Het lekken van geheimen in 'cyberspace'

J.H. Maat*

'ICT biedt kansen, maar verhoogt ook de kwetsbaarheid van een samenleving waarin steeds meer vitale producten en diensten met elkaar verweven zijn', zo wordt gesteld in de *Nationale Cyber Security Strategie* (Ministerie van Veiligheid en Justitie, 2011a, p. 2) die de minister van Veiligheid en Justitie op 22 februari 2011 presenteerde. Deze Nationale Cyber Security Strategie (NCSS) streeft naar meer digitale slagkracht door publiek-private samenwerking op het terrein van cyber security. 'Cyber security' wordt in de NCSS gedefinieerd als

> 'het vrij zijn van gevaar of schade veroorzaakt door verstoring of uitval van ICT of door misbruik van ICT. Het gevaar of de schade door misbruik, verstoring of uitval kan bestaan uit beperking van de beschikbaarheid en betrouwbaarheid van de ICT, schending van de vertrouwelijkheid van in ICT opgeslagen informatie of schade aan de integriteit van die informatie.' (Ministerie van Veiligheid en Justitie, 2011a, p. 3)

Sinds de presentatie van de NCSS zijn de Cyber Security Raad en het Nationaal Cyber Security Centrum opgericht, waarin publiek-private expertise op het terrein van cyber security gebundeld en verder ontwikkeld wordt. Ook verscheen in december 2011 het eerste Cybersecuritybeeld Nederland (CSBN). In dit lezenswaardige rapport wordt ingegaan op de kwetsbaarheden in de digitale samenleving en de dreigingen die uitgaan van vreemde mogendheden, private organisaties, 'hacktivisten', terroristen, beroepscriminelen en 'scriptkiddies'[1] (Ministerie van Veiligheid en Justitie, 2011b, p. 4).

* Mr. Johri Maat, MSSM is senior adviseur bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en gespecialiseerd in security science & management. Dit artikel is op persoonlijke titel geschreven.

1 Deze 'digitale vandalen' handelen vooral vanuit een baldadige motivatie en een behoefte aan een kick. Het zijn personen die met een minimum aan kennis, maar met enige interesse voor hacken en malware voor schade kunnen zorgen (Ministerie van Veiligheid en Justitie, 2011b, p. 16).

De nadruk ligt in het CSBN daarmee op *externe* dreigingsactoren met activiteiten als digitale (bedrijfs)spionage en sabotage, (identiteits)fraude, digitale verstoring en publicatie van vertrouwelijke gegevens. Minder tot geen aandacht is er in het CSBN voor *interne* dreigingsactoren (de 'eigen medewerkers') die zich – intentioneel of verwijtbaar – binnen organisaties schuldig maken aan de schending van de vertrouwelijkheid van in ICT opgeslagen informatie, oftewel het lekken van geheimen. Bij deze interne dreigingsactoren spelen echter voor een deel dezelfde kwetsbaarheden een rol als bij de externe dreigingsactoren.
Wanneer een geheim de media bereikt, leidt dit veelal tot de nodige ophef. Niet alleen vanwege nieuwsgierigheid naar de inhoud van het geheim, maar ook – met af en toe nauwelijks verholen leedvermaak – vanwege de soms (ogenschijnlijk) eenvoudige wijze waarop het geheim is uitgelekt. Dit soort incidenten leidt tot imagoschade voor de betrokken organisatie en heeft vaak een uitstralend effect naar de hele sector, vooal wanneer dit plaatsvindt binnen 'de overheid'. Terecht wordt in het CSBN opgemerkt dat dit over het geheel een beeld weergeeft van onvoldoende aandacht voor informatiebeveiliging en dat dit in sommige gevallen herkenbaar is, maar zeker niet algemeen van toepassing: organisaties die het wel goed doen en incidenten die niet plaatsvinden, halen nooit het nieuws (Ministerie van Veiligheid en Justitie, 2011b, p. 35). In dit artikel wordt met een focus op de overheid aandacht besteed aan het lekken van geheimen in relatie tot cybersecurity. Eerst zullen begrippen als geheimen en het lekken hiervan nader worden toegelicht. Vervolgens wordt mede aan de hand van de Wikileaks-affaire 'Cablegate' nader ingegaan op de bijzondere kwetsbaarheden die de ICT-ontwikkelingen van de afgelopen twee tot drie decennia met zich hebben meegebracht, waarna aandacht is voor te verwachten effecten van 'Het Nieuwe Werken'. Het artikel wordt afgesloten met een aantal aanbevelingen om de risico's rond geheimen in 'cyberspace' beter beheersbaar te maken.

Geheimen

Bij overheden wordt met heel veel informatie gewerkt. Hoewel overheidsinformatie in beginsel openbaar is (art. 8 lid 1 Wet openbaarheid van bestuur), is een deel van deze informatie zo

gevoelig dat onbevoegde kennisname kan leiden tot nadeel of zelfs schade aan belangen van overheden, burgers en bedrijven. Hierbij valt te denken aan – niet limitatief – de notulen en besluitenlijst van de ministerraad, een informantenregister van de Criminele Inlichtingendienst, informatie over internationale onderhandelingen, beveiligingsplannen van vitale objecten, diplomatieke stukken, informatie aangaande de veiligheid of slagkracht van de krijgsmacht, non-proliferatie, onderzoeken naar zware criminaliteit en financieel-economische informatie. Deze gevoelige informatie behoort wat bewerking, opslag, transport en vernietiging betreft adequaat te worden beveiligd en daartoe te worden gerubriceerd ('gelabeld') als 'geheime' informatie.[2] Er kunnen zowel formele geheimen als materiële geheimen worden onderscheiden. Als (al dan niet) gevoelige informatie correct is gerubriceerd (het staat er letterlijk op), kan men spreken van een 'formeel geheim'. Als gevoelige informatie niet correct is gerubriceerd (het staat er niet letterlijk op), maar de houder van de informatie begreep of had behoren te begrijpen dat de informatie gevoelig is en openbaarmaking een afbreukrisico vormt, dan kan men spreken van een 'materieel geheim'.

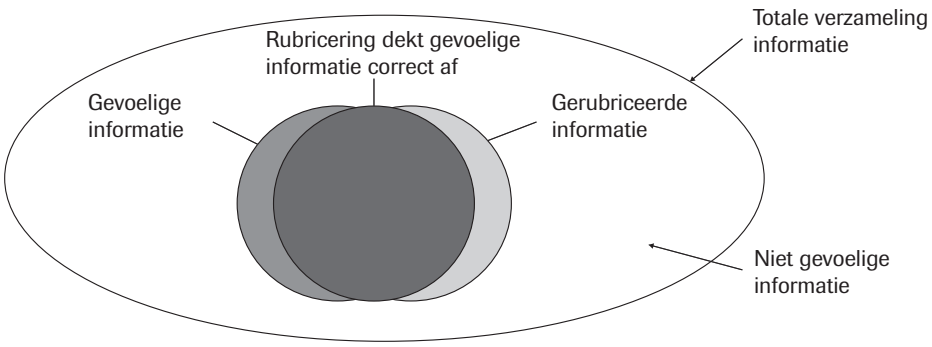
De bescherming van geheimen is geregeld in diverse wet- en regelgeving: het Europees Verdrag tot bescherming van de rechten van de mens en de fundamentele vrijheden (art. 10), het Wetboek van Strafrecht (art. 98, 98a, 98b, 98c, 272 en 463), de Ambtenarenwet (art. 125a lid 3), de Wet bescherming staatsgeheimen, de Wet op de Inlichtingen- en Veiligheidsdiensten (art. 85 en 86), de Wet openbaarheid van bestuur (art. 10 en 11), het Algemeen Rijksambtenarenreglement (art. 51), het Voorschrift informatiebeveiliging rijksdienst 2007 en het Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004.

Idealiter is de verzameling gerubriceerde informatie gelijk aan de verzameling gevoelige informatie. In de praktijk is dit niet volledig het geval, er is zowel informatie die ten onrechte is gerubriceerd, als

2 De Nederlandse rijksoverheid kent de volgende – oplopende – rubriceringen: Departementaal (Dep.) Vertrouwelijk, Staatsgeheim (Stg.) Confidentieel, Stg. Geheim en Stg. Zeer Geheim (art. 5 Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie 2004). Op de beveiligingseisen die voortvloeien uit de registratie van persoonsgegevens (zoals art. 13 Wet bescherming persoonsgegevens) wordt in deze bijdrage niet ingegaan.

informatie die ten onrechte niet is gerubriceerd. Dit laat zich goed illustreren aan de hand van het Eclips Model (figuur 1).

Figuur 1 Eclips Model



Exacte cijfers ontbreken, maar de schattingen van onjuist gerubriceerde informatie lopen uiteen van 50 tot 95% (Lemstra e.a., 2005, p. 26-27; Curtin, 2011, p. 20). Zowel het ten onrechte niet rubriceren als het ten onrechte wel rubriceren van informatie kan leiden tot het lekken van informatie.
Ten onrechte niet-gerubriceerde informatie zal in de regel niet de beveiliging krijgen die zij wel zou moeten hebben, waardoor deze informatie kwetsbaar is voor kennisname met schadelijke gevolgen. Onterecht of te hoog gerubriceerde informatie krijgt een zwaarder belang toegekend dan zij verdient, waarbij de indruk wordt gewekt dat men zo veel mogelijk geheim wil houden, waarmee deze informatie ook een bepaalde nieuwswaarde krijgt (Lemstra e.a., 2005, p. 26-27). Ten onrechte wel gerubriceerde informatie wordt zonder grond aan het publiek onthouden, waarbij zelfs sprake kan zijn van belemmering van geschiedschrijving en waarheidsvinding (Davids e.a., 2010, p. 429). Ten onrechte rubriceren kan ook leiden tot inflatie van de rubricering, waardoor men slordiger omgaat met dit soort informatie, ook als informatie nu juist wel terecht is gerubriceerd. Bovendien leidt onterecht rubriceren tot onnodige kosten en beperkingen in de bedrijfsvoering, waardoor er ook druk kan ontstaan om minder beveiligingsmaatregelen te hanteren, hetgeen de kwetsbaarheid vergroot (Maat, 2011c, p. 17).

Lekken

Bij lekken is er sprake van een 'interne' actor, iemand die (al dan niet bevoegd) houder is van of toegang heeft tot gevoelige of gerubriceerde informatie en die deze intentioneel of verwijtbaar naar buiten brengt. Er is dan sprake van compromittering.
Bij intentioneel lekken is in strafrechtelijke zin sprake van opzet. Dit kan gebeuren om persoonlijke redenen, zoals financieel gewin, het versterken van de eigen positie of het verkrijgen van aanzien. Daarnaast kan er sprake zijn van institutionele redenen, zoals het voortbestaan van de eigen organisatie, hiertoe behoort ook het zogenoemde 'geautoriseerde' lekken. Tot slot kan er sprake zijn van het dienen van publieke belangen, namelijk het melden van misstanden (Bovens e.a., 1993, p. 69).
Bij verwijtbaar lekken is in strafrechtelijke zin sprake van schuld, de actor heeft namelijk de (reële) mogelijkheid zich anders te gedragen. Hiervan is bijvoorbeeld sprake wanneer de actor geen gebruik maakt van de middelen die ter beschikking staan om geheimen te beschermen vanwege onder andere onachtzaamheid, onkunde of onprofessioneel handelen. Geheimen kunnen ook uitlekken door niet-verwijtbaar handelen (zoals overmacht), maar dat valt buiten het kader van dit artikel, net als compromittering door een externe actor zoals bij spionage.
Intentioneel lekken geschiedt door bewuste mondelinge, fysieke en digitale overdracht van geheime of gevoelige informatie. Variërend van het doormailen of het laten inzien van een stuk tot het voorlezen door de telefoon en een anonieme tas met stukken die aan de deur van bijvoorbeeld een journalist wordt gehangen.
Verwijtbaar lekken geschiedt bijvoorbeeld door het verlenen van ongeautoriseerde toegang (tot gebouwen of systemen), zich te verspreken of mee te laten lezen of luisteren (recepties, horeca, openbaar vervoer), het verliezen van documenten en onbeveiligde digitale gegevensdragers (USB-sticks), het verzenden van informatie via onbeveiligde kanalen (post, e-mail, fax), het verwerken van gerubriceerde informatie in ongerubriceerde documenten, het niet of onvoldoende beveiligd opbergen ('clean desk'-beleid) en het onjuist vernietigen van de gevoelige informatie (waardoor 'dumpster diving' – zoeken in afval naar bruikbare informatie – mogelijk is).

Lekken in 'cyberspace'

Lekken is dus op velerlei manieren mogelijk, zowel digitaal als 'analoog'. Hieronder zal echter verder worden ingezoomd op de relatie met 'cyberspace'. Dit kan heel goed aan de hand van een van de meest opmerkelijke lekaffaires van de afgelopen tijd: *Cablegate*. In november 2010 werd een grote hoeveelheid Amerikaanse diplomatieke berichten ('cables' genoemd) via onder meer Wikileaks – een activistische website die is opgezet om anoniem documenten over misstanden te 'droppen' – en kranten en weekbladen als *Le Monde*, *Der Spiegel*, *The Guardian* en *El Pais* wereldkundig gemaakt. Bradley Manning, een Amerikaanse militair in de rang van soldaat die als inlichtingenanalist in Irak gelegerd was, wordt ervan verdacht[3] – naast onder meer het laten uitlekken van een opname van een ernstig schietincident in Irak – ruim 250.000 van dit soort diplomatieke berichten gekopieerd te hebben van het 'Secret Internet Protocol Router Network' (SIPRNet) van het Amerikaanse ministerie van Defensie. SIPRNet geeft toegang tot een van de grootste databases ter wereld, met onder meer alle diplomatieke correspondentie van Amerikaanse ambassades in de belangrijkste steden ter wereld. SIPRNet was juist na de aanslagen van 11 september 2001 breder toegankelijk gemaakt om informatie beter te kunnen delen in de strijd tegen terrorisme. Hiertoe was de informatie toegankelijk voor meer dan drie miljoen functionarissen, bestaande uit militairen, analisten, inlichtingenofficieren en ook ingehuurde derden. Deze gevoelige informatie was voor deze grote groep van functionarissen niet alleen vrij toegankelijk te raadplegen, het was voor hen ook eenvoudig om informatie op een mobiele digitale gegevensdrager op te slaan. In een chatsessie op 22 mei 2010 met een voormalige hacker gaf Manning aan hoe eenvoudig dit was (de tekst is letterlijk overgenomen, inclusief spelfouten):

> 'funny thing is... we transfered so much data on unmarked CDs... (...) everyone did... videos... movies... music (...) all out in the open (...) bringing CDs too and from the networks was/is a common phenomeon (...) i would come in with music on a CD-RW (...) labelled with something like "Lady Gaga"... erase the

3 Ten tijde van het schrijven van dit artikel (december 2011) is de strafzaak tegen Bradley Manning net aangevangen. Er zijn echter voldoende feiten bekend om dit artikel aan de hand van deze casus te illustreren.

> music... then write a compressed split file (...) no-one suspected a thing (...) everyone just sat at their workstations... watching music videos / car chases / buildings exploding... and writing more stuff to CD/DVD... the culture fed opportunities (...) so... it was a massive data spillage... facilitated by numerous factors... both physically, technically, and culturally (...) perfect example of how not to do INFOSEC [Information Security; JHM] (...) listened and lip-synced to Lady Gaga's Telephone while exfiltratrating possibly the largest data spillage in american history (...) pretty simple, and unglamorous (...) weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis... a perfect storm.' (Manning, 2010).

Als motivatie gaf Manning aan dat hij misstanden openbaar wilde maken: 'i dont believe in good guys versus bad guys anymore... i only a plethora of states acting in self interest... with varying ethics and moral standards of course, but self-interest nonetheless (...) it belongs in the public domain' (Manning, 2010).
Door deze chatsessie raakte Manning ook in beeld als verdachte. De voormalige hacker met wie Manning de chatsessie had, heeft hier namelijk melding van gedaan bij de Amerikaanse autoriteiten.
Door het uitlekken van de informatie raakten de Verenigde Staten in grote verlegenheid. Niet alleen omdat de informatie onvoldoende beveiligd bleek te zijn, maar ook vanwege de inhoud van de informatie die ging over de Amerikaanse diplomatieke betrekkingen (Schoemaker, 2010; König, 2011, p. 7; Curtin, 2011, p. 20; Manning, 2010).[4]

Deze casus illustreert de drie problemen rond cyber security, namelijk de toename van het volume van digitaal en centraal opgeslagen geheime informatie, de toegang tot deze geheime informatie en de mobiliteit van deze geheime informatie.

Volume aan geheimen

Informatie wordt steeds meer digitaal opgeslagen. Het gaat hierbij zowel om 'nieuwe' informatie als 'oude' informatie die met

4 Interessant zijn ook de pogingen om Wikileaks plat te leggen, zowel digitaal als financieel, alsmede de tegenmaatregelen die vanuit Wikileaks en sympathisanten werden genomen (zie bijvoorbeeld Ministerie van Veiligheid en Justitie, 2011b, p. 18); dit valt echter buiten het kader van dit artikel.

terugwerkende kracht wordt gedigitaliseerd. Deze informatie wordt ook steeds meer centraal opgeslagen in datacenters, soms in eigen beheer, maar ook vaak uitbesteed aan derde partijen. Deze centrale opslag heeft voordelen ten aanzien van beheer en analyse. Door informatie te delen zou men bijvoorbeeld betere analyses moeten kunnen maken, voor dit laatste is SIPRNet zelfs opgezet. Maar hierdoor zitten er ook meer 'eieren in het mandje', een kwaadwillende heeft zo toegang tot meer geheime informatie en daarmee ook meer mogelijkheden om al deze informatie te lekken.

Toegang tot geheimen

Autorisatie van datasystemen blijkt vaak een probleem te zijn, dit speelde bijvoorbeeld ook bij de DigiNotar-affaire[5] een rol (Ministerie van Veiligheid en Justitie, 2011b, p. 23). Hierdoor kan men eenvoudig toegang krijgen tot geheime informatie. Vaak is er in het geheel geen sprake van differentiatie aan 'leesrechten', iedereen met een account kan overal bij. Dat was ook bij Cablegate het geval. Als deze differentiatie er wel is, dan komt het geregeld voor dat personen te veel leesrechten hebben. Soms omdat deze ten onrechte zijn toegekend en soms omdat bij functiewisseling deze leesrechten niet worden aangepast. Dit is overigens niet uniek voor de digitale opslag van informatie, menig kluis heeft een gebruikerscode die nooit wordt veranderd ondanks het verloop aan medewerkers, of erger: nog steeds de fabriekscode. Verder worden wachtwoorden onderling nog wel eens uitgewisseld, vaak met het oog op continuïteit bij ziekte of vakantie, maar ook uit gemakzucht of onwetendheid over de kwetsbaarheid die daardoor ontstaat.
Met het samenvoegen van dataverzamelingen groeit bijna automatisch ook de groep gebruikers die toegang heeft tot deze data. Hoe meer 'insiders' toegang hebben tot geheimen, des te groter de kans dat dit tot lekken leidt (Curtin, 2011, p. 7). Het SIPRNet was zonder restricties toegankelijk voor meer dan drie miljoen functionarissen. Sluitend toezicht op een dergelijke omvangrijke groep is welhaast onmogelijk, bovendien kan men vraagtekens zetten bij

5 DigiNotar was een bedrijf dat beveiligingscertificaten voor websites van veel overheden verzorgde. Nadat het bedrijf in juli 2011 was gehackt, konden kwaadwillenden valse beveiligingscertificaten in omloop brengen en zo internetters doorleiden naar malafide websites om bijvoorbeeld een betrouwbare website te imiteren, gebruikersnamen en wachtwoorden in handen te krijgen of kwaadaardige software te verspreiden.

het rubriceringsniveau van geheimen die zo breed bekend zijn. Niet voor niets geldt binnen het security-domein het adagium 'need to know' in plaats van 'nice to know'. De omvang van de kring van geïnformeerden van geheimen is geen exclusief Amerikaans probleem. In 2009 lekte bijvoorbeeld een ministerraadstuk uit rond het ontpolderen van de Zeeuwse Hedwigepolder, waardoor de spanningen in het toenmalige kabinet werden vergroot. Uit het onderzoek van de Rijksrecherche bleek dat deze informatie toegankelijk was voor minstens 235 personen. De Rijksrecherche constateerde in 2009 tevens dat het aanstaande rechtbankverzoek aangaande de noodregeling voor de DSB-bank bij meer dan 500 personen bekend was. Het uitlekken hiervan heeft het omvallen van deze bank in ieder geval versneld (Maat, 2011b, p. 49).

Mobiliteit van geheimen

Manning kon met enkele muisklikken ruim 250.000 documenten zonder beperkingen naar een cd branden, 'vermomd' als een zelfgebrande muziek-cd van Lady Gaga. Een dergelijk volume op papier zou heel wat minder makkelijk het veilige domein kunnen verlaten. Dit voorbeeld toont aan hoe de mobiliteit van informatie de afgelopen decennia enorm is toegenomen. Niet alleen door de toegenomen capaciteit van compacte gegevensdragers als cd's, dvd's en USB-sticks, maar ook door het gebruik van e-mail en internet. Het gemak waarmee men dankzij de technologische ontwikkelingen intentioneel kan lekken, blijkt uit de Cablegate-casus, maar ook als er geen intentie is om te lekken is het risico erg groot.
Bij het verzenden van een e-mailbericht bestaat bijvoorbeeld de kans dat men een verkeerde bijlage toevoegt of dat men een verkeerde geadresseerde selecteert. Als het bericht is verzonden, is er geen controle meer over, zeker niet als de bijlage niet is versleuteld. Eenmaal op internet geplaatste informatie laat zich niet of nauwelijks meer verwijderen. Dat bleek bijvoorbeeld tijdens Cablegate, waarbij men er niet in slaagde de 'Cables' van internet te krijgen door het internetdomein van Wikileaks te blokkeren of te hacken. De informatie werd gewoon op andere websites (zogenoemde 'mirrors') gezet. Maar zelfs als een organisatie zelf informatie op internet plaatst, is men de controle hierover al snel kwijt. Dat bleek bijvoorbeeld met de Prinsjesdagstukken in september 2011, waarbij een medewerker van een extern bedrijf, dat voor het ministerie van

Financiën werkzaamheden verricht, het bestand per abuis in een verkeerde directory had geplaatst, waardoor het direct raadpleegbaar was op internet. Door het aanpassen van het jaartal in het webadres (dit is nadrukkelijk géén hacken!) wist een internetter de tekst van de Miljoenennota te vinden, waarna deze dit via Twitter bekendmaakte.[6]
De snelheid van internet bleek ook toen een fotograaf op 8 april 2009 foto's maakte van een geheim stuk dat een commissaris van Scotland Yard onder zijn arm had bij het betreden van het kantoor van de Britse minister van Binnenlandse Zaken. De autoriteiten deden nog een D-notice de deur uit, die de media verbiedt te publiceren om redenen van staatsveiligheid, maar de foto was via internet al verspreid en buitenlandse media waren hier niet aan gebonden. Door dit uitlekken moest een antiterreuroperatie vervroegd worden uitgevoerd en de commissaris aftreden (Maat, 2011b, p. 48). Dat de alertheid na dit soort incidenten vaak maar van relatief korte duur is, bleek toen op 30 augustus 2011 een Britse minister op bijna dezelfde plaats exact dezelfde fout maakte, ditmaal met een gevoelig stuk over Afghanistan (Drury, 2011).
Bij al deze voorbeelden is er sprake van verwijtbaar lekken omdat men onvoorzichtig was, procedures niet juist zijn gevolgd of technische middelen niet zijn gebruikt.

Het Nieuwe Lekken

Centrale opslag van data, brede toegang tot data en de mobiliteit van de data zijn niet alleen de kenmerken van de Cablegate-casus, het zijn ook belangrijke elementen van 'Het Nieuwe Werken' (HNW), waarbij tijd- en plaatsonafhankelijk werken een centrale rol spelen. HNW biedt mensen en organisaties mogelijkheden om flexibeler om te gaan met arbeidstijd en werkomgeving. Hierbij staat onderling vertrouwen centraal, want er wordt gestuurd op resultaat en niet op aanwezigheid (Maat, 2011a, p. 22). Naast vele voordelen levert HNW ook informatiebeveiligingsproblemen op.

6 Minister-president aan de voorzitter van de Tweede Kamer der Staten-Generaal, 15 september 2011, referentie 3620297, geraadpleegd op www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2011/09/15/brief-minister-president-over-publiek-worden-miljoenennota.html, 17 september 2011.

Waar voorheen informatie veilig binnen het domein van de kantooromgeving bleef, wordt deze tegenwoordig steeds meer fysiek of digitaal mee naar buiten genomen. Dat kan met een mobiele digitale gegevensdrager als een USB-stick, laptop of tablet-pc zijn, maar ook door te mailen naar webdiensten als Hotmail, Gmail en clouddiensten, waarbij de data op externe – voor de gemiddelde gebruiker niet te traceren – servers worden opgeslagen. Een kwetsbaarheid waar ook het CSBN nader op ingaat (Ministerie van Veiligheid en Justitie, 2011b, p. 43).
Ook de vermenging van functies, waarbij zakelijke gevoelige of geheime informatie op privéapparatuur wordt geplaatst, werkt lekken in de hand. Deze apparatuur voldoet immers veelal niet aan de beveiligingseisen die de wet- en regelgeving verlangen – deze kwetsbaarheid wordt ook in het CSBN gesignaleerd (Ministerie van Veiligheid en Justitie, 2011b, p. 44) – en wordt bovendien vaak met derden (zoals huisgenoten) gedeeld. Vergelijkbaar zijn de risico's van privégebruik van zakelijke apparatuur waarbij derden de beschikking hebben over de wachtwoorden. Het is bijvoorbeeld meerdere keren voorgekomen dat geheime of gevoelige informatie uitlekte doordat deze op een computer stond waarmee de medewerker – of een van de kinderen – ook muziek via internet deelde. Door onjuiste instellingen zette men dan de gehele inhoud van de harde schijf open via internet in plaats van alleen de digitale muziekcollectie. Zelfs wanneer de computer is afgeschreven, kan de inhoud van de harde schijf tot lekken leiden. Diverse malen is het voorgekomen dat een afgedankte computer gevoelige informatie bevatte die niet of onjuist was gewist. Ook deze voorbeelden behoren tot verwijtbaar – want vermijdbaar – lekken.

Veilig faciliteren

De ontwikkelingen op het terrein van ICT en de alom aanwezigheid hiervan kunnen de indruk wekken dat ICT steeds toegankelijker, dus eenvoudiger is geworden. In werkelijkheid is de complexiteit – en daarmee de kans op fouten – juist enorm toegenomen. Het is dan ook zaak dat organisaties hierin meeontwikkelen, omdat medewerkers het anders zelf wel regelen, waarbij de organisaties de grip op het proces verliezen en de risico's op lekken – net als andere inbreuken op de informatiebeveiliging – onbeheersbaar worden.

Neem bijvoorbeeld 'cloud computing', waarbij door medewerkers gebruik kan worden gemaakt van software en dataopslag op externe servers zoals Google Docs. Hiermee raakt de organisatie de controle over de informatie kwijt, deze staat op servers van derden en valt waarschijnlijk zelfs onder een andere jurisdictie. Maar een organisatie kan ook een eigen 'cloud' creëren door bijvoorbeeld een 'virtual private network' (VPN) op te zetten waarop men inlogt en de werkzaamheden verricht. Hierdoor blijft de informatie onder controle van de organisatie en mocht de computer worden gestolen, dan staan er geen data op het apparaat zelf. Voor de acceptatie door de medewerkers is het dan wel van belang dat het minstens zo snel en prettig werkt als bijvoorbeeld Google Docs.
Een ander voorbeeld is het automatisch doorsturen van zakelijke e-mail naar privé-e-mailboxen zodat men e-mail ook thuis of op de privésmartphone kan ontvangen. Ook hierdoor kan gevoelige informatie buiten het domein van de organisatie raken. Door medewerkers een smartphone van het werk of webmailfaciliteiten aan te bieden is automatisch doorsturen naar externe e-mailadressen niet meer noodzakelijk en kan dit worden geblokkeerd. Maar dan moet de smartphone natuurlijk wel met een – niet makkelijk te raden – pincode worden vergrendeld en zal de medewerker extra zorgvuldig met inlognaam en wachtwoord om moeten gaan zodat een kwaadwillende niet via deze webmailfaciliteit in de digitale werkomgeving kan komen.
Beide voorbeelden zijn vormen waarbij veilig faciliteren van medewerkers mogelijk is, juist door gebruik te maken van de technologische ontwikkelingen, waardoor risico's gereduceerd kunnen worden. Maar men dient wel alert te blijven om te voorkomen dat de oplossing voor de ene kwetsbaarheid een andere kwetsbaarheid in het leven roept.
Naast dit soort technische factoren spelen ook organisatorische factoren een belangrijke rol, bijvoorbeeld door te investeren in bewustwording en werkbare procedures voor de medewerkers, zodat dezen op een verstandige wijze om kunnen gaan met de ruimte die ze krijgen in het uitvoeren van hun werkzaamheden. Hierbij hoort ook aandacht voor menselijke factoren als 'practical drift', waarbij de aandacht en discipline langzaamaan verslappen en risicovolle situaties ontstaan (Snook, 2000, p. 193), het sanctioneren van ongewenst gedrag en een goed werkende klokkenluidersregeling voor het intern en extern melden van vermoedens van misstanden. Lekken is

dan niet meer nodig als 'veilige' manier om een zaak aan te kaarten; Manning refereerde daar ook aan in zijn chatsessie. En door meer aandacht te besteden aan het rubriceringsproces zelf kan worden voorkomen dat informatie ten onrechte wel of niet wordt gerubriceerd. Bijvoorbeeld door het toepassen van een 'vier-ogen-principe', waarbij de rubricering op bepaalde informatie alleen kan plaatsvinden na akkoord van een collega of leidinggevende. Hierdoor hoeft alleen die informatie extra te worden beveiligd die dit verdient, waarmee onnodige uitgaven en beperkingen voor het werken met overige informatie kunnen worden voorkomen.

Besluit

Bradley Manning vatte zelf al samen waarom hij zo makkelijk kon lekken: 'weak servers, weak logging, weak physical security, weak counter-intelligence, inattentive signal analysis' (Manning, 2010). Daarom is het voor organisaties van belang dat er een goed ontworpen – met gelaagde en onafhankelijk van elkaar werkende maatregelen – en geïmplementeerd informatiebeveiligingsbeleid is. Op deze wijze kan men de reële risico's uit het hele spectrum – van interne en externe actoren, door intentioneel en verwijtbaar handelen – beter beheersbaar maken. Met een integrale aanpak wordt ook beter omgegaan met de schaarse middelen, de bestuurlijke aandacht en het beroep op bewustwording onder medewerkers. Maar bovenal is het van belang dat men – ook media en politiek – zich realiseert dat ondanks de mogelijkheden tot risicoreductie ook binnen het security-domein 'silver bullets' niet bestaan en het lekken van geheimen een terugkerend fenomeen zal blijven.

Literatuur

Bovens, M.A.P., H.G. Geveke e.a.
Strikt vertrouwelijk: lekken in het openbaar bestuur
Beleid en Maatschappij, nr. 2, 1993, p. 61-80

Curtin, D.M.
Top secret Europe
Amsterdam, Universiteit van Amsterdam, 2011

Davids, W.J.M., M.G.W. den Boer e.a.
Rapport Commissie van onderzoek besluitvorming Irak
Amsterdam, Boom, 2010

Drury, I.
Minister's blunder with memo outside No.10 reveals UK Government 'welcomes' Afghan president stepping down
Daily Mail, 31 augustus 2011 (geraadpleegd op www.dailymail.co.uk/news/article-2031780/Andrew-Mitchell-blunder-reveals-UK-welcomes-Afghan-president-stepping-down.html, 21 september 2011)

König, E.
In z'n nieuwe cel mag hij zelfs tv kijken
NRC Next, 21 april 2011, p. 7

Lemstra, W., E. Brouwers e.a.
Cultuur ondersteund door structuur: hét wapen tegen het lekken van vertrouwelijke informatie
Den Haag, Ministerie van Defensie, 2005

Maat, J.H.
Het Nieuwe Werken of De Nieuwe Kwetsbaarheid?
Security Management, januari/februari, 2011a, p. 32-34

Maat, J.H.
Verwijtbaar lekken = vermijdbaar lekken
Magazine nationale veiligheid en crisisbeheersing, augustus, 2011b, p. 48-49

Maat, J.H.
Rubriceren, een vak apart?
Security Management, oktober, 2011c, p. 16-18

Manning, B.
'This belongs in the public domain'
The Guardian, 1 december 2010 (geraadpleegd op www.guardian.co.uk/world/2010/dec/01/us-leaks-bradley-manning-logs, 2 januari 2012 (chatsessie))

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Voorschrift informatiebeveiliging rijksdienst – bijzondere informatie
Den Haag, 2004

Ministerie van Veiligheid en Justitie
Nationale Cyber Security Strategie: slagkracht door samenwerking (NCSS)
Den Haag, 2011a

Ministerie van Veiligheid en Justitie
Cybersecuritybeeld Nederland (CSBN)
Den Haag, 2011b

Schoemaker, R.
'Iedereen' heeft toegang tot 'geheim' netwerk
Webwereld, 29 november 2010 (geraadpleegd op http://webwereld.nl/nieuws/67940/-iedereen--heeft-toegang-tot--geheim--netwerk-vs.html, 10 maart 2011)

Snook, S.A.
Friendly fire. The accidental shootdown of U.S. black hawks over northern Iraq
Princeton (NJ), Princeton University Press, 2000

Summaries

The dynamics of cybercrime law in Europe and the Netherlands

B.J. Koops

Because of the special characteristics of the Internet, cybercrime inherently crosses national borders and has fewer natural barriers than classic cross-border crime. This triggers the question whether criminal law with its traditional national focus is able to combat cybercrime. Can legislatures respond to technological change with sufficient speed in an internationally aligned approach? This article tries to answer this question by mapping the dynamics of cybercrime law, focusing particularly on the interplay between European and Dutch legislative initiatives. It shows that the dynamics consist of a European framework of minimum standards on major issues, with much room for national legislatures to interpret the standards and to add initiatives of their own where the European framework remains silent. Although this has worked well so far, if cybercrime continues to transform into large-scale organised crime, a step-change in the dynamics towards more steering European approaches may be necessary.

Cybercrime and police; state of affairs in the Netherlands in 2012

W.Ph. Stol, E.R. Leukfeldt and H. Klap

In 2004 the main problem of the Dutch police concerning cybercrime was a lack of knowledge, for example about how to act in a digital world, about the character of cybercrime and about the effectiveness of measures. The main question in this article is if this situation has changed, and if so, how. Although the legislator has given the police special powers to fight crime in a digital world, the police still struggle with questions about what exactly are the powers they have. Although the police have invested in pilot projects and in the recruitment of digital experts, knowledge about 'policing a digital society' is not yet common in the police organisation – which is a shortcoming since 'digital is normal' in the lives of the common people. Although the police established digital aspects in police training, digital is not yet a common feature in police education. In sum, although the police in various ways pay attention

to digital aspects of policing, digital is not yet a regular part of the police organisation, police training and/or everyday police practice.

A safe cyberspace requires new thinking
R. Prins
This article describes the main security threats in cyberspace as well as the various types of actors behind these threats. The author discusses the reaction of existing and new state security agencies towards the new cyber threats. After analyzing the main obstacles in tracing cybercriminals he gives some recommendations for a more effective strategy against cybercrime.

Cyberwar? What war? More specific: what law?
A.R. Lodder and L.J.M. Boer
This article presents an overview of cyberwar from an international law perspective, in particular from the framework of the laws of war. It discusses some of the difficulties in applying these laws to cyber-attacks, further complicated by the characteristics of the Internet. A distinction is made between cyberwar, -crime, -espionage and -terrorism, and the different fields of law that apply to these distinct 'cyberevents'. Next to discussing several historic cyberattacks, the question is raised whether cyberwar is merely a hype or whether we should be taking this threat seriously. Rather than answering this question, the authors feel that the actual threat posed by 'cyber' is less important than the political and military prominence gained by this phenomenon in these past few years. The authors conclude by stating that a lot of work has yet to be done to address the issues raised by the occurrence of cyberwar.

The leaking of secrets in cyberspace
J.H. Maat
When it comes to cybersecurity usually little attention is payed to internal threats, i.e. from within organizations themselves which may – intentional or not – breach the confidentiality of digitally stored information. When a secret reaches the media, it often generates a lot of public attention. Not only because of the content or the curiosity-value of the secret itself, but also because of the – sometimes shockingly simple – way the secret has been leaked. This kind of security breach in particular gives rise to negative publicity, which not only impacts the organization which it concerns, but also

reflects badly on other peers in the sector, especially in the case of breaches that are government-related. In this article, the author explores the issues of the leaking of secrets in 'cyberspace' by using several examples – such as the WikiLeaks affair – to illustrate the effects of ICT developments in the last two to three decades on vulnerabilities in information security. The article then focuses on new developments in 'Alternative Workplace Strategies' and the related use of new technologies in relation to the vulnerabilities in information security. Organizations can reduce the threats by facilitating their employees with smart solutions which are also results of new technologies.

Sense and nonsense of a download-ban; actual developments and insights in digital piracy

H.B.M. Leeuw

In this contribution, the author explores some of the issues that are currently dominant in the debate revolving illegal downloading (also known as digital piracy). Four specific issues are addressed. Firstly, the legal status of downloading is discussed, followed by a brief analysis of a debate currently being held within the Dutch parliament dealing with this issue. Of particular interest is the proposed 'download-ban' which is intended to decrease digital piracy and increase legitimate sales. However, as will be demonstrated, this proposed ban is not without criticisms. Following this analysis, the question is raised what is actually empirically known about the impact of illegal downloading on the involved industries, and whether proposed measures such as a 'download-ban' can have the desired impact. Finally, the role of copyrights in the digital environment is explored.

Identity fraud and victimhood; a literature research into nature, size, risk factors and aftermath

J. van Wilsem

Identity fraud involves the theft of another person's identity information (e.g. bank account number and password), mostly for purposes of financial gain to the offender. The literature review summarizes main results from international and Dutch research with respect to the nature, size, risk factors and aftermath of identity fraud as well as the consequences for its victims. Though scientific research on these phenomena is taking place more and

more, much work yet remains to be done. This review ends with suggestions for future research on identity fraud.

Internet and fraud; a comparison between internet swindlers and classic swindlers

E.R. Leukfeldt and W.Ph. Stol

Based on different criminological theories in combination with the unique characteristics of the Internet, it is assumed that there are significant differences between cyber criminals and traditional criminals. This article compares the characteristics of fraudsters who use the Internet to execute their scams (e-fraudsters) and fraudsters who do not use the Internet (classic fraudsters). The personal characteristics, social economical background and criminal careers are compared. The main conclusion is that e-fraudsters are not 'new' criminals that only commit crimes because of the perceived benefits of the Internet. But the use of the Internet does make the perceived consequences of committing a fraud offense less severe, so offenders who use the Internet will commit fraud offenses earlier in life. Internet provides the opportunity for fraudsters to commit frauds at a younger age.

1 | 12

Justitiële verkenningen

Veiligheid in cyberspace

verschijnt 8 maal per jaar • jaargang 38 • maart

BOOM | LEMMA UITGEVERS

Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Veiligheid en Justitie

Inhoud

Voorwoord

Afgelopen maand gingen tienduizenden Europeanen de straat om te protesteren tegen het ACTA-verdrag, het Anti-Counterfeiting Trade Agreement dat een wereldwijde standaard moet zetten voor handhaving van intellectuele eigendomsrechten. De protesten zijn gericht tegen een onderdeel van het verdrag, de bestrijding van 'digitale piraterij': het gratis downloaden op internet van films en muziek waarop auteursrechten rusten. Nadat tal van ngo's zoals Bits of Freedom en Amnesty International zich al tegen het verdrag hadden gekeerd wegens de veronderstelde schending van burgerrechten, kregen ook politici zo hun bedenkingen. In navolging van enkele Oost-Europese landen trok Duitsland zijn steun voor het verdrag in, terwijl de Nederlandse Tweede Kamer zich in een motie keerde tegen ratificatie van het verdrag op dit moment. Eurocommissaris voor Justitie en Mensenrechten Viviane Reding verklaarde dat de bescherming van copyrights nooit een rechtvaardiging kan zijn voor de beperking van de vrijheid van meningsuiting of de vrijheid van informatie. Mensen afsluiten van internet wegens schending van auteursrechten is geen optie en zou nooit onderdeel mogen uitmaken van het EU-recht, aldus Reding. Zij wil dat het Europese Hof van Justitie een onderzoek instelt om na te gaan of het ACTA-verdrag fundamentele burgerrechten schendt.
De verwikkelingen rond het verdrag laten zien dat er een hevige strijd gaande is over welke regels gelden in cyberspace, ofwel op het internet. Naast de bescherming van commerciële belangen schuren ook maatregelen om een veilig internet te creëren vaak dicht aan tegen schending van de persoonlijke levenssfeer. En ruimere bevoegdheden voor politie en Justitie voor digitale opsporing – hoe gewenst ook – hebben vaak hetzelfde effect. Ook in het virtuele domein leidt het streven naar veiligheid tot een situatie waarin menig burger zich helemaal niet veilig voelt bij het idee dat al zijn communicatie en bewegingen op het internet kunnen worden nagetrokken.
De bovengenoemde actuele ontwikkelingen rond 'digitale piraterij' worden in een van de artikelen in dit themanummer nader geanalyseerd. Daarnaast is er aandacht voor cybercrimewetgeving, voor de vorderingen van de politie bij de bestrijding van cybercrime en voor fraude met identiteit en internettransacties. Het lekken van

geheimen in cyberspace komt eveneens aan bod, waarbij wordt teruggeblikt op de WikiLeaks-affaire. Voorts is er een artikel gewijd aan het fenomeen cyberwar.

In het openingsartikel van Koops staat de vraag centraal of het strafrecht met zijn traditionele nationale oriëntatie opgewassen is tegen allerlei snel veranderende vormen van cybercrime. De auteur gaat in op de dynamiek tussen Europese en nationale cybercrime-wetgeving, daarbij focussend op de Nederlandse initiatieven op dit terrein. De dynamiek bestaat hieruit dat de Europese regels minimumstandaarden hanteren voor de belangrijkste kwesties, waarbij veel ruimte is voor de lidstaten om de geformuleerde standaarden te interpreteren en zelf wetgeving te maken op punten waarover de Europese regels zwijgen. Tot nu toe heeft dit volgens de auteur goed gewerkt. Maar als cybercrime doorgaat zich te ontwikkelen tot grootschalige georganiseerde misdaad, zou het nodig kunnen zijn om de Europese kaders meer gewicht en sturing te geven.

Hoe de bestaande wetgeving inzake cybercrime door de Nederlandse politie wordt gehandhaafd, komt aan bod in de bijdrage van Stol, Leukfeldt en Klap. Zij stellen de vraag welke voortgang de politie in de afgelopen jaren heeft geboekt op dit terrein. Hoewel er is geïnvesteerd in proefprojecten, de rekrutering van digitale experts en de integratie van digitale aspecten in training en educatie, kan de politie nog nauwelijks bogen op concrete successen in de strijd tegen cybercrime. Bovendien heeft de politie soms moeite te bepalen welke bevoegdheden zij precies heeft bij de opsporing van cybercrime, zo wordt duidelijk uit het betoog.

Wat er gebeurt als de 'cybercops' er niet in slagen serieus tegenspel te bieden tegen criminele dreigingen op het internet, beschrijft Prins. Hij stelt dat particuliere cyberbewakers die leemte zullen vullen, vooral omdat er voor het bedrijfsleven grote belangen op het spel staan. Wijzend op situaties die zich al in de Verenigde Staten hebben voorgedaan waarschuwt de auteur dat deze particuliere bewakers de neiging hebben wettelijke voorschriften – bijvoorbeeld inzake privacy – nogal losjes te interpreteren. Net zoals de veiligheid op straat een primaire overheidstaak is, zo geldt dat ook voor de veiligheid op internet, zo meent hij. De auteur inventariseert de verschillende typen dreigingen evenals de actoren daarachter en bespreekt de reactie van overheden daarop. Na een analyse van de belangrijkste obstakels bij de opsporing van cybercriminelen doet

hij enkele aanbevelingen voor een meer effectieve overheidsstrategie tegen cybercrime.
Cyberwar is misschien wel de meest tot de verbeelding sprekende dreiging op internet, en is tegelijkertijd het meest omstreden. Volgens verschillende deskundigen is de cyberwardreiging niet meer dan een hype opgeklopt door commerciële webbeveiligers. Lodder en Boer gaan kort in op dit debat. Hoewel de actuele dreiging van cyberoorlog discutabel is, staat vast dat het onderwerp binnen de politiek, het leger en internationale bondgenootschappen zeer veel aandacht krijgt, zo stellen zij. De auteurs concentreren zich op de vraag of het internationaal recht, in het bijzonder het oorlogsrecht, is toegesneden op cyberwar. Zij onderscheiden daarbij cyberwar, -misdaad, -spionage en -terrorisme. Na een bespreking van verschillende historische cyberincidenten wordt nagegaan welke rechtsgebieden relevant zijn bij deze verschillende incidenten.
Bedreiging van cyberveiligheid komt echter niet alleen van buiten, zo stelt Maat in zijn artikel, maar ook van binnenuit organisaties. Door de digitalisering is informatie mobieler geworden dan ooit. Enorme hoeveelheden al dan niet gevoelige informatie kunnen op een simpele usb-stick worden meegenomen, terwijl interne netwerken van organisaties en bedrijven kwetsbaar blijken te zijn voor hackers. De auteur gaat in op verschillende gevallen van het lekken van geheimen in cyberspace, zoals de WikiLeaks-affaire, om de kwetsbaarheid van de huidige informatiemaatschappij te illustreren. Vervolgens bespreekt hij de ontwikkelingen rond 'Het Nieuwe Werken' en het daaraan gepaard gaande gebruik van nieuwe technologie. Met enkele voorbeelden laat de auteur zien hoe organisaties de cyberveiligheid kunnen vergroten door medewerkers slimme, technologisch geavanceerde oplossingen te bieden.
Vervolgens verleggen we de aandacht naar enkele vormen van cybercrime, te beginnen bij een webactiviteit die vooralsnog is toegestaan, maar de vraag is: hoelang nog? Het gratis downloaden van film en muziek waarop auteursrechten rusten zou volgens een recent wetsontwerp van de staatssecretaris van Veiligheid en Justitie Fred Teeven moeten worden verboden. Leeuw bespreekt de voors en tegens van een downloadverbod tegen de achtergrond van recente ontwikkelingen rond 'digitale piraterij'. Daarbij betrekt hij resultaten van empirisch onderzoek naar de gevolgen van illegaal

downloaden op de betrokken industrieën. Ten slotte gaat de auteur in op de rol van auteursrechten in een digitale omgeving.
Daarna is er aandacht voor identiteitsfraude en slachtofferschap. Van Wilsem bespreekt de belangrijkste resultaten van internationaal en Nederlands onderzoek naar dit fenomeen. Daarbij gaat hij in op de vraag hoe omvangrijk digitale id-fraude is, wat de risicofactoren zijn, de schade en de nasleep voor de slachtoffers. De auteur doet voorts enkele suggesties voor vervolgonderzoek.
Het laatste artikel van dit themanummer is gewijd aan fraude samenhangend met de verkoop van goederen en diensten via internet. Het is een vorm van fraude die als gevolg van de groei van websites als Marktplaats, flink is toegenomen in de afgelopen jaren. Leukfeldt en Stol stellen de vraag of er met internetfraude een nieuw type dader is opgestaan. Daartoe vergelijken zij internetfraudeurs met klassieke fraudeurs. De belangrijkste conclusie luidt dat de twee groepen, gelet op factoren als sociaaleconomische klasse, sociale binding, werkloosheid en dergelijke erg op elkaar lijken. Het enige verschil is dat internetfraudeurs gemiddeld jonger zijn.

Marit Scheepmaker