

Wat maakt cybercriminaliteit anders?

Cybercriminaliteit neemt toe, net als de schade die dit aanricht. Begrijpen wat cybercriminaliteit is en welk marktfalen voor de bloei ervan zorgt, kan bestrijding effectiever maken. Een introductie.

BASTIAAN OVERVEST

Wetenschappelijk medewerker bij het Centraal Planbureau (CPB)

TATIANA KISELEVA

Wetenschappelijk medewerker bij het CPB

BAS STRAATHOF

Programmaleider bij het CPB

Het overgrote deel van de Nederlandse consumenten en bedrijven is aangesloten op internet en gebruikt direct en indirect een heel scala aan digitale diensten. Terwijl de samenleving steeds verder digitaliseert, verschuift de dreiging van het fysieke domein naar het cyberdomein (CPB, 2016). Bij cybercriminaliteit gebruikt de crimineel digitale methoden om 'klassieke' misdrijven als fraude en diefstal te plegen, of richt hij zich op digitale doelwitten zoals het verstoren van de ICT. Zie de voorbeelden onderaan deze pagina.

In de periode tussen 2004 en 2014 daalde het totale aantal klassieke misdrijven met zo'n dertig procent (De Waard, 2015). In diezelfde periode groeide de cybercrime echter. Zo is het aantal aangiftes van 'computervrederebreuk' (de strafrechtelijke term voor *hacken*) meer dan verdubbeld (CBS, 2015a). Inmiddels komt cybercriminaliteit vaak voor. In 2015 waren er 19 cybercrime-delicten per 100 inwoners, even veel als bij vermogensdelicten (CBS, 2015b). Een verschil met vermogensdelicten is dat slachtoffers van cybercrime nauwelijks aangifte doen – de aangiftebereidheid ligt een factor vier lager. Dit kan samenhangen met de lage verwachtingen wat betreft de opsporing door

de politie, maar ook met de beperktheid van de financiële schade. Lage aangiftepercentages kunnen cybercrime nog aantrekkelijker maken voor criminelen.

OVEREENKOMSTEN EN VERSCHILLEN

Cybercriminaliteit lijkt op een digitale versie van klassieke criminaliteit. Zo is de aard van het misdrijf vaak gelijk, bijvoorbeeld diefstal, afpersing of vernieling. En net als bij gewone criminaliteit kunnen hackers individueel te werk gaan of zich organiseren in een bende. Ook kunnen potentiële slachtoffers bij beide typen misdrijven maatregelen nemen om de kans te verkleinen dat ze het slachtoffer ervan worden of om, als dat dan toch gebeurt, de schade ervan te beperken.

Toch zijn er belangrijke verschillen die relevant zijn voor potentiële slachtoffers, opsporingsdiensten en beleidsmakers. Ten eerste zijn de schaalvoordelen bij cybercrime groter. De marginale kosten voor een 'fysieke' inbraak zijn redelijk constant, terwijl een effectief ransomware-programma zonder veel extra kosten opgeschaald en internationaal ingezet kan worden. Dit zorgt ervoor dat cybercrime in korte tijd een grote groep slachtoffers kan maken. Ook kan de individuele opbrengst van een misdrijf veel hoger zijn in het cyberdomein. De digitale bankovervallers van de Carbanak-bende bijvoorbeeld haalden in 2015 een buit binnen van tussen de 250 miljoen en 1 miljard euro (NCSC, 2015).

Ten tweede zijn criminelen in het cyberdomein moeilijker op te sporen. Redenen hiervoor zijn dat het eenvoudig is om anoniem te blijven op internet, dat cybercriminaliteit

DDoS-aanval

Een internet-intermediair en sites die daarvan afhankelijk zijn worden onbereikbaar als er te veel informatie opgevraagd wordt. Op 21 oktober 2016 gingen Amazon, Spotify en Twitter offline toen cybercriminelen met gehackte slecht beveiligde apparaten, zoals printers en beveiligingscamera's, deze sites overbelastten.

Centrale bankoverval

De banken digitaliseren – en de bankrovers digitaliseren mee. De centrale bank van Bangladesh werd in 2016 voor 81 miljoen dollar benadeeld. Waarschijnlijk was dit het werk van hackers die toegang hadden tot het SWIFT-systeem voor internationale interbancaire transacties.

Ransomware

Ziekenhuizen zijn kwetsbaar voor cybercriminelen die medische dossiers en IT versleutelen en pas weer toegankelijk maken voor het ziekenhuis nadat er losgeld betaald is. Ransomware-aanvallen overkwamen meerdere ziekenhuizen in het buitenland in 2016.

vaak grensoverschrijdend is – hacks vinden vaak vanuit het buitenland plaats – en dat slachtoffers van cybercrime soms pas na lange tijd doorhebben dat ze gehackt zijn. Cybercriminelen gebruiken vaak bitcoins voor hun onderlinge transacties en voor de betalingen die slachtoffers moeten doen (Europol, 2015). Hierbij maken zij gebruik van ‘bitcoinmixers’, een dienst waarbij bitcoins in een ‘grabbelton’ gegooid worden met het doel om transacties verder te anonimiseren. Daarnaast kunnen cybercriminelen goedkoop inkomsten uit criminele activiteiten witwassen: de kosten van witwassen zouden hierdoor zijn afgenomen met veertig tot vijftien cent per criminele euro (FD, 2017).

Ten derde is preventie problematischer bij cybercrime dan bij klassieke criminaliteit. Met de voortdurende digitalisering nemen ook de mogelijkheden voor hackers toe. Potentiële slachtoffers zijn zich vaak niet bewust van die nieuwe risico's, weten niet hoe groot het risico is of welke voorzorgsmaatregelen er genomen kunnen worden. Ook staat de verzekeringmarkt voor cyberrisico nog in de kinderschoenen. Voor verzekeraars lijkt dit geen aantrekkelijke niche vanwege het morele gevaar (*moral hazard*) – door het digitale karakter van cybercrime is het moeilijk te bewijzen dat er sprake was van een hack. Ook is de schade van cybercrime moeilijker te kwantificeren dan bij klassieke vermogensmisdriven.

MARKTFALEN

Helaas bestaat er geen simpele *patch* tegen cybercriminaliteit. Er is sprake van verschillende soorten marktfaalen en probleemgebieden die samen cybercrime mogelijk maken. Zie CPB (2016) voor een uitgebreide analyse. Een belangrijk gegeven in het cyberdomein is de verbondenheid van gebruikers. Via digitale netwerken (zoals internet of sociale media), maar ook via vitale processen (zoals de distributie van elektriciteit of het betalingsverkeer) heeft de beveiligingskeuze van de ene gebruiker gevolgen (externe effecten) voor andere gebruikers. Bijvoorbeeld, een onbeveiligde privé-computer kan deel uitmaken van een groep gehackte computers (botnet), die ingezet worden voor aanvallen op websites (een DDoS-aanval). De eigenaren van de besmette computers merken nauwelijks iets van de hack – laat staan dat ze aansprakelijk zijn voor de DDoS-aanval – en hebben hierdoor mogelijk te weinig oog voor cyberveiligheid.

Verder bevat software meestal programmeerfouten die ICT kwetsbaar maakt voor aanvallen. Vanwege asymmetrische informatie (intern bij de software-aanbieder en tussen de aanbieder en de afnemer) en onvolledige contracten is dit een hardnekkig fenomeen. Ook hebben gebruikers vaak maar een beperkt inzicht in de kwaliteit en noodzaak van

veiligheidsoplossingen. Een gevolg kan zijn dat gebruikers hun keuze baseren op de enige harde observeerbare variabele – de prijs.

OPGAVEN VOOR BELEID

Opsporingsdiensten zouden, net als cybercriminelen, de digitale schaalvoordelen beter kunnen benutten. Dit kan bijvoorbeeld door het vergroten van de online-aanwezigheid van de politie en het instellen van een digitaal aangifteloket. Ook kunnen opsporingsdiensten zich richten op het beperken van de schaalvoordelen van criminelen. Dit kan door toezicht of regulering van de digitale infrastructuur van criminelen (zoals bitcoinmixers, *bad hosting*-bedrijven of Tor-servers).

Ook is er aandacht nodig voor de achterliggende kwetsbaarheden. Hoe zou bijvoorbeeld aansprakelijkheid geregeld moeten zijn voor software en hardware? Wie is verantwoordelijk voor het ontdekken en mitigeren van een aanval? Welke beveiligingsvoorwaarden kan de overheid opleggen aan organisaties en burgers? En hoe moet zij dat doen? Waar ligt de verantwoordelijkheid voor het digitale systeemrisico bij de vitale processen?

LITERATUUR

CBS (2015a) *Tabellen criminaliteit en rechtshandhaving 2014*. Den Haag: Centraal Bureau voor de Statistiek.

CBS (2015b) *Veiligheidsmonitor 2015*. Den Haag: Centraal Bureau voor de Statistiek.

CPB (2016) *Risicorapportage cyberveiligheid economie*. Den Haag: Centraal Planbureau.

Europol (2015) *The internet organised crime threat assessment 2015*. Den Haag: Europol.

FD (2017) Bitcoin is reservemunt van de onderwereld geworden. *Het Financieel Dagblad*, 3 januari 2017.

NCSC (2015) *Cybersecuritybeeld Nederland CSBN 2015*. Den Haag: Nationaal Cyber Security Centrum.

Waard, J. de (2015) *Daling van (geregistreerde) criminaliteit: trends en mogelijke verklaringen*. Achtergronddocument. Den Haag: Ministerie van Veiligheid en Justitie.

In het kort

- ▶ De schaalvoordelen, innovatie en relatieve anonimiteit van digitale technieken maken ze tot aantrekkelijke instrumenten voor criminelen.
- ▶ Opsporingsdiensten moeten deze digitale technieken beter inzetten, en ook moet er aandacht komen voor wie er eigenlijk aansprakelijk is voor de kwetsbaarheden in software en hardware.

Gehackte e-mail

De afgelopen Amerikaanse verkiezingen werden verstoord door de publicatie van e-mails van presidentskandidaat Hillary Clinton die uit de e-mailbox van de Democratische campagneleider kwamen. Russische aanvallers hadden deze mailbox gehackt via een valse (phishing) e-mail.

Datalekken

Bescherming van digitale informatie is lastig, zo blijkt uit talloze datalekken. Bij de Autoriteit Persoonsgegevens werden vorig jaar 5500 datalekken gemeld. Yahoo! liet in december 2016 weten dat gegevens, zoals adressen en wachtwoorden, van meer dan 1 miljard gebruikers waren gelekt.

Spionage

‘Statelijke actoren’ zouden proberen het netwerk van Nederlandse bedrijven binnen te dringen om gevoelige gegevens, zoals intellectueel eigendom, te bemachtigen. ASML maakte twee jaar geleden bekend dat buitenstaanders toegang hadden tot een deel van hun IT-systemen.