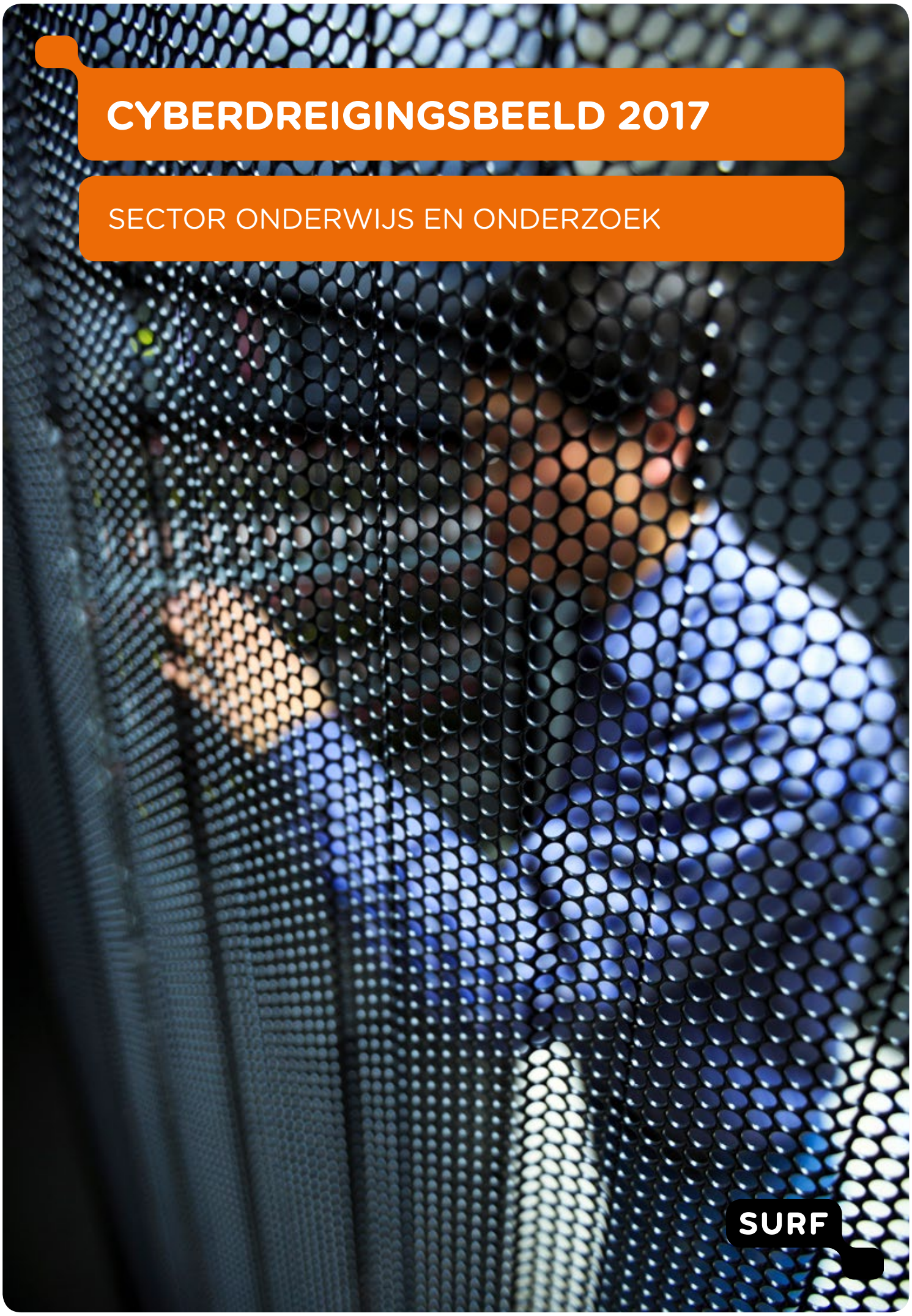
CYBERDREIGINGSBEELD 2017

SECTOR ONDERWIJS EN ONDERZOEK



SURF

INHOUDSOPGAVE

Samenvatting **4**

Terminologie **6**

1 inleiding **8**
ontwikkelingen 8
aanvallers 9

2 Criminaliteit en spionage nemen toe **10**
Snelle ontwikkeling 10
Ransomware 10
Digitale spionage 11
Politieke, militaire maar ook economische motieven 11
Moeilijk te traceren aanvallen 11
Geavanceerde infrastructuur aantrekkelijke doorvoerhaven voor aanvallen 12
Conclusie 12

3 Opkomst en groei van het Internet of Things **13**
Grote securityproblemen 13
Verdubbeling aantal aanvallen 13
IoT-apparaten extra kwetsbaar 14
Conclusie 14

4 Weerbaarheid onderwijs en onderzoek op orde **15**
Samenwerking nodig 15
Awareness kan beter 15
Conclusie 16

5 Toenemende digitalisering **17**
Bring your own device 17
Gevoelige informatie goed beveiligen 17
Algemene verordening gegevensbescherming 17
Conclusie 18

6 Denial-of-serviceaanvallen gaan overminderd door **19**
Gevolgen goed te overzien 19
Aanvallen tegen lage kosten uit te voeren 19
Conclusie 19

7 Kwetsbaarheden blijven problematisch **20**
Kwetsbaarheden in besturingssystemen én IoT-apparaten 20
Zero-daykwetsbaarheden 21
Kwetsbaarheden van mobiele apparaten 21
Conclusie 22

8 aanvallers **23**
Verschillende motieven en vaardigheidsniveaus 23
Invloed van actoren op dreigingen 24
Conclusie 25

9 bronnen **26**

VOORWOORD

De toenemende digitalisering van Nederland, en dus ook van het Nederlandse onderwijs en onderzoek, biedt ongekende mogelijkheden voor de vernieuwing van het onderwijs. Nieuwe onderwijsvormen zijn zeer afhankelijk van veilige en betrouwbare ICT. Dat maakt ons echter ook kwetsbaarder voor aanvallen. Het afgelopen jaar werd gekenmerkt door denial-of-serviceaanvallen met behulp van Internet-of-Things-apparaten en een enorme toename van ransomware-besmettingen die in sommige gevallen voor flinke schade hebben gezorgd. Het meest sprekende voorbeeld is de ransomwarebesmetting bij de Deense multinational Maersk, waardoor onder andere bij zusterbedrijf APM Terminals in Rotterdam dagenlang geen schepen gelost of geladen konden worden. Maersk schat de financiële schade van dat incident op enkele honderden miljoenen dollars en was pas na bijna een maand weer volledig operationeel. Het is dan ook zaak dat organisaties weten welke dreigingen er zijn, tijdig maatregelen nemen om die dreigingen tegen te gaan en snel kunnen handelen als er toch iets gebeurt.

De SURF-community's SCIRT en SCIPR bieden een geweldig platform voor het uitwisselen van informatie, waardoor instellingen snel op de hoogte zijn van problemen die zich voordoen bij andere instellingen. Binnen de sector onderwijs en onderzoek zijn problemen door ransomware vooralsnog dan ook beperkt gebleven. Maar de enorme verspreiding van dit soort malware en het toenemend aantal varianten maakt het noodzakelijk hierop alert te blijven en meer geautomatiseerde methodes te ontwikkelen om informatie over dreigingen snel te kunnen delen.

Privacybescherming neemt een prominentere plaats in dan ooit. Begin 2016 is de meldplicht datalekken van kracht geworden. De Autoriteit Persoonsgegevens kan boetes opleggen wanneer niet wordt voldaan aan deze meldplicht. En op 25 mei 2018 wordt de Algemene verordening gegevensbescherming (AVG) van kracht, die nog verdergaande eisen stelt aan het beschermen van persoonsgegevens en nog hogere boetes mogelijk maakt. De mogelijke impact hiervan moet niet onderschat worden. SURF biedt diverse hulpmiddelen die instellingen op weg helpen om aan de AVG te voldoen en er zijn verschillende initiatieven om daarin samen te werken. Spionage, zowel door staten als door criminele organisaties, is een probleem dat volgens de inlichtingendiensten blijft toenemen. Ook hiervoor geldt dat instellingen zich bewust moeten zijn van de mogelijkheid dat gevoelige informatie gestolen kan worden. Ze moeten verder goed weten wat er gebeurt in hun IT-omgeving en effectieve tegenmaatregelen nemen.

Dit rapport schetst een beeld van de ontwikkelingen die hebben plaatsgevonden tussen oktober 2016 en oktober 2017 en het effect op de meest relevante dreigingen voor instellingen voor onderwijs en onderzoek. Uit het rapport blijkt dat er vooruitgang wordt geboekt met informatiebeveiliging, maar ook dat er nieuwe uitdagingen op ons afkomen, zoals de toename van het aantal Internet-of-Things-apparaten, de toenemende digitalisering van studenten, docenten, onderzoekers en andere medewerkers van instellingen, en de sterk toenemende spionage door zowel criminelen als statelijke actoren.

Erik Fledderus
Algemeen directeur SURF

Marjolein Jansen
Vice-voorzitter Vrije Universiteit Amsterdam en Ambassadeur Cybersecurity SURF

SAMENVATTING

Dit Cyberdreigingsbeeld geeft bestuurders en security officers van instellingen in onderwijs en onderzoek een helder beeld van ontwikkelingen waarop ze moeten focussen om hun informatiebeveiliging en privacybescherming te verbeteren. Tijdens de onderzoeksperiode (oktober 2016 – oktober 2017) hebben we ontwikkelingen in kaart gebracht die invloed hebben op het dreigingsbeeld voor onderwijs en onderzoek. Het gaat om de volgende ontwikkelingen:

Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan. Volgens het NCSC en de veiligheidsdiensten blijft de dreiging van digitale spionage onverminderd hoog en proberen andere staten op die manier informatie weg te sluizen.

De kwetsbaarheid van het Internet of Things (IoT) heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven. Het aantal IoT-apparaten zal de komende jaren sterk toenemen tot wellicht meer dan 75 miljard apparaten wereldwijd in 2025. Veel van die apparaten hebben kwetsbaarheden die nauwelijks gepatcht worden en zijn onvoldoende beveiligd.

Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging. Met de weerbaarheid van Nederlandse organisaties is het in het algemeen slecht gesteld en recente incidenten tonen aan dat de impact van incidenten enorm kan zijn. De weerbaarheid in de sector onderwijs en onderzoek lijkt beter op orde te zijn.

Toenemende digitalisering van burgers (en dus van studenten, docenten, onderzoekers en andere medewerkers van onderwijs- en onderzoeksinstellingen) verandert het dreigingslandschap. Studenten, docenten, onderzoekers en andere medewerkers van instellingen maken steeds meer gebruik van mobiele apparaten, in veel gevallen hun eigen smart phones of tablets (BYOD). Hiermee vervaagt de grens tussen privé- en bedrijfsgegevens en wordt de controle op oneigenlijke toegang tot kritieke gegevens lastiger. Medio 2018 wordt de Algemene verordening gegevensbescherming van kracht en moeten organisaties processen op orde hebben voor het beschermen van persoonsgegevens en het melden van eventuele incidenten.

Denial-of-serviceaanvallen blijven voortduren maar zijn wel onder controle. Uit statistieken van SURFcert blijkt dat denial-of-serviceaanvallen onverminderd doorgaan. Daarbij lijkt een groot deel afkomstig van studenten gezien de opvallende afname tijdens vakantieperiodes. SURFnet, samen met de instellingen, heeft adequate oplossingen om deze aanvallen te mitigeren waardoor de impact beperkt blijft.

Kwaadwillenden maken nog steeds misbruik van kwetsbaarheden, ook op mobiele apparaten, om toegang tot kritieke systemen te verkrijgen. Veel kwetsbaarheden, inclusief zero-daykwetsbaarheden worden te laat of niet, gepatcht. Dit geeft kwaadwillenden veel mogelijkheden om aanvallen uit te voeren die moeilijk te detecteren zijn.

Om deze ontwikkelingen het hoofd te bieden, zijn onderwijs- en onderzoeksinstellingen in allerlei verbanden bezig om samen weerbaarder te worden. In de SURF-community's SCIRT en SCIPR wordt veel informatie uitgewisseld waardoor instellingen van elkaar leren, en er zijn SURF-diensten zoals Cybersave Yourself, SURFaudit en SURFcert die instellingen helpen hun informatiebeveiliging te verbeteren.

Aanvallers

Er zijn veel verschillende typen aanvallers, van script kiddies tot beroepscriminelen en statelijke actoren. Ieder type aanvaller heeft een bepaalde vaardigheid en motivatie om aanvallen uit te voeren. Daardoor zijn onschuldige aanvallen door bijvoorbeeld script kiddies niet meer dan vervelend, terwijl aanvallen door beroepscriminelen aanzienlijke schade aanrichten. Omdat vooral de geavanceerde aanvallen door beroepscriminelen en statelijke actoren moeilijk te detecteren zijn, moeten instellingen ook geavanceerdere middelen inzetten om zich hiertegen te wapenen.

Type Dreiging	**Manifestatie van dreiging**	**Risico**		
Type Dreiging	Gebeurtenis	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen • Fraude door verkrijgen van data over toetsen en opgaven	MIDDEN	HOOG	HOOG
2. Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Activist doet zich voor als onderzoeker • Student doet zich voor als medewerker en manipuleert studieresultaten	HOOG	MIDDEN	LAAG
3. Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	LAAG	LAAG	LAAG

Tabel 1: Relevante dreigingen voor onderwijs- en onderzoeksinstellingen

TERMINOLOGIE

100 GE	100 Gigabit Ethernetaansluiting, bijvoorbeeld op de AMS-IX of bij een internetleverancier als KPN of Ziggo.
Actor	Degene/groep die verantwoordelijk is voor een kwaadaardig incident.
AMS-IX	Amsterdam Internet Exchange – het belangrijkste internetknooppunt van Nederland en een van de grootste internetknooppunten van de wereld. Bijna al het internetverkeer met het buitenland loopt via de AMS-IX.
AVG	Algemene verordening gegevensbescherming (ook GDPR – General Data Protection Regulation (EU) 2016/679). Vervanger van de Wet bescherming persoonsgegevens die al sinds 2016 geldig is, maar op 25 mei 2018 in alle landen van de EU van kracht wordt.
Awareness	Algemene term om aan te geven in hoeverre mensen, of een organisatie, zich bewust zijn van beveiligingsrisico's en welke maatregelen nodig zijn om die tegen te gaan.
Big data	Grote hoeveelheid gegevens, die in groten getale binnenkomen, ongestructureerd worden opgeslagen en kosteneffectieve, innovatieve vormen van informatieverwerking vereisen die beter inzicht, besluitvorming en procesautomatisering mogelijk maken (Gartner).
Botnet	Verzameling softwarerobots die automatisch en zelfstandig, meestal kwaadaardige acties uitvoeren. Het botnet wordt aangestuurd door zogenaamde Command & Control (ook C&C of C2) servers.
Cryptoware	Ransomware die bestanden versleutelt, zodat ze niet meer geopend kunnen worden.
DDoS	Distributed Denial-of-Service. Een denial-of-serviceaanval waarbij een systeem of webapplicatie door meerdere computers, bijvoorbeeld een botnet, onbeschikbaar wordt gemaakt voor gebruikers.
Drive-by download	Download die ongemerkt, vaak geautomatiseerd, plaatsvindt bij het bezoek aan een website. Heeft tot doel een kwaadaardig programma op de computer van het slachtoffer te installeren.
Dyn	Bedrijf, dat DNS-beheerdiensten levert. Is sinds 2016 onderdeel van Oracle.
IoT	Internet of Things (Internet der Dingen). Concept waarbij alledaagse apparaten als videocamera's, wasmachines en koelkasten zijn aangesloten op het internet, met elkaar kunnen communiceren en zelfs met een zekere autonomie kunnen functioneren.
Jaff	Ransomware die wordt verspreid via spamberichten. Onderscheidt zich van andere ransomwarevarianten door het hoge losgeld (2 bitcoin = meer dan 10.600 euro op 31 oktober 2017).
Malware	Kwaadaardige software die gebruikt wordt om een computersysteem opzettelijk te verstoren. Het doel daarvan varieert van onbruikbaar maken tot het verzamelen van informatie.
Mirai	Kwaadaardige software die Internet-of-Things-apparaten infecteert en dan laat deelnemen aan een botnet.

NCSC	Nationaal Cyber Security Centrum van het ministerie van Justitie en Veiligheid. Het fungeert als het centrale informatieknooppunt en expertisecentrum voor cybersecurity in Nederland. De missie van het NCSC is het bijdragen aan het vergroten van de weerbaarheid van de Nederlandse samenleving in het digitale domein, en daarmee aan een veilige, open en stabiele informatiesamenleving (www.ncsc.nl).
Petya	Cryptowarefamilie die zich richt op Windows-systemen. Na besmetting wordt het filesysteem versleuteld.
Phishing	Een vorm van internetfraude die tot doel heeft gegevens aan een gebruiker te ontfutselen. Denk aan inloggegevens of bankgegevens. De fraudeur doet zich voor als een vertrouwde persoon of instantie om het slachtoffer te misleiden.
Ransomware	Kwaadaardige software (malware) die een computersysteem blokkeert totdat losgeld (ransom) is betaald.
Serpent	Cryptoware die wordt verspreid via spamberichten. Na infectie worden bestanden versleuteld met een sterk versleutelingsalgoritme. Onderscheidt zich van andere cryptoware door het losgeld dat wordt verhoogd als niet binnen 7 dagen wordt betaald.
Spam	Ongewenste elektronische berichten met als doel reclame te verspreiden of ontvangers te verleiden naar een bepaalde (vaak kwaadaardige) website te gaan.
Statelijke actor	Persoon of groep die in opdracht van of namens een staat verantwoordelijk is voor een kwaadaardig incident. Vaak is dit een (buitenlandse) inlichtingendienst.
Wannacry	Ransomware voor Windows-systemen. Wordt verspreid via phishing-e-mails en door gebruik te maken van een kwetsbaarheid in het Windows-besturingssysteem (EternalBlue).
Zero-day-kwetsbaarheid	Kwetsbaarheid in programmatuur die nog niet bekend is of waarvoor nog geen beveiligingsupdate beschikbaar is.

1. INLEIDING

In de voorgaande edities van het 'Cyberdreigingsbeeld – sector onderwijs en onderzoek' zijn zeven typen dreigingen gedefinieerd die invloed hebben op de processen onderwijs, onderzoek en bedrijfsvoering op universiteiten, hogescholen en mbo-instellingen (zie tabel 1, pagina 8).

Die dreigingen bestaan nog steeds. Voor het onderwijsproces zijn vooral *Identiteits-fraude* en *Manipulatie van digitaal opgeslagen data type dreigingen* die een grote negatieve impact kunnen hebben, terwijl voor het onderzoeksproces *Verkrijging en openbaarmaking van data* en *Spionage* de meeste negatieve gevolgen kunnen veroorzaken. Voor de bedrijfsvoering geldt dat eveneens voor *Verkrijging en openbaarmaking van data*.

We hebben echter ook vastgesteld dat alle instellingen voor onderwijs en onderzoek vooruitgang boeken als het gaat om informatiebeveiliging, dat in allerlei gremia wordt nagedacht over verdere verbetering daarvan en dat stappen worden gezet om dit gezamenlijk op te pakken.

Deze versie bouwt voort op de eerdere edities van het Cyberdreigingsbeeld, maar legt de nadruk op ontwikkelingen die in de afgelopen periode (van oktober 2016 tot oktober 2017) hebben plaatsgevonden, en welke invloed ze hebben op onderwijs en onderzoek. Die ontwikkelingen zijn in kaart gebracht aan de hand van gesprekken met security officers van instellingen en informatie die uit de SCIRT- en SCIPR-community's komt. Daarnaast zijn diverse publieke bronnen geraadpleegd.

Zo weten bestuurders van instellingen en security officers op welke ontwikkelingen ze moeten focussen om hun informatiebeveiliging en privacybescherming te verbeteren.

Ontwikkelingen

Op 21 juni 2017 heeft de Nationaal Coördinator Terrorismebestrijding en Veiligheid het Cybersecuritybeeld Nederland 2017 aan de Tweede Kamer aangeboden, met de veelzeggende conclusie: "Digitale weerbaarheid Nederland blijft achter op groeiende dreiging" [1]. Hierin worden vijf kernbevindingen genoemd die invloed hebben op de Nederlandse samenleving, waarvan de volgende het meest betrekking hebben op de sector onderwijs en onderzoek:

- Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan.
- De kwetsbaarheid van het Internet of Things heeft tot verstorende aanvallen geleid die de noodzaak tot het versterken van de digitale weerbaarheid onderschrijven.
- Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging.

Deze ontwikkelingen worden respectievelijk in de hoofdstukken 2, 3 en 4 besproken.

De samenleving digitaliseert in toenemende mate [2]. Denk maar aan het Internet of Things, big data, social media, digitale leeromgevingen, en het groeiende aantal mobiele apparaten en de toenemende mogelijkheden van die apparaten. In hoofdstuk 5 gaan we hier dieper op in.

Uit statistieken van SURFcert en diverse publicaties blijkt dat denial-of-service-aanvallen een blijvend probleem zijn. Ook blijft het beeld bestaan dat er een duidelijke afname van het aantal alerts tijdens vakanties is. Deze ontwikkeling bekijken we in hoofdstuk 6.

Kwetsbaarheden komen voor in alle software. Wanneer een softwareleverancier een lek in zijn product ontdekt, wordt (meestal) een patch uitgebracht. Er zijn echter kwetsbaarheden die al ontdekt zijn, maar nog niet bekend zijn bij de leverancier (zero-daykwetsbaarheid). Hoofdstuk 7 gaat in op deze ontwikkeling.

Aanvallers

Tot slot bespreken we in hoofdstuk 8 de verschillende actoren die een rol spelen bij aanvallen, wat hun vaardigheden en motieven zijn en op welke typen dreigingen ze invloed hebben.

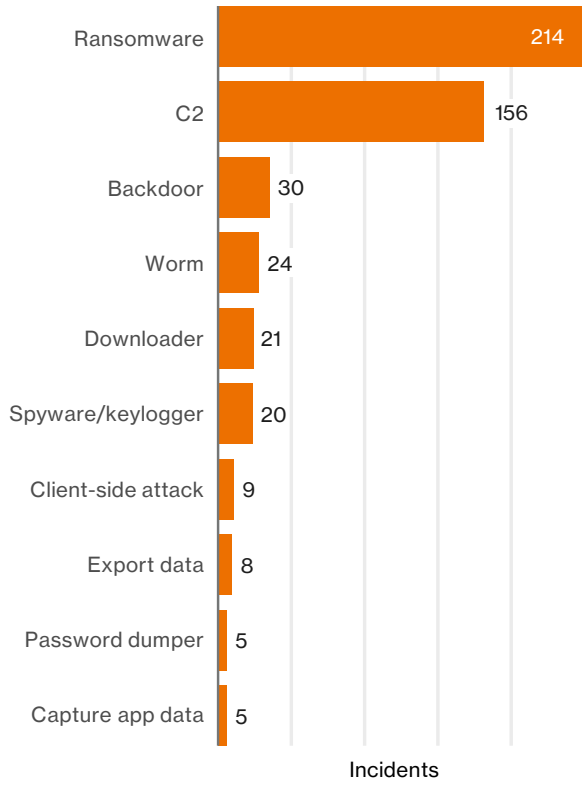
2. CRIMINALITEIT EN SPIONAGE NEMEN TOE

Snelle ontwikkeling

Uit publicaties van zowel de AIVD en de MIVD [4] als het NCSC [1] blijkt dat criminele en statelijke actoren de grootste dreiging vormen voor de Nederlandse digitale veiligheid en dat die zich sneller ontwikkelen dan andere actoren.

Ransomware

Beroepscriminelen maken veelvuldig gebruik van ransomware en onderwijsinstellingen zijn hiervan ook het doelwit. Dit blijkt uit verschillende infectiepogingen met ransomware die hebben plaatsgevonden bij onderwijsinstellingen tijdens de onderzoeksperiode [bron: SCIRT [5] mailinglijst]. Hierbij zijn onder andere de ransomwarevarianten Wannacry, Petya, Jaff en Serpent gesignaleerd; sommige daarvan kunnen zich door het hele netwerk verplaatsen als ze eenmaal binnengedrongen zijn, waardoor de infectie van een enkele machine al voldoende is om een heel netwerk te besmetten [6]. De initiële infectie kan door een phishingmail of een spammail gebeuren. Vooral phishingmails zijn steeds moeilijker te onderscheiden van een reguliere e-mail, waardoor de kans groot is dat één systeem geïnfecteerd raakt. Ook wordt nog steeds gebruikt gemaakt van zogenaamde drive-by downloads. Tijdens het bezoeken van een reguliere website wordt ongemerkt (en volledig automatisch) malware gedownload of wordt de gebruiker doorgezet naar een door de criminelen gecontroleerde website.



Figuur 1: Meest voorkomende malware bij cyberincidenten (bron: Verizon – DBIR 2017 [38])

Digitale spionage

In het jaarverslag 2016 van de AIVD [7] wordt aangegeven dat de dreiging van digitale spionage onverminderd hoog is en dat andere staten via die weg informatie proberen weg te sluizen. Dit werd ook in al in het jaarverslag 2015 van de AIVD [8] genoemd: “De AIVD heeft een recordaantal cyberspionage-aanvallen op Nederlandse overheidsinstellingen onderkend.” Hierbij worden China, Iran en Rusland als voornaamste statelijke actoren genoemd, waarbij de AIVD vaststelt dat de aanvallers op zoek waren naar zeer specialistische en soms zelfs experimentele technologie die zijn marktwaarde nog moet bewijzen. Niet genoemd in de AIVD/MIVD-rapportages zijn diensten in de VS en andere westerse mogendheden [9] die ook gretig gebruik maken van de mogelijkheden die het internet biedt om informatie te verzamelen, zowel bij vijandige staten als bij bondgenoten.

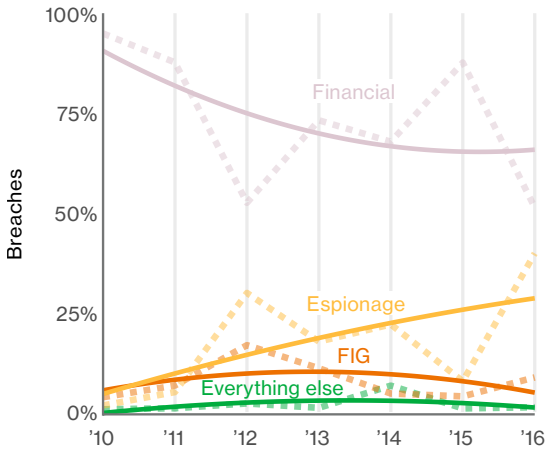
Politieke, militaire maar ook economische motieven

De motieven van statelijke actoren (inlichtingendiensten) beperken zich niet tot politieke beïnvloeding en het verkrijgen van militaire of staatgeheime informatie. Ook economische motieven spelen een grote rol. Door het verkrijgen van geheime (bedrijfs)informatie en intellectueel eigendom kunnen landen concurrentievoordeel behalen zonder dat daarvoor grote investeringen, bijvoorbeeld in onderzoek, in die landen nodig zijn.

> *“Met waardevolle informatie op technisch en wetenschappelijk gebied kunnen buitenlandse staten ook hun afhankelijkheid van kennis en producten uit het buitenland verminderen. Zo verbeteren zij hun economische concurrentiepositie of geopolitieke machtspositie, bijvoorbeeld door een versnelde modernisering van hun krijgsmacht.”* [4]

Moeilijk te traceren aanvallen

Statelijke actoren beschikken over veel middelen en grote kennis en kunde, en hun geavanceerde aanvallen zijn moeilijk te traceren. Volgens de AIVD/MIVD blijken bedrijven en instellingen onvoldoende te weten hoe zij zich tegen cyberspionage moeten wapenen [4] en daardoor zijn cyberaanvallen vaak succesvol. Daar komt bij dat veel organisaties niet eens weten dat ze slachtoffer zijn, totdat ze gewaarschuwd worden door bijvoorbeeld een inlichtingendienst [10].



Figuur 2: Motieven van actoren, waarbij FIG staat voor Fun, Ideology and Grudge (bron: Verizon – DBIR 2017 [38])

Geavanceerde infrastructuur aantrekkelijke doorvoerhaven voor aanvallen

De goedontwikkelde ICT-infrastructuur van ons land blijft aantrekkelijk als doorvoerhaven voor digitale aanvallen. De AIVD heeft diverse statelijke actoren geïdentificeerd die misbruik maken van onze infrastructuur voor aanvallen op derde landen. Hierdoor wordt Nederland ongewild betrokken bij de verspreiding van digitale aanvallen die een inbreuk vormen op de economische, militaire en politieke belangen van andere landen [7]. Binnen de al goedontwikkelde ICT-infrastructuur van Nederland is die van SURFnet zeer goed ontwikkeld. Deze is met 2 100 GE-poorten direct gekoppeld aan de AMS-IX, een van de grootste internetknooppunten van de wereld, en is daarmee zeer interessant voor verschillende typen cybercriminelen.

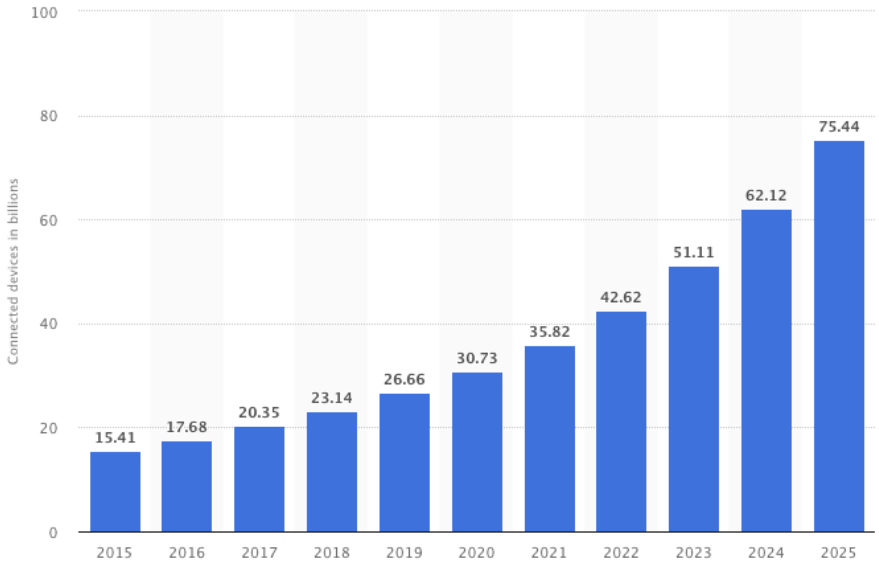
Conclusie

Uit de rapportage van de AIVD en MIVD blijkt dat in Nederland beroepscriminelen en statelijke actoren actief zijn bij allerlei organisaties. Ook internationale rapporten ondersteunen deze bevindingen. Het is dus belangrijk hierop voorbereid te zijn en ervoor te zorgen dat signalen die wijzen op dit soort activiteit, vroegtijdig onderkend worden.

3. OPKOMST EN GROEI VAN HET INTERNET OF THINGS

Grote securityproblemen

Het aantal IoT-apparaten blijft groeien en zal de komende jaren sterk toenemen, van ruim 20 miljard in 2017 tot, naar verwachting, meer dan 30 miljard in 2020 en zelfs meer dan 75 miljard in 2025 [11] [12]. Tegelijkertijd zijn de securityproblemen met IoT-apparaten immens. Ze bevatten kwetsbaarheden die niet of nauwelijks gepatcht worden en veel van die apparaten worden geleverd met een vast ingesteld wachtwoord of een (default) wachtwoord dat de gebruiker zou moeten veranderen. Maar de meeste gebruikers weten niet dat ze het wachtwoord moeten veranderen of hoe dat moet. Er zijn wel ideeën over het wettelijk afdwingen van betere beveiliging van IoT-apparaten of het instellen van een keurmerk (vergelijkbaar met KEMA-KEUR of de CE-markering), maar het is de vraag hoe effectief dit is in de huidige wereldwijde markt [13] [14] [15].



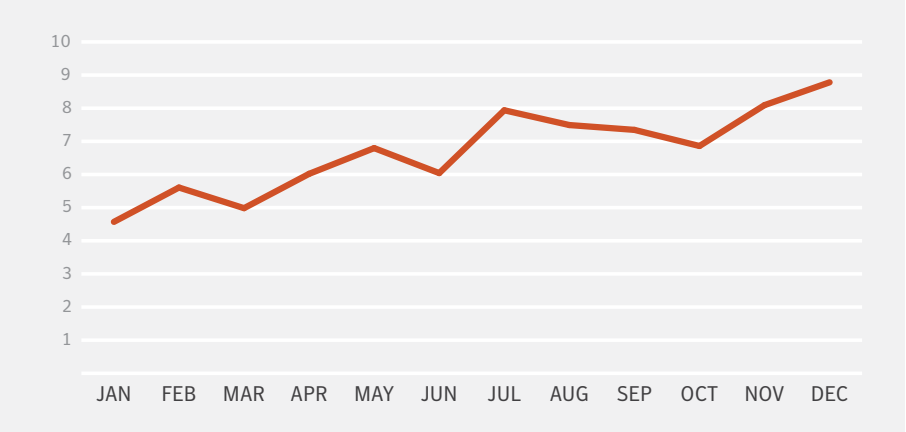
Figuur 3: Verwachte wereldwijde toename van IoT-apparaten tot 2025 (bron: Statista)

Verdubbeling aantal aanvallen

In een onderzoek van Symantec [16] blijkt dat er er bijna een verdubbeling is geweest in 2016 van het aantal aanvallen op IoT-apparaten (in een testomgeving). In januari werd per uur van gemiddeld 4,6 unieke IP-adressen een scan (mogelijke voorbode van een aanval) uitgevoerd, oplopend tot 8,8 in december (zie figuur 4). IoT-apparaten kunnen misbruikt worden als onderdeel van een botnet (Mirai), maar ook als opstapje ('stepping stone') dienen om andere systemen in een intern netwerk aan te vallen. Daarbij kunnen kwaadwillenden ook persoonsgegevens buitmaken.

IoT-apparaten extra kwetsbaar

Omdat IoT-apparaten minder goed beveiligd zijn dan laptops, desktopsystemen of servers, is het voor kwaadwillenden makkelijker om daarop met succes aanvallen uit te voeren.



Figuur 4: Aantal aanvallen per uur op IoT-apparaten (bron: Symantec – ISTR 22)

Conclusie

Er is een enorme toename van het aantal IoT-apparaten te verwachten en bovendien is er een toename van het aantal aanvallen op IoT-apparaten. Gecombineerd met de vooralsnog slechte beveiliging van deze apparaten zal dit een enorme verandering van het dreigingslandschap teweegbrengen, waarop instellingen moeten anticiperen.

4. WEERBAARHEID ONDERWIJS EN ONDERZOEK OP ORDE

Samenwerking nodig

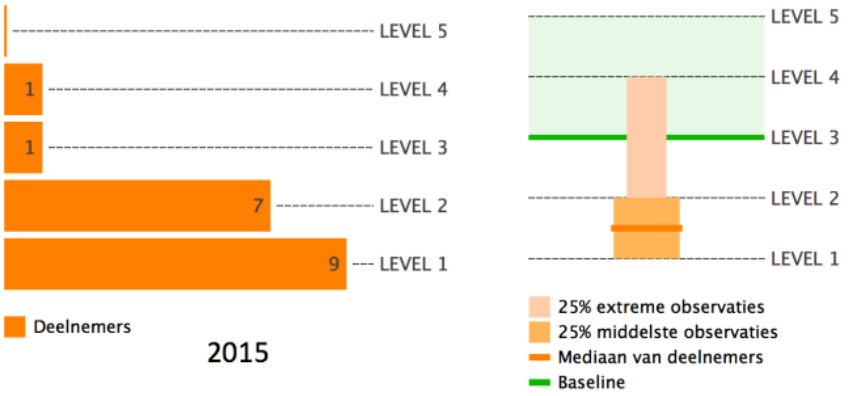
Recente incidenten illustreren dat het met de weerbaarheid van Nederlandse organisaties in het algemeen slecht gesteld is en dat er enorme kosten met incidenten gemoeid kunnen zijn [17] [18] [19] [20]. De toenemende digitalisering maakt iedereen kwetsbaarder voor cyberdreigingen. Er is daarom meer samenwerking tussen alle belanghebbenden nodig. De Cyber Security Raad [24] en de Wetenschappelijke Raad voor het Regeringsbeleid [22] benadrukken in hun adviezen aan de regering het belang van samenwerking. In september 2017 heeft minister Kamp aangekondigd dat er in 2018 een Digital Trust Centre wordt opgericht, om bedrijven te helpen weerbaarder te worden tegen cyberdreigingen [23]. Verder coördineert het NCSC al enige tijd het Nationaal Detectie Netwerk [24] dat als doel heeft om schade ten gevolge van digitale gevaren en risico's te beperken of voorkomen door het delen van dreigingsinformatie.

Bij instellingen voor onderwijs en onderzoek die zijn aangesloten bij SURF bestaan al samenwerkingsverbanden op verschillende niveaus. Er zijn community's om informatie uit te wisselen, zoals SCIRT (uitvoerend) [25] en SCIPR (beleidsmatig) [25] en er zijn diensten zoals SURFcert [26], SURFaudit [27] en Cybersave Yourself [28] om informatiebeveiliging bij instellingen op een hoger peil te brengen.

Uit statistieken van SURFcert en discussies in de SCIRT-community blijkt dat de weerbaarheid van instellingen voor onderwijs en onderzoek behoorlijk op orde is. Er wordt bijvoorbeeld snel informatie uitgewisseld als er sprake is van een malware-uitbraak waardoor andere, nog niet getroffen instellingen alvast maatregelen kunnen nemen.

Awareness kan beter

Een van de uitkomsten van de SURFaudit-benchmark 2015 [29] was dat er op het vlak van informatiebeveiligingsbewustzijn wel nog veel winst te behalen valt. Bijvoorbeeld maatregel 7.2.2 "Alle medewerkers van de organisatie en, voor zover relevant, contractanten krijgen een passende bewustzijnsopleiding en -training en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie" uit het normenkader Informatiebeveiliging HO 2015 scoorde ruim onder de baseline:



Figuur 5: Detailscore uit SURFaudit-benchmark 2015 - maatregel 7.2.2

Conclusie

De instellingen voor onderwijs en onderzoek lijken het beter te doen dan Nederlandse organisaties in het algemeen op het vlak van digitale weerbaarheid. In deze sector bestaan ook al een aantal samenwerkingsverbanden die de weerbaarheid moeten vergroten. Toch blijkt dat er ook nog ruimte is voor verbetering bij de instellingen voor onderwijs en onderzoek, met name op het gebied van awareness.

5. TOENEMENDE DIGITALISERING

Bring Your Own Device

De samenleving wordt steeds meer afhankelijk van digitale informatietechnologie. Iedere Nederlander heeft langzamerhand een of meer apparaten die (min of meer) permanent aangesloten zijn op het internet. Studenten, docenten, onderzoekers en andere medewerkers van onderwijs- en onderzoeksinstellingen maken steeds vaker gebruik van eigen apparaten. Dit BYOD-concept (Bring Your Own Device) maakt het mogelijk met eigen devices verbinding te maken met systemen waarop mogelijk gevoelige informatie staat.

Gevoelige informatie goed beveiligen

De uitdaging voor instellingen is om gevoelige informatie goed te beveiligen en alleen toegang te verlenen wanneer dat toegestaan is aan de gebruiker, en om ervoor te zorgen dat die informatie op de juiste manier gebruikt wordt.

Vragen die daarbij horen zijn: hoeveel en welke data mag een instelling verzamelen, hoe moeten die data beschermd worden, hoe lang moeten – of mogen – die data bewaard worden, wie krijgt er toegang tot die data en waarvoor mogen die data gebruikt worden?

Zo ontstaan er allerlei initiatieven om die schijnbaar tegenstrijdige eisen met elkaar te verzoenen. TNO bijvoorbeeld werkt aan TrustTester [30] voor het veilig valideren van persoonlijke gegevens en de stichting Privacy by Design [31] beheert IRMA (I reveal My Attributes), dat beoogt relevante eigenschappen van jezelf aan anderen te bewijzen op een privacyvriendelijke manier.

Er zijn mogelijk (juridische) complicaties: wie is er verantwoordelijk bij verlies van een privé-apparaat of als het geïnfecteerd raakt met een virus? Mag de instelling het apparaat dan bijvoorbeeld wissen om te voorkomen dat gevoelige informatie op straat komt te liggen?

Wellicht is dit bij docenten, onderzoekers en andere medewerkers nog te overzien, bijvoorbeeld door apparaten door de instelling te laten verstrekken. Bij studenten ligt dit al een stuk lastiger, terwijl die toch ook toegang hebben tot gevoelige informatie.

Algemene verordening gegevensbescherming

Er is nieuwe wetgeving gekomen die de gevolgen van informatiebeveilings-problemen kan verergeren. Zo is op 1 januari 2016 de meldplicht datalekken van kracht geworden met een nieuwe toezichthouder die hoge boetes kan uitdelen om krachtig op te treden tegen overtreders [32]. In Europa is in 2016 de Algemene verordening gegevensbescherming (AVG – Regulation (EU) 2016/679) ingevoerd. Die vervangt op 25 mei 2018 de Wet bescherming persoonsgegevens (Wpb), na een overgangsperiode van twee jaar, en wordt dan ook van kracht in alle EU-lidstaten. Daarmee wordt het boeteplafond substantieel verhoogd. Extra organisatorische en technische maatregelen zijn dan ook vereist om persoonsgegevens adequaat te beschermen.

Door alle media-aandacht voor de AVG zijn privacy en informatiebeveiliging bij alle overheden, bedrijven en instellingen scherp op het netvlies komen te staan. Organisaties zijn druk bezig zich goed voor te bereiden op 25 mei 2018.

Maar deze wet maakt informatiebeveiliging nog gecompliceerder: als persoonsgegevens op straat komen te liggen is de organisatie daarvoor waarschijnlijk verantwoordelijk en kunnen flinke boetes worden opgelegd door de Autoriteit Persoonsgegevens.

Figuur 6: Ook bij SURF tellen we af tot de AVG van kracht wordt (foto 3 november 2017)

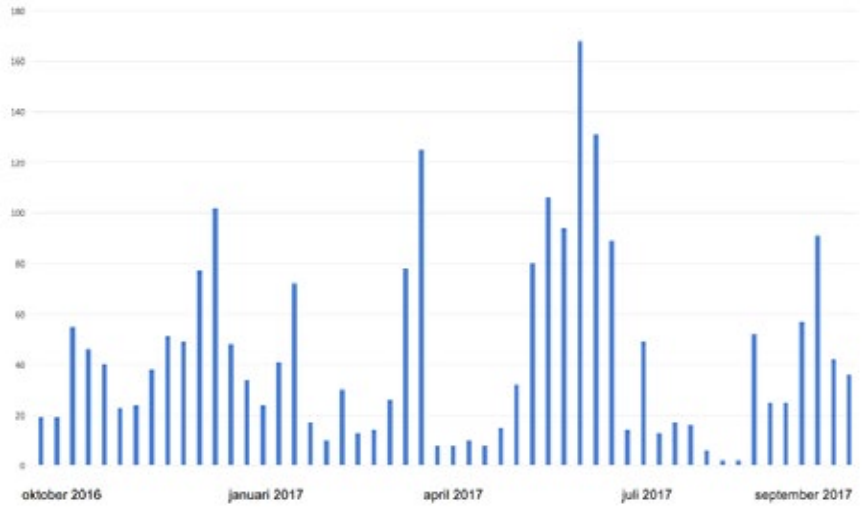
Conclusie

Het beschermen van gevoelige data wordt complexer. Dit komt door het toenemende gebruik van privé-apparaten voor toegang tot mogelijk gevoelige informatie van onderwijs- en onderzoeksinstellingen, en door de daarmee gepaard gaande vermenging van persoonlijke en bedrijfsdata. Bovendien vereist het van kracht worden van de AVG een benadering van gegevensbescherming die rekening houdt met de specifieke eisen die aan persoonsgegevens worden gesteld.

6. DENIAL-OF-SERVICE-AANVALLEN GAAN OVERMINDERD DOOR

Gevolgen goed te overzien

Uit gegevens van SURFcert blijkt dat, hoewel denial-of-serviceaanvallen onverminderd doorgaan, de gevolgen ervan goed te overzien zijn. Het totaal aantal meldingen dat bij SURFcert wordt geregistreerd, neemt niet structureel toe. In 2016 was het gemiddelde aantal meldingen per week ruim 50, terwijl in dezelfde periode van 2017 het gemiddelde bijna 45 per week was. De gevolgen van al die meldingen zijn minimaal.



Figuur 7: Aantal DDoS meldingen per week – bron: SURFcert

In de grafiek valt op dat vooral de maanden april/mei en juli/augustus aanmerkelijk rustiger zijn dan de rest van het jaar. Deze periodes vallen samen met respectievelijk de meivakantie en de zomervakantie, ook opvallend is de piek voor de zomervakantie. Dit wijst erop dat veel denial-of-serviceaanvallen door studenten worden uitgevoerd.

Aanvallen tegen lage kosten uit te voeren

De opkomst van zogenaamde booter of stresser services, DDoS as a Service, maakt het steeds makkelijker dit soort aanvallen tegen lage kosten uit te voeren. Er is daarvoor nog amper eigen kennis nodig, een betaling met creditcard of bitcoin is al voldoende [33] [34].

Conclusie

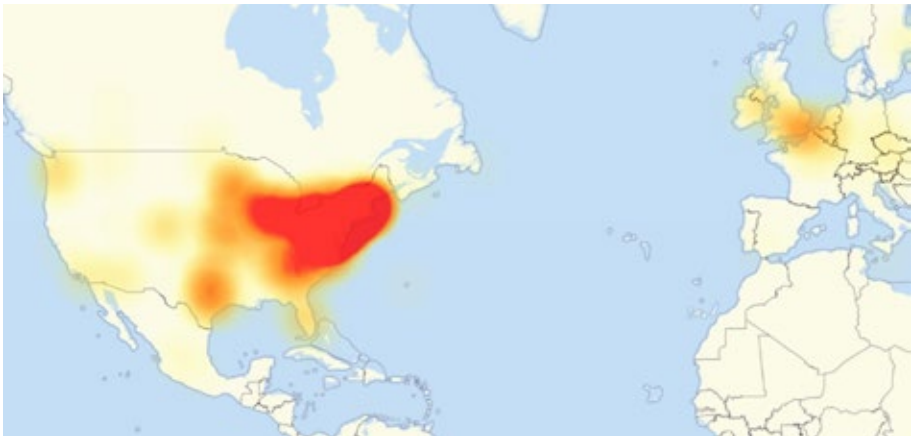
Denial-of-serviceaanvallen zijn een blijvend verschijnsel dat echter redelijk onder controle is, ondanks de mogelijkheden voor kwaadwillenden om gebruik te maken van goedkope diensten die weinig kennis en kunde vereisen om een aanval uit te voeren. Het is echter wel belangrijk om alert te blijven en ervoor te zorgen dat mitigerende maatregelen effectief zijn en blijven.

7. KWETSBAARHEDEN BLIJVEN PROBLEMATISCH

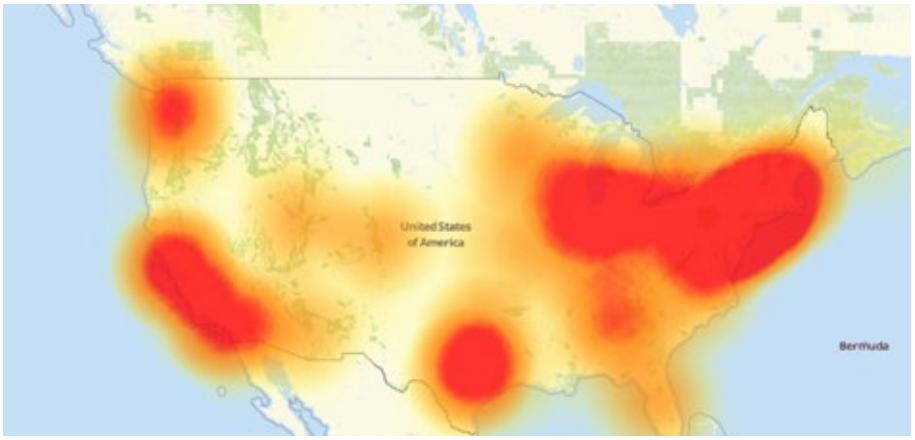
Kwetsbaarheden in besturingssystemen én IoT-apparaten

In de grote besturingssystemen (Windows, macOS en Linux) worden ieder jaar veel softwarekwetsbaarheden gevonden. Maar ook IoT-apparaten bevatten veel kwetsbaarheden. De gaten in de grote besturingssystemen worden regelmatig gedicht (patching), maar bij IoT-apparaten gebeurt dit nauwelijks. Bovendien bevatten IoT-apparaten veel configuratiefouten die niet of moeilijk te herstellen zijn voor de gebruiker. En doordat er veel IoT-apparaten zijn, kan misbruik van zo'n kwetsbaarheid een enorm effect hebben. Dit gebeurde bijvoorbeeld in 2016 met het Mirai-botnet dat eind 2016 de website van Brian Krebs platlegde [35]. Dit botnet werd ook gebruikt bij de Dyn-attack in oktober 2016, waardoor een aantal grote internetdiensten zoals Paypal, Twitter, Spotify en Github onbereikbaar waren [36].

Onderstaande illustraties geven aan welke regio's last hadden van de Dyn-attack en laten zien dat de tweede aanval in de VS veel heftiger was. Dit is gemeten op het netwerk van Level3, een van 's werelds grootste internetproviders.



Figuur 8: Internetproblemen op 21 oktober 2016 's ochtends als gevolg van de eerste DDoS-aanval op Dyn (bron: Threatpost)



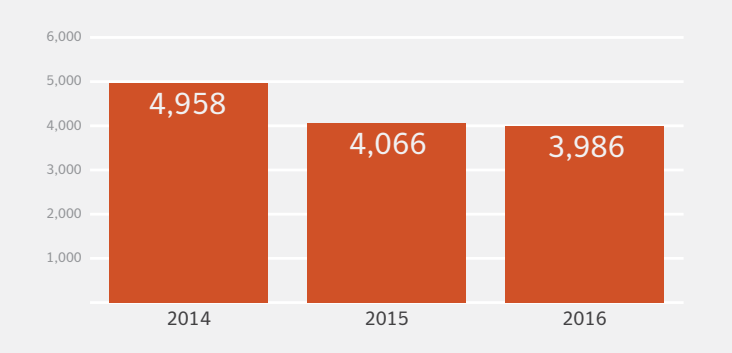
Figuur 9: Internetproblemen op 21 oktober 2016 's avonds als gevolg van de tweede DDoS-aanval op Dyn (bron: Threatpost)

Zero-daykwetsbaarheden

Van oudsher proberen criminelen en statelijke actoren onbekende en nog niet gepatchte kwetsbaarheden, zogenaamde zero-daykwetsbaarheden, te gebruiken om systemen binnen te dringen [9].

Een voorbeeld hiervan is de EternalBlue-exploit die is gebruikt in de Wannacry-ransomwareaanval van mei 2017 en later de NotPetya-aanval. Naar verluidt is de EternalBlue-exploit ontwikkeld door de Amerikaanse NSA [37].

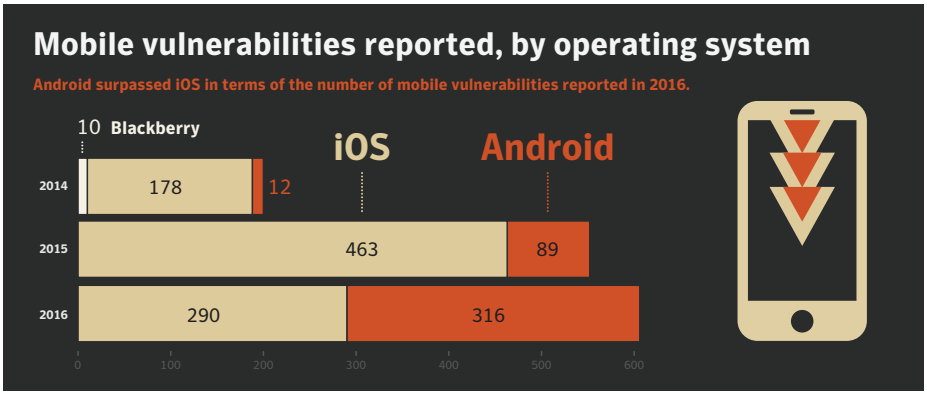
Volgens Symantec is er in 2016 wel een lichte daling van het aantal zero-daykwetsbaarheden geweest, mogelijk als gevolg van responsible-disclosureprogramma's en verbeterde softwareontwikkeling. Symantec veronderstelt dat zero-daykwetsbaarheden daardoor wat moeilijker zijn te vinden voor kwaadwillenden en dat ze daarom andere, makkelijkere, manieren zijn gaan gebruiken om aanvallen uit te voeren [16].



Figuur 10: Aantal zero-daykwetsbaarheden per jaar (bron: Symantec – ISTR 22)

Kwetsbaarheden van mobiele apparaten

Een punt van zorg is de toename van het aantal kwetsbaarheden op mobiele apparaten zoals smartphones en tablets. Omdat studenten, docenten, onderzoekers en andere medewerkers steeds meer gebruik willen en mogen maken van deze apparaten, is dit een groeiende bedreiging voor onderwijs en onderzoek. De meeste smartphones en tablets worden niet centraal beheerd en zijn onderdeel van een BYOD-beleid (Bring Your Own Device). Dit is een enorme uitdaging voor het effectief beveiligen van gevoelige data in studentinformatiesystemen zoals Osiris en EduArte.



Figuur 11: Toename van kwetsbaarheden in mobiele besturingssystemen (bron Symantec – ISTR 22)

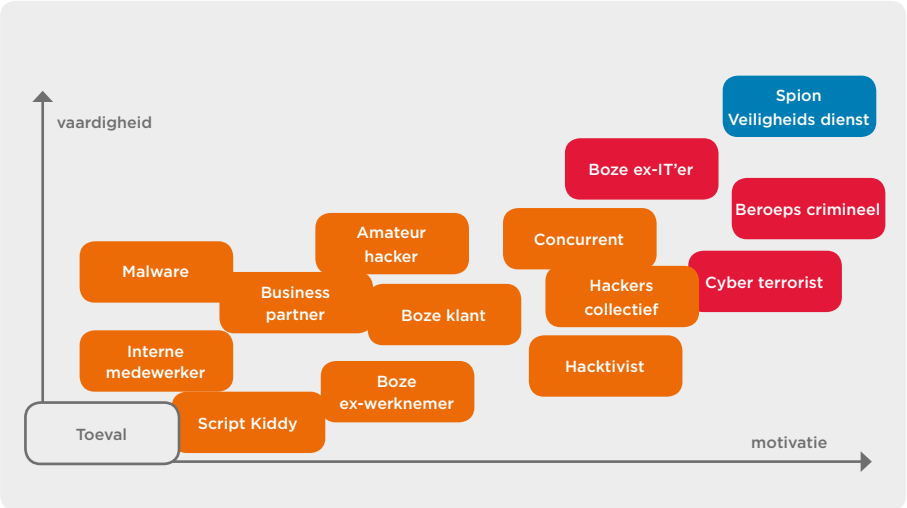
Conclusie

Kwaadwillenden maken nog veelvuldig gebruik van kwetsbaarheden in software, hoewel er een lichte daling is van zero-daykwetsbaarheden. Het patchen van kwetsbaarheden gebeurt nog steeds te weinig en te laat. Hierdoor lopen instellingen grote risico's die ze goed in kaart moeten brengen om ze te kunnen tegengaan.

8. AANVALLERS

Verschillende motieven en vaardigheidsniveaus

Actoren, die verschillende motieven en vaardigheidsniveaus hebben, zijn verantwoordelijk voor het uitvoeren van aanvallen:



Figuur 12: Vaardigheid en motivatie van actoren

Voor de sector onderwijs en onderzoek spelen zes actoren een rol, hier qua vaardigheden en motieven van laag tot zeer hoog gerangschikt:

1. **Medewerkers – vaardigheid: laag**
   Medewerkers zijn gebaat bij goede evaluaties en prestaties; het manipuleren van HR-dossiers kan daarom voor hen interessant zijn. Door dreigend ontslag of een reorganisatie kunnen medewerkers uit rancune schade toebrengen. Sommige medewerkers zijn in potentie zeer vaardig en ze hebben al toegang tot systemen en netwerken. Andere medewerkers zijn zich vaak niet bewust van dreigingen op het gebied van cybersecurity, waardoor ze slordig omgaan met gevoelige informatie. Ze worden in een aantal gevallen meer gedreven door efficiëntie en gemak.

2. **Studenten – vaardigheid: laag tot gemiddeld**
   Studenten zijn gebaat bij een goede studievoortgang, daarom kan het manipuleren van studieresultaten voor hen interessant zijn. Ze hebben al toegang tot veel systemen en netwerken en sommigen zijn zeer vaardig. Veel studenten zijn zich vaak niet bewust van dreigingen op het gebied van cybersecurity, waardoor ze slordig omgaan met gevoelige informatie.

3. **Activisten en cybervandalen – vaardigheid: laag tot gemiddeld**
   Activisten beschikken over behoorlijke kennis en vaardigheden om data te stelen of systemen en netwerken ontoegankelijk te maken. Bovendien is er een grote kans dat ze buitgemaakte data publiceren. Cybervandalen zijn op zoek naar erkenning binnen hun eigen groep en zoeken soms een groot publiek om hun acties te laten zien. Cyberjihadisten zijn erop uit gevoelige data te vergaren om die vervolgens te publiceren uit propaganda overwegingen.

4. **Concurrenten – vaardigheid: laag tot gemiddeld**
   Commerciële partijen zijn gebaat bij het vroegtijdig verkrijgen van informatie van concurrenten. Hetzelfde kan gelden voor rivaliserende partnerinstellingen die bijvoorbeeld geïnteresseerd zijn in elkaars onderzoeksdata. Kennis en kunde zijn aanwezig, maar die zullen in het algemeen niet gauw worden ingezet tegen collega-instellingen.

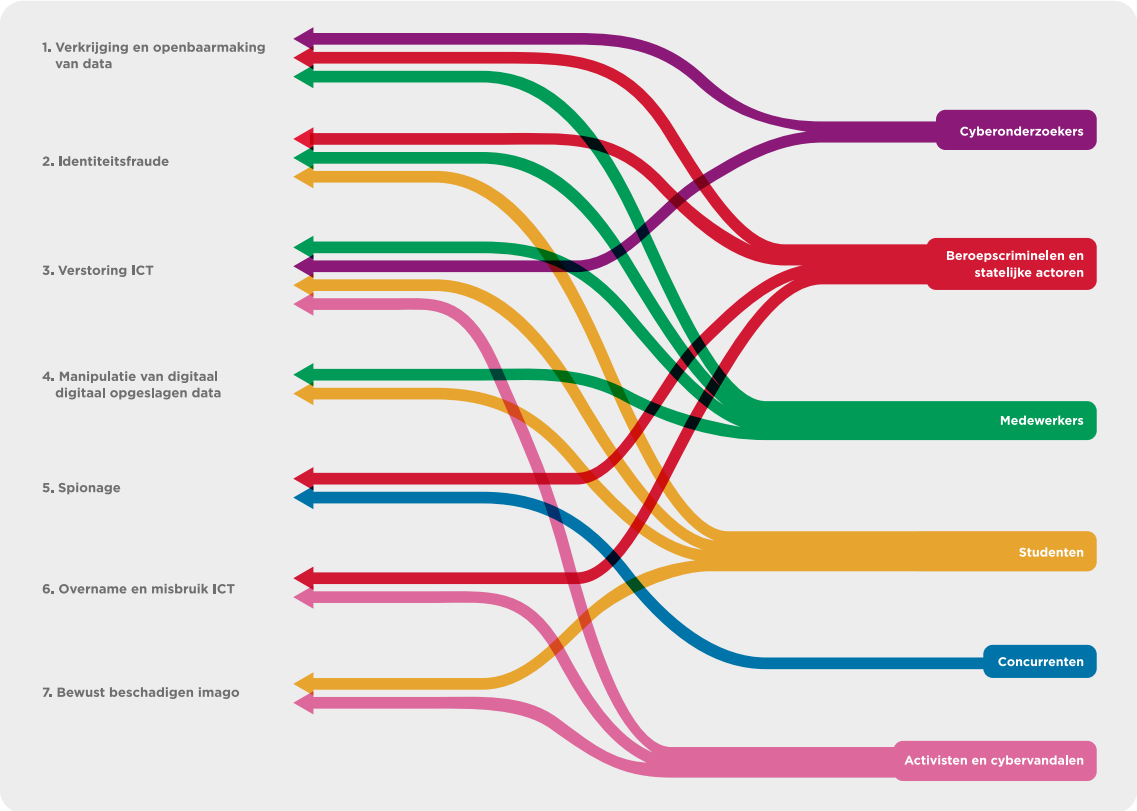
5. **Cyberonderzoekers – vaardigheid: hoog**
   Cyberonderzoekers zijn in feite hackers, maar handelen met een goed doel. Als ze problemen vinden, zullen ze in het algemeen de betreffende instelling waarschuwen (responsible disclosure). Ze zijn zeer vaardig en handelen niet altijd in overeenstemming met de wensen van de instelling.

6. **Beroepscriminelen en statelijke actoren – vaardigheid: hoog tot zeer hoog**
   Beroepscriminelen zijn vooral gedreven door financieel gewin. Ze verkopen gestolen data of proberen losgeld te innen door data tijdelijk ontoegankelijk te maken. Ze organiseren zich in toenemende mate, zodat hun kans van slagen groter wordt.

   In het kader van terrorisme- en misdaadbestrijding worden veel data verzameld, maar ook bedrijfseconomische motieven (geïnteresseerd in intellectueel eigendom en innovatieve kennis) kunnen een drijfveer zijn voor buitenlandse inlichtingendiensten.

Invloed van actoren op dreigingen

Onderstaande afbeelding laat zien op welke dreigingen (zie tabel 1, pagina 5) de verschillende actoren een effect hebben:



Figuur 13: Invloed van actoren op dreigingen

Conclusie

Er zijn veel verschillende typen aanvallers, van script kiddies tot beroepscriminelen en statelijke actoren. Terwijl onschuldige aanvallen door bijvoorbeeld script kiddies niet meer dan vervelend zijn, kunnen aanvallen door beroepscriminelen aanzienlijke schade aanrichten. Omdat vooral de geavanceerde aanvallen door beroepscriminelen en statelijke actoren moeilijk te detecteren zijn, moeten instellingen ook geavanceerdere middelen inzetten om zich hiertegen te wapenen.

BRONNEN

[1] NCSC, „Cybersecuritybeeld Nederland," 21 06 2017. [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2017.html. [Geopend 29 09 2017].

[2] VSNU, „VSNU Publicaties," 5 september 2016. [Online]. Available: http://www.vsnu.nl/files/documenten/Publicaties/VSNU_De_Digitale_Samenleving.pdf. [Geopend 29 09 2017].

[3] B. Bosma, „SURF | Cybedreigingsbeeld 2016 - SURFnet," 17 11 2016. [Online]. Available: https://www.surf.nl/kennisbank/2016/cyberdreigingsbeeld-2016.html. [Geopend 27 10 2017].

[4] AIVD, „Bent u zich bewust van de risico's van cyberspionage?," 22 05 2017. [Online]. Available: https://www.aivd.nl/actueel/nieuws/2017/05/22/bent-u-zich-bewust-van-de-risicos-van-cyberspionage. [Geopend 10 08 2017].

[5] SURF, „SURFnet Community van Incident Response Teams (SCIRT)," [Online]. Available: https://www.surf.nl/diensten-en-producten/scirt/index.html. [Geopend 29 09 2017].

[6] Microsoft, „TN New ransomware, old techniques: Petya adds worm capabilities," 27 06 2017. [Online]. Available: https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/. [Geopend 29 09 2017].

[7] AIVD, „Jaarverslag 2016: dreiging voor Nederland onverminderd hoog," 04 04 2017. [Online]. Available: https://www.aivd.nl/actueel/nieuws/2017/04/04/jaarverslag-2016-dreiging-voor-nederland-onverminderd-hoog. [Geopend 29 09 2017].

[8] AIVD, „Jaarverslag AIVD 2015," 21 04 2016. [Online]. Available: https://www.aivd.nl/publicaties/jaarverslagen/2016/04/21/jaarverslag-aivd-2015. [Geopend 29 09 2017].

[9] The Guardian, „The Snowden Files," 02 12 2013. [Online]. Available: https://www.theguardian.com/world/2013/dec/02/nsa-files-spying-allies-enemies-five-eyes-g8. [Geopend 29 09 2017].

[10] AIVD, „Speech Rob Bertholee symposium iBestuur 'Grip op cybersecurity'," 22 05 2017. [Online]. Available: https://www.aivd.nl/publicaties/toespraken/2017/05/22/speech-rob-bertholee-symposium-ibestuur-grip-op-cybersecurity. [Geopend 29 09 2017].

[11] Statista, „IoT: number of connected devices worldwide 2012-2025," 11 10 2017. [Online]. Available: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. [Geopend 11 10 2017].

[12] Juniper, „IoT Connected Devices to Triple to Over 38Bn Units," 28 07 2017. [Online]. Available: https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020. [Geopend 11 10 2017].

[13] NRC-Handelsblad, „D66 wil keurmerk voor beveiliging IoT-apparaten," 20 11 2016. [Online]. Available: https://www.nrc.nl/nieuws/2016/11/20/d66-wil-keurmerk-voor-beveiliging-iot-apparaten-a1532668. [Geopend 29 09 2017].

[14] Domotica.nl, „Chipgiganten sporen EU aan om Internet of Things-keurmerk in te voeren," 07 06 2017. [Online]. Available: https://domotica.nl/2017/06/07/chipgiganten-richtlijnen-iot/. [Geopend 29 09 2017].

[15] NEN, „NEN richt normcommissie Internet of Things ('IoT') op," 03 10 2017. [Online]. Available: https://www.nen.nl/NEN-Shop/ICTnieuwsberichten/NEN-richt-normcommissie-Internet-of-Things-IoT-op.htm. [Geopend 10 10 2017].

[16] Symantec, „Internet Security Threat Report," 04 2017. [Online]. Available: https://www.symantec.com/security-center/threat-report. [Geopend 24 10 2017].

[17] Tweakers, „Ook Q-park krijgt te maken met aanval van ransomware," 14 05 2017. [Online]. Available: https://tweakers.net/nieuws/124649/ook-q-park-krijgt-te-maken-met-aanval-van-ransomware.html. [Geopend 27 10 2017].

[18] Deloitte, „Cyber Value at Risk in The Netherlands 2017," 25 09 2017. [Online]. Available: https://www2.deloitte.com/nl/nl/pages/risk/articles/cyber-value-at-risk-in-the-netherlands-2017.html. [Geopend 29 09 2017].

[19] Tweakers, „Aanval met NotPetya-malware kost Maersk tot 256 miljoen euro," 16 08 2017. [Online]. Available: https://tweakers.net/nieuws/128411/aanval-met-notpetya-malware-kost-maersk-tot-256-miljoen-euro.html. [Geopend 27 10 2017].

[20] Tweakers, „Minstens vier ziekenhuizen in Verenigd Koninkrijk getroffen door malware," 14 01 2017. [Online]. Available: https://tweakers.net/nieuws/120059/minstens-vier-ziekenhuizen-in-verenigd-koninkrijk-getroffen-door-malware.html. [Geopend 27 10 2017].

[21] CSR, „CSR Advies," 06 2017. [Online]. Available: https://www.cybersecurityraad.nl/binaries/CSR-advies%202017%20nr.%202%20-%20Naar%20een%20lande-lijk%20dekkend%20stelsel%20van%20informatieknooppunten_tcm56-269317.pdf. [Geopend 29 09 2017].

[22] WRR, „Veiligheid in een wereld van verbindingen," 10 05 2017. [Online]. Available: https://www.wrr.nl/publicaties/rapporten/2017/05/10/veiligheid-in-een-wereld-van-verbindingen. [Geopend 29 09 2017].

[23] Rijksoverheid, „Kamerbrief over oprichting Digital Trust Centre," 23 09 2017. [Online]. Available: https://www.rijksoverheid.nl/documenten/kamerstukken/2017/09/23/kamerbrief-oprichting-van-een-digital-trust-centre. [Geopend 29 09 2017].

[24] NCSC, „Nationaal Detectie Netwerk | NCSC," [Online]. Available: https://www.ncsc.nl/samenwerking/nationaal-detectie-netwerk.html. [Geopend 24 09 2017].

[25] SURF, „SCIPR - community voor informatiebeveiligers en privacy officers," [Online]. Available: https://www.surf.nl/diensten-en-producten/scipr/index.html. [Geopend 29 09 2017].

[26] SURF, „SURFcert," [Online]. Available: https://www.surf.nl/diensten-en-producten/surfcert/index.html. [Geopend 24 09 2017].

[27] SURFaudit, „SURFaudit," [Online]. Available: https://www.surf.nl/diensten-en-producten/surfaudit/index.html. [Geopend 24 09 2017].

[28] SURF, „Cyber Save Yourself," [Online]. Available: https://www.cybersaveyourself.nl/. [Geopend 24 09 2017].

[29] B. Bosma, „Rapport Resultaten SURFaudit benchmark 2015," SURF, 09 06 2016. [Online]. Available: https://www.surf.nl/kennisbank/2016/resultaten-surfaudit-benchmark-2015.html. [Geopend 24 09 2017].

[30] TNO, „TrustTester: veilig valideren van persoonlijke gegevens," 2016. [Online]. Available: https://www.tno.nl/nl/aandachtsgebieden/industrie/networked-information/information-creation-van-data-naar-informatie/trusttester-veilig-valideren-van-persoonlijke-gegevens/. [Geopend 29 09 2017].

[31] Stichting Privacy by Design, „Privacy by Design Foundation," 2016. [Online]. Available: https://privacybydesign.foundation/. [Geopend 29 09 2017].

[32] Overheid.nl, „Boetebeleidsregels Autoriteit Persoonsgegevens 2016," 2016. [Online]. Available: http://wetten.overheid.nl/BWBR0037543/2016-01-16. [Geopend 29 09 2017].

[33] A. Orlowski, „Meet DDoSaaS," The Register, 12 09 2016. [Online]. Available: https://www.theregister.co.uk/2016/09/12/denial_of_service_as_a_service/. [Geopend 27 10 2017].

[34] D. Smith, „The Growth of DDoS-as-a-Service: Stresser Services," Radware, 18 09 2017. [Online]. Available: https://blog.radware.com/security/2017/09/growth-of-ddos-as-a-service-stresser-services/. [Geopend 27 10 2017].

[35] C. Osborne, „Krebs on Security booted off Akamai network after DDoS attack proves pricey," ZDNET, 23 09 2016. [Online]. Available: http://www.zdnet.com/article/krebs-on-security-booted-off-akamai-network-after-ddos-attack-proves-pricey/. [Geopend 24 10 2017].

[36] L. Franceschi-Bicchierai, „Blame the Internet of Things for Destroying the Internet Today," Motherboard, 21 10 2016. [Online]. Available: https://motherboard.vice.com/en_us/article/vv7xg9/blame-the-internet-of-things-for-destroying-the-internet-today. [Geopend 24 10 2017].
[37] B. Krebs, „Eternal Blue - Krebs on Security," 17 06 2017. [Online]. Available: https://krebsonsecurity.com/tag/eternal-blue/. [Geopend 27 10 2017].
[38] Verizon, „2017 Data Breach Investigations Report," Verizon, 2017.

COLOFON

Auteur
Bart Bosma

Redactie
Jan Michielsen

Ontwerp
Vrije Stijl, Utrecht

Fotografie
iStock

December 2017

SURF

+31 (0)88 787 30 00
www.surf.nl

INTEGRALE
VEILIGHEID
HOGER ONDERWIJS