Criminaliteit in de cyberwereld[1]

Marcel Spruit, lector informatiebeveiliging, Haagse Hogeschool.
Jos Groot, senior inspecteur, Inspectie Openbare Orde en Veiligheid.

Cyberwereld

De samenleving is in hoog tempo aan het digitaliseren. Een groot deel van de activiteiten vindt inmiddels plaats in de digitale wereld, oftewel de cyberwereld. We communiceren via digitale telefoon en e-mail, winkelen en bankieren op het internet, spelen op het internet en doen daar ook zaken.[2] Ook criminele activiteiten vinden voor een steeds groter deel plaats in de cyberwereld.[3] Niet alleen de zware criminelen, maar ook de zakkenrollers van voorheen, opereren op het internet. Soms voeren criminelen nieuwe activiteiten uit, bijvoorbeeld in een spelomgeving zoals World of Warcraft, en is het de vraag in hoeverre deze activiteiten strafbaar zijn. Meestal echter houden criminelen het in de cyberwereld bij de bestaande strafbare feiten en voegen hier een nieuwe modus operandi aan toe. Diefstal van creditcardgegevens en het vervolgens plunderen van bankrekeningen komt in de plaats van diefstal door zakkenrollen. Maar diefstal blijft diefstal.

De politie heeft de taak maatschappelijke onveiligheid te bestrijden, ook als dit het gevolg is van de inzet van digitale hulpmiddelen en zich daarmee geheel of gedeeltelijk in of via de cyberwereld afspeelt. De focus van de politie staat echter nog sterk gericht op de fysieke wereld. Er is dan ook een verandering in de politieorganisatie nodig om in te spelen op de veranderingen in de criminaliteit.

Cybercrime

Criminaliteit in of via de cyberwereld wordt aangeduid met de term cybercrime. Bij cybercrime worden digitale hulpmiddelen ingezet voor het plegen van criminaliteit. Enkele voorbeelden van toegepaste technieken zijn:

- Computervirus.
- Worm.
- Trojaans paard.
- Rootkit.
- Phishing.
- Spam.
- Port scanner.
- Botnet.

Het bijzondere van cybercrime is dat naast de lichte criminaliteit – bijvoorbeeld oplichting op Marktplaats.nl – en de zware criminaliteit – bijvoorbeeld kinderporno of botnetaanvallen op grote bedrijven – een nieuwe tussenvorm is ontstaan, namelijk de grootschalige lichte criminaliteit. Hierin worden veel slachtoffers ieder met een kleine schade opgezadeld. Voor de betrokken criminelen tellen de vele kleine bedragen op tot een grote winst en dus een gunstige business

---

[1] Gepubliceerd in “Van buiten leren”, Politie Haaglanden, Den Haag, 2011, pag. 41-47.

[2] A. Lööf en H. Seybert, “Internet usage in 2009 - Households and Individuals”, Eurostat, 46/2009; “Geldgids”, Consumentenbond, 2010.

[3] “Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010”, GOVCERT.NL, 2010; “Symantec Global Internet Security Threat Report, Trends for 2009”, M. Fossi e.a., Symantec, 2010.

case. De kleine schades bij de vele slachtoffers blijven voor de politie vaak ‘onder de radar’. In de praktijk betekent dit dat de zakkenroller op straat wordt aangepakt, terwijl de digitale zakkenroller ongestraft zijn gang kan gaan.

Cybercrime levert inmiddels een zeer grote maatschappelijke schade, alleen al voor Nederland geschat op meer dan een miljard euro per jaar.[4] Cybercrime is echter lastig aan te pakken. Dit heeft een aantal oorzaken:

- Cybercrime wordt veelal pas opgemerkt als het al gebeurd is.
- Er wordt vaak geen aangifte gedaan van cybercrime.
- Cybercrime wordt vaak niet als zodanig geregistreerd bij de politie.
- Het is internationaal, dus daders kunnen overal zitten, ook in het buitenland.
- Cybercrime maakt vaak gebruik van nieuwe en complexe technieken.
- De technieken kunnen snel aangepast worden om opsporing te bemoeilijken.

Het gevolg is dat de politie grote moeite heeft met het opsporen en pakken van cybercriminelen.

Aangifte

Van cybercrime wordt vaak geen aangifte gedaan. Dit heeft meerdere oorzaken. Zo hebben slachtoffers van lichte en grootschalige lichte cybercrime veelal niet de behoefte om aangifte te doen omdat de individuele schade klein is. Daarnaast kan gêne bij het slachtoffer aangifte in de weg staan. Zo denken veel mensen die door cybercrime getroffen zijn dat het aan hun eigen onkunde te wijten is. Bij bedrijven kan angst voor imagoschade de reden zijn om geen aangifte te doen. Zo koesteren banken hun imago van betrouwbaarheid en daarin passen geen cybercrime-incidenten.

Toch zijn er mensen en bedrijven die aangifte doen van cybercrime. Bij de politie wordt dit niet altijd adequaat opgenomen.[5] Er zijn gevallen gemeld waar de politie de aangever (onterecht) naar een andere instantie verwees, bijvoorbeeld in het geval van phishing werd doorverwezen naar de betreffende bank. De politie registreert aangiften van cybercrime veelal niet als zodanig. Hoewel dit in principe niet onterecht is, wordt het zo erg moeilijk om te herkennen wanneer het om grootschalige lichte cybercrime gaat. Dit herkennen wordt nog verder bemoeilijkt doordat de politie de informatie over aangiften in het algemeen niet met andere korpsen deelt.

Met de aangiften die gedaan worden, gebeurt vaak weinig. Er zijn dan ook steeds meer mensen die iemand kennen die getroffen is door cybercrime, terwijl er nauwelijks gevallen bekend zijn van cybercriminelen die opgepakt zijn. Daardoor ontstaat het beeld dat de politie niet in staat is cybercrime aan te pakken. Dit beeld wordt versterkt door berichten over ondeskundig opereren van de politie op dit terrein. Zo werd eind 2010 een kinderpornomaker opgepakt, maar pas nadat de Amerikaanse opsporingsinstanties de Nederlandse politie op het juiste spoor hadden gezet. En vervolgens blunderde de politie met het veiligstellen van het digitale bewijsmateriaal.[6] Een ander recent voorbeeld is het Bredolab-botnet dat door één Armeniër opgezet was en waar een omvangrijk politieteam, ondersteund door verscheidene andere partijen, aan te pas moest komen om het uit de lucht te halen.[7]

---

[4] “The cost of cyber crime”, Detica and The Office of Cyber Security and Information Assurance in the Cabinet Office, 2011;
“ICT Barometer over cybercrime”, Ernst & Young, 2011.

[5] S. Veenstra, M. Toutenhoofd en W.Stol, "Politie ontbeert kennis over cybercrime", Secondant 5, 2010.

[6] “Grootschalig onderzoek seksueel misbruik jonge kinderen”, Arrondissementsparket Amsterdam, 12 december 2010.

[7] “Bredolab-botnet is nooit opgerold”, Computable, 2 november 2010.

Binnen de politie wordt hier en daar geopperd dat er zo weinig aangiften van cybercrime zijn, dat de politie er dan ook maar weinig aandacht aan zou moeten besteden. Gezien de hiervoor genoemde oorzaken voor het kleine aantal aangiften van cybercrime, lijkt dat niet de juiste weg.

Organisatie

De politie ontplooit verscheidene initiatieven tegen cybercrime, zowel op landelijk niveau, als op korpsniveau. Op landelijk niveau is er het specifiek op cybercrime gerichte Team High Tech Crime. Bovendien loopt al enkele jaren het Programma Aanpak Cybercrime.[8] Op korpsniveau zijn er de Bureaus Digitale Expertise waar verscheidene initiatieven genomen worden om cybercrime beter aan te pakken.[9]

Toch is de politie nog niet in staat om voldoende in te spelen op cybercrime.[10] Dit zal ook niet gebeuren zolang de politie haar focus niet meer verschuift van de fysieke wereld van voorheen naar de geïntegreerde fysieke en digitale wereld van nu.

Om cybercrime adequaat aan te kunnen pakken, zijn er aanpassingen in de politieorganisatie nodig:

- Meer kennis van de cyberwereld en cybercrime. Veel politiemensen hebben hun focus nog gericht op de fysieke wereld, terwijl in de samenleving de fysieke en de digitale wereld al geïntegreerd zijn. Dit vergt binnen de politie meer kennis van digitale technieken, toepassingen en cybercrime.
- Meer capaciteit voor de aanpak van cybercrime. Door het beperkte aantal specialisten voor de aanpak van cybercrime, kan de politie zowel landelijk als op korpsniveau slechts weinig cybercrimezaken behandelen. Extra specialisten kunnen binnen de politie gezocht worden, maar kunnen ook van buiten de politie aangetrokken worden.
- Meer flexibiliteit van de politieorganisatie. Maatschappelijke veranderingen, en vooral veranderingen in de cyberwereld, volgen elkaar steeds sneller op. De politieorganisatie moet in staat zijn deze veranderingen bij te benen. Dat vraagt om een flexibele organisatie.

Leiderschap

De eisen die de aanpak van cybercrime aan de politie stellen, betekenen het een en ander voor de leidinggevenden:

- Zij moeten hun antenne meer op de cyberwereld en cybercrime richten en leren zich daarvan bewust te worden/zijn (‘van buiten leren’).
- Zij moeten leiding geven aan de noodzakelijke aanpassingen in de organisatie. Om te beginnen zal het aangifteproces moeten verbeteren. Maar ook het delen van kennis over cybercrime binnen en tussen de korpsen, het samenwerken met externe partijen en het snel inspelen op maatschappelijke veranderingen zullen moeten verbeteren.
- Zij moeten zorgen voor voldoende specialisten die uitvoering geven aan het aanpakken van hightech criminaliteit, maar daarnaast, waar dat nodig is, ook anderen in de politieprocessen kunnen ondersteunen om cybercrime te herkennen en aan te pakken.
- Zij moeten zorgen dat iedereen in de politieorganisatie over voldoende kennis beschikt. Dit betekent onder meer dat alle politiemensen iets over de cyberwereld en cybercrime

[8] H. Klap, “Programmaplan Programma Aanpak Cybercrime”, Programma Aanpak Cybercrime, 2008.

[9] R. Elderhorst, “Innovatieve ontwikkelingen en initiatieven BFO/DE”, Bureau Forensische Opsporing, 2011.

[10] “Aanpak cyberdreigingen”, Inspectie Openbare Orde en Veiligheid, 2011.

moeten weten. Niet iedereen hoeft daarin specialist te zijn, maar voldoende basiskennis is een vereiste.

- Zij moeten zelf ook beschikken over de minimale basiskennis over de cyberwereld en cybercrime. Enerzijds vanuit de voorbeeldfunctie en anderzijds omdat een groot deel van het politiewerk zich daar afspeelt, of af gaat spelen. Bovendien moeten leidinggevenden kunnen herkennen of politiemensen over voldoende kennis beschikken; ook bij de specialisten.

De leidinggevenden zijn verantwoordelijk voor het stellen van prioriteiten. Gezien de taak van de politie om maatschappelijke onveiligheid te bestrijden, hoort de aanpak van cybercrime daarbij. Het lijkt niet verstandig om voor het verbeteren van de aanpak van cybercrime te wachten tot de politiek ingrijpt en prioriteiten gaat stellen. Temeer daar de burger dan gesterkt wordt in de mening dat de politie niet in staat is om zelf cybercrime effectief aan te pakken.

Achtergrondinformatie

J. Makkink en L. van Nes, “Korpsstrategie op het gebied van Digitalisering”, Acestes, 2010.

“Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010”, GOVCERT.NL, 2010.

“ICT Barometer over cybercrime”, Ernst & Young, 2011.

“De Nationale Cyber Security Strategie”, verscheidene auteurs van verscheidene partijen, 2011.