Centraal Planbureau

CPB Notitie | 3 juli 2017

Risicorapportage Cyberveiligheid Economie

Uitgevoerd op verzoek van het ministerie van Veiligheid en Justitie

Centraal Planbureau

CPB Notitie

Centraal Planbureau
Bezuidenhoutseweg 30
2594 AV Den Haag
Postbus 80510
2508 GM Den Haag

T 088 9846000
I www.cpb.nl

Contactpersoon
Bastiaan Overvest
Bas Straathof

Aan: Ministerie van VenJ

Datum: 3 juli 2017
Betreft: Risicorapportage Cyberveiligheid Economie

1 Inleiding

De samenleving digitaliseert. De vijf meest waardevolle bedrijven ter wereld zijn ict-bedrijven, Nederlanders maken volop gebruik van internet en ook de overheid zet steeds meer in op digitale middelen. Met de digitalisering neemt ook het economische belang van cyberveiligheid toe. Cyberveiligheid draagt bij aan het benutten van economische kansen en voorkomt schade door uitval of verstoring van ict. Uitval of verstoring kan per ongeluk gebeuren (bijvoorbeeld door softwarefouten) en opzettelijk (bijvoorbeeld door een cybercrimineel).

Het doel van de risicorapportage cyberveiligheid economie 2017 (rce 2017) is om meer inzicht te krijgen in het belang van cyberveiligheid voor de economie.[1] Centrale vragen zijn: Welke ontwikkelingen doen zich voor op het gebied van cyberveiligheid? En wat zijn daarvan de gevolgen of risico's voor de economie en samenleving? Waar mogelijk komen ook beleidsopties aan de orde.

De rce 2017 geeft een economische analyse van cyberveiligheid. Marktfalen en economische gevolgen staan hierbij centraal. Marktfalen kan leiden tot minder of juist meer cyberveiligheid dan maatschappelijk gezien optimaal is. Een gebrek aan veiligheid belemmert het gebruik van ict, maar maximale veiligheid is meestal ook niet optimaal: de kosten van volledige veiligheid wegen vaak niet op tegen de baten ervan voor de maatschappij. Een economische analyse geeft inzicht in (economische) risico's en mogelijke beleidsantwoorden.

[1] De risicorapportage is mede gefinancierd door het ministerie van Veiligheid en Justitie. Aan deze notitie is geschreven door Bastiaan Overvest, Bas Straathof, Rinske Windig, Anne Marieke Braam en Roel van Elk (allen CPB) en Tatiana Kiseleva (thans DNB). Michel van Leeuwen (NCTV/NCSC), Lucien Engelen (Radboud UMC), Marcel Heldoorn (Patiëntenfederatie Nederland), Dennis Broeders (WRR). Ronald van der Luit (EZ) en Paul Ducheine (Defensie) danken we voor hun suggesties en commentaar. De verantwoordelijkheid voor de rapportage ligt volledig bij het CPB.

Dit rapport begint met belangrijkste risico's en een terugblik op de afgelopen twaalf maanden. Hoofdstuk 2 bespreekt een aantal 'probleemgebieden', hoofdstuk 3 dreigingen en manifestaties en het laatste hoofdstuk zoomt in op gegevensstromen in de gezondheidszorg.[2] De probleemgebieden die aan bod komen zijn ict-afhankelijkheid van vitale processen (2.1), opsporing van cybercriminaliteit (2.2), softwarekwetsbaarheden (2.3), de markt voor cyberveiligheid (2.4) en encryptie en authenticatie (2.5). De besproken dreigingen en manifestaties zijn diefstal van bedrijfsgeheimen (3.1), phishing en malafide websites (3.2), datalekken (3.3) en ransomware (of 'gijzelsoftware') in paragraaf 3.4.

1.1 Hoofdpunten

De belangrijkste conclusies van deze rapportage zijn:

- Staatshackers (hackers in dienst van een land) richten zich ook in Nederland op politieke partijen en democratische instituties. Deze interventies zetten internationale economische relaties onder druk en schaden zo de economische belangen van Nederland als kleine open economie.
- Elf procent van de Nederlanders geeft aan slachtoffer te zijn geweest van cybercriminaliteit. Dit is een lichte daling ten opzichte van vorig jaar.
- Cybercriminelen ontlenen schaalvoordelen aan digitale infrastructuur (bijvoorbeeld voor anonieme communicatie of voor anonieme betalingen). Het internationale karakter van cybercriminaliteit beperkt de mogelijkheden van opsporingsdiensten om deze schaalvoordelen tegen te gaan. Hierdoor blijft de pakkans laag en blijven criminele activiteiten winstgevend. Snelle internationale samenwerking kan helpen om effectief op te treden.
- Inlichtingendiensten maken gebruik van softwarekwetsbaarheden ('zero-days'). Onrechtmatige publicatie van deze informatie leidt tot een plotseling onveiliger ict-omgeving voor gebruikers en maatschappelijke schade. Een afwegingskader en een reactieplan zijn beleidsopties die deze schade kunnen voorkomen of beperken. Een afwegingskader helpt bij de beoordeling of een zero-day gebruikt kan worden voor inlichtingendoeleinden of gemeld moet worden bij de aanbieder van de software. Gegeven dat de zero-day is gelekt beperkt een goed voorbereid reactieplan de maatschappelijke schade.
- Encryptie maakt het mogelijk om wereldwijd intellectueel eigendom, concurrentiegevoelige informatie en persoonsgegevens te beschermen. Verzwakking van encryptie via het inbouwen van 'achterdeurtjes' beperkt dit. Aan de andere kant maken achterdeurtjes het voor inlichtingendiensten eenvoudiger om grootschalig communicatie te analyseren.

[2] De overwegingen bij de keuze voor dit speciale onderwerp zijn het grote maatschappelijke belang van de gezondheidszorg en het feit dat in de zorg veel vertrouwelijke gegevens gegenereerd, gedeeld en gelekt worden. In de rce 2016 was het speciale onderwerp DDoS-aanvallen.

- Er is relatief weinig bekend over de omvang van schade door cybercriminaliteit. Dit kan ertoe leiden dat ict-gebruikers zich onvoldoende bewust zijn van de risico's. Meer informatie, bijvoorbeeld door statistisch onderzoek of meer openheid door bedrijven kan de bewustwording vergroten.
- Grote datalekken en andere cyberincidenten komen soms pas jaren later aan het licht. Reputatiemechanismen werken hierdoor niet optimaal, wat het belang van encryptie, preventief toezicht en beveiligingsstandaarden vergroot.
- Incidenten bij ziekenhuizen en gemeenten laten zien dat risico's op datalekken juist bij decentrale administratieve gegevensstromen liggen.
- Een verplichte publieke infrastructuur voor gegevensuitwisseling in de zorgsector kan naleving van normen makkelijker maken, voorkomt afhankelijkheid van een enkele private partij en kan burgers inzicht geven in wie toegang tot hun gegevens heeft. Onderzocht kan worden of deze voordelen opwegen tegen de risico's.

1.2 Terugblik 2016/2017

Wat waren de belangrijkste gebeurtenissen en ontwikkelingen op het gebied van cyberveiligheid? We beperken ons in deze paragraaf tot de periode tussen de publicatie van de vorige risicorapportage en 29 juni 2017.

Gebeurtenissen – internationaal

- Juni 2016. Diefstal interne correspondentie Democratische Partij in de Verenigde Staten door Russische hackers. Publicatie van 20.000 e-mails via WikiLeaks.
- Oktober 2016. Grote DDoS-aanval met botnet van Internet of Things-apparaten zoals beveiligingscamera's en smart-tv's.
- December 2016. Datalek een miljard accounts bij Yahoo! bekendgemaakt. Het lek vond plaats in 2013 en 2014.
- April 2017. Hackerscollectief 'The Shadow Brokers' publiceert geheime informatie van Amerikaanse NSA over hacktechnieken.
- Mei 2017. Grootschalige ransomware-campagne 'WannaCry' infecteert onder meer Telefónica in Spanje, fabrieken van Renault in Frankrijk en meerdere ziekenhuizen van de Britse NHS.
- Juni 2017. Tienduizenden bedrijven in meer dan zestig landen worden besmet met het 'Petya' (ook wel ExPetr) virus. De malware verwijdert gegevens op geïnfecteerde computers.

Beleidsontwikkelingen – internationaal

- Juli 2016. Richtlijn Beveiliging netwerk- en informatiesystemen (NIB) aangenomen door het Europees Parlement.
- November 2016. Verenigd Koninkrijk presenteert Nationale Cyber Security Strategy voor 2016 tot 2021.

Gebeurtenissen – nationaal

- Februari 2017. Mogelijk datalek ontdekt bij de Belastingdienst.
- Maart 2017. DDoS-aanvallen op Stemwijzer en Kieskompas.
- Maart 2017. Ransomware aangetroffen bij de Tweede Kamer.
- Mei 2017. Parkeergarages Q-Park besmet met ransomware WannaCry.
- Juni 2017. In Nederland worden onder meer TNT Express en APM Terminals geraakt door Petya.

Beleid – nationaal

- Juli 2016. Antigijzelsoftwareproject No More Ransom opgezet door politie.
- Oktober 2016. Adviesrapport van Herna Verhagen 'Digitaal droge voeten'.
- December 2016. Wet computercriminaliteit III aangenomen door Tweede Kamer.
- Februari 2017. Wet op de inlichtingen- en veiligheidsdiensten aangenomen door Tweede Kamer.
- Februari 2017. Oprichting Veilige E-mail Coalitie.
- Juni 2017. Wetsvoorstel Cybersecuritywet.

De risicorapportage van 2016 noemde een aantal risico's voor de cyberveiligheid en deed aanbevelingen voor beleidsmakers. Wat is daarmee gebeurd? Tabel 1.1 vat voor de belangrijkste risico's en beleidsopties de ontwikkelingen samen sinds de publicatie van de risicorapportage in juli 2016.

Tabel 1.1 Terugblik op hoofdpunten risicorapportage 2016

Hoofdpunt juli 2016	Terugblik
Financieel gedreven cybercriminaliteit neemt toe	Wereldwijde ransomware-aanval besmet honderdduizenden pc's in meer dan 150 landen.
Heroverweeg internationale afspraken over export cyberkennis	Exportrestricties voor informatiebeveiliging en computers zijn verhelderd of afgezwakt[3]
Productaansprakelijkheid om softwareveiligheid te verbeteren	Ministerie van EZ onderzoekt opties voor veiliger software. Cyber Security Raad publiceert uitleg juridisch kader.
Regels voor authenticatie- en encryptiestandaarden kunnen beter gehandhaafd worden	'Veilige E-mail Coalitie' van bedrijfsleven en overheid om standaarden in te voeren[4]
Omvangrijke datalekken en DDoS-aanvallen blijven waarschijnlijk	Meerdere grote datalekken en DDoS-aanvallen in de afgelopen periode
Geavanceerde aanvallen kunnen financiële sector bedreigen	Enkele nieuwe incidenten bij banken in het buitenland

[3] Zie de verklaring van de plenaire bijeenkomst van het Wassenaar Arrangement.
[4] Lees hier de intentieverklaring van de Coalitie.

2 Probleemgebieden

2.1 Ict-afhankelijkheid van vitale processen

Kern

- Staatshackers richten zich ook in Nederland op politieke partijen en democratische instituties.
- De dreiging voor de veiligheid van vitale processen komt vooral van staatshackers; dit kan ook internationale economische relaties onder druk zetten.
- Delen van informatie in internationaal verband is nodig om vitale organisaties te beschermen tegen cyberdreigingen. De NIB-richtlijn kan hier aan bijdragen.

Ontwikkelingen

Vitale processen zijn diensten die van essentieel belang zijn voor het functioneren van de maatschappij en waarvan uitval direct grote consequenties heeft.[5] Voorbeelden van vitale processen zijn de levering van elektriciteit of drinkwater en opslag van nucleair materiaal. Bedrijven en overheidsorganisaties die verantwoordelijk zijn voor vitale processen maken – net als iedereen – steeds meer gebruik van ict.

In het buitenland vonden verschillende incidenten plaats, waaronder de besmetting met ransomware van provider Telefónica en de Britse National Health Service[6], de hack van een grote Braziliaanse bank[7], verspreiding van malware via de Poolse financiële toezichthouder[8] en de uitval van Amazon Web Services.[9] Er zijn duidelijke aanwijzingen dat de Noord-Koreaanse overheid de hacks van het betalingssysteem SWIFT in begin 2016 heeft georganiseerd.[10]

Significante verstoringen van Nederlandse processen waren onder andere onderbrekingen van enkele uren bij overheidsdiensten DigiD en MijnOverheid.[11] Hierdoor kon niet worden ingelogd op overheidssites van de Belastingdienst en het UWV. Daarnaast heeft het NCSC in 2016 signalen ontvangen dat bedrijven uit vitale sectoren geconfronteerd werden met ransomware, DDoS-aanvallen en phishing, maar deze incidenten hebben niet tot ernstige verstoringen geleid.[12] 27 juni 2017 bleek dat het havenbedrijf APM Terminals getroffen was door het 'Petya' virus. Welke

[5] Zie deze toelichting van de NCTV over welke processen vitaal zijn.
[6] Zie bijvoorbeeld dit artikel in de New York Times.
[7] Cybercriminelen zouden toegang hebben gehad tot de websites, interne e-mail en servers. (bron)
[8] Meerdere Poolse banken zouden volgens dit artikel besmet zijn geraakt.
[9] Tijdens de storing waren verschillende apps, IoT-apparaten en websites als Github, Citrix en Expedia onbereikbaar. (bron)
[10] Bron: Group IB, 2017. (link)
[11] Zie bijvoorbeeld dit nieuwsbericht.
[12] Bron: NCSC (2016), Cybersecuritybeeld Nederland 2016 ('CSBN 2016'). (link)

gevolgen deze besmetting heeft voor de scheepvaartafwikkeling in Rotterdam is op het moment van schrijven nog onbekend.

Het afgelopen jaar is beïnvloeding van verkiezingen[13] door staatshackers een concreet en substantieel risico geworden. In de Verenigde Staten werden de verkiezingen van 2016 verstoord door de vermoedelijk Russische[14] hack van e-mails van de Democratische Partij en ook in Frankrijk werd in mei 2017 een grote hoeveelheid, deels gefingeerde, gehackte e-mails van de campagne van presidentskandidaat Emmanuel Macron online geplaatst. Naast hacks vormt ook manipulatie van verkiezingen met big data-technieken een risico.[15] Bovendien is de verspreiding van desinformatie ('nepnieuws') in het digitale domein eenvoudig.[16] Dit soort manipulatie kan van invloed zijn geweest op de Amerikaanse en Franse presidentsverkiezingen en het Brexit-referendum.[17]

In het democratische proces hebben zich in Nederland meerdere incidenten voorgedaan. Zo bleken in maart van 2017 computers van de Tweede Kamer besmet met ransomware[18], vonden DDoS-aanvallen plaats op de Stemwijzer en de Kieswijzer[19] en probeerden hackers toegang te krijgen tot informatie over het onderzoek naar de aanslag op vlucht MH17.[20] De AIVD (2017) bevestigt dat Rusland ook in Nederland de publieke opinie probeert te beïnvloeden en onderzoekt Russische activiteiten.[21] Deze beïnvloedingspogingen lijken in Nederland vooralsnog niet succesvol.[22]

Naast deze incidenten waren er zorgen over de betrouwbaarheid van de procedures voor de Tweede Kamerverkiezing. Hoewel stemcomputers vanwege het risico op manipulatie al sinds 2007 zijn vervangen door het potlood[23], wordt in de telprocedures nog steeds gebruik gemaakt van digitale middelen zoals usb-sticks en software. Deze bleken kwetsbaar te zijn voor beïnvloeding door cybercriminelen of staatshackers.[24] Om de risico's zoveel mogelijk te beperken heeft de overheid de

---

[13] Verkiezingen zijn geen vitaal proces volgens de strikte definitie van de NCTV, maar beïnvloeding van verkiezingen wel van grote invloed op langere termijn.
[14] Volgens dit rapport van drie Amerikaanse inlichtingendiensten gaf president Poetin opdracht om de Amerikaanse verkiezingen te beïnvloeden, waarschijnlijk met de bedoeling om Donald Trump te helpen.
[15] Zie dit achtergrondartikel in Scientific American.
[16] In een empirische analyse van nepnieuws op Amerikaanse sociale media laten Alcott en Gentzkow (2017) zien dat pro-Trump nepberichten 30 miljoen keer op Facebook gedeeld werden, tegen 8 miljoen keer voor pro-Clinton nepberichten. Zie Alcott, H. en M. Gentzkow, 2017, Social Media and Fake News in the 2016 Election, *Journal of Economic Perspectives*, vol. 31(2): 211-236.
[17] Zie de bijdrage van Rid Thomas aan de verhoren door de Amerikaanse senaat, dit artikel in The Guardian en dit artikel in de New York Times.
[18] Zie dit artikel in *de Volkskrant*.
[19] Zie dit artikel *in Financieel Dagblad*.
[20] Zie dit bericht van RTL Nieuws.
[21] Zie het jaarverslag van de AIVD (2017), p. 7.
[22] Zie dit artikel van CNBC.
[23] Er zijn overigens geen aanwijzingen dat stemcomputers daadwerkelijk gemanipuleerd zijn. Allers en Kooreman (2007) vinden voor de periode 1994 tot en met 2006 geen significante effecten van de stemcomputer op de opkomst en uitslag bij de verkiezingen voor gemeenteraden of de Tweede Kamer. Zie Allers, M. en P. Kooreman, 2007, Stemmachines beïnvloeden verkiezingsuitkomsten niet, *ESB*, 628-630.
[24] Zie het rapport 'Onderzoek OSV en proces' van Fox-IT (2017). (link)

procedures bij de verkiezingen aangepast.[25] Deze incidenten laten zien dat de afhankelijkheid van ict ook democratische processen kwetsbaar maakt.

Organisaties met vitale processen zijn nu nog niet verplicht om cyberincidenten te melden bij het NCSC. Volgens het wetsvoorstel voor de 'Cybersecuritywet' krijgen deze organisaties een meldplicht voor ict-inbreuken. Deze meldplicht vergroot waarschijnlijk het inzicht in cyberdreigingen voor de vitale infrastructuur. Cyberdreigingen voor het ene vitale proces kunnen zich ook voordoen bij het andere vitale proces en dit wetsvoorstel maakt het mogelijk dat veiligheids- en 'vitale' organisaties van elkaars ervaringen op het terrein van cyberveiligheid kunnen leren.

Om de digitale veiligheid van vitale processen binnen Europa te verbeteren heeft het Europees Parlement in juli 2016 de 'Netwerk- en Informatiebeveiliging (NIB-) richtlijn' aangenomen. Deze richtlijn verplicht lidstaten om internationaal kennis uit te wisselen en samen te werken. De 'Cybersecuritywet' moet de NIB-richtlijn in Nederland implementeren.

Risico's

Aanvallen van staatshackers vormen het grootste risico voor vitale processen. Voor 'gewone' cybercriminelen zijn vitale processen niet het meest aantrekkelijke doelwit, omdat vitale processen doorgaans sterker beveiligd zijn dan andere doelwitten. Dit geldt ook voor het politieke domein, waar het risico bestaat op digitale beïnvloeding van democratische instituties via hacken, het verspreiden van nepnieuws en gegevensdiefstal.

Een bijkomend risico van aanvallen door staatshackers is het risico op escalatie. Internationale economische betrekkingen kunnen verder onder druk komen te staan[26] en het slachtoffer van een cyberaanval kan een tegenaanval richten op het aanvalsland. De (pogingen tot) beïnvloeding van verkiezingen lijken gericht op het bevorderen van protectionisme waardoor concrete risico's ontstaan voor internationale samenwerkingsverbanden en verdragen waaronder de Europese Unie, NAFTA, NAVO en het Verdrag van Parijs. Dit is nadelig voor het functioneren van de open Nederlandse economie.

Een ander risico is dat informatie over geavanceerde aanvallen op vitale processen onvoldoende gedeeld wordt. Informatiedeling gebeurt al op nationaal niveau binnen de door het NCSC gefaciliteerde 'Information Sharing and Analysis Centres (ISAC's). Het voorstel voor de meldplicht in de 'Cybersecuritywet' draagt daar verder aan bij. Internationale samenwerking is nodig om aanvallen van staatshackers te voorkomen.

---

[25] Kamerbrief BZK van 3 maart 2017. (link)
[26] Zo wezen de Verenigde Staten eind 2016 35 Russische diplomaten in reactie op de bemoeienis van Rusland op de Amerikaanse presidentsverkiezingen en besloot de Europese Unie in februari van 2017 om de boycot van Russische producten te verlengen.

Hiervoor verplicht de Europese NIB-richtlijn de lidstaten om een samenwerkingsgroep op te richten waarin expertise en informatie gedeeld moeten worden.

2.2 Opsporing cybercriminaliteit

Kern

- Elf procent van de Nederlanders zegt slachtoffer te zijn geweest van cybercriminaliteit, een lichte daling ten opzichte van het voorgaande jaar.
- Cybercriminaliteit blijft winstgevend; technologische ontwikkelingen zoals het Internet of Things, cybercrime-as-a-service en bitcoinmixers bieden nieuwe doelwitten en verlagen de kosten voor criminelen; de pakkans blijft laag.
- Deze voortdurende innovatie door cybercriminelen bemoeilijkt opsporing. Ook blijft opsporing lastig door de lage aangiftebereidheid en het internationale karakter van cybercriminaliteit.
- Opsporing van cybercriminaliteit kan effectiever door toezicht op cybercrime-as-a-service diensten en meer internationale samenwerking.

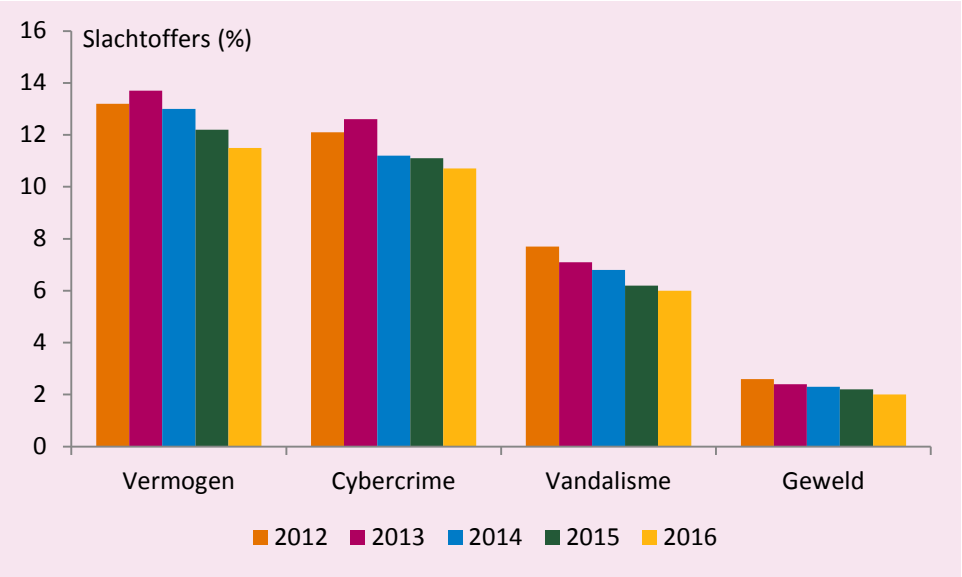
Ontwikkelingen

Cybercriminaliteit[27] is al lang geen zeldzaam verschijnsel meer. In Nederland komt het net zo vaak voor als vermogensdiefstal: volgens een steekproef vonden in 2016 achttien cyberdelicten plaats per honderd inwoners.[28]

Er zijn geen harde aanwijzingen dat de dreiging van cybercriminaliteit voor huishoudens of bedrijven toeneemt. Zo lijkt het aantal cyberdelicten zelfs te zijn gedaald in de afgelopen jaren (zie Figuur 2.1). In 2016 was 10,7 procent van de Nederlanders slachtoffer van een of meer cyberdelicten terwijl dit in 2015 op 11,1 procent lag. Bij andere delicten was de daling in het aantal slachtoffers groter, waardoor het aandeel van cybercrime toenam.

[27] Het onderwerp van deze paragraaf is cybercriminaliteit in brede zin. Specifieke vormen, zoals phishing en ransomware komen in het volgende hoofdstuk aan bod. De economische gevolgen van cybercriminaliteit komen daar ook aan de orde.
[28] CBS Veiligheidsmonitor 2016. Het CBS vraagt naar vijf vormen van cybercriminaliteit: identiteitsfraude, koop- en verkoopfraude, hacken en cyberpesten.

Figuur 2.1 Slachtofferschap cybercriminaliteit en andere delicten



Bron: CBS Veiligheidsmonitor.

In 2016 gaf 7,6 procent van de slachtoffers een cyberdelict aan bij de politie.[29] Bij traditionele delicten lag dit percentage op 24,7. In 2015 werden 2.180 politie-aangiftes van 'computervredebreuk' geregistreerd.[30] Het Openbaar Ministerie nam in dat jaar 124 cybercriminaliteitszaken in behandeling. Dit steeg[31] in 2016 naar 171 – een laag aantal gegeven dat elf procent van de bevolking aangeeft slachtoffer te zijn geweest.

Cybercriminaliteit kan direct kosten opleveren, zoals in het geval van (ver)koopfraude[32] of fraude met internetbankieren[33]. Ook kunnen de kosten indirect zijn, zoals investeringen van tijd en geld in veiligheidsoplossingen.

Nieuwe technologieën veranderen de aard van cybercriminaliteit. In het afgelopen jaar is bijvoorbeeld gebleken dat 'Internet of Things' (IoT) apparaten vaak slecht beveiligd zijn. In 2016 werden bijvoorbeeld naar schatting anderhalf miljoen IoT-apparaten besmet met Mirai-malware. Deze apparaten vormen een groot botnet waarmee ongekend grote DDoS-aanvallen uitgevoerd konden worden.[34] Ook de opkomst van smartphones biedt kansen voor criminelen: vanwege het kleinere scherm trappen mensen sneller in een phishing e-mail op een telefoon dan op een pc.

[29] Bron: CBS Veiligheidsmonitor 2016.
[30] Bron: CBS Tabellen criminaliteit en rechtshandhaving 2015.
[31] Bron: Jaarbericht Openbaar Ministerie 2016.
[32] De Fraudehelpdesk bijvoorbeeld ontving in 2015 hierover 3.625 meldingen. De gemiddelde kostenpost was ruim drieduizend euro.
[33] De Nederlandse Vereniging van Banken meldt dat in 2016 de fraude bij internetbankieren 822.000 euro bedroeg. Dit is een daling van 78 procent ten opzichte van 2015. (link)
[34] Zie bijvoorbeeld hier of hier.

Gebruikers van mobiele apps veronderstellen dat deze goed gecontroleerd zijn door het platform, maar toch bleken in 2016 honderden apps onveilig.[35]

Cybercriminelen kunnen verschillende schakels in het criminele 'productieproces' uitbesteden en zich verder specialiseren. Voorbeelden hiervan zijn de verhuur van botnets[36], distributie van ransomware[37] of platforms die helpen bij het witwassen van bitcoins.

Een andere technologische ontwikkeling is te zien bij blockchainmunten. Cybercriminelen gebruiken onderling bitcoins en ook het losgeld bij ransomware moet vaak in bitcoins voldaan worden.[38] Bitcoins zijn eenvoudig anoniem aan te kopen, maar het betalingsverkeer van de schuilnaam is traceerbaar. Deze onvolledige anonimiteit maakt het lastig om illegale winsten te verzilveren. Bitcoinmixers maken het gebruik van bitcoins een stuk anoniemer. Ze doorbreken de link tussen bitcointransacties en schuilnamen door gebruikers onderling bitcoins te laten ruilen, waardoor witwassen eenvoudiger wordt. Nieuwe alternatieven voor bitcoin zoals Ethereum proberen nog meer de privacy en anonimiteit te beschermen. Ethereum is momenteel na bitcoin de waardevolste blockchainmunt.[39]
De politie heeft in 2016 een aantal successen geboekt. Een voorbeeld is de oprichting van www.nomoreransom.org door het Team High Tech Crime van de Nationale Politie, Europol en cybersecuritybedrijven. Deze site helpt slachtoffers van ransomware met het ontsleutelen van hun gegevens. Een ander voorbeeld is het oprollen van een groot botnet, genaamd Avalanche, eind 2016 in een gecoördineerde politie-actie in tien verschillende landen.[40]

Eind december 2016 is het Wetsvoorstel computercriminaliteit 3 (WCC3) door de Tweede Kamer aangenomen. Deze wet geeft de politie bij verdenking van een ernstig misdrijf de mogelijkheid om heimelijk en op afstand onderzoek te doen in verdachte apparaten als pc's of servers, en gegevens ontoegankelijk te maken. Dit kan bijvoorbeeld wenselijk zijn als een server gebruikt wordt voor een DDoS-aanval of een ransomware-campagne. De wet beperkt zich in principe tot Nederland. Als het verdachte apparaat in het buitenland staat, blijft een rechtshulpverzoek nodig. Alleen bij een urgent probleem en onzekerheid over vanuit welk land de aanval plaatsvindt, mag de politie direct optreden.

Risico's

De winstgevendheid van cybercriminaliteit lijkt niet te dalen. Hierdoor blijft cybercriminaliteit een hardnekkig probleem voor opsporingsdiensten. Ict geeft

[35] Bron: Intel Security Mobile Threat Report 2016. (link)
[36] Zie bijvoorbeeld dit artikel over DDoS-as-a-service.
[37] Zie bijvoorbeeld dit artikel van Trend Micro.
[38] Bron: Europol (2016), p. 8.
[39] Bron: https://coinmarketcap.com/currencies/#EUR, bezocht op 6 april 2017.
[40] Zie bijvoorbeeld dit nieuwsbericht.

cybercriminelen voordelen die 'gewone' criminelen niet hebben.[41] Zo is het op internet eenvoudiger om anoniem te blijven dan op straat, is digitaal opschalen eenvoudiger en is het eenvoudiger om over landsgrenzen heen actief te zijn. Terwijl technische innovaties en ontwikkelingen steeds nieuwe mogelijkheden geven aan criminelen, missen opsporingsdiensten soms de expertise of de bevoegdheden om daarop in te spelen. Daarbij bemoeilijkt een verdere nationaliseringstrend (Brexit, Rusland) – via afnemend vertrouwen tussen opsporingsdiensten – het opsporen van internationale cybercriminaliteit.

Een ander risico is dat hackers IoT-apparatuur nog vaker besmetten met ransomware of botnetmalware, of de apparatuur zelfs uitschakelen. Uitschakeling van een IoT-apparaat kan tot economische vervolgschade leiden als civiele of industriële processen daar afhankelijk van zijn. Zo worden industriële robots veelvuldig zonder beveiliging op internet aangesloten.[42]

Beleidsopties

Voor het tegengaan van cybercriminaliteit is een efficiënte en internationale samenwerking van opsporingsdiensten belangrijk. Een te onderzoeken optie is dat landen elkaar toestaan om landsgrensoverschrijdend op te treden in het cyberdomein.[43] Dit kan in bilaterale convenanten of Europese regelgeving afgesproken worden. Net als de WCC3 nu al voorstelt, zou wetshandhaving moeten voldoen aan beschermende voorwaarden als een rechterlijke toetsing.

Daarnaast kan het toezicht op cybercrime-as-a-service versterkt worden. Diensten zoals bitcoinmixers en DDoS-as-a-service kunnen zowel voor legitieme als criminele doeleinden worden gebruikt.[44] Onderzocht kan worden hoe het criminele gebruik kan worden tegengegaan zonder legitiem gebruik onnodig in te perken.

2.3 Softwarekwetsbaarheden

Kern

- Kwetsbaarheden in IoT-apparaten ontstaan deels doordat aanbieders een afweging maken tussen veiligheid en gebruiksgemak.
- Inlichtingendiensten maken gebruik van onbekende softwarekwetsbaarheden, zogeheten 'zero-days. Wanneer deze vervolgens worden gepubliceerd door derden, kan dit leiden tot een plotseling onveiliger ict-omgeving voor gebruikers.

[41] Overvest e.a. (2017) bespreken de economie van cybercriminaliteit en niet-cybercriminaliteit. Zie Overvest, B.M., T. Kiseleva en S.M. Straathof, 2017, Wat maakt cybercriminaliteit anders?, *ESB*, 4746: 698-699.
[42] Zie deze studie door Trendmicro.
[43] De Verenigde Staten heeft unilateraal besloten om hacken van apparatuur in het buitenland voor opsporingsdiensten mogelijk te maken. Zie dit artikel.
[44] Een organisatie zou DDos-as-a-service kunnen gebruiken om de stabiliteit van de eigen website te controleren.

- Zorgplichten, beveiligingsstandaarden en een reactieplan voor inlichtingendiensten bij het lekken van zero-days kunnen de impact van softwarekwetsbaarheden verminderen.

Ontwikkelingen

Softwarekwetsbaarheden komen veel voor. Ook bij grote besturingssystemen als Windows van Microsoft en OSX van Apple worden jaarlijks tientallen kwetsbaarheden gevonden. Een technologische oorzaak is de toenemende complexiteit van software.[45] Bij complexere software is de kans op een fout waarschijnlijk groter en de kans op ontdekking (per fout) kleiner.

Een economische oorzaak is dat aanbieders en gebruikers een (soms impliciete) afweging maken tussen factoren als gebruiksgemak, prijs en veiligheid. Honderd procent veilige software is zelden de beste uitkomst van deze afweging. Het gaat mis als aanbieders en gebruikers de effecten op anderen niet meewegen of ongelijk geïnformeerd zijn over risico's.

IoT-apparaten zijn een voorbeeld van producten waar maatschappelijk gezien een onwenselijke afweging gemaakt wordt tussen gebruiksgemak en veiligheid. Bij dit type apparaten zijn gebruiksvriendelijkheid ('plug & play') en productontwikkelingssnelheid belangrijke voorwaarden voor commercieel succes. Dit kan ten koste gaan van veiligheid, bijvoorbeeld als apparaten communicatie tussen apparaten niet versleutelen of zwakke standaardwachtwoorden (zoals *admin* of *0000*) gebruiken.

Slecht beveiligde IoT-apparaten vormen vooral een risico omdat het veel apparaten betreft: het aantal IoT-apparaten wordt geschat op 15 miljard en naar verwachting groeit dit naar 200 miljard in 2020.[46] In 2016 werden tienduizenden IoT-apparaten besmet met Mirai-malware. Deze apparaten vormen een groot botnet waarmee ongekend grote DDoS-aanvallen uitgevoerd worden.[47] Ook kunnen slecht beveiligde apparaten van afstand uitgeschakeld[48] of besmet worden met ransomware.[49] Omdat industriële robots veelvuldig zonder beveiliging op het internet aangesloten worden, zijn ook productieprocessen kwetsbaar voor eenvoudige aanvallen.[50]

In de afgelopen maanden is duidelijk geworden dat inlichtingendiensten een grote voorraad onbekende softwarekwetsbaarheden (zero-days[51]) bezitten. In maart 2017

---

[45] Een maatstaf om softwarecomplexiteit in te schatten is het aantal regels code. In 1992 waren 2,5 miljoen regels voldoende voor Windows 3.1. Het Microsoft Office pakket beslaat nu ca. 44 miljoen regels.
[46] Bron: *A guide to Internet of things* van Intel (2016).
[47] Zie bijvoorbeeld dit bericht op Krebsonsecurity.
[48] Bron: dit artikel op tweakers.net over BrickerBot.
[49] Een voorbeeld is de besmetting van smart tv's, zoals hier beschreven wordt.
[50] Zie deze studie door Trendmicro.
[51] Een zero-day is een onbekende fout of zwakke plek in software waar nog geen oplossing voor bestaat. Zero-days kunnen gebruikt worden om bijvoorbeeld malware te installeren of gegevens te onderscheppen.

publiceerde WikiLeaks documenten waaruit blijkt dat de CIA zero-days heeft voor onder andere auto's, smarttelevisies, browsers en besturingssystemen. Het hackerscollectief 'The Shadow Brokers' publiceerde vanaf augustus 2016 zero-days van de Amerikaanse NSA voor onder andere Windows. Met de kennis over de zero-days zouden hackers binnen een week al duizenden pc's hebben geïnfiltreerd.[52] In mei 2017 bleek de ransomware 'WannaCry' gebaseerd op een gelekte NSA-zero-day. Ook het 'Petya' virus dat eind juni wereldwijd computers besmette lijkt hier (mede) gebruik van te maken. De kwetsbaarheid was weliswaar hersteld door Microsoft, maar veel gebruikers hadden de 'patch' nog niet geïnstalleerd.

Risico's

Slecht beveiligde IoT-apparaten kunnen gemakkelijk gehackt worden. Dit levert financiële en operationele risico's op voor de eigenaren van deze apparaten, vervolgschade voor partijen die afhankelijk zijn van de IoT-apparaten en overlast voor slachtoffers van aanvallen van IoT-botnets.

Bij het ontwikkelen en aanhouden van zero-days door inlichtingendiensten bestaat het risico dat deze onbedoeld plotseling en op grote schaal in het publieke domein komen. Softwareleveranciers moeten dan op korte termijn veel patches ontwikkelen en gebruikers moeten snel de software op hun apparaten bijwerken. Omdat deze processen tijd vergen, zullen na een zero-day-lek grote groepen gebruikers geruime tijd met onveilige software werken.

Beleidsopties

Er zijn verschillende opties om software en andere ict-producten beter te beveiligen. Een betere benutting van bestaande regels kan al helpen.[53] Nu ondersteunen aanbieders de software maar voor een beperkte periode, bijvoorbeeld twee jaar, ook al is de levensduur van het apparaat veel langer. Aanbieders kunnen vooraf aangeven hoe lang het apparaat minimaal ondersteund wordt. Een andere optie is het stellen van beveiligingsstandaarden voor bepaalde producten. Van IoT-apparaten kan bijvoorbeeld vereist worden dat gebruikers zelf een wachtwoord instellen.[54]

Om de impact van het lekken van softwarekwetsbaarheden te beperken, kan worden gedacht aan een verplichting voor inlichtingendiensten om een reactieplan op te stellen. Met dit plan – vergelijkbaar met de 'living wills' of afwikkelplannen van banken – zijn inlichtingendiensten voorbereid op een onbedoelde publicatie van zero-days. Een reactieplan zou een beschrijving van de softwarekwetsbaarheid moeten bevatten, alle beschikbare informatie over herstelmogelijkheden en een protocol dat beschrijft wie wanneer geïnformeerd wordt. Of een inlichtingendienst een adequaat reactieplan heeft opgesteld en uitgevoerd kan achteraf vastgesteld

[52] Bron: The Register. (link)
[53] Zie dit overzicht van het juridisch kader over zorgplichten op het gebied van cyberveiligheid.
[54] De Europese Commissie onderzoekt momenteel de noodzaak en mogelijkheden om via het aansprakelijkheidsrecht de veiligheid van software te verbeteren. Zie bijvoorbeeld hier.

worden. Naast een reactieplan kunnen inlichtingendiensten een afwegingskader gebruiken om bij een nieuwe zero-day in te schatten of deze gemeld moet worden bij de software-aanbieder of gebruikt kan worden voor de werkzaamheden van de inlichtingendiensten.

2.4 Markt voor cyberveiligheid

Kern

- Organisaties besteden de beveiliging van ict en vertrouwelijke gegevens steeds vaker uit aan gespecialiseerde bedrijven.
- De Nederlandse markt voor cyberverzekeringen is nog klein.
- Overheid, bedrijven en huishoudens kunnen de noodzaak en kwaliteit van cyberveiligheidsproducten moeilijk vaststellen, waardoor zij zich niet altijd optimaal beschermen.
- Een 'bug bounty'-programma kan de cyberveiligheid van de digitale overheid verbeteren.

Ontwikkelingen

Op de 'markt voor cyberveiligheid' wordt cyberveiligheidsexpertise door uiteenlopende bedrijven aangeboden. Er is een breed scala aan cyberveiligheidsproducten en -diensten. Denk hierbij aan bijvoorbeeld beveiligingsadviezen, antivirussoftware, identificatiesystemen en hacktesten (of 'pentesting'). Bedrijven laten de beveiliging van ict en bescherming van data steeds meer over aan externe leveranciers. Zo is het gebruik van betaalde clouddiensten door bedrijven tussen 2014 en 2016 gestegen van 28 naar 35 procent.[55] Het uitbesteden van cyberveiligheid aan vertrouwde aanbieders kan een oplossing zijn voor gebrek aan ict-kennis bij bedrijven.

Een relatief nieuwe dienst op de markt voor cyberveiligheid is een cyberverzekering. Met een cyberverzekering worden risico's op schade door cyberincidenten gedekt. Specifiek kan het hierbij gaan om aansprakelijkheid bij schade, kosten voor herstel, opgelegde boetes door toezichthouders en kosten door ransomware. Deze markt is nog klein, maar groeit snel.[56] Naar schatting van het Verbond van Verzekeraars heeft de Nederlandse markt voor cyberverzekeringen een premievolume van 10 miljoen euro. Ter vergelijking: in 2015 bedroeg de premieomzet voor aansprakelijkheid 1 miljard euro en voor rechtsbijstand 700 miljoen euro.

Het is nog onduidelijk hoe de markt voor cyberverzekeringen zich verder zal ontwikkelen. Een mogelijke oorzaak van de beperkte omvang van de huidige markt is dat de schade van cyberincidenten moeilijk te kwantificeren is. Een andere mogelijke

[55] CBS Cybersecuritymonitor 2017.
[56] Volgens dit bericht in het FD zal de premie-omzet meer dan verdubbelen tussen 2017 en 2020.

oorzaak is dat bedrijven door een gebrek aan betrouwbare informatie zich onvoldoende bewust zijn van de kans en impact van cyberincidenten.

Cyberverzekeringen kunnen dekking bieden voor het losgeld bij ransomware of voor de boete van de Autoriteit Persoonsgegevens.[57] Dergelijke dekkingen zijn maatschappelijk gezien onwenselijk; het maakt van ransomware een winstgevender crimineel verdienmodel en kan de afschrikwekkende werking van een boete tegengaan.

Risico's

Een risico voor de markt voor cyberveiligheid is dat onzekerheid blijft bestaan over de noodzaak en kwaliteit van de marktoplossingen. Hierdoor lopen bedrijven onnodige financiële risico's of geven juist teveel geld uit aan schijnoplossingen. Dit probleem wordt veroorzaakt door asymmetrische informatie: gebruikers hebben meestal minder goed zicht op de effectiviteit van beveiligingsoplossingen. Op hun beurt hebben veiligheidsaanbieders soms een prikkel om dreigingen te overdrijven.

Ook bij de overheid bestaat het risico op een onvoldoende veilige benutting van ict. De Rijksoverheid heeft zich als doel gesteld om alle burgers en bedrijven vanaf 1 januari 2018 digitaal van dienst te zijn (de 'Digitale Overheid'). Deze ambitie impliceert dat overheidsorganisaties een groot aantal diensten moeten digitaliseren. Dit zal gepaard moeten gaan met een grote publieke vraag naar cyberveiligheidsdiensten. Publieke opdrachtgevers hebben echter vaak beperkte kennis van ict en cyberveiligheid, kampen met een gebrekkige besluitvormingsstructuur of geven kleinere aanbieders te weinig kansen door onnodig strikte toelatingseisen bij aanbestedingen.[58] Hierdoor worden technologische mogelijkheden niet altijd goed en veilig benut. Dit vormt een risico voor de veiligheid van digitale overheidsdiensten.

Beleidsopties

Om de onzekerheid over nut en noodzaak van cyberveiligheid te verminderen is meer en vooral betrouwbare informatie nodig. Het CBS doet in 2017 onderzoek naar cyberveiligheid bij Nederlandse bedrijven en kan zo onzekerheid verminderen. Een tweede mogelijke oplossing is een certificeringssysteem. De Europese Commissie zal in september 2017 hiervoor maatregelen voorstellen.[59] Een derde optie is een publiek cyber-expertisecentrum voor het mkb. Het is echter nog onzeker of het mkb 'te veel' risico loopt en of oneerlijke concurrentie ontstaat voor private cyberveiligheidsbedrijven.

---

[57] Zie bijvoorbeeld deze beschrijving van een cyberverzekering die dekking biedt voor losgeld en opgelegde boetes.
[58] Bron: rapport van de Tijdelijke Commissie ICT (2015).
[59] Zie http://ec.europa.eu/newsroom/document.cfm?doc_id=44527.

Een mogelijkheid om de veiligheid van digitale overheidsdiensten beter te borgen, is de invoering een financiële prikkel ('bug bounty') voor het melden van kwetsbaarheden bij de Rijksoverheid. Hierbij hoort ook een 'responsible disclosure policy' zodat vooraf duidelijk is hoe de overheid omgaat met meldingen. De overheid stimuleert (ethische) hackers zo om kwetsbaarheden in digitale diensten te rapporteren. Dit vergroot de kans dat kwetsbaarheden tijdig hersteld kunnen worden.

2.5 Encryptie en authenticatie

Kern

- Encryptie en authenticatie worden steeds eenvoudiger en het gebruik ervan neemt toe.
- Het politiek draagvlak voor 'achterdeurtjes' neemt toe.
- Encryptie versterkt privacy en helpt bedrijven om wereldwijd intellectueel eigendom, concurrentiegevoelige informatie en persoonsgegevens te beschermen. Aan de andere kant maken achterdeurtjes het voor inlichtingendiensten eenvoudiger om grootschalig communicatie te analyseren.
- Nederland heeft een kabinetsstandpunt over encryptie en is daarmee internationaal een voorloper.

Ontwikkelingen

Encryptie en authenticatie zijn technieken die het risico op phishing, hacks en datalekken kunnen beperken. Encryptie (of versleuteling) is een middel om toegang tot informatie te beperken tot personen met de juiste codes. Voorbeelden van encryptietechnieken zijn bijvoorbeeld het 'Pretty Good Privacy' (PGP) programma[60], het 'Transport Layer Security' (TLS) protocol[61] of het Signal Protocol[62]. Authenticatietechnieken helpen bij de identificatie van personen of machines. Voorbeelden van authenticatietechnieken zijn de combinatie van een gebruikersnaam en een wachtwoord, de vingerafdruk of de 'tokens' die sommige banken gebruiken.

Encryptie wordt eenvoudiger om te gebruiken doordat communicatieplatformen (semi-)automatisch informatie versleutelen. Encryptie-aanbieders innoveren ook, bijvoorbeeld met programma's die automatisch gevoelige informatie versleutelen zodra die verzonden wordt.[63] Wereldwijd rapporteert Google een sterke stijging van

[60] PGP was de versleutelingstechniek van telefoons die tot 2016 veel door criminelen gebruikt werden. In 2016 heeft de Nederlandse politie een server in beslag genomen met daarop versleutelde communicatie (bron) en in maart van dit jaar heeft de politie de berichten weten te kraken (bron).
[61] TLS is een beveiligingsprotocol waarmee e-mails worden versleuteld. Zowel de afzender als de ontvanger moet TLS gebruiken om een beveiligde verbinding te maken.
[62] Dit is het protocol waar onder andere WhatsApp gebruik van maakt om chats te beveiligen.
[63] Zie bijvoorbeeld deze gebruikerservaring.

de adoptie van TLS. In ruim drieënhalf jaar groeide dit van 27 procent eind 2013 naar 84 procent in maart 2017.

De overheid onderzoekt nieuwe alternatieven voor het bestaande DigiD. Momenteel loopt een proef met Idensys. Dit is een methode om veilig en eenvoudig, bijvoorbeeld via een app of selfie, in te loggen. De overheid experimenteert ook met iDIN, een nieuwe dienst waarmee burgers zich via de bestaande authenticatie-methoden van hun bank kunnen identificeren. Ook investeert de overheid een half miljoen euro in sterke encryptie.[64]

Door twee factoren staat de betrouwbaarheid van encryptie en authenticatie onder druk. Ten eerste komen regelmatig kwetsbaarheden van bestaande technieken aan het licht. Zo blijkt nu dat tweefactor-autorisatie op basis van sms relatief gemakkelijk te omzeilen is[65], zijn versleutelde PGP-berichten gekraakt[66] en lijkt ook de versleuteling van WhatsApp niet altijd en overal gegarandeerd.[67]

Ten tweede oefenen inlichtingendiensten en politici soms druk uit op aanbieders om encryptie te verzwakken. Zo zou Yahoo op verzoek van de Amerikaanse overheid sinds 2015 e-mails doorzoeken voor inlichtingendiensten.[68] In de nasleep van de aanslag in maart 2017 bij het Engelse Lagerhuis werd gepleit voor verzwakking van encryptie van communicatietoepassingen zoals WhatsApp.[69] En in de Verenigde Staten dienden twee senatoren een wetsvoorstel in dat voorziet in achterdeurtjes.[70]

Risico's

Het verzwakken van encryptie vergroot de mogelijkheden voor inlichtingendiensten om grootschalig communicatie te analyseren, maar brengt risico's met zich mee. Ten eerste is het een technologische uitdaging om de toegang tot 'achterdeurtjes' te beperken tot een selecte groep inlichtingendiensten. Als de technische mogelijkheid bestaat om versleutelde communicatie of bestanden te kraken dan zullen anderen die kennis ook proberen te bemachtigen. Ten tweede kan een inperking van encryptie het vertrouwen in online diensten of transacties schaden. Dit kan op den duur leiden tot veranderingen in het gedrag van mensen en bedrijven. Beperkingen op encryptie kunnen bijvoorbeeld het risico op diefstal van intellectueel eigendom vergroten. Een mogelijk gevolg hiervan is dat bedrijven minder geneigd zijn om te innoveren.

Beperkingen op encryptie in niet-EU-landen, daarentegen, bieden kansen voor aanbieders van cloud- of communicatiediensten op de Interne Markt. Europese

---

[64] Zie dit bericht.
[65] Lees bijvoorbeeld dit achtergrondstuk in Wired.
[66] Zie hier.
[67] Volgens dit artikel zou het gaan om de webversie van WhatsApp.
[68] Zie bijvoorbeeld dit artikel van Reuters en dit bericht op nu.nl.
[69] Zie bijvoorbeeld dit nieuwsbericht.
[70] Zie hier het persbericht van senator Richard Burr.

aanbieders kunnen dan namelijk meer bescherming bieden dan concurrenten uit niet-EU-landen.

Beleidsoptie

Sterke encryptie draagt bij aan cyberveiligheid, en aan privacy en bescherming van bedrijfsgegevens in het bijzonder. Nederland heeft een kabinetsstandpunt[71] over encryptie dat erop neer komt dat beperkingen ten aanzien van encryptie onwenselijk zijn. Dit draagt bij aan de hiervoor genoemde doelen.

3 Dreigingen en manifestaties

3.1 Diefstal bedrijfsgeheimen

Kern

- Er is weinig bekend over incidenten waarbij bedrijfsgeheimen gestolen worden, waardoor bedrijven zich mogelijk onvoldoende bewust zijn van de mogelijkheid van diefstal.
- Het risico van diefstal van bedrijfsgeheimen verkleint de prikkel om te investeren in onderzoek en ontwikkeling.
- Bedrijven kunnen digitale (encryptie, authenticatie) en niet-digitale middelen (zoals octrooien of screening van werknemers) inzetten om kennis te beschermen.
- Bedrijven zouden meer openheid kunnen geven over incidenten, bijvoorbeeld door in het jaarverslag daarover te rapporteren.

Ontwikkelingen

Diefstal van technologische kennis is een oud fenomeen. In 552 na Christus smokkelden twee Byzantijnse monniken een paar zijderupsen uit China, om zo het Chinese zijdemonopolie te breken. In onze tijd wordt diefstal van bedrijfsgeheimen gezien als een van de grotere kostenposten van cyberonveiligheid voor bedrijven. Zo waarschuwt Verhagen (2016) voor cyberdreigingen die gericht zijn op intellectueel kapitaal. Deloitte (2016) schat de economische kosten voor Nederland van diefstal van intellectueel eigendom en strategische informatie op 2,5 miljard euro per jaar.[72]

Over diefstal van bedrijfsgeheimen in het cyberdomein bestaat veel onzekerheid. Hoewel digitale diefstal van bedrijfsvertrouwelijke informatie als een belangrijk risico wordt gezien, zijn er weinig incidenten publiekelijk bekend. Eén voorbeeld is het bedrijf ASML, dat in zijn jaarverslag van 2015 melding maakt van aanvallen door

[71] De Kamerbrief over encryptie is hier te vinden.
[72] Zie H. Verhagen, 2016, Nederland digitaal droge voeten en Deloitte, 2016, Cyber Value at Risk in the Netherlands.

hackers. Volgens ASML hadden de aanvallen geen impact op de bedrijfsvoering.[73] Een ander voorbeeld is het Nederlands-Duitse bedrijf Rheinmetall Defence. Chinese hackers zouden vanaf 2012 toegang hebben gehad tot technologische informatie van het bedrijf.[74]

Het is opmerkelijk dat zo weinig incidenten aan het licht komen, aangezien bedrijven volgens inlichtingendiensten vaak het doelwit zijn van aanvallen. Beursgenoteerde bedrijven zijn bovendien wettelijk verplicht om koersgevoelige informatie zo snel mogelijk publiek te maken. Als commercieel gevoelige informatie van grote Nederlandse bedrijven regelmatig gestolen wordt, zou je daar dus ook regelmatig persberichten over verwachten.

Een mogelijke verklaring voor het uitblijven van dergelijke berichten is dat bedrijven wel aangevallen worden, maar dat hackers er nauwelijks in slagen om koersgevoelige informatie te stelen. Een tweede verklaring is dat incidenten vanwege veiligheidsredenen of andere overwegingen geheim gehouden worden – ook al staat dat op gespannen voet met de meldingsplicht uit de Wet financieel toezicht. Een derde verklaring, die minder waarschijnlijk lijkt, is dat hacks nauwelijks plaatsvinden bij Nederlandse beursgenoteerde bedrijven.

Risico's

Het risico op diefstal van bedrijfsgeheimen kan nadelige gevolgen hebben voor de economie.[75] Zo kan dit de prikkel voor bedrijven om te investeren in r&d of marktonderzoek verminderen. Het risico op diefstal en gebruik van nieuwe kennis door concurrenten vermindert immers de verwachte opbrengsten van deze investeringen.[76]

Om te voorkomen dat een bedrijf wordt beconcurreerd met de resultaten van haar eigen bedrijfsgeheimen, is een goede bescherming van intellectueel eigendom noodzakelijk. Door de beperkte berichtgeving over diefstal van bedrijfsgeheimen, zijn bedrijven zich mogelijk onvoldoende bewust van de risico's. Hierdoor investeren zij mogelijk te weinig in de (digitale) bescherming van hun intellectueel eigendom.

Het risico op diefstal lijkt vooral groot wanneer sprake is van handelsbelemmeringen tussen landen. De landen die nu geassocieerd worden met digitale spionage (China, Rusland, Noord-Korea) zijn ook landen waarvoor handelsbeperkingen gelden. Dit is

---

[73] Zie bijvoorbeeld dit bericht op Tweakers.
[74] Lees bijvoorbeeld dit nieuwsbericht van *de Volkskrant*.
[75] Friedman et al. bieden een economische analyse van bedrijfsgeheimen en laten zien waarom bedrijven soms goede redenen hebben om geen formeel intellectueel eigendom (octrooi) aan te vragen. Zie Friedman, D., W. Landes en R. Posner, 1991, Some Economics of Trade Secret Law, *Journal of Economic Perspectives*, vol. 5(1): 61-72.
[76] Empirisch onderzoek van Aghion et al. (2015) over de Europese Interne Markt laat zien dat sterkere bescherming van intellectueel eigendom leidt tot meer innovatie in competitieve sectoren. Zie Aghion, P., P. Howitt en S. Prantl, 2015, Patent rights, product market reforms, and innovation, *Journal of Economic Growth*, vol. 20(3): 223-262.

geen nieuw fenomeen: tijdens de Koude Oorlog gold er een handelsembargo. Glitz en Myersson (2017) laten op basis van Stasi-archieven en industriële data zien dat Oost-Duitse spionnen werkten bij West-Duitse bedrijven.[77] Ze laten zien dat door de spionage de productiviteitsverschillen tussen beide landen sterk afnamen, met name voor sectoren met de hoogste handelsbarrières.

Beleidsopties

Bedrijven kunnen cruciale informatie beter beschermen, bijvoorbeeld door gebruik van encryptie en authenticatie-technieken of screening van werknemers.

Behalve extra geheimhouding kan een bedrijf in bepaalde gevallen ook een octrooi aanvragen. Zolang de juridische bescherming van een octrooi adequaat is, beschermt een octrooi een bedrijf op een indirecte manier tegen diefstal door concurrenten. Als inbreuken op Europese octrooien in China (en vice versa) nauwelijks aangepakt kunnen worden, dan tast dat internationale verdienmogelijkheden aan en lokt het diefstal van technologische kennis uit. Naleving van internationale afspraken over het respecteren van elkaars intellectueel eigendom voorkomt dat.[78]

Ten slotte kan transparantie door bedrijven over cyberincidenten bijdragen aan een grotere bewustwording van de risico's op bedrijfsdiefstal. Dit kan bijvoorbeeld via een verplichting voor grote bedrijven om in het jaarverslag te rapporteren over cyberveiligheidsincidenten.

3.2 Phishing en malafide websites

Kern

- Phishing is het startpunt voor veel cybercriminaliteit.
- In 2016 steeg het aantal meldingen van phishingmails en het aantal ontdekte malafide websites.
- Het blijft moeilijk voor elke gebruiker om in alle omstandigheden nep van echt te onderscheiden; focus moet daarom liggen op preventie.

Ontwikkelingen

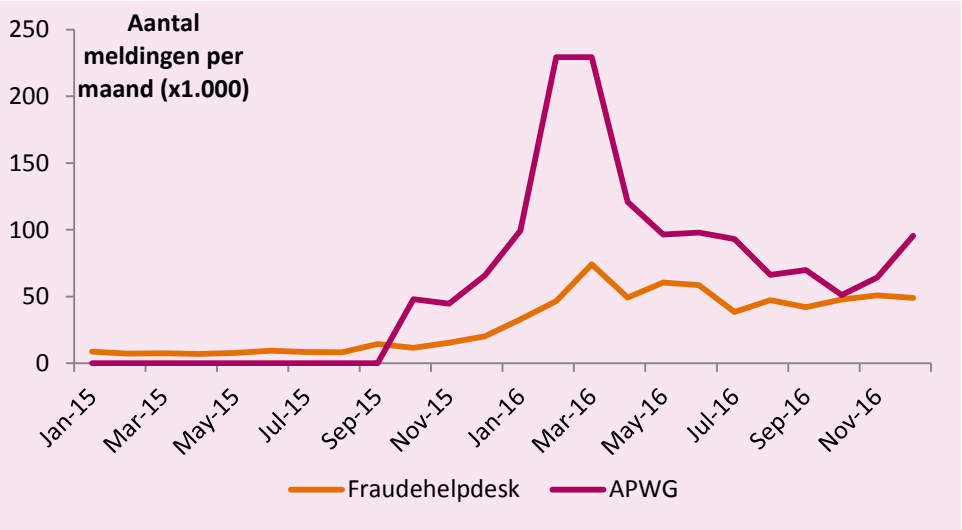
'Phishing' is een verzamelbegrip voor diverse soorten frauduleuze e-mails. Via deze e-mails proberen verzenders om persoonsgegevens te achterhalen, malware te installeren[79], spam te versturen of een nepfactuur[80] te innen. Volgens sommige

[77] A. Glitz en E. Myersson, 2017, Industrial Espionage and Productivity. (link)
[78] Volgens een rapport van de Amerikaanse overheid is de bescherming van intellectueel eigendom in China nog onvoldoende. (Bron)
[79] Tussen april 2016 en februari 2017 bevatten gemiddeld 1 op de 250 e-mails malware volgens Symantec Monthly Threat Report. (link)
[80] Volgens dit Volgens dit artikel van Fortune zouden Facebook en Google op deze manier zelfs voor honderd miljoen dollar zijn opgelicht.

experts start zelfs 91 procent van alle cybercriminaliteit met een phishingmail.[81] Soms worden ontvangers via de phishingmail naar een malafide website (of 'phishingsite') geleid. In maart 2016 is op deze manier in de Verenigde Staten de e-mail van verschillende leden van de Democratische Partij gehackt.[82]

In 2016 was een sterke stijging te zien van het aantal meldingen van phishingmails, zie Figuur 3.1 . Rapporteerde de Fraudehelpdesk in 2015 nog zo'n tienduizend meldingen per maand, in 2016 is dat aantal gestegen naar bijna vijftigduizend. Een kanttekening bij deze gegevens is dat de toename van het aantal meldingen slechts een indicator is voor de toename in het werkelijke gebruik van phishing. De toename in het aantal meldingen kan ook veroorzaakt worden door een grotere bekendheid van de meldpunten.

Figuur 3.1 Aantal meldingen van phishingmails sterk toegenomen in 2016



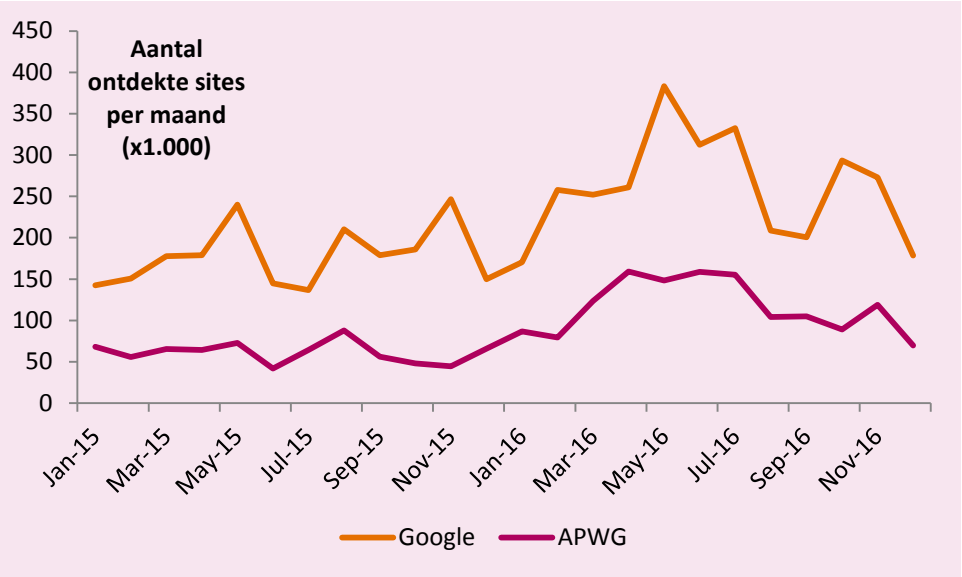
Bron: Fraudehelpdesk en Anti-Phishing Working Group (APWG).

Ook het aantal malafide websites is gestegen (Figuur 3.2). In 2016 ontdekte Google 3,1 miljoen malafide sites, bijna een miljoen meer dan in 2015.

Een logische verklaring voor deze stijging is dat phishing nog steeds winstgevend is. Cybercriminelen slagen er kennelijk steeds in om beveiligingsmaatregelen te omzeilen en voldoende betrouwbaar over te komen.

[81] Dit onderzoek van Trend Micro uit 2012 stelt bijvoorbeeld dat 91 procent van de gerichte aanvallen via phishing verloopt, net als een rapport uit 2016 van PhishMe.
[82] Zie bijvoorbeeld dit nieuwsbericht.

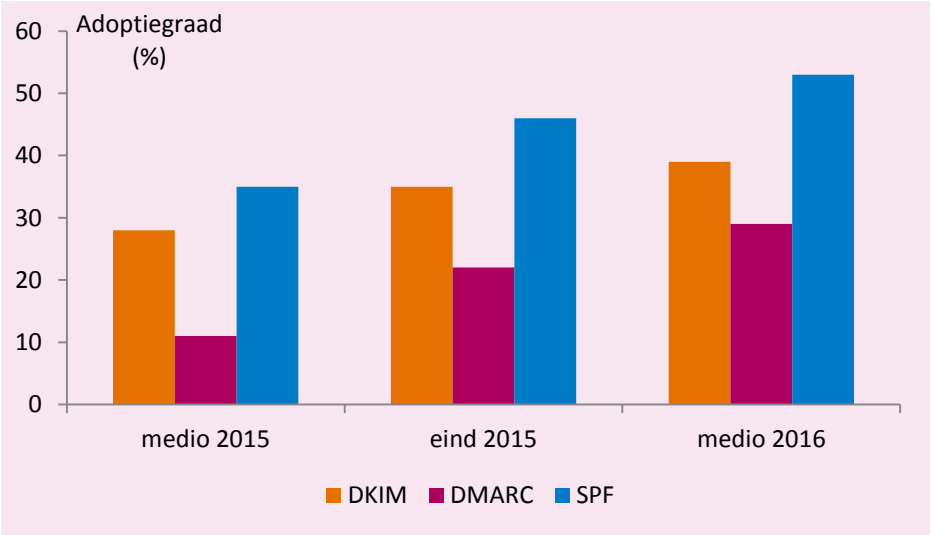
Figuur 3.2 Aantal ontdekte phishingssites toegenomen in 2016



Bron: Google Transparency Report en APWG.

Er bestaan standaarden voor veiliger e-mail (met name DMARC, DKIM en SPF). Deze standaarden helpen om vervalsing van de naam van de afzender of de inhoud van het bericht te voorkomen. In februari van 2017 hebben bedrijven en overheidorganisaties afgesproken om invoering van deze standaarden te stimuleren.[83] Tussen medio 2015 en medio 2016 is de adoptie van deze standaarden onder overheidsorganisaties weliswaar gestegen van gemiddeld vijfentwintig naar gemiddeld veertig procent, maar blijft nog achter bij de doelstellingen.

Figuur 3.3 Adoptiegraad standaarden gestegen



Bron: Forum Standaardisatie. Noot: adoptiegraad onder ca. 150 overheidsdomeinen.

[83] Dit is de Veilige E-mail Coalitie. Zie hiervoor meer informatie.

Een andere verklaring is dat cybercriminelen nieuwe strategieën toepassen, zoals 'homografische' aanvallen[84] of berichten die zijn gepersonaliseerd met openbare of gestolen gegevens.[85]

Risico's

Phishingmails en malafide websites zijn steeds vaker niet van echt te onderscheiden. Het is aannemelijk dat phishing winstgevend blijft en daarmee schade blijft aanrichten. Economische schade kan ontstaan via diverse vormen van cybercriminaliteit die volgen op een geslaagde phishingmail. Minder zichtbaar, maar wel aanwezig, is het effect van phishing op het vertrouwen in e-mail en de preventiekosten.

Beleidsopties

Als een betrouwbaar ogende phishingmail gebruikers weet te bereiken, zal er altijd een groep zijn die erin trapt. Het is daarom belangrijk om te voorkomen dat phishingmails zover komen. Dit kan door het gebruik van beveiligingsstandaarden zoals DKIM, DMARC en SPF te stimuleren.

3.3 Datalekken

Kern

- Datalekken worden vaak pas laat ontdekt – soms pas jaren nadien.
- Hoe later een lek ontdekt wordt, hoe minder zinvol repressief (ex post) toezicht is. Effectieve bescherming van persoonsgegevens zal daarom ook gericht moeten zijn op het voorkomen van datalekken.

Ontwikkelingen

Steeds meer persoonlijke en zakelijke gegevens worden door overheden, bedrijven of maatschappelijke organisaties digitaal bewaard. Bij een datalek worden deze gegevens vernietigd, gewijzigd of heeft een onbevoegd persoon onbedoeld inzage. Datalekken kunnen het gevolg zijn van onzorgvuldigheid (denk aan het verlies van een USB-stick met persoonsgegevens) of van cybercriminaliteit. Criminelen kunnen bijvoorbeeld creditcardgegevens misbruiken of personen afpersen met persoonsgevoelige informatie. Deels komt de schade ook terecht bij de organisatie waar het datalek plaatsvond.[86]

---

[84] Deze aanval maakt gebruik van het feit dat sommige letters uit verschillende alfabetten, zoals Latijnse, Cyrillische of Armeense schrift er in Unicode hetzelfde uitzien. Zie hier voor meer informatie.
[85] Gestolen gegevens van miljoenen LinkedIn-gebruikers werden bijvoorbeeld in 2016 gebruikt voor een phishingcampagne. (bron)
[86] Krishnamoorthy (2016) laat zien dat de waarde van beursgenoteerde bedrijven met gemiddeld 0,3 procent daalt na een datalek. Zie Krishnamoortyh, S., 2016, Stock market impact of privacy breach disclosures & their sentiment-based countermeasures (ex-ante), *Master's thesis Vrije Universiteit Amsterdam*.

Datalekken kunnen erg omvangrijk zijn, zoals de Panama Papers (2,6 terabyte aan fiscale gegevens) en bij Yahoo! (gegevens van anderhalf miljard accounts). Datalekken kunnen ook pas met een grote vertraging bekend worden. Het lek bij Yahoo! bijvoorbeeld vond plaats in 2013, maar werd pas in 2016 bekend. Vorig jaar werd ook bekend dat bij Myspace al in 2013 miljoenen logingegevens waren gestolen.[87] In februari 2017 waarschuwde het programma *Zembla* voor het risico op datalekken bij de Belastingdienst in de periode 2013 tot 2016.

Over het totale aantal datalekken bestaat veel onzekerheid. Tabel 3.1 geeft een overzicht van schattingen uit vijf verschillende internationale bronnen. In omvang lopen deze schattingen sterk uiteen.

Tabel 3.1: Schattingen aantal datalekken

Bron	Bereik	Aantal datalekken 2015	Aantal datalekken 2016
Symantec	Wereldwijd	1211	1209
Privacy Rights Clearinghouse	Verenigde Staten	157	538
Risk Based Security	Wereldwijd	3930	4149
Gemalto	Wereldwijd	1673	1792
Verizon	82 landen	2260	1935

In Nederland werden in 2016 5.849 meldingen gedaan bij toezichthouder Autoriteit Persoonsgegevens (AP[88]). In het eerste kwartaal van 2017 waren dit er al 2300.[89] In de meeste gevallen (45 procent) ontstaat een datalek door het versturen aan een verkeerde ontvanger. Datalekken door phishing, hacking of malware kwamen in zeven procent van de gevallen voor. Zeven procent lijkt misschien weinig, maar digitale datalekken kunnen veel meer gegevens bevatten.[90] In de periode januari 2016 tot maart 2017 heeft de AP geen boetes opgelegd.

Risico's

Een risico van datalekken is dat deze vervolgschade kunnen aanrichten via misbruik van de vrijgekomen informatie. Wanneer illegaal verkregen persoonsgegevens te koop zijn, kunnen criminelen deze informatie bijvoorbeeld gebruiken voor spearphishing. Dit lijkt gebeurd te zijn met gegevens van miljoenen LinkedIn-gebruikers. Deze waren in 2012 gelekt en bleken in 2016 gebruikt te worden voor een phishingcampagne.[91]

[87] Zie dit artikel van PC Mag.
[88] In Nederland is het melden van datalekken sinds januari 2016 verplicht. Alle organisaties die onder de Wet Bescherming Persoonsgegevens vallen (dus ook mkb-bedrijven en kleine zelfstandigen) moeten een ontdekt lek binnen 72 uur melden bij de AP.
[89] Zie dit persbericht van de AP.
[90] AP noemt bijvoorbeeld een datalek in een klantportaal waarbij gegevens over 680.000 personen mogelijk zichtbaar waren.
[91] Zie deze blog van Fox-IT.

Een tweede risico is dat datalekken blijven voorkomen doordat organisaties te zwakke prikkels hebben om deze te voorkomen. De prikkel om datalekken te voorkomen kan bijvoorbeeld zwak zijn bij organisaties met een machtspositie (zoals een ziekenhuis of overheidsorganisatie). Als afnemers na het bekend worden van een datalek bij zo'n organisatie niet kunnen overstappen naar een andere organisatie dan werkt het reputatiemechanisme minder sterk. Ook worden datalekken vaak pas laat bekend, waardoor belanghebbenden (afnemers, bestuurders, toezichthouder) – als ze al geïnformeerd worden – pas laat kunnen ingrijpen. Ten slotte kan de prikkel voor preventie zwak zijn als organisaties verwachten dat een boete van de toezichthouder onwaarschijnlijk is.

Beleidsopties

Bij het toezicht op de bescherming van persoonsgegevens is preventie een belangrijk aandachtspunt. Dit kan bijvoorbeeld via marktscans, on-site controles of informatie te geven over beveiligingsstandaarden. Preventief toezicht vraagt ook om een geloofwaardig en proportioneel sanctiebeleid.

3.4 Ransomware

Kern

- Over het aantal feitelijke besmettingen van ransomware is weinig bekend.
- Verspreiders van ransomware gebruiken nieuwe technologische mogelijkheden, zoals IoT-apparaten, nieuwe softwarekwetsbaarheden en botnets, en nieuwe oplossingen om doelwitten met een hoge betalingsbereidheid te besmetten.
- Het risico bestaat dat ict-gebruikers de impact van ransomware onderschatten waardoor data verloren gaat of processen uitvallen.

Ontwikkelingen

Tot mei 2017 was het lastig om het risico van ransomware goed te kunnen duiden. Er zijn namelijk geen administratieve gegevens over de prevalentie van ransomware en slachtoffers van cybercriminaliteit doen zelden aangifte bij de politie. Wel steeg het aantal ontdekte ransomware-varianten sterk, van 35 in 2015 naar 193 in 2016.[92] Ook vonden enkele opmerkelijke incidenten plaats. Een Oostenrijks hotel kon bijvoorbeeld geen nieuwe kamersleutels uitgeven door ransomware[93] en ook computers in de Tweede Kamer zouden besmet zijn.[94]

Het risicobeeld van ransomware veranderde op 12 mei 2017. Op die dag infecteerde de ransomware-variant 'WannaCry' wereldwijd in hoog tempo honderdduizenden computers.[95] Zo raakten onder andere het Spaanse telecombedrijf Telefónica en

[92] Bron: F-Secure. (link)
[93] Zie dit bericht in Wired.
[94] Volgens bijvoorbeeld dit bericht op nu.nl.
[95] Zie bijvoorbeeld dit Wikipedialemma.

Engelse ziekenhuizen besmet.[96] WannaCry lijkt gebruik te maken van een softwarekwetsbaarheid in Windows ('Eternal Blue') die in april gelekt zou zijn door hackers. Eind juni 2017 verscheen een nieuw virus, 'Petya', dat zich voordoet als ransomware maar het lijkt erop dat Petya gegevens overschrijft (vernietigd) in plaats van te versleutelen.

Het gebruik van de zero-day is illustratief voor het feit dat cybercriminelen innoveren. Behalve naar nieuwe softwarekwetsbaarheden gaan hackers ook op zoek naar nieuwe kwetsbare software. Waar ransomware eerder vooral op pc's werd aangetroffen, kunnen nu ook tablets of telefoons met Android[97] en smarttelevisies[98] besmet raken. Ook zijn er aanpassingen van het verdienmodel. Het programma Popcorn Time bijvoorbeeld biedt het slachtoffer de keuze tussen betaling van losgeld of het delen van een link waarmee anderen besmet raken. Als minstens twee contacten van het slachtoffer betalen worden de gegevens vrijgegeven.[99] Voor cybercriminelen wordt het verspreiden van ransomware gemakkelijker door ransomware-as-service diensten.[100]

Ransomware kan ook een bijverdienste zijn voor cybercriminelen – in plaats van het hoofdverdienmodel. In het geval van het GameOver botnet waren veel computers wereldwijd besmet – met name met het doel om gericht geld te stelen van bedrijven en rijke particulieren. Niet alle besmette computers in het botnet kwamen hiervoor in aanmerking en om daar toch aan te verdienen ontwikkelden de hackers de ransomware CryptoLocker.[101]

In juli 2016 ging het project NoMoreRansom van start. Het is een initiatief van Europol, de Nederlandse politie en enkele cybersecurity bedrijven. NoMoreRansom helpt de slachtoffers van ransomware om hun bestanden te ontgrendelen. Vanaf juli 2016 tot maart 2017 kregen wereldwijd 75.000 mensen hun bestanden terug via NoMoreRansom.[102]

Risico's

Door de relatieve onbekendheid van de omvang van ransomware en de steeds veranderende strategieën van ransomware-verspreiders kunnen ict-gebruikers de kans en de gevolgen van een besmetting onderschatten.[103] Hierdoor kan onnodig

---

[96] De impact bij Telefónica van het virus op de bedrijfsvoering was beperkt (bron). Als gevolg van de besmetting bij de National Health Service was er geen toegang tot patiëntengegevensen vielen verbindingen met medische apparatuur uit. Het medisch personeel moest daarom overgaan op pen en papier en eigen mobiele telefoons. (bron)
[97] Dit zou al sinds 2014 gebeuren. Zie deze uitleg van Kaspersky over Koler-ransomware.
[98] Zie dit bericht van PC World.
[99] Zie dit bericht in Wired.
[100] Zie bijvoorbeeld hier.
[101] Bron: het artikel 'Inside the Hunt' in Wired. (link)
[102] Lees dit nieuwsbericht in NRC.
[103] Hoewel door WannaCry ransomware volop aandacht heeft gekregen, lijkt het aantal (bekende) infecties in Nederland beperkt te zijn gebleven tot parkeerbedrijf Q-Park. Zie dit artikel in de Telegraaf.

dataverlies optreden en kunnen processen die afhankelijk zijn van gegijzelde software (tijdelijk) uitvallen.

Beleidsopties

Om het inzicht in ransomware te vergroten kan meer onderzoek gedaan worden naar deze vorm van cybercriminaliteit. Bedrijven en overheidsorganisaties kunnen ook meer openheid geven over de aantallen besmettingen en de organisatorische gevolgen daarvan. Om voor nieuwe ransomware-varianten snel oplossingen te vinden, zoals ontgrendelings- of preventietechnieken, kan de overheid een financiële prikkel geven aan (ethische) hackers.

4 Gegevensstromen in de gezondheidszorg

Kern

- De mogelijkheden voor eHealth nemen toe, maar zorgverleners delen medische dossiers relatief weinig met elkaar en met zorggebruikers.
- Meldingen van datalekken en incidenten bij gemeenten laten zien dat risico's op datalekken juist bij (decentrale) administratieve gegevensstromen liggen.
- Een verplichte publieke infrastructuur voor gegevensuitwisseling kan naleving van normen makkelijker maken, voorkomt afhankelijkheid van een enkele private partij en kan burgers inzicht geven in wie toegang tot hun gegevens heeft. Onderzocht kan worden of deze voordelen opwegen tegen de risico's.
- Toezichthouders zullen zelf ook technische expertise over informatiebeveiliging moeten hebben om effectief te kunnen functioneren.

4.1 Inleiding

De zorgsector is primair van belang voor de gezondheid van de bevolking, maar ook haar economische belang is substantieel: de uitgaven aan de gezondheidszorg zijn verantwoordelijk voor veertien procent van het bruto binnenlands product. Bovendien draagt een gezonde (beroeps-)bevolking bij aan welvaart en welzijn. Cybersecurity is daarbij extra belangrijk in de zorgsector, omdat grote hoeveelheden persoonsgegevens ontstaan en gedeeld worden.

Net zoals in andere sectoren, brengt digitalisering in de zorg aandachtspunten voor cyberveiligheid met zich mee. Zo kwamen wereldwijd meer ransomware-infecties voor in de zorgsector dan in andere sectoren.[104] In mei 2017 raakten veertig ziekenhuizen van de Britse National Health Service besmet met de ransomware-variant WannaCry. Ook Nederlandse ziekenhuizen blijken kwetsbaar: vijftien van de

[104] Zie bijvoorbeeld hier.

25 ondervraagde ziekenhuizen (60 procent) is in de afgelopen drie jaar geraakt door een gijzelvirus.[105] De gevolgen waren verstrekkend: zo hadden veel zorgverleners geen toegang meer tot medische gegevens, moesten verschillende afdeling gesloten worden en werden patiënten bij andere ziekenhuizen ondergebracht.[106] Nederlandse ziekenhuizen bleken niet kwetsbaar voor WannaCry.

Binnen het zorgstelsel worden veel administratieve gegevens uitgewisseld. Het gaat dan onder meer om rekeningen van zorgverleners en medicijngebruik. Deze uitwisseling van administratieve gegevens is een direct gevolg van de organisatie van het zorgstelsel. Als semipublieke sector is de gezondheidszorg meer gereguleerd dan andere sectoren van de economie. Hierdoor zijn zorgorganisaties verplicht om informatie uit te wisselen met bijvoorbeeld toezichthouders en verzekeraars. Ook worden administratieve gegevens veel gebruikt voor (medisch) onderzoek.

De omvangrijke uitwisseling van persoonsgegevens in de zorgsector valt terug te zien in de meldingen van datalekken bij de AP. Bijna een derde van het totaal aantal meldingen komt uit de gezondheidszorg (zie kader). Dat is dubbel zoveel als het aandeel van de sector in de economie.

Meldplicht datalekken en de zorgsector

Sinds 1 januari 2016 zijn instellingen onder de Wet Meldplicht Datalekken verplicht om datalekken bij de AP te melden. In het eerste kwartaal van 2017 kwamen vanuit de zorg 666 meldingen binnen bij de AP; 27 procent van het totaal aantal meldingen (bron). In 55 procent van de gevallen ging het om eenvoudige incidenten waarbij persoonsgegevens aan een verkeerde ontvanger waren verstuurd; vier procent van de meldingen betreffen hacking, malware of phishing (bron). Het aantal persoonsgegevens wat kwetsbaar is geweest, verschilt sterk per melding. In 32 gevallen waren de gevolgen zodanig dat de AP een onderzoek heeft ingesteld. Naast meldingen vanuit de zorgsector kwamen er 331 meldingen vanuit gemeenten – een deel daarvan is zorggerelateerd.

Een voorbeeld van een incident in de gezondheidszorg is een groot datalek in het Antoni van Leeuwenhoek ziekenhuis, waarbij een onbeveiligde harde schijf met persoonlijke- en medische gegevens van 781 patiënten uit een auto werd gestolen (bron: NOS). Ook werd in mei 2017 een usb-stick van een medewerker van Roche Diagnostics Nederland gestolen met hierop gegevens van bijna 2000 patiënten van het VUmc (bron).

Datalekken komen lang niet altijd boven water (bron: Kaspersky). Binnen de gezondheidszorg geeft 31 procent van de organisaties aan het laatste incident te hebben gemeld bij de AP, tegenover 47 procent in de financiële sector. Het relatief hoge aantal meldingen in de zorgsector komt dus niet door een hogere meldingsbereidheid, maar reflecteert waarschijnlijk de kwetsbaarheid van de sector voor datalekken.

In dit hoofdstuk geven we een overzicht van de risico's die gepaard gaan met gegevensstromen in de gezondheidszorg. We beginnen met risico's rond de uitwisseling van medische dossiers en administratieve gegevens in het Nederlandse

[105] Bron: dit bericht van NOS.
[106] Bron: Wired.

zorgstelsel. Opkomende technologieën, nieuwe spelers en alternatief gebruik van medische gegevens komen daarna aan bod. De laatste sectie vat de belangrijkste risico's en beleidsopties samen.

4.2 Het Nederlandse zorgstelsel

In het Nederlandse zorgstelsel wisselt een grote diversiteit aan organisaties informatie met elkaar uit. Figuur 4.1 geeft de belangrijkste van deze gegevensstromen weer, zowel voor medische dossiers als voor administratieve gegevens. De figuur maakt onderscheid tussen zeven categorieën actoren: poortwachters, zorgverleners, verzekeraars, administratiekantoren, gegevensverwerkers, onderzoeksinstellingen en toezichthouders.

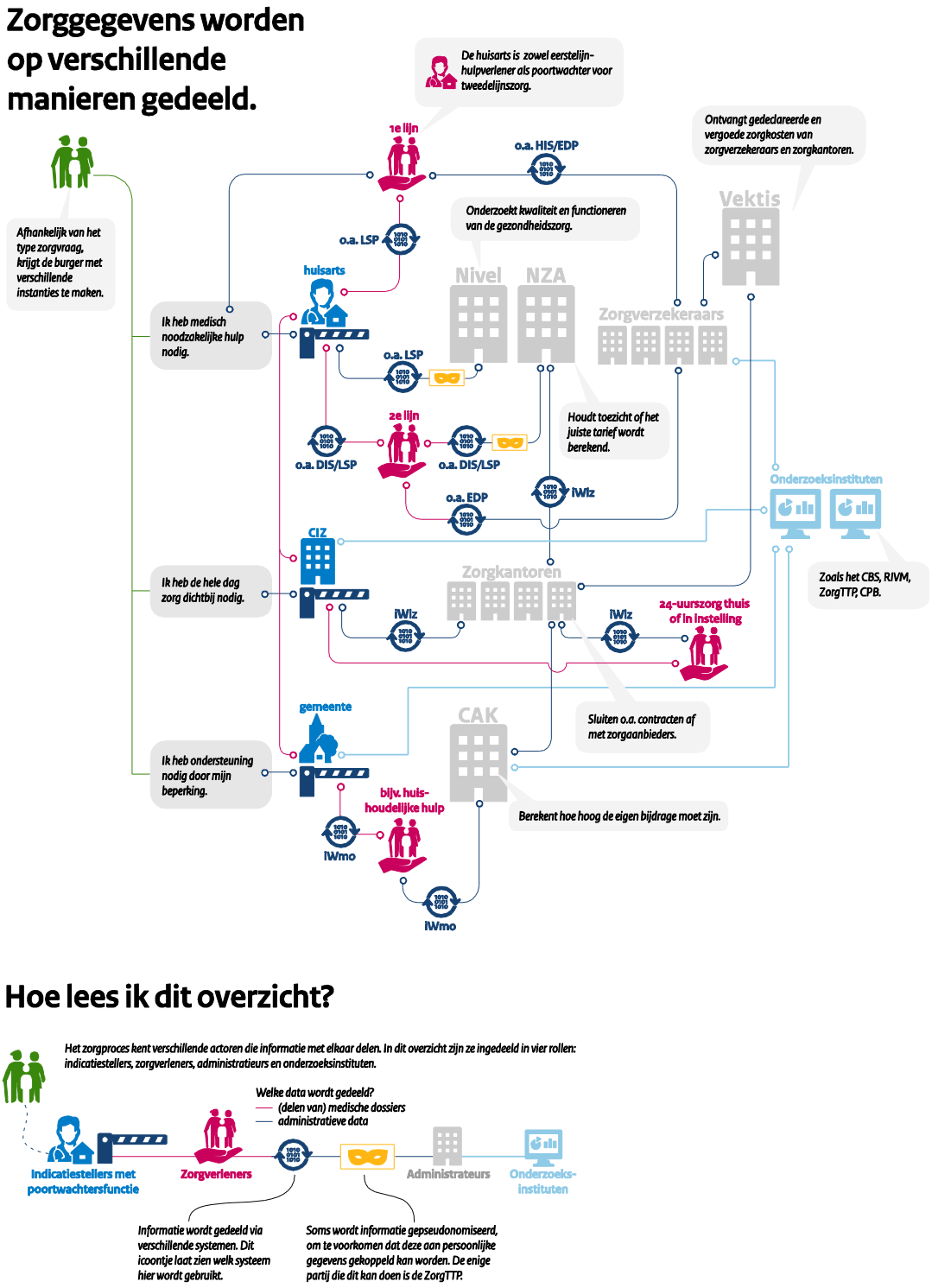
Poortwachters en zorgverleners

De complexe organisatie van het Nederlandse zorgstelsel heeft het neveneffect dat veel administratieve gegevens worden uitgewisseld. Daarnaast is het noodzakelijk om (delen van) het medisch dossier te delen met zorgverleners om toegang tot zorg te krijgen. Zo is alle eerstelijnszorg, zoals een bezoek aan de huisarts en tandarts, vrij toegankelijk, maar is voor andere vormen van zorg een verwijzing of een indicatie nodig. Afhankelijk van de soort zorg ('cure' of 'care'), kan men voor toegang terecht bij verschillende *poortwachters*, te weten: de huisarts, het Centrum indicatiestelling zorg (CIZ) en gemeenten. Binnen de cure indiceert de huisarts voor medisch noodzakelijke hulp (Zorgverzekeringswet; Zvw). Binnen de care indiceert het CIZ voor 24-uurs zorg dichtbij (Wet langdurige zorg; Wlz) en gemeenten voor ondersteuning in de thuissituatie (Wet maatschappelijke ondersteuning; Wmo).

Binnen de cure maken zorgverleners gebruik van onder andere het landelijk schakelpunt (LSP) voor het opslaan en delen van medische gegevens. Op het LSP zijn huisartsen, apotheken, ziekenhuizen en zorggroepen (ketenzorg) aangesloten. 91 procent van de huisartsen is inmiddels aangesloten.[107] Het *gebruik* van LSP lijkt lager te liggen: van de huisartsen geeft 68 procent aan het LSP te gebruiken.[108] Voor het verzamelen van gegevens over welke zorg door zorgaanbieders is geleverd en gedeclareerd gebruiken ziekenhuizen het DBC-informatiesysteem (DIS).

[107] Zie deze pagina van VZVZ, bezocht op 20 juni 2017.
[108] Bron: Nictiz (2016), fig. 9.1 (link). Omdat huisartsen naast het LSP ook andere communicatiemiddelen gebruiken, ligt het aandeel van het LSP bij gegevensuitwisseling lager dan het percentage aangesloten huisartsen.

Figuur 4.1 Vooral administratieve gegevens worden tussen veel organisaties gedeeld



Hoe lees ik dit overzicht?

Binnen de care wordt veelal gebruik gemaakt van iStandaarden. Deze informatiestandaarden worden beheerd door het Zorginstituut Nederland en zijn een verzameling van regels en afspraken over de uitwisseling van medische gegevens tussen gebruikers. Een variant van de iStandaard is de iWlz. Deze standaard wordt

verplicht gebruikt door zorgverleners, het CAK, het CIZ en zorgkantoren om te communiceren over Wlz-zorg. Het gaat hierbij om medische gegevens. Voor zorg die wordt vergoed vanuit de Wmo is er de iWmo. De iWmo wordt gebruikt door aanbieders van zorg en ondersteuning, gemeenten en het CAK. Werken met de iWmo is niet verplicht. Daarnaast hebben zorginstellingen hun eigen informatiesystemen en vaak hun eigen patiëntenportalen.

Het huidige stelsel vergt van alle huisartsen en gemeenten dat zij zelf hun informatiebeveiliging organiseren. Dit brengt het risico met zich mee dat huisartsen medische gegevens onvoldoende beveiligen zodat informatiesystemen kwetsbaar blijken voor bijvoorbeeld ransomware-aanvallen. Daarnaast kunnen datalekken ontstaan die onopgemerkt kunnen blijven. Ook bij gemeenten bestaat een risico dat zij zich onvoldoende bewust zijn van het belang van een beveiliging van medische gegevens. Zelfs bij grote gemeenten zoals Rotterdam en Eindhoven is geconstateerd dat informatiebeveiliging tekort schiet.[109]

Burgers hebben het recht om te bepalen wie inzicht in hun medische gegevens krijgt, maar kunnen niet nagaan of poortwachters en zorgverleners in de praktijk aan hun wensen voldoen. Ook kunnen zij niet controleren hoe hun medisch dossier beveiligd is. Grote zorgorganisaties, zoals ziekenhuizen, hebben een veel grotere prikkel om een goede reputatie op het gebied van informatiebeveiliging op te bouwen dan kleine poortwachters en zorgverleners. Een ziekenhuis zal bij een incident meer media-aandacht krijgen dan bijvoorbeeld een huisarts. Daarnaast zullen grote organisaties statistisch gezien vaker incidenten meemaken dan kleine organisaties bij een gelijk beveiligingsniveau. Bij kleinere organisaties zal het reputatiemechanisme daardoor minder goed werken.

Een tweede probleem bij kleine organisaties is dat de kosten van beveiliging tegen sommige incidenten te groot kunnen zijn. Hier zijn twee redenen voor. Ten eerste zijn veel soorten beveiligingskosten onafhankelijk van de schaal waarop ze worden toegepast. Ten tweede zijn de baten van preventie bij kleine organisaties lager vanwege beperkte aansprakelijkheid: de financiële schade voor de zorgorganisatie kan niet groter zijn dan de kosten van een faillissement.

De beperkte marktprikkels voor cyberveiligheid bij (kleinere) poortwachters en zorgverleners vergroot het belang van toezicht op deze categorie door de AP en de IGZ. De verscheidenheid aan informatiesystemen bij huisartsen en gemeenten maakt het daarbij wel kostbaar voor deze toezichthouders om te controleren of zij gegevens adequaat beschermen.[110] Hierdoor ontstaat het risico dat poortwachters en zorgverleners onvoldoende investeren in cyberveiligheid.[111]

---

[109] Zie bijvoorbeeld het artikel “Wij weten alles van u” in *De Groene Amsterdammer*, 3 mei 2017.
[110] Bij de zorginstellingen die door het AP zijn onderzocht bleken de voorzorgsmaatregelen onvoldoende. (Bron)
[111] Zo signaleerde de AP eind 2016 dat patiëntportalen van ziekenhuizen onvoldoende beveiligd zijn. (Bron)

Verzekeraars

Met het invoeren van de gereguleerde marktwerking in 2006 hebben zorgverzekeraars een andere rol gekregen. Naast het afhandelen van declaraties en betalingen hebben zij de taak om als zorginkoper contracten af te sluiten met zorgverleners. Zorgverzekeraars ontvangen van zorgverleners administratieve gegevens over medische behandelingen en medicijngebruik voor het uitvoeren van deze taken. Vektis ontvangt op geautomatiseerde wijze declaratiebestanden van zorgverzekeraars en beschikt hierdoor over een dataset met administratieve data, waaronder persoonsgegevens, medicijngebruik van verzekerden, de verzekerde zorg in Nederland en demografische gegevens.

Vektis en verzekeraars beschikken over administratieve gegevens waaruit de gezondheid van iedere Nederlander af te leiden valt. Risico's op datalekken en onvoldoende beveiliging lijken op dit moment echter beperkt omdat verzekeraars baat hebben bij een goede reputatie. Verzekeringsnemers kunnen immers naar een andere verzekeraar overstappen als zij hun huidige verzekeraar niet vertrouwen – al is de keuze uit zorgverzekeraars beperkt.

Administratiekantoren, gegevensverwerkers, onderzoeksinstellingen en toezichthouders

Gegevens die via verschillende informatiesystemen (zoals de DIS) worden uitgewisseld mogen (deels) voor onderzoeksdoeleinden worden gebruikt. Met behulp van deze gegevens worden onder andere de gezondheid van inwoners en wachtlijsten in de zorg in kaart gebracht. Ook wordt hiermee onderzoek gedaan ter bevordering van de kwaliteit van zorg. Voorbeelden van onderzoeksinstellingen zijn het CBS en het RIVM. Het CBS is de enige partij in Nederland die mag koppelen op basis van burgerservicenummers (BSN). Andere partijen moeten hun gegevens zo gebruiken dat deze niet tot een individueel persoon herleidbaar zijn. Om patiëntengegevens te beschermen zijn er organisaties die persoonsgegevens pseudonimiseren.[112] De stichting ZorgTTP voert pseudonimisaties uit voor onder meer (zorg)instellingen, overheden, publiekrechtelijke organen en onderzoeksbureaus.[113]

Toezichthouders, zoals de Nederlandse Zorgautoriteit (NZa), AP en IGZ zien erop toe dat publieke zorgbelangen worden nageleefd. De NZa houdt vooral toezicht op het gedrag van zorgverleners en zorgverzekeraars en heeft hiertoe toegang tot administratieve gegevens. De AP ziet erop toe dat de privacy van burgers niet in het geding komt en kan boetes opleggen, wanneer de informatiebeveiliging van zorgorganisaties niet op orde is. Deze boetes kunnen vanaf mei 2018 oplopen tot 20

[112] De AP (2016) heeft aangegeven dat persoonsgegevens ook na pseudonimisering tot personen herleidbaar kunnen zijn en dus persoonsgegevens blijven (link).
[113] Open source alternatieven voor pseudonimisatie, zoals PEP (link), zijn beschikbaar maar worden weinig gebruikt.

miljoen of 4 procent van de jaaromzet. De toezichthouders hebben zelf geen toegang tot medische dossiers. De IGZ bewaakt de kwaliteit van zorgaanbieders en kan onder strenge voorwaarden inzage krijgen in medische dossiers.

Toezichthouders zijn belangrijk omdat zorggebruikers zelf geen zicht hebben in de activiteiten van administratiekantoren en onderzoeksinstellingen. Ook kunnen zorggebruikers meestal niet overstappen naar andere organisaties. Administratiekantoren en onderzoeksinstellingen hebben hierdoor niet altijd een sterke prikkel om een goede reputatie te onderhouden.[114] Dit geldt ook voor dataverwerkers zoals ZorgTTP die een centrale rol spelen in het beveiligen van gegevensstromen. Een gebrekkig reputatiemechanisme vergroot het risico op grootschalige datalekken en algemene tekortkomingen aan cyberveiligheid, tenzij toezichthouders voldoende tegenwicht kunnen bieden.

4.3 Opkomende technologieën en nieuwe datastromen

Een fundamenteel gevolg van digitalisering is dat er nieuwe algemeen toepasbare technologieën komen, zoals online platformen, robots en big data (Bijlsma, Overvest en Straathof 2016). Deze technologieën bieden voordelen voor patiënten, cliënten en zorgverleners en gaan gepaard met nieuwe risico's voor cybersecurity. Deze risico's komen voort uit nieuwe databronnen, nieuwe aanbieders van producten en diensten en nieuwe toepassingen voor data.

Nieuwe databronnen

Digitalisering zorgt voor een reeks aan producten en diensten die ook een medische toepassing kunnen hebben. Mobiele apparaten zoals smartphones, smartwatches en Fitbits monitoren lichaamsbeweging en hartslag ook bij gezonde mensen. Deze apparaten stellen gebruikers in staat om medische data te meten, te delen en door anderen te laten analyseren. Sommige medische testen en onderzoeken, bijvoorbeeld voor diabetes en Parkinson, kunnen eenvoudig via apps worden uitgevoerd. Soms zijn patiënten daarbij rechtstreeks afhankelijk van apparatuur die met het internet verbonden is.

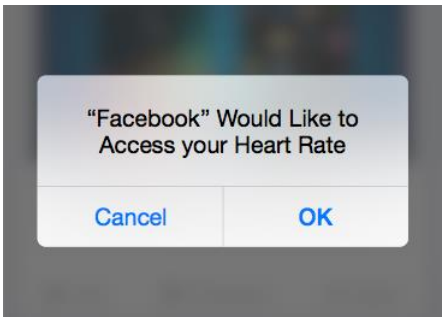
Apparaten met een medische toepassing zijn niet de enige soort databron over gezondheid. Meer indirecte bronnen zoals zoekopdrachten op internet, IoT-apparaten, sociale media of aankopen in supermarkten kunnen steeds beter gebruikt worden om aspecten van iemands gezondheid af te leiden.

Datastromen volgen niet alleen uit de formele verantwoordelijkheden die organisaties hebben in de zorgsector, maar vloeien ook voort uit het gebruik van

[114] Deze organisaties kunnen onderling verschillen in het belang van reputatie: zo kan een datalek bij het CBS gevolgen hebben voor bereidheid van burgers en bedrijven om vrijwillig gegevens aan het CBS verstrekken.

technologie. Met de digitalisering van de samenleving groeit ook het scala aan apparaten en databronnen dat inzicht kan geven in iemands gezondheid. De bescherming van gezondheidsgegevens is daardoor niet langer de exclusieve verantwoordelijkheid van de zorgsector, maar strekt zich uit naar bedrijven met uiteenlopende achtergronden.

Figuur 4.2 Gegevens over gezondheid zijn eenvoudig te delen



Nieuwe aanbieders

Techbedrijven zoals Apple, Google, Amazon en Facebook leveren producten en diensten die ook toepasbaar op de gezondheidszorg zijn. Soms faciliteren deze bedrijven rechtstreeks medische toepassingen. De *HealthKit* en *ResearchKit* van Apple bieden bijvoorbeeld een platform voor gezondheidsapps die gebruik kunnen maken van mobiele apparaten. De *ResearchKit* is expliciet gericht op medische onderzoeken en kan ook gebruikt worden met accessoires van derden (zoals bloeddrukmeters). Een ander voorbeeld is de inzet van *machine learning* door Google bij het stellen van diagnoses.[115]

Techbedrijven zijn zich over het algemeen bewust van cybersecurity risico's en hebben een reputatie als betrouwbare leverancier te verliezen. Bij diensten gericht op gezondheid is er een sterk reputatiemechanisme: een blunder bij een gezondheidsdienst kan nadelig zijn voor het vertrouwen in alle diensten die het bedrijf aanbiedt. Een beperkt risico zou hier kunnen zijn dat medische gegevens in Nederland als gevoeliger worden ervaren dan in de (vaak Amerikaanse) thuismarkten van deze bedrijven. Een ander risico is dat ook bedrijven met een slechte beveiliging gezondheidsapps kunnen aanbieden op een platform dat gebruikers als veilig ervaren. Platforms kunnen aanbieders van apps screenen, maar zijn ook gebaat bij de toegankelijkheid van het platform.
Niet alleen techbedrijven richten zich op gezondheidszorg, ook elektronicabedrijven ontwikkelen steeds meer medische apparatuur. In beginsel werkt bij deze bedrijven hetzelfde reputatiemechanisme als bij techbedrijven. Wel zijn cybersecurity risico's voor deze categorie bedrijven relatief nieuw – wat zich kan vertalen in het uitblijven van veiligheidsupdates voor software in medische apparaten (vooral als zij op het

[115] Zie bijvoorbeeld hier.

netwerk zijn aangesloten). Dat deze bedrijven nog worstelen met de cyberveiligheid van medische appratuur blijkt onder andere uit een enquête van Ponemon Institute (2017) onder fabrikanten en professionele gebruikers van medische apparatuur.[116] Zo geeft tachtig procent van de fabrikanten en zorgorganisaties aan dat medische apparatuur moeilijk te beveiligen is. En slechts 37 procent van de fabrikanten heeft er vertrouwen in dat kwetsbaarheden in medische apparatuur ontdekt kunnen worden. Ook is de verantwoordelijkheid voor de veiligheid van medische apparatuur niet goed belegd: zo geeft een derde van de respondenten aan dat niemand hoofdverantwoordelijk is voor cyberveiligheid. Grotere fabrikanten, zoals Philips, zijn hun reputatie op het gebied van cybersecurity aan het uitbouwen[117] en kunnen met het aanbieden van cyberveilige apparaten concurrentievoordeel behalen.

Nieuwe toepassingen data

Er ontstaan niet alleen voortdurend nieuw databronnen, ook worden de mogelijkheden voor data-analyse steeds groter. Doordat de kosten van computerberekeningen en dataopslag steeds verder dalen (wet van Moore) kunnen analysetechnieken zoals *machine learning* steeds beter toegepast worden.

Uit de combinatie van nieuwe databronnen en betere analysetechnieken ontstaan nieuwe toepassingen voor data. Medische toepassingen liggen op het terrein van diagnose en behandeling. Niet-medische toepassingen zijn er ook, bijvoorbeeld voor verzekeraars.

Machine learning is op kleine schaal succesvol toegepast bij de diagnose van huidkanker en diabetes. Een veelgebruikte methode bij automatisering van diagnoses is om een neuraal netwerk te laten trainen door experts. Deze vorm van diagnose heeft als voordelen dat een neuraal netwerk in potentie beter kan diagnosticeren dan experts en dat een neuraal netwerk simultaan voor meerdere patiënten gebruikt kan worden – en onafhankelijk van de locatie. Een smartphone kan bijvoorbeeld al signaleren of iemand een verhoogd risico op bepaalde complicaties loopt.[118] Naarmate meer en betere toepassingen van machine learning ontstaan, zullen diagnoses en het bepalen van bijbehorende behandelingen verschuiven van individuele zorgverleners naar de bedrijven die diagnose en behandelsuggesties als dienst aanbieden. De afhankelijkheid van ict in de zorg zal hierdoor toenemen.

Medische gegevens kunnen ook gebruikt worden voor niet-medische doeleinden. Zorgverzekeraars kunnen bijvoorbeeld hun eigen administratieve gegevens en die van andere partijen gebruiken om contracten met zorgverleners te optimaliseren om het aanbod van zorg beter op de vraag te laten aansluiten. Ook kunnen zij deze gegevens gebruiken om gericht polissen aan te bieden en risicovolle

[116] Link naar onderzoek van Ponemon.
[117] Zie bijvoorbeeld hier het beveiligingsbeleid van Philips Healthcare.
[118] Met de Apple Watch kan bijvoorbeeld een hartstoornis worden gedetecteerd. Zie dit artikel.

verzekeringsnemers te mijden.[119] Daarnaast kunnen gezondheidsgegevens onderdeel zijn van persoonlijke profielen die gebruikt worden voor bijvoorbeeld gerichte advertenties en het gericht benaderen van kiezers bij verkiezingen en referenda (zie paragraaf 2.1).

Een risico dat kan ontstaan uit al deze nieuwe toepassingen van gezondheidsgegevens is dat het verzamelen en delen van data op een ondoorzichtige manier plaatsvindt, vooral door bedrijven van buiten de EU. Toezichthouders kunnen hierdoor weinig zicht hebben op de beveiliging van datastromen.

4.4 Beleidsopties

In het huidige beleid spelen de zorgkoepels, verenigingen van zorgverleners, vaak een initiërende rol. Zo heeft het NCSC in samenwerking met de koepels een Information Sharing and Analysis Centre (ISAC) voor de zorg opgezet om cyberveiligheid informatie uit te wisselen. Ook hebben GGZ Nederland, de NVZ en de NFU eind 2016 het initiatief genomen om een Computer Emergency Response Team (CERT) op te richten voor acute cyberveiligheidsproblemen in de zorg: Z-CERT.

De Zorg-ISAC en de het Z-CERT zijn samenwerkingsverbanden die cyberveiligheid in de zorgsector rechtstreeks kunnen vergroten. Daarnaast hebben beleidmakers drie soorten instrumenten om cyberveiligheid verder te bevorderen:

- verplichte normen;
- toezicht en
- veilige publieke diensten, zoals ict-infrastructuur.

Verplichte normen kunnen een basis vormen voor het bieden van informatiebeveiliging omdat zij beveiligingsexpertise beter toegankelijk maken. Daarnaast faciliteert het een veilige informatie-uitwisseling tussen organisaties. Zolang een norm vrijwillig is, geeft deze geen extra prikkel om gegevens te beschermen. Zo voldeed in 2015 slechts 56 procent van de Nederlandse ziekenhuizen aan de norm voor informatiebeveiliging in de gezondheidszorg (NEN-7510[120]). Het aandeel ziekenhuizen dat hiervoor ook gecertificeerd is, is met 21 procent nog lager.[121] Sinds mei 2017 is deze norm wettelijk verplicht voor het gebruik van burgerservicenummers in de zorg. [122] Het toezicht op naleving ligt bij de AP voor

[119] Verzekeraars zijn wettelijk verplicht om iedereen te accepteren voor een basisverzekering. Zij kunnen hun marketinginstrumenten wel op bepaalde bevolkingsgroepen richten.
[120] Sinds mei 2016 wordt gewerkt aan een nieuwe versie van de NEN-7510 die naar verwachting vanaf oktober 2017 in gebruik genomen kan worden. Deze nieuwe norm zou beter moeten aansluiten bij internationale normen.
[121] Bron: RIVM. (link)
[122] Regeling gebruik burgerservicenummer in de zorg (link).

zover het de bescherming van persoonsgegevens raakt, en bij de NZA voor zover het over ordening van de zorgverzekeringsmarkt gaat.[123]

Omdat NEN-7510 betrekking heeft op een deel van de informatiebeveiliging in de zorg,[124] kan de overheid onderzoeken of aanvullende normen voor bijvoorbeeld netwerkkwaliteit en gegevensintegriteit ook verplicht gesteld kunnen worden. Ook kan worden onderzocht of het toezicht op informatiesystemen in de zorg meer integraal kan worden vormgegeven.[125]

Het gebruik van normen alleen kan niet voldoende veiligheid bieden. De reden hiervoor is dat dreigingen bij cyberveiligheid vaak onvoorspelbaar zijn: ernstige zwakheden kunnen ook in goed ontworpen informatiesystemen voorkomen. Cybercriminelen en staatshackers blijven innoveren. Vanwege deze strategische interactie biedt het gebruik van normen bij cyberveiligheid minder zekerheid dan bij verkeersveiligheid of gezondheidszorg zelf het geval is. Toezichthouders kunnen daarom niet volledig vertrouwen op certificering door derden bij controle van de cyberveiligheid van een organisatie. Zij zullen zelf technische expertise over informatiebeveiliging moeten opbouwen om effectief te kunnen functioneren.

Kleine organisaties, waaronder hulpverleners in de eerste lijn, gebruiken nu verschillende systemen naast elkaar. Het verplichten van normen voor informatiebeveiliging kan leiden tot convergentie naar een klein aantal private en publieke systemen, omdat uitwisseling van gegevens tussen systemen kostbaarder wordt. Het is daarbij de vraag of het wenselijk is dat het zorgstelsel voor gegevensuitwisseling afhankelijk wordt van een enkel privaat bedrijf. Bij afhankelijkheid kan de overheid overwegen om poortwachters en zorgverleners te verplichten om via een veilige publieke infrastructuur gegevens uit te wisselen (zoals het LSP).

Een publieke infrastructuur voor gegevensuitwisseling heeft als bijkomende voordelen dat ook kleine zorgorganisaties eenvoudig aan normen voor informatiebeveiliging kunnen voldoen en dat het mogelijk wordt om burgers eenvoudig inzicht te geven in wie toegang heeft tot hun gegevens. Als zorggebruikers eenvoudig kunnen nagaan wat er met hun gegevens gebeurt, dan kan dat zorgverleners een extra prikkel geven om veilig om te gaan met persoonsgegevens. Het LSP biedt patiënten nu al de mogelijkheid om na te gaan wie toegang heeft tot

[123] Artikelen 13 en 15 van de Wet gebruik burgerservicenummer in de zorg (link).
[124] De volgende gebieden van informatiebeveiliging vallen niet binnen het onderwerp en toepassingsgebied van NEN 7510-1 en NEN 7510-2: a) methodieken en statistische testen voor het doeltreffend anonimiseren van persoonlijke gezondheidsinformatie; b) methodieken voor het pseudonimiseren van persoonlijke gezondheidsinformatie; c) de netwerkkwaliteit van dienstverlening en methoden voor het meten van de beschikbaarheid van netwerken die worden gebruikt voor gezondheidsinformatica; en d) gegevenskwaliteit (onderscheiden van gegevensintegriteit).
[125] Nu zijn de IGZ, de AP en de NZa verantwoordelijk voor het toezicht op verschillende aspecten van hetzelfde informatiesysteem.

hun gegevens, maar uiteraard alleen voor zover informatie via het LSP is uitgewisseld.

Een verplicht gebruik van een publieke infrastructuur brengt twee risico's met zich mee. Een eerste risico is dat bij het wegvallen van infrastructuur grootschalige problemen kunnen ontstaan – er is een risico op een *single point of failure*. Dit risico kan beperkt worden door pluriformiteit[126] en decentraal te organiseren – bijvoorbeeld met blockchain technologie. Een tweede risico is dat als verplichte infrastructuur niet gebruikersvriendelijk is ontworpen, zorgverleners gebruik zullen gaan maken van onveilige alternatieven. Een strategie om dit risico te vermijden is om eerst vrijwillig gebruik van de publieke infrastructuur te stimuleren door te investeren in gebruiksgemak.

Meldingen van datalekken en incidenten bij gemeenten laten zien dat risico's op datalekken juist bij (decentrale) administratieve gegevensstromen liggen. De overheid zou daarom kunnen onderzoeken of de voordelen van een verplichte publieke infrastructuur voor gegevensuitwisseling in de zorg opwegen tegen de risico's. Een publieke infrastructuur kan de cyberveiligheid (en dus ook de privacy) in de zorgsector vergroten en kan ook de kwaliteit van de zorgverlening verbeteren.

[126] Zo kunnen burgers nu al op verschillende manieren inloggen bij de overheid en zorgorganisaties, zie bijvoorbeeld hier.

Dit is een uitgave van:

Centraal Planbureau
Bezuidenhoutseweg 30
Postbus 80510 | 2508 GM Den Haag
T (088) 984 60 00

info@cpb.nl | www.cpb.nl

Juli 2017