De aanpak van cybercrime door regionale eenheden van de politie - Van intake van cybercrime naar opsporing en Vervolging (2020)

P. Boekhoorn
Politiekunde 102

Thema: 1.2 Cybercrime

Doelstelling

Het doel van deze verkennende studie is inzicht te krijgen in de organisatorische en inhoudelijke aanpak van cybercrime door drie politie-eenheden van de Nationale Politie. Daarbij is de focus gericht op de aanpak van de politie in het gehele proces van aangifte tot en met de opsporing van cybercrime, met bijzondere aandacht voor cyberteams.

Onderzoeksvragen:

De algemene vraagstelling naar de organisatorische en inhoudelijke aanpak van cybercrime door de regionale politie-eenheden is in de volgende deelvragen uiteengelegd:

- Op welke wijze is de aanpak van cybercrime bij de politie-eenheden georganiseerd
- en welke rol hebben cybercrimeteams hierin?
- Hoe verlopen de intake en screening van cybercrime bij de politie?
- Welke rol heeft een cybercrimeteam bij de opbouw en overdracht van deskundigheid
- inzake cybercrime binnen de politie-eenheid?
- Welke rol speelt informatie en analyse voor het cybercrimeteam bij de aanpak van
- cybercrime?
- Welke opbrengsten behalen de cyberteams naar aantal cybergerelateerde zaken en
- naar inhoudelijke aanpak/methodiek?
- Is er samenwerking bij deze aanpak met andere eenheden, landelijke eenheid
- (Team High Tech Crime) en externe partijen?

Methoden van onderzoek

- Literatuurstudie en documentenstudie
- Interviews

Samenvatting

Uit een politie evaluatie uit 2016 is gebleken dat de cybercrime aanpak ontoereikend was. Dit heeft geleid tot een intensivering van de aanpak die vanaf 2015 op regionaal niveau geleid heeft tot regionale ‘cybercrimeteams’. Deze teams vormen het uitgangspunt van dit verkennende onderzoek naar de organisatorische en inhoudelijke aanpak van cybercrime. Het onderzoek richt zich op de politie-eenheden Noord-Holland, Rotterdam en Oost Nederland. Naast een literatuur- en documentatie studie zijn er interviews uitgevoerd met een verscheidenheid aan politiemedewerkers in deze drie eenheden. Daarnaast zijn interviews uitgevoerd op landelijk niveau en ook bij het OM en andere samenwerkingspartners.

Bij de bestrijding van cybercrime onderscheidt de politie een aantal taken: preventie, verstoring, schadebeperking en opsporing. Het onderzoek wijst uit dat het aantal aangiften van cybercrime bij de politie in 2018 is toegenomen en er meer cybercrimezaken door de politie worden aangepakt en opgelost; al is het ophelderingspercentage niet hoger dan 8,3%. De teams bestaan uit tactische rechercheurs en variëren in grootte tussen de 5-25. In de aangiften bij de politie zijn enkele hoofdvormen van cybercrime te herkennen, zoals Tech Support Scam en hacken. Iemand die melding doet van cybercrime of gedigitaliseerde cybercrime (in de praktijk moeilijk van elkaar te scheiden) komt bij de politie als eerste in contact met een medewerker Intake & Service. Dit wordt als een knelpunt ervaren vanwege hun relatieve onbekendheid met cyberdelicten, ondanks de voorlichting die zij hebben gekregen. De kwaliteit van de aangifte is vaak laag waardoor belangrijke informatie in de aangifte ontbreekt. Dit leidt tot het niet in behandeling nemen van aangiften die reeds in de casescreening zitten.

De cyberteams registreren vooral ‘brengzaken’ en werken vooral aan veelvoorkomende cybercrime zaken waar men incidentgericht op reageert. Incidenteel worden ook grotere, complexere zaken gedraaid. Voor de cyberteams in de onderzochte eenheden geldt dat er een grote behoefte is om de specialistische digitale kennis binnen de generieke opsporing te versterken. Door de complexiteit van en tijdsbeslag aan één cyberzaak, waaraan men maanden bezig kan zijn, loopt een cyberteam het risico dat men het aantal afgesproken cyberzaken, niet haalt. De behoefte om meer cyberdeskundigheid op te bouwen met fenomeenonderzoeken botst met de noodzaak om de kwantitatieve doelen te behalen.

In de politie cyberbeelden is relatief weinig informatie opgenomen over mogelijke dadergroepen. Een aanzienlijk deel van het financieel gemotiveerde cybercrime wordt naar verwachting wel gepleegd door Nederlandse beroepscriminelen die niet alleen in het digitale domein actief zijn. Een belangrijk kenmerk van cybercrime is dat deze niet gebiedsgebonden is. Deze verkenning wijst uit dat desalniettemin slechts op incidentele basis sprake is van een operationele samenwerking tussen de cyberteams van politie-eenheden. Overdracht en samenwerking tussen de cyberteams is tot nu toe beperkt en de focus van de inzet van de cyberteams is vooral gericht op hun eigen werkgebied. Zaken die overgedragen worden aan het OM worden vaak afgedaan met een sepot omdat men daar bij voorbaat uitgaat van een kansloze vervolging omdat de dader niet kan worden aangehouden.

Het rapport wordt afgesloten met aanbevelingen.