u of uw bedrijf.

Q3. Slachtofferschap – frequentie
Hoe vaak is uw bedrijf slachtoffer geworden van ransomware?
☐ 1 keer [door naar Q4]
☐ 2 keer [Onderstaande melding weergeven voordat men doorgaat naar Q4:]
☐ 3 keer [Onderstaande melding weergeven voordat men doorgaat naar Q4:]
☐ 4 keer of vaker [Onderstaande melding weergeven voordat men doorgaat naar Q4:]

*U heeft aangegeven dat uw bedrijf meerdere keren slachtoffer is geworden van ransomware. Wilt u de vervolgvragen in dit onderzoek alstublieft alleen beantwoorden over de **laatste keer** dat dit gebeurde?*

Q4. Slachtofferschap – wanneer
Wanneer is uw bedrijf (voor het laatst) slachtoffer geworden van ransomware?
☐ Een jaar geleden of minder
☐ Tussen 1 en 2 jaar geleden
☐ Tussen de 2 en 4 jaar geleden
☐ 5 of meer jaar geleden

Q5. Type ransomware
Had de ransomware aanval een van de volgende kenmerken?
☐ Ik zag een scherm, pop-up of bericht waarin stond dat apparaten waren vergrendeld (*locked*)
☐ Ik zag een scherm, pop-up of bericht waarin stond dat gegevens of bestanden waren versleuteld (*encrypted*).
☐ Ik zag een bericht, zogenaamd van een wetshandhavingsinstantie (bijv. FBI, ministerie van Justitie), dat me informeerde dat ik betrapt was op het uitvoeren van een illegale of ongewenste activiteit online.
☐ Geen van bovenstaande
☐ Ik weet het niet meer

Q6. Type apparaat
Welke apparaten of systemen waren geblokkeerd of versleuteld? (Meerdere antwoorden mogelijk)
☐ Computer(s) (desktop of laptop)
☐ Mobiele telefoon(s) of smartphone(s)
☐ Tablet(s)
☐ Computerserver(s)
☐ Cloudopslag (bijvoorbeeld iCloud, OneDrive)
☐ Back-up(s)
☐ Anders, namelijk … [open antwoord]

Q7. Type data
Welk type bestanden of gegevens waren geblokkeerd of versleuteld? Als alle apparaten van uw bedrijf geheel geblokkeerd of versleuteld waren, vragen we u aan te geven welke type bestanden op deze apparaten waren opgeslagen (Meerdere antwoorden mogelijk)
☐ Persoonsgegevens (bijv. informatie over naam, adres, inloggegevens, kopie paspoort)
☐ Data van klanten en/of patiënten
☐ Data van medewerkers
☐ Productgegevens
☐ Patenten en auteursrecht
☐ Financiële gegevens en boekhouding
☐ Anders, namelijk … [open antwoord]
☐ Weet ik niet

Q8. Besmetting
Met de kennis die u nu heeft, hoe denkt u dat de ransomware op een apparaat of systeem binnen uw bedrijf is gekomen?
☐ Ik of een medewerker klikte op een link of opende een bijlage in een e-mail
☐ Ik of een medewerker klikte op een link, advertentie of pop-up tijdens het surfen op internet
☐ Een bedrijf waar de gegevens van mijn bedrijf bekend waren was gehackt
☐ Er zat een kwetsbaarheid of beveiligingslek in software of een systeem wat mijn bedrijf gebruikte
☐ Ik of een medewerker had een applicatie of software geïnstalleerd die kwaadaardig bleek te zijn
☐ Anders, namelijk … [open antwoord]
☐ Weet ik niet

Q9. Eerste emotie
Op enig moment hebben de criminelen uw bedrijf om geld gevraagd om weer toegang te krijgen tot bestanden, gegevens of apparaten. Dit noemen we een losgeldbericht.

Wat voelde u toen u geconfronteerd werd met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik voelde me boos
☐ Ik voelde afkeer
☐ Ik voelde me bang
☐ Ik voelde me nerveus
☐ Ik voelde me verdrietig
☐ Ik voelde me ontspannen
☐ Ik voelde me blij
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q10. Eerste reactie
Welke van de volgende dingen heeft u gedaan toen u werd geconfronteerd met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik heb de verbinding met internet verbroken [door naar Q11]
☐ Ik heb apparaten opnieuw opgestart [Door naar Q11]
☐ Ik heb apparaten teruggezet naar fabrieksinstellingen [door naar Q11]
☐ Ik heb hulp gezocht binnen mijn bedrijf [door naar Q12]
☐ Ik heb hulp of advies gezocht op internet [door naar Q12]
☐ Ik heb hulp of advies gezocht van een bekende [door naar Q12]
☐ Ik heb hulp of advies gezocht van een organisatie of instantie [door naar Q12]
☐ Ik heb bestanden of gegevens geprobeerd te herstellen vanaf een back-up [door naar Q11]
☐ Ik heb geprobeerd om een programma te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen [door naar Q11]
☐ Ik heb geprobeerd bestanden weer te openen door hun extensie terug te veranderen naar hun originele formaat [door naar Q11]
☐ Ik heb het losgeld betaald [door naar Q12]
☐ Ik heb niks gedaan [door naar Q12]
☐ Ik heb iets anders gedaan, namelijk … [door naar Q11

Bij antwoordoptie 10g pop-up met nadere toelichting: *Een bestandsextensie is een toevoeging aan het einde van een bestandsnaam die aanduidt om wat voor soort bestand het gaat, zoals .docx of .jpg.*

Q11. Eerste reactie – gevolg
U heeft zelf geprobeerd om bestanden, gegevens of apparaten van uw bedrijf terug te krijgen. Is dat gelukt?
☐ Ja, volledig
☐ Ja, gedeeltelijk
☐ Nee

Blok 3: Afpersing
We zullen u nu enkele vragen stellen over het losgeldbericht en hoe uw bedrijf gereageerd heeft.
Bij woord 'losgeldbericht' pop-up met nadere toelichting: *Als u slachtoffer bent geworden van ransomware zal u in de meeste gevallen geïnformeerd worden via* **een losgeldbericht** *op uw scherm of een tekstbestand op uw apparaat. Het losgeldbericht bevat meestal informatie over hoe u moet betalen en wat er gebeurt als u dat niet doet.*

Q12. Hoogte losgeld
Hoeveel losgeld werd van uw bedrijf geëist?
Noteer het bedrag en de valutasoort (bijv. euro's, dollars, bitcoin). Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐[Open antwoord – tekst]

[Vraag is verplicht]

Q13. Deadline
Hoelang had uw bedrijf de tijd om het losgeld te betalen?
Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐ Minder dan 24 uur
☐ 1-3 dagen
☐ 4-6 dagen
☐ 7 of meer dagen
☐ Dat stond niet in het losgeldbericht

Q14. Contact met daders
Heeft u of iemand anders contact opgenomen met de daders?
☐ Ja, ikzelf of een collega heeft contact opgenomen met de daders [door naar Q15]
☐ Ja, een bekende heeft namens mijn bedrijf contact opgenomen met de daders [door naar Q15]
☐ Ja, ik heb iemand ingehuurd om namens mijn bedrijf contact op te nemen met de daders [door naar Q15]
☐ Nee, ik heb geen contact opgenomen met de daders [door naar Q19]

Q15. Contact – hoe
Hoe heeft u (of iemand namens uw bedrijf) contact opgenomen met de daders?
☐ Via e-mail
☐ Via een chatsysteem op een website of portaal van de daders
☐ Telefonisch
☐ Via een ander communicatiemiddel, namelijk … [open antwoord]

Q16. Contact – doel
Met welk doel heeft u (of iemand namens uw bedrijf) contact opgenomen met de daders? (Meerdere antwoorden mogelijk)
☐ Om vast te stellen of het losgeldbericht echt was [door naar Q19]
☐ Om te informeren over de hoogte van het losgeld (bijvoorbeeld omdat dit in het losgeldbericht niet vermeld stond) [door naar Q19]
☐ Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline [door naar Q17]
☐ Om vast te stellen welke bestanden of gegevens door de criminelen waren gestolen [door naar Q19]
☐ Om hulp te vragen **bij** het betalen (bijvoorbeeld bij het aanschaffen van bitcoin) [door naar Q19]
☐ Om hulp te vragen **na** het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens) [door naar Q19]
☐ Om tijd te rekken [door naar Q19]
☐ Anders, namelijk … [open antwoord] [door naar Q19]

Q17. Onderhandelen – doel
U heeft aangegeven dat er is onderhandeld met de daders. Met welk doel is er onderhandeld? (Meerdere antwoorden mogelijk)
☐ Om het losgeldbedrag te verlagen [door naar Q18]
☐ Om langer de tijd te krijgen [door naar Q18]
☐ Om een andere reden, namelijk … [open antwoord] [door naar Q18]
☐ Er is niet onderhandeld [door naar Q19]

Q18. Onderhandelen – resultaat
Wat was de uitkomst van de onderhandeling? (Meerdere antwoorden mogelijk)
☐ Het losgeldbedrag is verlaagd
☐ De deadline is verlengd
☐ Geen verandering
☐ Anders, namelijk …[open antwoord]

Q19. Aanvullende dreiging
Hebben de daders op enig moment gedreigd met een van de volgende dingen? (Meerdere antwoorden mogelijk)
☐ Er is gedreigd met het verwijderen van de decryptiesleutel
☐ Er is gedreigd met het lekken van bestanden of gegevens
☐ Er is gedreigd met boetes van de Autoriteit Persoonsgegevens
☐ Er is gedreigd met het inlichten van concurrenten
☐ Er is gedreigd met het inlichten van de pers
☐ Er is gedreigd met een DDoS-aanval
☐ Er is gedreigd met iets anders, namelijk … [open antwoord]
☐ Geen van bovenstaande

Bij antwoordoptie 19a pop-up met nadere toelichting: *Met een decryptiesleutel kunnen ontoegankelijk gemaakte bestanden ontsleuteld worden.*

Bij antwoordoptie 19f pop-up met nadere toelichting*: Een Distributed Denial of Service (DDoS)-aanval is een poging van cybercriminelen om ontzettend veel verzoeken naar een netwerk of website te versturen waardoor deze onbereikbaar wordt voor gebruikers. Dit is te vergelijken met een digitale file.*

Q20. Losgeld – betaald
Heeft uw bedrijf het gevraagde losgeld betaald?
☐ Ja, mijn bedrijf heeft een deel van het gevraagde bedrag betaald [door naar Q21]
☐ Ja, mijn bedrijf heeft het volledige bedrag betaald [door naar Q21]
☐ Nee, mijn bedrijf heeft niet betaald [door naar Q23]

Q21. Hoogte losgeld – betaald
Hoeveel losgeld heeft uw bedrijf betaald?
Noteer het bedrag en de valutasoort (bijv. euro's, dollars, bitcoin). Indien u het niet meer precies weet, probeert u het dan zo goed mogelijk te schatten.
☐[Open antwoord – tekst]
☐ Zeg ik liever niet

Q22. Reden – betaald
Wat was de reden dat uw bedrijf betaald heeft? (Meerdere opties mogelijk)
☐ Het gevraagde bedrag was niet heel hoog en mijn bedrijf kon het makkelijk betalen
☐ Het betalen van het losgeld was goedkoper dan geen zaken kunnen doen
☐ Een bekende adviseerde om het losgeld te betalen
☐ Een IT- of cybersecurityspecialist adviseerde om het losgeld te betalen
☐ Mijn bedrijf had geen back-ups van de bestanden en gegevens die ontoegankelijk waren
☐ Mijn bedrijf had een verzekering die de kosten van het losgeld dekte
☐ De geblokkeerde of versleutelde bestanden, gegevens of apparaten waren belangrijk, mijn bedrijf wilde deze niet verliezen
☐ Ik vertrouwde erop dat mijn bedrijf na betaling weer toegang tot apparaten, bestanden en gegevens zou krijgen
☐ Ik was bang dat de criminelen de bestanden of gegevens zouden lekken (met anderen delen) of dat er andere vervelende gevolgen zouden zijn als mijn bedrijf niet betaalde
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties

[door naar Q24]

Q23. Reden – niet betaald
Wat was de reden dat uw bedrijf **niet** betaald heeft? (Meerdere opties mogelijk)
☐ Het gevraagde bedrag was te hoog en mijn bedrijf kon het niet betalen
☐ Het betalen van het losgeld was duurder dan geen zaken kunnen doen
☐ De politie adviseerde om het losgeld niet te betalen
☐ Een bekende adviseerde om het losgeld niet te betalen
☐ Een IT- of cybersecurityspecialist adviseerde om het losgeld niet te betalen
☐ Mijn bedrijf had back-ups van de bestanden of gegevens die ontoegankelijk waren
☐ Mijn bedrijf had geen verzekering die de kosten van het losgeld dekte
☐ De versleutelde bestanden, gegevens of apparaten waren niet belangrijk
☐ Ik vertrouwde er niet op dat mijn bedrijf na betaling weer toegang tot apparaten, bestanden en gegevens zou krijgen
☐ Ik was niet bang dat de criminelen de bestanden of gegevens zouden lekken (met andere delen) of dat er andere vervelende gevolgen zouden zijn als mijn bedrijf niet betaalde
☐ Het is onethisch om criminelen te betalen
☐ Het lukte mijn bedrijf niet om de betaling te doen
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties

[door naar Q24]

Q24. Toegang – terug
Heeft uw bedrijf weer toegang tot uw bestanden, gegevens of apparaten gekregen?
☐ Ja, volledig
☐ Ja, gedeeltelijk
☐ Nee

Q25. Data – gelekt
Heeft u het idee dat bestanden of gegevens van uw bedrijf zijn gedeeld met of verkocht zijn aan anderen?
☐ Ja
☐ Nee
☐ Weet ik niet

Blok 4: Gevolgen
De volgende vragen gaan over de gevolgen die u en uw bedrijf heeft ervaren.

Q26. Gevolgen – emotioneel
Heeft dit incident een of meer van de volgende (tijdelijke) emotionele of psychische gevolgen gehad voor u persoonlijk? (Meerdere antwoorden mogelijk). Ik …
☐ … voel(de) me minder veilig
☐ … had minder vertrouwen in mensen

☐ … beleefde het voorval telkens opnieuw
☐ … had slaapproblemen
☐ … had angstklachten en/of paniekaanvallen
☐ … had of heb depressieve klachten
☐ … had of heb minder vertrouwen in mijn eigen digitale vaardigheden
☐ … ervaarde andere emotionele of psychische gevolgen, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q27. Gevolgen
Heeft dit incident een of meer andere gevolgen gehad voor uw bedrijf? (Meerdere antwoorden mogelijk)
☐ Ik of personeel was verhinderd in het uitvoeren van dagelijkse werkzaamheden
☐ Verlies aan inkomsten, waarde van aandelen of inkomen
☐ Ik of personeel heeft extra tijd besteed aan het oplossen van het incident of het inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders
☐ Mijn bedrijf heeft kosten gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk
☐ Mijn bedrijf heeft bestanden of gegevens verloren
☐ Boetes van regelgevers of wetgevers, of verwante juridische kosten
☐ Reputatieschade
☐ Onderbreking van levering van goederen of diensten aan klanten, begunstigden of gebruikers van diensten
☐ Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders
☐ Mijn bedrijf heeft een schadevergoeding, compensatie of korting verleend aan klanten
☐Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q28. Kosten
In sommige gevallen leidt ransomware tot meer financiële gevolgen dan alleen de kosten van het losgeld, zoals kosten voor reparatie of herstel. Hoe hoog zou u de kosten van het incident schatten voor uw bedrijf bovenop het gevraagde losgeld?
☐ Geen
☐ Minder dan € 1.000
☐ € 1.000 tot € 5.000
☐ € 5.000 tot € 10.000
☐ € 10.000 tot € 50.000
☐ € 50.000 tot € 100.000
☐ € 100.000 tot € 250.000
☐ € 250.000 tot € 500.000
☐ € 500.000 of meer
☐ Weet ik niet

Q29. Geld – terug
Is de financiële schade (inclusief de eventuele kosten van het losgeld) vergoed (bijvoorbeeld via een verzekering)?
☐ Ja, de financiële schade is volledig vergoed [door naar Q30]
☐ Ja, een gedeelte van de financiële schade is vergoed [door naar Q30]
☐ Nee, de financiële schade is niet vergoed [door naar Q31]
☐ Mijn bedrijf heeft dit aangevraagd en nog geen beslissing ontvangen [door naar Q30]
☐ Er was geen financiële schade [door naar Q31]

Q30. Geld terug – wie
Door welke instantie is de financiële schade (inclusief de eventuele kosten van het losgeld) vergoed of bij welke instantie heeft uw bedrijf een aanvraag gedaan voor een vergoeding?
☐ Bank of financiële instelling
☐ Verzekeringsmaatschappij
☐ Anders, namelijk …

Q31. Gedragsverandering
Welke gevolgen heeft het incident gehad voor de online activiteiten of beveiligingsmaatregelen van uw bedrijf? (Meerdere antwoorden mogelijk).
☐ Mijn bedrijf heeft een ander besturingssysteem genomen
☐ Mijn bedrijf maakt (vaker) back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Mijn bedrijf heeft een wachtwoordbeleid ingevoerd dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen
☐ Mijn bedrijf heeft een antivirusproduct aangeschaft
☐ Mijn bedrijf heeft een firewall aangeschaft die zowel volledige IT-netwerken als individuele apparaten beschermt
☐ Mijn bedrijf laat beveiligingssoftware netwerken en apparaten scannen op virussen of andere kwaadaardige software
☐ Mijn bedrijf monitort gebruikers- of netwerkactiviteiten
☐ Mijn bedrijf voert updates van besturingssystemen, apps en/of software direct uit zodra ze beschikbaar zijn
☐ Mijn bedrijf heeft IT-administratie en toegangsrechten beperkt tot specifieke gebruikers
☐ Mijn bedrijf houdt IT-administratie en toegangsrechten goed bij
☐ Mijn bedrijf heeft specifieke regels opgesteld voor het veilig opslaan van bestanden met persoonsgegevens
☐ Mijn bedrijf heeft een ander standaardbrowser genomen
☐ Mijn bedrijf heeft gevoelige bestanden en gegevens versleuteld

☐ Mijn bedrijf heeft veiligheidsrestricties ingevoerd van apparaten die eigendom zijn van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)
☐ Toegang tot het bedrijfsnetwerk is alleen toegestaan op apparaten die eigendom zijn van het bedrijf
☐ Mijn bedrijf heeft gescheiden wifi-netwerken voor personeel en gasten
☐ Mijn bedrijf heeft tweestapsverificatie ingesteld (2 stappen in plaats van 1 stap om in te loggen)
☐ Mijn bedrijf heeft iemand (intern of extern) in dienst genomen die verantwoordelijk is voor cybersecurity
☐ Mijn bedrijf heeft een bedrijfscontinuïteitsplan opgesteld
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Blok 5: Contact instanties
We willen u nu vragen stellen over de partijen waarmee uw bedrijf contact heeft opgenomen naar aanleiding van het ransomware incident.

Q32. Contact met derden
Heeft uw bedrijf met volgende partijen contact opgenomen naar aanleiding van het ransomware-incident voor advies, ondersteuning of om melding te maken van het incident? (Meerdere antwoorden mogelijk)

De politie
☐ Ja
☐ Nee

Uw bank of financiële instelling
☐ Ja
☐ Nee

Uw verzekeringsmaatschappij
☐ Ja
☐ Nee

Een cybersecuritybedrijf of IT-leverancier
☐ Ja
☐ Nee

Autoriteit Persoonsgegevens
☐ Ja
☐ Nee

No More Ransom
☐ Ja
☐ Nee

Slachtofferhulp
☐ Ja
☐ Nee

Fraudehelpdesk
☐ Ja
☐ Nee

Andere organisatie, namelijk … [open antwoord]
☐ Ja
☐ Nee

Pop-up met nadere toelichting bij 'No More Ransom': No More Ransom is een initiatief van het Team High-Tech Crime van de Nationale Politie, het European Cybercrime Centre van Europol, Kapersky en McAfee. Het heeft tot doel slachtoffers van ransomware te helpen bij het herstellen van hun versleutelde gegevens zonder dat zij de criminelen hiervoor betalen, onder andere door het aanbieden van ontsleuteltools.

[Routing: bij elke 'ja' bij Q32b t/m Q32i, door naar Q33]
[Routing: Bij Q32a 'ja' door naar Q34]
[Routing: indien 'nee' bij Q32b t/m Q32i, door naar Q38]

Q33. Contact – elke organisatie
Hoe tevreden bent u over het contact dat uw bedrijf met [organisatie Q32b t/m Q32h] heeft gehad?

Zeer ontevreden				Zeer tevreden
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

[Door naar Q39, tenzij (ook) contact gehad met politie, dan door naar Q34]

Q34. Contact met politie – doel
Met welk doel nam uw bedrijf contact op met de politie? (Meerdere antwoorden mogelijk)
☐ Voor hulp en/of informatie [door naar Q37]
☐ Om aangifte te doen [door naar Q35]
☐ Mijn bedrijf wilde geen aangifte doen, alleen het incident melden [door naar Q35]

Pop-up met nadere toelichting:
*U kunt een **melding** doen als u wilt dat de politie op de hoogte is van wat u is overkomen, zonder dat er een onderzoek wordt ingesteld of de dader wordt vervolgd. De politie kan de situatie in de gaten houden.*
*Bij een **aangifte** verzoekt u de politie om een onderzoek te starten. U heeft dan een document (proces-verbaal) getekend en een aangifteboekje mee naar huis gekregen.*

Q35. Aangifte
Is er een aangifte gedaan bij de politie waarbij een proces-verbaal is ondertekend?
☐ Ja
☐ Nee

[Door naar Q36]

Q36. Reden van melding bij politie
Wat is de belangrijkste reden dat uw bedrijf het incident gemeld heeft en/of aangifte heeft gedaan bij de politie?
☐ Om te voorkomen dat dit opnieuw bij mijn bedrijf gebeurt
☐ Om te voorkomen dat de dader dit opnieuw bij een ander kan doen
☐ Ik wil dat de dader gepakt wordt
☐ Om een veiligere (online) wereld te creëren
☐ Het is de plicht van mijn bedrijf om aangifte/melding te doen
☐ Om de schade vergoed te krijgen
☐ Anders, namelijk … [open antwoord]

[Door naar Q38]

Q37. Reden van geen melding bij politie
Wat is de belangrijkste reden dat uw bedrijf het incident niet gemeld heeft en/of geen aangifte heeft gedaan bij de politie?
☐ Mijn bedrijf heeft het zelf of met behulp van een andere partij opgelost
☐ Het is niet zo belangrijk
☐ Het kost te veel moeite
☐ Het heeft geen zin, de politie zal er toch niets aan doen
☐ De politie heeft niet de kennis om dit type delict aan te pakken
☐ Het is eerder een zaak voor een andere instantie dan de politie
☐ Mijn bedrijf heeft weinig vertrouwen in de politie
☐ Mijn bedrijf wilde melding/aangifte doen, maar de politie wilde de melding/aangifte niet opnemen
☐ Mijn bedrijf heeft de schade al vergoed gekregen (het losgeld en/of overige kosten)
☐ Mijn bedrijf is bang dat de dader wraak zal nemen
☐ Ik schaam me dat mijn bedrijf slachtoffer is geworden van het delict
☐ Ik schaam me dat mijn bedrijf het losgeld betaald heeft

☐ Ik vind dat het eigenlijk mijn/onze eigen schuld is
☐ Mijn bedrijf is bang voor reputatieschade
☐ Het lukt niet om digitaal een melding/aangifte te doen
☐ Anders, namelijk … [open antwoord]

[Door naar Q38]

Q38. Politie – tevredenheid
Hoe tevreden bent u over het contact dat uw bedrijf met de politie heeft gehad?

Zeer ontevreden				Zeer tevreden
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q39. Standpunt van politie
De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?

Helemaal oneens				Helemaal mee eens
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q40. Standpunt van politie – contact
[Alleen voor respondenten die bij Q32a 'nee' hebben ingevuld]
Heeft dit standpunt eraan bijgedragen dat uw bedrijf geen contact heeft gezocht met de politie?
☐ Ja
☐ Nee

Q41. Standpunt van politie – melding
[Alleen voor respondenten die bij Q34 optie 2 of 3 hebben ingevuld]
Heeft dit standpunt eraan bijgedragen dat uw bedrijf uiteindelijk geen melding of aangifte heeft gedaan bij de politie?
☐ Ja
☐ Nee

Q42. Overig
Zijn er nog belangrijke zaken die u wilt delen over het ransomware-incident of het contact met de instanties?

[Open antwoord – tekst]
_____

Afsluiting
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname aan dit onderzoek.

Wilt u verder praten over of melding maken van wat u is overkomen? Dan kunt u contact opnemen met een van de volgende instanties:
Politie Nederland[50]
Autoriteit Persoonsgegevens[51]
No More Ransom[52]
Slachtofferhulp Nederland[53]
Fraudehelpdesk[54]

50 https://www.politie.nl/
51 https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-door-ransomware
52 https://www.nomoreransom.org/nl/index.html
53 https://www.slachtofferhulp.nl/gebeurtenissen/fraude/malware-en-ransomware/
54 https://www.fraudehelpdesk.nl/ondernemers-fraude/uw-computerbestanden-worden-gegijzeld/

Bijlage 4 Vragenlijst 2B

Inleiding
In deze vragenlijst gaan we in op een specifieke vorm van online criminaliteit: ransomware. Ransomware wordt ook wel gijzelsoftware genoemd. Hierbij blokkeren of versleutelen criminelen bestanden, gegevens of appara(a)t(en) van uw bedrijf waardoor die niet meer te gebruiken zijn. U kunt daardoor bijvoorbeeld niet meer bij data van klanten. Criminelen vragen losgeld om de bestanden te ontsleutelen.

In deze vragenlijst zullen we vragen stellen over wat u zou doen als uw bedrijf slachtoffer zou worden van ransomware. U hoeft geen slachtoffer te zijn geweest van ransomware om de vragenlijst in te vullen. Er zijn geen goede of foute antwoorden, we willen graag uw mening weten.

Blok 1: Achtergrondkenmerken
We stellen u eerst enkele algemene vragen.

Q1. Tijd online
Hoeveel tijd spendeert u doorgaans online voor uw bedrijf?
☐ Minder dan 1 keer per maand
☐ Minimaal 1 keer per maand, maar niet wekelijks
☐ Minimaal 1 keer per week, maar niet dagelijks
☐ Dagelijks
☐ Meerdere keren per dag
☐ Minstens ieder uur (tijdens de uren dat ik aan het werk ben)
☐ Ik ben (bijna) continu online (tijdens de uren dat ik aan het werk ben)

Q2. Activiteiten
Welke van de volgende mogelijkheden heeft of gebruikt uw bedrijf? (Meerdere antwoorden mogelijk)
☐ Accounts of pagina's op sociale media (zoals Facebook of Twitter)
☐ De mogelijkheid voor klanten om online te bestellen, te reserveren, te betalen voor producten of diensten, of een schenking te doen
☐ De mogelijkheid voor klanten om online toegang te krijgen tot (enkele) van uw diensten
☐ Een online bankrekening waarnaar klanten betalingen kunnen overmaken

☐ Een industrieel controlesysteem
☐ Een Enterprise Resource Planning (ERP)-systeem
☐ Financiële of boekhoudingssoftware
☐ Het elektronisch opslaan van bedrijfsgegevens of persoonlijke gegevens van klanten, begunstigden, gebruikers of donateurs
☐ Anders, namelijk [open]
☐ Geen van bovenstaande
☐ Weet ik niet

Q3. Verzekering
Er zijn algemene verzekeringspolissen die dekking bieden voor de gevolgen van een cyberaanval. Er zijn ook specifieke verzekeringspolissen voor dit doeleinde. Welke van de volgende gevallen omschrijft het beste uw situatie?
☐ Mijn bedrijf heeft een specifieke verzekering voor cybersecurity
☐ De cybersecurityverzekering van mijn bedrijf is onderdeel van een bredere verzekeringspolis
☐ Mijn bedrijf is niet verzekerd tegen cybersecurity-incidenten
☐ Weet ik niet

Q4. Jaaromzet
Wat is de jaaromzet van uw bedrijf, in euro's?
☐ Minder dan € 100.000
☐ € 100.000 tot € 500.000
☐ € 500.000 tot € 1.000.000
☐ € 1.000.000 tot € 2.500.000
☐ € 2.500.000 tot € 5.000.000
☐ Meer dan € 5.000.000
☐ Zeg ik liever niet
☐ Weet ik niet

Q5. Cybersecuritymaatregelen
Welke van de volgende beveiligingsmaatregelen neemt uw bedrijf? (Meerdere antwoorden mogelijk)
☐ Back-ups van bestanden en gegevens op een externe harde schijf, clouddienst of server
☐ Een wachtwoordbeleid dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen
☐ Up-to-date antivirusproduct
☐ Firewalls die zowel uw volledige IT-netwerk beschermen, als individuele apparaten beschermen
☐ Beveiligingssoftware die netwerken(en) en apparaten scant op virussen of andere kwaadaardige software
☐ Monitoring van gebruikers- of netwerkactiviteiten

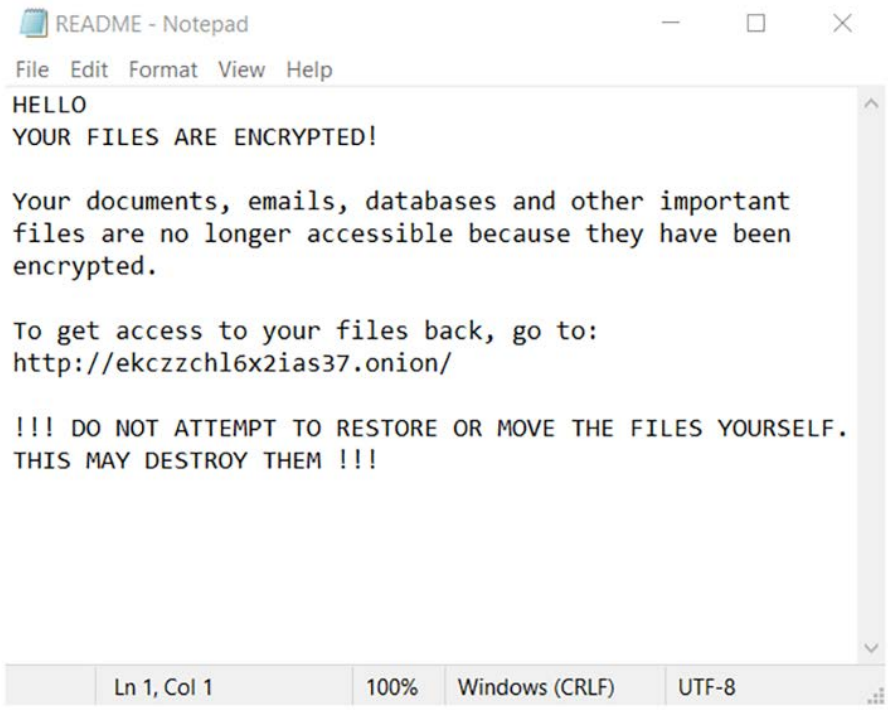
☐ Uitvoeren van updates van besturingssystemen, apps en/of software wanneer beschikbaar
☐ IT-administratie en toegangsrechten zijn beperkt tot specifieke gebruikers
☐ IT-administratie en toegangsrechten worden goed bijgehouden en zijn bijgewerkt
☐ Specifieke regels voor het veilig opslaan van bestanden met persoonsgegevens
☐ Versleuteling van gevoelige bestanden en gegevens
☐ Veiligheidsrestricties van apparaten die eigendom zijn van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)
☐ Toegang tot het bedrijfsnetwerk is alleen toegestaan op apparaten die eigendom zijn van het bedrijf
☐ Gescheiden wifi-netwerken voor personeel en gasten
☐ Tweestapsverificatie (2 stappen in plaats van 1 stap om in te loggen)
☐ Iemand (intern of extern) in dienst die verantwoordelijk is voor cybersecurity
☐ Een bedrijfscontinuïteitsplan
☐ Geen van bovenstaande
☐ Anders, namelijk … [open]
☐ Weet ik niet

Q6. Verantwoordelijk voor cybersecurity
Bent u (eind)verantwoordelijk voor de cybersecurity binnen uw organisatie?
☐ Ja
☐ Nee

Blok 2: Vignet
Er volgt er een scenario waarbij een organisatie getroffen wordt door ransomware.

Probeert u zich voor te stellen dat dit uw organisatie is en u diegene bent die een beslissing moet nemen over het wel of niet betalen van losgeld en het melden van het incident. We willen graag weten wat u in dat geval zou doen. Er zijn geen goede of foute antwoorden, we willen graag uw mening weten.

De volgende boodschap staat op een van de computers binnen uw organisatie:



Door de criminelen wordt u doorgestuurd naar een gepersonaliseerde website waarop het volgende bericht te zien is:

Alle data en systemen van uw organisatie zijn ontoegankelijk gemaakt, inclusief data die essentieel zijn voor de bedrijfscontinuïteit. Als gevolg is de bedrijfsvoering stil komen te liggen. Binnen uw organisatie is er **wel/geen** back-up van deze gegevens beschikbaar. De criminelen eisen **1%/25% van de jaaromzet** van uw organisatie in bitcoin. U heeft een (cybersecurity)organisatie ingeschakeld voor hulp. De mensen om u heen en deze organisatie adviseren u om **wel/niet** het losgeld te betalen.

Q8. Controlevraag 1
Hoeveel losgeld wordt er door de cybercriminelen geëist?
☐ 1% van de jaaromzet van uw organisatie in bitcoin
☐ 25% van de jaaromzet van uw organisatie in bitcoin

Voordat men door kan naar 'Q9' pop-up met volgende tekst: Door de criminelen wordt **1%/25% van de jaaromzet van uw organisatie** in bitcoin aan losgeld geëist. [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q9. Controlevraag 2
Hebben de criminelen gedreigd met het lekken van vertrouwelijke data?
☐ Ja
☐ Nee
Voordat men door kan naar 'Q10' pop-up met volgende tekst: Door de criminelen is **wel/niet gedreigd met het lekken van vertrouwelijke data**, waaronder financiële rapporten, intellectueel eigendom, werknemers- en klantgegevens. [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q10. Controlevraag 3
Is er binnen de organisatie een back-up van de versleutelde gegevens beschikbaar?
☐ Ja
☐ Nee

Voordat men door kan naar 'Q11' pop-up met volgende tekst: Binnen de organisatie is er **een/geen back-up** van de versleutelde gegevens **beschikbaar**. [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

Q11. Controlevraag 4
Is geadviseerd te betalen door de mensen om u heen en de ingehuurde (cybersecurity) organisatie?
☐ Ja
☐ Nee

Voordat men door kan naar 'Q12' pop-up met volgende tekst: De mensen om u heen en de ingehuurde (cybersecurity)organisatie adviseren om **wel/niet** te betalen. [Routing o.b.v. versie van vignet die respondenten hebben gekregen]

We zullen u nu wat vragen stellen over het scenario.

Q12. Eerste gedachte
Wat zou u voelen als u geconfronteerd zou worden met het losgeldbericht? (Meerdere antwoorden mogelijk)
☐ Ik zou me boos voelen
☐ Ik zou afkeer voelen
☐ Ik zou me bang voelen
☐ Ik zou me nerveus voelen
☐ Ik zou me verdrietig voelen
☐ Ik zou me ontspannen voelen
☐ Ik zou me blij voelen
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q13. Eerste reactie
Welke van de volgende dingen zou u doen als u geconfronteerd zou worden met het losgeldbericht?

☐ Ik zou de verbinding met internet verbreken
☐ Ik zou apparaten opnieuw opstarten
☐ Ik zou apparaten terugzetten naar fabrieksinstellingen
☐ Ik zou zelf proberen om mijn bestanden, gegevens of apparaten terug te krijgen
☐ Ik zou hulp of advies zoeken op internet
☐ Ik zou hulp of advies zoeken van een bekende
☐ Ik zou hulp of advies zoeken van een organisatie of instantie
☐ Ik zou proberen bestanden of gegevens te herstellen vanaf een back-up
☐ Ik zou proberen een programma te gebruiken om de ransomware te verwijderen of de bestanden en gegevens te ontsleutelen
☐ Ik zou proberen de bestanden weer te openen door hun extensie terug te veranderen naar hun originele formaat
☐ Ik zou niks doen
☐ Ik zou iets anders doen, namelijk …

Bij antwoordoptie 13g pop-up met nadere toelichting: *Een bestandsextensie is een toevoeging aan het einde van een bestandsnaam die aanduidt om wat voor soort bestand het gaat, zoals .docx of .jpg.*

Q14. Waarschijnlijkheid van betalen
Hoe waarschijnlijk is het dat u ervoor kiest om in deze situatie het losgeld te betalen?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q15. Reden van betalen
Wat is de reden dat uw bedrijf het losgeld zou betalen? (Meerdere antwoorden mogelijk)
☐ Het gevraagde bedrag is niet heel hoog en mijn bedrijf zou het kunnen betalen
☐ Het betalen van het losgeld zou goedkoper zijn dan geen zaken kunnen doen
☐ Mijn bedrijf zou de geblokkeerde of versleutelde bestanden, gegevens of apparaten niet willen verliezen
☐ Ik zou erop vertrouwen dat mijn bedrijf na betaling weer toegang tot apparaten, bestanden en gegevens zou krijgen
☐ Ik zou bang zijn dat de criminelen de bestanden of gegevens zouden lekken (met anderen delen) of dat er andere vervelende gevolgen zouden zijn als mijn bedrijf niet betaalt

☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties
☐ Ik zou het losgeld **niet** betalen

Q16. Reden van niet betalen
Wat is de reden dat uw bedrijf het losgeld **niet** zou betalen? (Meerdere antwoorden mogelijk)
☐ Het gevraagde bedrag is te hoog en mijn bedrijf zou het niet kunnen betalen
☐ Het betalen van het losgeld zou duurder zijn dan geen zaken kunnen doen
☐ Mijn bedrijf zou de versleutelde bestanden, gegevens of apparaten niet belangrijk vinden
☐ Ik zou er niet op vertrouwen dat mijn bedrijf na betaling weer toegang tot apparaten, bestanden en gegevens zou krijgen
☐ Ik zou niet bang zijn dat de criminelen de bestanden of gegevens zouden lekken (met andere delen) of dat er andere vervelende gevolgen zouden zijn als mijn bedrijf niet betaalt
☐ Het is onethisch om criminelen te betalen
☐ Ik zou niet weten hoe ik de betaling zou moeten doen
☐ Anders, namelijk … [open antwoord]
☐ Geen van de bovenstaande opties
☐ Ik zou het losgeld **wel** betalen

Q17. Waarschijnlijkheid van melden
Hoe waarschijnlijk is het dat u ervoor kiest om in deze situatie het incident te melden en/of aangifte te doen?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q18. Melden – partij
Bij welke van de volgende organisaties zou u het incident melden? (Meerdere antwoorden mogelijk)
☐ De politie
☐ Uw bank of financiële instelling
☐ Uw verzekeringsmaatschappij
☐ No More Ransom
☐ Een cybersecuritybedrijf of IT-leverancier
☐ Autoriteit Persoonsgegevens
☐ Slachtofferhulp
☐ Fraudehelpdesk
☐ Andere organisatie, namelijk …

Pop-up met nadere toelichting bij 'No More Ransom': No More Ransom is een initiatief van het Team High-Tech Crime van de Nationale Politie, het European Cybercrime Centre van Europol, Kaspersky en McAfee. Het heeft tot doel slachtoffers van ransomware te helpen bij het herstellen van hun versleutelde gegevens zonder dat zij de criminelen hiervoor betalen, onder andere door het aanbieden van ontsleuteltools.

[Indien 'ja' bij politie, door naar Q19. Indien 'nee' bij politie, door naar Q20]

Q19. Reden van melding bij politie
Wat is de reden dat uw bedrijf het incident zou melden en/of aangifte zou doen bij de politie? (Meerdere antwoorden mogelijk)
☐ Om te voorkomen dat dit opnieuw bij mijn bedrijf gebeurt
☐ Om te voorkomen dat de dader dit opnieuw bij een ander kan doen
☐ Ik zou willen dat de dader gepakt wordt
☐ Om een veiligere (online) wereld te creëren
☐ Het is mijn plicht om aangifte/melding te doen
☐ Om de schade vergoed te krijgen
☐ Anders, namelijk … [open antwoord]

[Door naar Q21]

Q20. Reden van geen melding bij politie
Wat is de reden dat uw bedrijf het incident niet zou melden en/of geen aangifte zou doen bij de politie? (Meerdere antwoorden mogelijk)
☐ Mijn bedrijf zou het zelf of met behulp van een andere partij oplossen
☐ Het is niet zo belangrijk
☐ Het kost te veel moeite
☐ Het heeft geen zin, de politie zou er toch niets aan doen
☐ De politie heeft niet de kennis om dit type delict aan te pakken
☐ Het is eerder een zaak voor een andere instantie dan de politie
☐ Mijn bedrijf heeft weinig vertrouwen in de politie
☐ Mijn bedrijf zou bang zijn dat de dader wraak zal nemen
☐ Ik zou me schamen dat mijn bedrijf slachtoffer is geworden van het delict
☐ Ik zou me schamen dat mijn bedrijf het losgeld betaald heeft
☐ Ik zou vinden dat het eigenlijk mijn/onze eigen schuld is
☐ Mijn bedrijf zou bang zijn voor reputatieschade
☐ Anders, namelijk … [open antwoord]

[Door naar Q22]

Q21. Standpunt van politie
De politie heeft het standpunt dat slachtoffers het geëiste losgeld niet moeten betalen. Wat vindt u hiervan?

Helemaal oneens				helemaal mee eens
☐ 1	☐ 2	☐ 3	☐ 4	☐ 5

Q22. Standpunt politie – betalen
Zou dit standpunt uw keuze om te **betalen** beïnvloeden?
☐ Ja
☐ Nee

Q23. Standpunt politie – contact
Zou dit standpunt uw keuze om **contact op te nemen** met de politie beïnvloeden?
☐ Ja
☐ Nee

Q24. Standpunt politie – melden
Zou dit standpunt uw keuze om het incident te **melden en/of aangifte te doen** bij de politie beïnvloeden?
☐ Ja
☐ Nee

Q25. Contact – daders
Zou u in dit scenario contact opnemen met de daders?
☐ Ja, ikzelf of een collega zou contact opnemen met de daders [door naar Q26]
☐ Ja, ik zou een bekende namens mijn bedrijf contact laten opnemen met de daders [door naar Q26]
☐ Ja, ik zou iemand inhuren om namens mijn bedrijf contact op te nemen met de daders [door naar Q26]
☐ Nee, ik zou geen contact opnemen met de daders [door naar Q28]

Q26. Contact – doel
Met welk doel zou u (of iemand namens u) contact opnemen met de daders? (Meerdere antwoorden mogelijk)
☐ Om vast te stellen of het losgeldbericht echt is [door naar Q28]
☐ Om te onderhandelen over bijvoorbeeld de hoogte van het losgeld of de deadline [door naar Q27]
☐ Om vast te stellen welke bestanden of gegevens door de criminelen zijn gestolen [door naar Q28]
☐ Om hulp te vragen **bij** het betalen (bijvoorbeeld bij het aanschaffen van bitcoin) [door naar Q28]

☐ Om hulp te vragen **na** het betalen (bijvoorbeeld bij het terugkrijgen van bestanden of gegevens) [door naar Q28]
☐ Om tijd te rekken [door naar Q28]
☐ Anders, namelijk … [open antwoord] [door naar Q28]

Q27. Onderhandelen – doel
U heeft aangegeven dat u in deze situatie zou onderhandelen met de daders. Met welk doel zou u onderhandelen? (Meerdere antwoorden mogelijk)
☐ Om het losgeldbedrag te verlagen
☐ Om langer de tijd te krijgen
☐ Om een andere reden, namelijk … [open antwoord]
☐ Ik zou niet onderhandelen

Q28. Perceptie gevolgen – emotioneel
Stel u wordt geconfronteerd met het losgeldbericht. Wat zouden voor u persoonlijk de (tijdelijke) emotionele of psychische gevolgen zijn? Ik zou … (Meerdere antwoorden mogelijk)
☐ … me minder veilig voelen
☐ … minder vertrouwen in mensen hebben
☐ … het voorval telkens opnieuw beleven
☐ … slaapproblemen hebben
☐ … angstklachten en/of paniekaanvallen hebben
☐ … depressieve klachten hebben
☐ … minder vertrouwen hebben in mijn eigen digitale vaardigheden
☐ … andere emotionele of psychische gevolgen ervaren, namelijk … [open antwoord]
☐ Geen van bovenstaande opties
☐ Weet ik niet

Q29. Perceptie gevolgen
Welke van de andere gevolgen zou het incident voor u hebben? (Meerdere antwoorden mogelijk)
☐ Ik of personeel zou verhinderd zijn in het uitvoeren van dagelijkse werkzaamheden
☐ Verlies aan inkomsten, waarde van aandelen of inkomen
☐ Ik of personeel heeft extra tijd besteed aan het oplossen van het incident of het inlichten van klanten, begunstigden, belanghebbenden, studenten of ouders
☐ Mijn bedrijf zou kosten hebben gemaakt vanwege reparatie of herstel van bijvoorbeeld een apparaat of netwerk
☐ Mijn bedrijf zou bestanden of gegevens verloren zijn
☐ Boetes van regelgevers of wetgevers, of verwante juridische kosten
☐ Reputatieschade
☐ Onderbreking van levering van goederen of diensten aan klanten, begunstigden of gebruikers van uw diensten
☐ Klachten van klanten, begunstigden, belanghebbenden, studenten of ouders

☐ Mijn bedrijf zou een schadevergoeding, compensatie of korting verleend hebben aan klanten
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Q30. Perceptie van kosten
In sommige gevallen leidt ransomware tot meer financiële gevolgen dan alleen de kosten van het losgeld, zoals kosten voor reparatie of herstel. Hoe hoog zou u in deze situatie de kosten van het incident schatten bovenop het gevraagde losgeld?
☐ Geen
☐ Minder dan € 1.000
☐ € 1.000 tot € 5.000
☐ € 5.000 tot € 10.000
☐ € 10.000 tot € 50.000
☐ € 50.000 tot € 100.000
☐ € 100.000 tot € 250.000
☐ € 250.000 tot € 500.000
☐ € 500.000 of meer
☐ Weet ik niet

Q31. Cybersecuritymaatregelen
Denkt u dat u in deze situatie aanvullende beveiligingsmaatregelen zou nemen naar aanleiding van het incident? (Meerdere antwoorden mogelijk).
☐ Ja [door naar Q32]
☐ Nee [door naar Q33]

Q32. Cybersecuritymaatregelen – wat
Welke van de volgende beveiligingsmaatregelen zou uw bedrijf nemen naar aanleiding van het incident? (Meerdere antwoorden mogelijk).
☐ Mijn bedrijf zou een ander besturingssysteem nemen
☐ Mijn bedrijf zou (vaker) back-ups maken van bestanden en gegevens op een externe harde schijf, cloudopslag of server
☐ Mijn bedrijf zou een wachtwoordbeleid invoeren dat ervoor zorgt dat gebruikers sterke wachtwoorden kiezen
☐ Mijn bedrijf zou een antivirusproduct aanschaffen
☐ Mijn bedrijf zou een firewall aanschaffen die zowel het volledige IT-netwerk beschermt, als individuele apparaten
☐ Mijn bedrijf zou beveiligingssoftware, netwerken en apparaten laten scannen op virussen of andere kwaadaardige software
☐ Mijn bedrijf zou gebruikersactiviteiten monitoren
☐ Mijn bedrijf zou updates van besturingssystemen, apps en/of software direct uitvoeren zodra ze beschikbaar zijn

☐ Mijn bedrijf zou IT-administratie en toegangsrechten beperken tot specifieke gebruikers
☐ Mijn bedrijf zou IT-administratie en toegangsrechten goed bijhouden en bijgewerkt houden
☐ Mijn bedrijf zou specifieke regels opstellen voor het veilig opslaan van bestanden met persoonsgegevens
☐ Mijn bedrijf zou een andere standaardbrowser nemen
☐ Mijn bedrijf zou gevoelige bestanden en gegevens versleutelen
☐ Mijn bedrijf zou veiligheidsrestricties invoeren van apparaten die eigendom zijn van het bedrijf (bijvoorbeeld beperkte mogelijkheden om software op laptops te installeren)
☐ Mijn bedrijf zou toegang tot het bedrijfsnetwerk alleen toestaan op apparaten die eigendom zijn van het bedrijf
☐ Mijn bedrijf zou gescheiden wifi-netwerken hebben voor personeel en gasten
☐ Mijn bedrijf zou tweestapsverificatie instellen (2 stappen in plaats van 1 stap om in te loggen)
☐ Mijn bedrijf zou iemand (intern of extern) in dienst nemen die verantwoordelijk is voor cybersecurity
☐ Mijn bedrijf zou een bedrijfscontinuïteitsplan opstellen
☐ Anders, namelijk … [open antwoord]
☐ Geen van bovenstaande opties

Blok 3: Slachtofferschap
We stellen u tot slot enkele vragen over slachtofferschap van ransomware.

Q33. Gepercipieerde kwetsbaarheid – ander
Hoe groot schat u de gemiddelde kans dat een organisatie in Nederland slachtoffer zou worden van ransomware?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q34. Gepercipieerde kwetsbaarheid – zelf
Hoe groot schat u de gemiddelde kans dat uw organisatie slachtoffer zou worden van ransomware?

Matrix or slider

Helemaal niet waarschijnlijk										Zeer waarschijnlijk
☐ 0%	☐ 10	☐ 20	☐ 30	☐ 40	☐ 50	☐ 60	☐ 70	☐ 80	☐ 90	☐ 100%

Q35. Slachtoffer – ander
Kent u iemand die ooit slachtoffer is geworden van ransomware, waarbij bestanden, gegevens of apparaten geblokkeerd of versleuteld zijn door criminelen en er om losgeld is gevraagd om hier weer toegang tot te krijgen?
☐ Ja
☐ Nee

Tot slot
Dit is het einde van de vragenlijst. We willen u vriendelijk bedanken voor uw deelname in dit onderzoek.

Bijlage 5 Verdeling vignetten over groepen (deelstudie 2)

Tabel 1 Verdeling van vignetten onder burgers (n=4.082)

Groep	Vignet				Verdeling	
	Hoogte losgeld	Geadviseerd om te betalen	Back-up	Gedreigd met lekken	N	%
1	250 euro	Nee	Nee	Ja	258	6,3%
2	250 euro	Nee	Ja	Ja	259	6,3%
3	250 euro	Ja	Nee	Ja	256	6,3%
4	250 euro	Ja	Ja	Ja	242	5,9%
5	2.500 euro	Nee	Nee	Ja	254	6,2%
6	2.500 euro	Nee	Ja	Ja	238	5,8%
7	2.500 euro	Ja	Nee	Ja	274	6,7%
8	2.500 euro	Ja	Ja	Ja	273	6,7%
9	250 euro	Nee	Nee	Nee	231	5,7%
10	250 euro	Nee	Ja	Nee	274	6,7%
11	250 euro	Ja	Nee	Nee	242	5,9%
12	250 euro	Ja	Ja	Nee	239	5,9%
13	2.500 euro	Nee	Nee	Nee	288	7%
14	2.500 euro	Nee	Ja	Nee	253	6,2%
15	2.500 euro	Ja	Nee	Nee	255	6,2%
16	2.500 euro	Ja	Ja	Nee	247	6,1%

Tabel 2 Verdeling van vignetten onder zzp'ers (n=1.769)

Groep	Vignet				Verdeling	
	Hoogte losgeld	**Geadviseerd om te betalen**	**Back-up**	**Gedreigd met lekken**	**N**	**%**
1	1% van jaaromzet	Nee	Nee	Ja	123	6,9%
2	1% van jaaromzet	Nee	Ja	Ja	106	6%
3	1% van jaaromzet	Ja	Nee	Ja	123	7%
4	1% van jaaromzet	Ja	Ja	Ja	114	6,4%
5	25% van jaaromzet	Nee	Nee	Ja	101	5,7%
6	25% van jaaromzet	Nee	Ja	Ja	102	5,7%
7	25% van jaaromzet	Ja	Nee	Ja	112	6,3%
8	25% van jaaromzet	Ja	Ja	Ja	97	5,5%
9	1% van jaaromzet	Nee	Nee	Nee	117	6,6%
10	1% van jaaromzet	Nee	Ja	Nee	119	6,8%
11	1% van jaaromzet	Ja	Nee	Nee	99	5,6%
12	1% van jaaromzet	Ja	Ja	Nee	96	5,4%
13	25% van jaaromzet	Nee	Nee	Nee	118	6,7%
14	25% van jaaromzet	Nee	Ja	Nee	104	5,9%
15	25% van jaaromzet	Ja	Nee	Nee	126	7,1%
16	25% van jaaromzet	Ja	Ja	Nee	113	6,4%

Tabel 3 Verdeling van vignetten onder mkb'ers (n=732)

Groep	Vignet				Verdeling	
	Hoogte losgeld	**Geadviseerd om te betalen**	**Back-up**	**Gedreigd met lekken**	**N**	**%**
1	1% van jaaromzet	Nee	Nee	Ja	48	6,6%
2	1% van jaaromzet	Nee	Ja	Ja	65	8,9%
3	1% van jaaromzet	Ja	Nee	Ja	35	4,8%
4	1% van jaaromzet	Ja	Ja	Ja	52	8%
5	25% van jaaromzet	Nee	Nee	Ja	43	5,9%
6	25% van jaaromzet	Nee	Ja	Ja	59	8%
7	25% van jaaromzet	Ja	Nee	Ja	48	6,6%
8	25% van jaaromzet	Ja	Ja	Ja	40	5,5%
9	1% van jaaromzet	Nee	Nee	Nee	44	6%
10	1% van jaaromzet	Nee	Ja	Nee	38	5,2%
11	1% van jaaromzet	Ja	Nee	Nee	49	6,7%
12	1% van jaaromzet	Ja	Ja	Nee	52	7,1%
13	25% van jaaromzet	Nee	Nee	Nee	43	5,8%
14	25% van jaaromzet	Nee	Ja	Nee	46	6,3%
15	25% van jaaromzet	Ja	Nee	Nee	38	5,2%
16	25% van jaaromzet	Ja	Ja	Nee	32	4,4%

Bijlage 6 Informatiebrief en informed consent interviews

INFORMATIEBRIEF
over het interview en het onderzoek:

'Factoren die bijdragen aan onderhandelen, betalen en melden door slachtoffers van ransomware'

Geachte heer/mevrouw,

Met deze brief willen wij uw medewerking vragen aan een interview in het kader van het onderzoek 'Factoren die bijdragen aan onderhandelen, betalen en melden door slachtoffers van ransomware' dat momenteel uitgevoerd wordt door de Haagse Hogeschool in opdracht van Politie & Wetenschap.

Doel onderzoek
Het doel van het onderzoek is om slachtofferschap van ransomware in kaart te brengen en meer inzicht te krijgen in de factoren die bijdragen aan het onderhandelen, betalen en melden door slachtoffers van ransomware. In een eerdere fase is dit onderzocht aan de hand van vragenlijsten onder Nederlandse burgers en bedrijven. In de huidige fase is het doel om door middel van **interviews met experts** te achterhalen hoe verschillende organisaties slachtoffers adviseren te handelen in het geval van slachtofferschap, en in hoeverre slachtoffers deze adviezen opvolgen.

Door uw deelname aan een interview kan er meer inzicht verkregen worden in hoe uw organisatie slachtoffers van ransomware ondersteunt en/of adviseert.

Interview
Een interview duurt ongeveer een uur. In overleg wordt vastgesteld op welke manier (online of live), datum en tijdstip het interview wordt gehouden. Met uw toestemming zal er een geluidsopname van het interview gemaakt worden en zullen er tijdens het interview schriftelijke aantekeningen gemaakt worden.

Privacy
De informatie die u in het interview geeft, wordt alleen voor dit onderzoek gebruikt. Uw gegevens worden anoniem verwerkt. Dit betekent dat u niet met naam en toenaam in een onderzoekpublicatie wordt genoemd: u blijft volledig onbekend. Ook zal de informatie die u deelt niet rechtstreeks naar u herleidbaar zijn.

Onderzoekers
Sifra Matthijsse – De Haagse Hogeschool
Susanne van 't Hoff-de Goede – De Haagse Hogeschool
Rutger Leukfeldt – De Haagse Hogeschool/Nederlands Studiecentrum voor Criminaliteit en Rechtshandhaving

INFORMATIE
over het interview en het onderzoek:

'Factoren die bijdragen aan onderhandelen, betalen en melden door slachtoffers van ransomware'

- Ik ben over het interview en het onderzoek geïnformeerd.
- Ik heb de schriftelijke informatie gelezen.
- Ik ben in de gelegenheid gesteld om vragen over het interview en het onderzoek te stellen.
- Ik heb over mijn deelname aan het interview en het onderzoek kunnen nadenken.
- Ik geef toestemming voor het maken van een geluidsopname en schriftelijke aantekeningen tijdens het interview.
- Mijn deelname aan het onderzoek is vrijwillig.
- Ik heb het recht om mijn toestemming op ieder moment weer in te trekken, zonder dat ik daarvoor een reden hoef op te geven.

Ik stem toe met deelname aan het onderzoek.

Naam:
Datum:
Handtekening:

Ondergetekende (onderzoeker) verklaart dat de hierboven genoemde persoon over het onderzoek is geïnformeerd. Hij/zij verklaart tevens dat de deelnemer van een voortijdige beëindiging van de deelname aan dit onderzoek geen nadelige gevolgen zal ondervinden.

Naam:
Functie:
Datum:
Handtekening:

Bijlage 7 Interviewprotocol

1. Introductie
– Voorstellen, doel onderzoek en interview
– Informed consent
– Vragen vooraf

2. Achtergrond expert
– Activiteiten/diensten organisatie
– Functie/werkzaamheden respondent
– Op welke wijze kennis of ervaring opgedaan met ransomware

3. Ondersteuning en/of advisering slachtoffers
– Kenmerken slachtoffers
  • Hoeveel
  • Individuen/organisaties/andere kenmerken
  • Hoe organisatie respondent gevonden
  • In welke fase van incident contact
– Hoe wordt er geadviseerd & vanuit welke overweging(en) m.b.t:
  • Contact/onderhandelen
  • Betalen
  • Melden
  • Nazorg
– Opvolging adviezen
– Tevredenheid van slachtoffers

4. Resultaten vragenlijsten

Onderhandelen
Hoewel ongeveer 27 tot 40% van de respondenten in een hypothetisch scenario zou onderhandelen, liggen daadwerkelijke cijfers lager. 0% van de burgers en zzp'ers heeft onderhandeld, 26,7% van de mkb'ers die contact heeft opgenomen, heeft onderhandeld.
– Vergelijking met beeld respondent
– Verklaring verschil

Betalen
Ongeveer 4% van de burgers en tussen de 6 en 8% van de ondernemers betaalt het losgeld. Voornaamste reden om wel te betalen is vertrouwen op herstel en niet willen verliezen van data. Voornaamste reden om niet te betalen is geen vertrouwen in herstel, onethisch om criminelen te betalen en het hebben van back-ups (laatste alleen voor mkb).
– Vergelijking met beeld respondent
– Moet de betalingsbereidheid verlaagd worden? Hoe?

In het hypothetische scenario is betalingsbereidheid bovendien voor burgers gerelateerd aan de hoogte van het losgeld, dreigen met lekken en advies om te betalen, voor zzp'ers een back-up en advies om te betalen en voor mkb'ers de hoogte van het losgeld en advies om te betalen.
– Vergelijking met beeld respondent
– Hoe kijkt u aan tegen het feit dat geadviseerd worden om te betalen ook leidt tot een hogere betalingsbereidheid?

Melden
Burgers en ondernemers kloppen vaker bij een cybersecuritybedrijf of IT-leverancier aan dan bij de politie.
– Vergelijking met beeld respondent
– Verklaring
– Is dit problematisch? Waarom?

Hoewel ongeveer 88 tot 93% van de respondenten in een hypothetisch scenario zou melden bij de politie, liggen de daadwerkelijke cijfers lager. 15,6% van de burgers, 12,3% van zzp'ers en 26,7% van de mkb'ers heeft gemeld bij de politie. Het daadwerkelijke aangiftepercentage ligt tussen 1 en 2% voor burgers en zzp'ers, en 10% voor mkb'ers.

Voornaamste reden om wel melden is willen dat de dader gepakt wordt en voorkomen dat het bij een ander gebeurt. Voornaamste reden om niet te melden is voor burgers het zelf opgelost hebben en dat het geen zin heeft omdat de politie er toch niets aan doet.
– Vergelijking met beeld respondent
– Verklaring verschil
– Moet de meldingsbereidheid verhoogd worden? Hoe?

Standpunt politie heeft voor 20-30% invloed op keuze om contact op te nemen met de politie en 20-40% keuze voor daadwerkelijke melding/aangifte.
– Vergelijking met beeld respondent
– Hoe kijkt u aan tegen het feit dat geadviseerd worden om niet te betalen maakt dat een kleine groep geen contact opneemt met of melding doet bij de politie?

5. Aanpak
– Goede punten en verbeterpunten in advisering en ondersteuning van slachtoffers
– Wat ontbreekt er nog?

6. Afsluiting

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***

   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

2. ***Cameratoezicht. Goed bekeken?***

   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002

3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***

   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***

   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003

5. ***Cameratoezicht. De menselijke factor***

   A. Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003

6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlist-methodiek***

   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)

7. ***Hooligans in beeld.Van informatie naar aanpak***

   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005

8. ***Richtlijnen auditieve confrontatie***

   J.H. Kerstholt, A.G. van Amelsvoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/NFI, Den Haag, 2005

9. ***Niet verschenen***

10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***

    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006

11. ***Inzoomen en uitzoomen op Zaandam***

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. ***Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking***

E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/ Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. ***Cold cases – een hot issue***

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. ***Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?***

A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. ***Tussen aangifte en zaak. Een referentiekader voor het aangifteproces***

W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. ***Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie***

M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. ***Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden***

E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. ***Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken***

G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. ***Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren***

G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. ***Solosurveillance. Kosten en baten***

S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. ***Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners***

M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. ***Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving***

B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. ***Informatiemanagement binnen de politie. Van praktijk tot normatief kader***

V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. ***Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept***

H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. ***Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders***

I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. ***Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren***

W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. ***Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering***

E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. ***De politie aan zet: de aanpak van veelplegers in Deventer***

I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. ***Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland***

O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. ***Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk***

G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. ***Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten***

A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***

J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***

M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politiefunctionarissen***

H. Sollie, Universiteit Twente, Enschede, 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***

M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***

R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***

A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***

W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***

J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***

J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***

H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***

H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijningsvormen***

L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012

43. ***De organisatie van de opsporing van cybercrime door de Nederlandse politie***

N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/ Kees de Vey Mestdagh, Groningen, 2012

44. ***Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg***

I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude, 2012

45. ***Tegenspraak in de opsporing. Verslag van een onderzoek***

R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen, 2012

46. ***Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten***

I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude, 2012

47. ***M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing***

M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2012

48. ***Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen***

Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem, 2012

49. ***Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus***

H. Ferwerda, T. van Ham & B. Bremmers, Bureau Beke, Arnhem, 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***

H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht, 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***

A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

51a. ***De operationele politiebriefing onderzocht (2). Een actie(vervolg)onderzoek om tot een effectievere politiebriefing te komen***

A. Scholtens, Crisislab, Renswoude 2015

52. ***Sociale media: factor van invloed op onrustsituaties?***

R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VD-MMP, Houten, 2013

53. ***De terugkeer van zedendelinquenten in de wijk***

C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen, 2013

54. ***Van meld- naar aantoonplicht. Een onderzoek naar een systeem van digitale surveillance***

C. Veen & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen, 2013

55. ***Heterdaadkracht in twee Haagse pilotgebieden***

B. van Dijk, J.B. Terpstra & P. Hulshof, Politieacademie, Apeldoorn/DSP-groep, Amsterdam, 2013

56. ***Inzet op Maat. Onderzoek naar kenmerken en mogelijkheden van duurzame inzetbaarheid van oudere medewerkers***

H. de Blouw, I.R. Kolkhuis Tanke & C.C. Sprenger, Politieacademie, Apeldoorn, 2013

57. ***Interventies in de opsporing. Impulsen in kwaliteit en effectiviteit van het opsporingsproces***

R.M. Kouwenhoven, R.J. Morée & P. van Beers, Twynstra Gudde, Amersfoort, 2013

58. ***De plaats delict in beeld. Fotografie in de dagelijkse en gesimuleerde praktijk***

G. Vanderveen & J. Roosma, Instituut voor Strafrecht & Criminologie, Universiteit Leiden, 2013

59. ***Jeugdgroepen van toen. Een casusonderzoek naar de leden van drie criminele jeugdgroepen uit het einde van de vorige eeuw***

H. Ferwerda, B. Beke & E. Bervoets, Bureau Beke, Arnhem/Beke Advies, Arnhem/LokaleZaken, Rotterdam, 2013

60. ***Tussen hei en hoofdbureau. Leiderschapsontwikkeling bij de politie***

W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2013

61. ***Gemeentelijk blauw. Het dagelijks werk van gemeentelijke handhavers in beeld***

E. Bervoets, J. Bik & M. de Groot, LokaleZaken, Rotterdam, 2013

62. ***Excessief geweld op en om de voetbalvelden. Praktijkonderzoek naar omvang, ernst en aanpak van 'voetbalgeweld'***

P. Duijvestijn, B. van Dijk, P. van Egmond, M. de Groot, D. van Sommeren & A. Verwest, DSP-groep, Amsterdam, 2013

63. ***Beeld van gezag bij de politie. Maatschappelijke verbeelding en de impact van gezagsbeelden op burgers***

H. de Mare, B. Mali, M. Bleecke & G. van den Brink, m.m.v. Motivaction, Tilburg University, Stichting IVMV, Leiden, 2014

64. ***Informatiegestuurde dienders. Informatiesturing tussen theorie en praktijk***

A. van Sluis, P. Siep, V. Bekkers, m.m.v. M. Thaens & G. Straten, Center for Public Innovation, Erasmus Universiteit, Rotterdam, 2014

65. ***Hard op weg. Onderzoek aanpak verkeersveelplegers***

B. Bieleman, M. Boendermaker, R. Mennes & J. Snippe, Intraval, Groningen/ Rotterdam, 2014

66. ***Tussen hulp en hype. De inzet van opsporingsberichtgeving in ontvoeringszaken***

Y.M.M. Schoenmakers, J.V.O.R. Doekhie & J.C. Knotter, Yvette Schoenmakers Onderzoek en advies, Weesp, 2014

67. ***Nachtdienst bij de politie en verkeersveiligheid. Onderzoek naar ervaringen van politieagenten met verkeersonveiligheid in woon-werkverkeer na de nachtdienst***

P. Boekhoorn, BBSO, Nijmegen, 2014

68. ***Buit van woninginbraak. Onderzoek onder inbrekers en helers***

J. Snippe, M. Sijtstra, R. Mennes & B. Bieleman, Intraval, Groningen/ Rotterdam, 2014

69. ***Privaat blauw. Portiers, evenementbeveiligers en voetbalstewards op risicovolle locaties en tijdens risicovolle momenten***

E. Bervoets & S. Eijgenraam, LokaleZaken, Rotterdam, 2014

70. ***Met grof geschut. Reconstructie van een moordonderzoek binnen de criminele woonwagenwereld***

I. van Leiden, B. Bremmers & H. Ferwerda, Bureau Beke, Arnhem, 2014

71. ***Met fluwelen handschoenen? Politie en de omgang met verwarde personen in Amsterdam***

J. Kuppens, T. Appelman, T. van Ham & A. van Wijk, Bureau Beke, Arnhem, 2015

72a. ***Vermisten op de kaart. Aard en omvang van langdurige vermissingen***

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2015

73. ***Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad***

M. den Hengst, M. Bruinsma, Y. Schoenmakers, W. Niepce, Bureau Bruinsma, Tilburg, 2015

74. ***De bestuurlijke rapportage. Gezamenlijke inspanning in de aanpak van (georganiseerde) criminaliteit en overlast***

I. Gorissen, m.m.v. R.H. Johannink, PBLQ, Den Haag, 2015

75. ***De aangifte van delicten bij de multichannelstrategie van de politie***

P. Boekhoorn & J. Tolsma, Bureau Boekhoorn/Radboud Universiteit, Nijmegen, 2016

76. ***Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende aangiftecriminaliteit***

R. Kouwenhoven & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

77. ***Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie***

A. Scholtens, M. den Hengst & R. Waterreus, Crisislab, Renswoude/ Politieacademie, Apeldoorn, 2016

78. ***Hoe lang kun je 'schijt hebben'? Dertien desisters uit criminele jeugdgroepen aan het woord***

C.E. Hoogeveen, A.E. van Burik & B.J. de Jong, m.m.v. E.M. Klooster, Bureau Alpha, 's-Hertogenbosch/VanMontfoort, Woerden, 2016

79. ***Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing***

A. van Wijk & L. Scholten, m.m.v. B. Bremmers, Bureau Beke, Arnhem, 2016

80. ***Verbale leugendetectie-wizards***

G. Bogaard & E.H. Meijer, Maastricht University, Maastricht, 2016

81. ***Mensenhandel in de prostitutie opsporen zonder aangifte? Een vervolgonderzoek om de doorzettingsmacht van de politie te verduidelijken***

M. Goderie, m.m.v. R. Kool, Goderie Onderzoek, Klarenbeek, 2016

82. ***De onvindbaren. Op zoek naar voortvluchtige veroordeelden in Nederland***

Y. Schoenmakers, I. de Groot, J. van Zanten, A. van Rooyen & J. Baars, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2017

83. ***Elke dump is een plaats delict. Dumping en lozing van synthetisch drugsafval: verschijningsvormen en politieaanpak***

Y. Schoenmakers, S. Mehlbaum, M. Everartz & C. Poelarends, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2016

83A. ***De Intelligence Paradox. Lessen uit de integrale pilot Analyse Synthetische Drugs in Oost-Nederland***

Y. Schoenmakers, S. Mehlbaum, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2019

84. ***Naar handhaafbare noodbevelen en noodverordeningen. Een analyse van het gemeentelijke noodrecht***

A.J. Wierenga, C. Post & J. Koornstra, Rijksuniversiteit Groningen, Centrum voor Openbare Orde en Veiligheid, 2016

85. ***Vermisten op het spoor. Rechercheren naar langdurige vermissingen***

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

86. ***De aard van het beestje. Kenmerken en achtergronden van dierenmishandelaars***

A. van Wijk & M. Hardeman, Bureau Beke, Arnhem, 2017

87. ***Modus operandi van de recherche. De rechercheprakijk in moord- en verkrachtingszaken***

A. van Wijk, I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

88. ***Over grenzen in de sport. De rol van de politie in de aanpak van seksueel grensoverschrijdend gedrag in de sport in samenwerking met relevante partners***

A. van Wijk, M. Hardeman, L. Scholten & M. Olfers, Vrije Universiteit Amsterdam, Bureau Beke, Arnhem, 2017

89. ***Defensiehulp. Legergroene bijstand aan de politie bij handhaving van de rechtsorde***

E. Bervoets, m.m.v. S. Eijgenraam, T. Dijkhuizen & J. van de Werken, Bureau Bervoets, Amersfoort, 2017

90. ***Tussen onder en boven. Productie en distributie van softdrugs in Noord- Nederland***

J. Snippe, R. Mennes, M. Sijtstra & B. Bieleman, Intraval, Groningen/Rotterdam, 2017

91. ***Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie***

T. van Ham, L. Scholten, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

92. ***Notoire straten. Over de lokale inbedding van georganiseerde criminaliteit***

S. Mehlbaum, Y. Schoenmakers & J. van Zanten, Mehlbaum Onderzoek, Amsterdam, 2018

92A. ***De wortel en de stok. Praktijklessen uit een gebiedsgerichte probleemaanpak van ondermijning***

S. Mehlbaum, Y. Schoenmakers, Mehlbaum Onderzoek, Amsterdam, 2019

93. ***Ondermijning door criminele 'weldoeners'***

M. Bruinsma, R. Ceulen & T. Spapens, m.m.v. C. Deij, Tilburg University, Tilburg/Bureau Bruinsma, Tilburg, 2018

94. ***Kiezen voor politie. Een onderzoek onder mbo-studenten met een migratie – achtergrond in het veiligheidsdomein***

S. de Winter-Koçak, E. Klooster & M. Day, m.m.v. S. Mehlbaum, M. van Vugt & K. Leschonski, Verwey-Jonker Instituut, Utrecht, 2018

95. ***Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen***

S. Mehlbaum & R. van Steden, m.m.v. M. van Dijk, Vrije Universiteit Amsterdam, Mehlbaum Onderzoek, Amsterdam, 2018

96. ***Een klacht is een gratis advies***

G. Jacobs, T. Hak, G. Vanderveen, M. Flory, T. Thuis, S. Valkeman & M. Franken, Erasmus Universiteit, Rotterdam, 2018

97. ***Voortgezet crimineel handelen tijdens detentie: je gaat het pas zien als je het doorhebt***

A. Verwest, W. Buysse, P. van Egmond, D. Hofstra, DSP-groep, Amsterdam, 2019

98. ***Zorg voor kinderen bij aanhouding van ouders; Best practices uit binnen- en buitenland***

J. Reef, N. Ormskerk, Universiteit Leiden, 2019

99. ***Aankoopfraude uit het buitenland***

J. Jansen, S. Westers, S. Twickler, W. Stol, NHL Stenden Hogeschool / Politieacademie

100. ***Grijs vakmanschap? Taakgerelateerd ongeoorloofd handelen binnen de politie***

R. Chr. van Halderen (diss. Avans Hogeschool), 2019

101. ***Niet meer doen! Een onderzoek naar de INDIGO-afdoening***

A. van Wijk, S. Dickie, J. van Esseveldt, Bureau Beke, Arnhem, 2019

102. ***De aanpak van cybercrime door regionale eenheden van de politie. Van intake van cybercrime naar opsporing en vervolging***

P. Boekhoorn, BBSO, Nijmegen, 2020

103. ***In- en doorstroom van nieuwkomers in beeld. Opgetekende lessen uit acht casussen rond de opvang van asielzoekers in Nederland.***

J. Kuppens, Bureau Beke, Arnhem 2020

104. ***De lading van vuurwapens. Een onderzoek naar de impact van illegale vuurwapens in Nederland.***

H. Ferwerda, J. Wolsink en I. van Leiden, Bureau Beke, Arnhem 2020

105. ***Q-teams. De politie onderweg naar toekomstbestendige opsporing en vervolging?***

P. van Egmond, A. Swami-Persaud, A. Verwest, DSP-groep, Amsterdam 2020

106. ***Onderwereld boven water? Zoektocht naar georganiseerde criminaliteit in de Noordelijke zeehavens***

N. Struiksma, C. Boxum, S.J. Hollenberg, N.O.M. Woestenburg, Pro Facto, Groningen 2020

107. ***Benutten van digitale sporen***

R. Zuurveen, W. Ph. Stol, Onderzoeksgroep Cybersafety. NHL Stenden en CyberScienceCenter 2020

108. ***Kansen en knelpunten binnen de financiële opsporing***

L.N. de Swart, G.P.J.M op 't Hoog, B.M.J Slot, A. Winkel. Ecorys 2021

109. ***Black box van gemeentelijke online monitoring. Een wankel fundament onder een stevige praktijk***

W. Bantema, S. Westers, M. Hoekstra, R. Herregodts, S. Munneke. NHL Stenden Hogeschool / Rijksuniversiteit Groningen, 2021

110. ***Ondermijning langs zijpaden. Een verkennend onderzoek naar de aard, omvang en aanpak van ondermijnende criminaliteit in relatie tot kleine havens en luchthavens, railtransport en binnenvaart in Noord-Brabant en Zeeland.***

S. van Nimwegen, T. Spapens, R. Ceulen, Tilburg University/Nationale Politie, 2021

111. ***Meer dan een ruzie. Politie in de netwerkaanpak huiselijk geweld.***

K.D. Lünnemann, S. ter Woerds, Verwey-Jonker Instituut 2021

112. ***Van verhalen naar verbalen. Een verkennende studie naar de aanpak van ondermijnende drugscriminaliteit in het Noordzeekanaalgebied en de haven van Amsterdam***

Y. Eski, M. Boelens, A. Mesic, H. Boutellier, Vrije Universiteit Amsterdam/ Verwey-Jonker Instituut 2021

113. ***Weten, doen en leren. Een proeftuinonderzoek naar gebiedsgerichte opsporing***

E. Bervoets, J. Broekhuizen, K. van den Akker, J. Landsman, Bureau Bervoets, Amersfoort 2021

114. Zuiver op de graat? Over de betrokkenheid van de visserij bij maritieme drugssmokkel

S. Mehlbaum, K. van den Akker, A. Verweij, A. Wester m.m.v. R. van der Borden en M. Dekker, Mehlbaum Onderzoek, Halfweg 2021

115. Kinderen als slachtoffer, getuige of dader van huiselijk geweld. Aard en afhandeling van door de politie bij ZSM aangebrachte zaken van huiselijk geweld waarbij minderjarigen zijn betrokken.

V. van Koppen, M. Bruggeman, R. Houston, J. Harte, VU Amsterdam 2022

116. Wachters aan het woord. Dilemma's van accountants, advocaten, belastingadviseurs en notarissen in hun rol als poortwachter.

K. van Wingerde, C. Hofman, Erasmus Universiteit Rotterdam, Erasmus school of law, 2022.

117. Ooggetuigenidentificaties: het verband tussen subjectieve zekerheid en accuraatheid. Een experimentele studie en her-analyse van bestaand onderzoek volgens Nederlandse confrontatieprotocollen

M. Sauerland, N. Tupper, A.G. van Amelsvoort, Maastricht University 2022

118. Het fenomeen vechtafspraken: vier jaar later. Onderzoek naar de profielen van de deelnemers, kenmerken van de vechtgroepen en − nieuwe ontwikkelingen ten aanzien van − het fenomeen vechtafspraken

J. Wolsink, H. Ferwerda, Bureau Beke, Arnhem 2022

119. Strip- en omkatfabrieken. Een fenomeenstudie als basis voor inzicht, awareness en aanpak

H. Ferwerda, J. Wolsink, Bureau Beke, Arnhem 2022

120. Bestuurlijke rapportage bij sluitingen van drugspanden. Onderzoek naar het succesvol opstellen, aanbieden en opvolgen van bestuurlijke rapportages in artikel 13b Opiumwet-zaken

L.M. Bruijn, R. Mennes, J.A. de Muijnck, M. Vols voor Breuer&Intraval en Rijksuniversiteit Groningen 2022

121. Mismatch. Een verkennend fenomeenonderzoek naar het plegen van zedendelicten na contact via een datingsite of datingapp

J. Wolsink, J. Kuppens, N. Brouwer, H. Ferwerda, Bureau Beke, Arnhem 2023

122. Over een andere boeg. Lessen en uitdagingen in de integrale samenwerking tegen maritieme smokkel

M. Boelens, D. de Rijk, Y. Eski, Boelens Onderzoek & Advies/Vrije Universiteit Amsterdam, 2023

123. Nieuwe tijden. Bijdrage van het bedrijfsleven aan de publieke opsporing

E. Bervoets, J. Broekhuizen, K. van den Akker, m.m.v. Storm van Merkesteijn, Bureau Bervoets, 2024

124. De politieaanpak van sociale conflicten

I. van Duijneveldt, S. Nafie, M. van Tooren, A. Visser, Andersson Elffers Felix, 2024

125 Bloemen op de begraafplaats. De aanpak van een complottheorie in Bodegraven. En wat we daarvan kunnen leren

M. Eysink Smeets, H. Moors, L. de Veen, M. Koelink. Onderzoeksbureau EMMA en Onderzoeksbureau LEV, m.m.v. Hogeschool Inholland, gefinancierd door Onderzoeksprogramma Politie & Wetenschap, Politieacademie, 2025

126 Geklapt, gefilmd en gedeeld. Onderzoek naar hybride straatgeweld onder jongeren

S. Mehlbaum, K. van den Akker, J. Broekhuizen, A. Verweij, m.m.v. Marloes van Lochem, 2025

Ransomware wordt beschouwd als een van de voornaamste online dreigingen, maar er is weinig bekend over de prevalentie, aard en impact van slachtofferschap in Nederland. Bovenal is er meer inzicht nodig in hoe slachtoffers reageren, bijvoorbeeld als het gaat om onderhandelen, betalen en melden. Dit onderzoek biedt inzicht in slachtofferschap van ransomware onder Nederlandse burgers, zelfstandigen zonder personeel (zzp) en midden-klein bedrijven (mkb).

De onderzoeksvragen zijn beantwoord aan de hand van een vragenlijst onder slachtoffers (n=856 burgers, n=188 ondernemers), een vragenlijst met een fictief ransomwarescenario onder niet-slachtoffers (n=4,082 burgers, n=2,501 ondernemers) en interviews met experts (n=10).

Ongeveer 4,5% van de burgers en zzp'ers en 11,5% van de mkb'ers is ooit slachtoffer geworden van ransomware, wat bij een deel heeft geleid tot financiële of emotionele gevolgen. Slechts een enkele ondernemer onderhandelde na een aanval, hoewel niet-slachtoffers hier vaker toe bereid waren. De meeste respondenten betaalden het losgeld niet, mede ingegeven door een gebrek aan vertrouwen in herstel van toegang na betaling of ethische overwegingen. Factoren zoals de hoogte van de losgeldeis, het hebben van een back-up, de dreiging van het lekken van data en advies om te betalen, speelden tevens een rol in de beslissing om te betalen, hoewel er verschillen tussen groepen waren.

Ondanks dat de meerderheid van de niet-slachtoffers contact zou opnemen met de politie, deed slechts een klein deel van de daadwerkelijke slachtoffers dit. Velen zochten hulp bij een andere partij, zoals een cybersecuritybedrijf. Redenen om de politie niet te benaderen waren onder andere dat respondenten het probleem zelf of met behulp van een andere partij hebben opgelost en de overtuiging dat de politie er niets aan zou doen. Daarnaast was de meldingsbereidheid voor burgers gerelateerd aan de hoogte van de losgeldeis en het advies om te betalen.

Aan de hand van de uitkomsten biedt het onderzoek aanknopingspunten voor de aanpak van ransomware en de rol van de politie en andere publieke of private partijen hierin.

De reeks Politiekunde is een uitgave van het Onderzoeksprogramma Politie & Wetenschap. Publicaties in de reeks Politiekunde betreffen in het algemeen concrete handelingen, modellen, instrumenten of werkwijzen die direct bruikbaar zijn voor de politiepraktijk.

Meer informatie vind je op www.politieenwetenschap.nl.

ISBN 978-90-1241-0700

Sdu