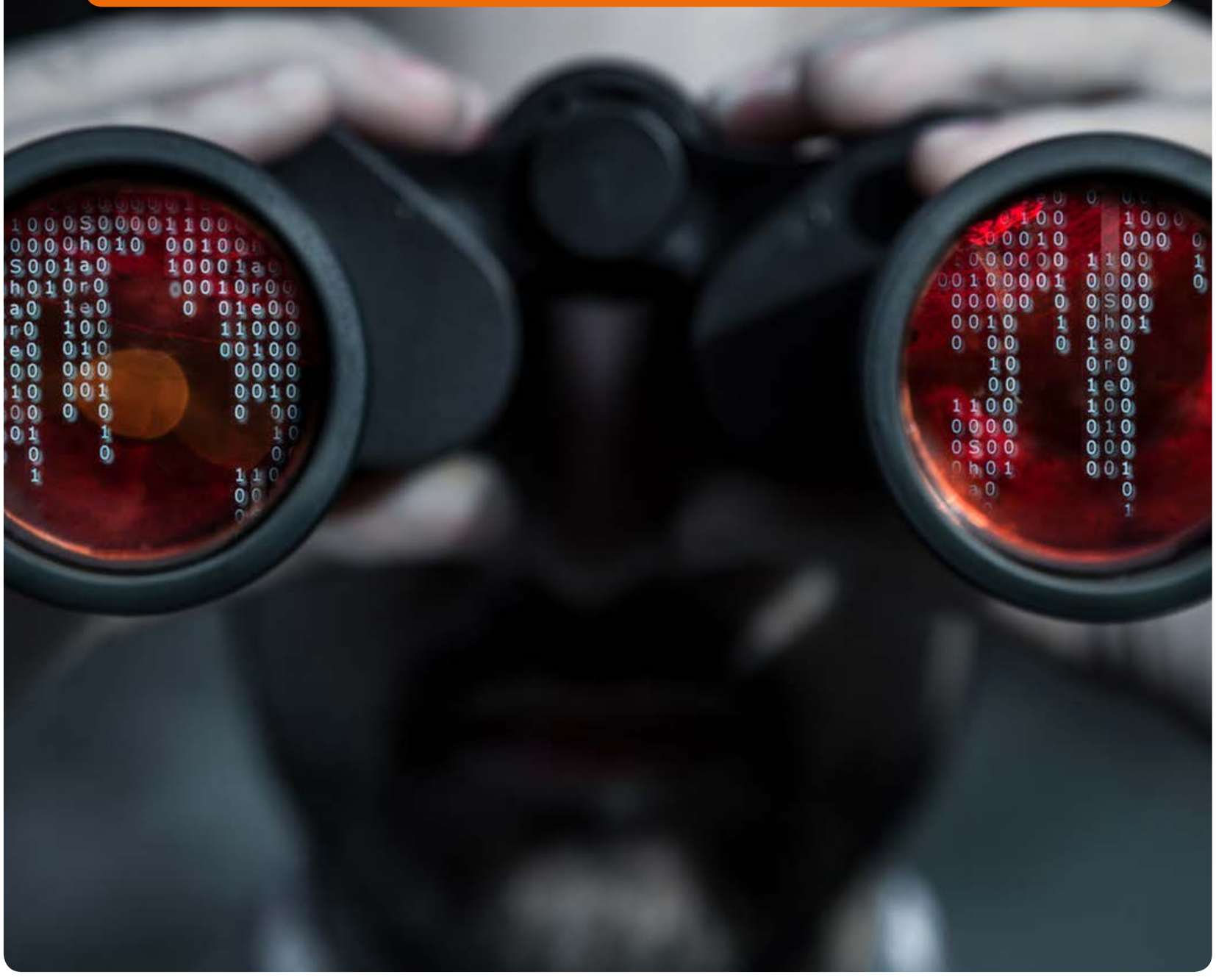
CYBERDREIGINGSBEELD 2016

SECTOR ONDERWIJS EN ONDERZOEK



INHOUDSOPGAVE

SURF

VOORWOORD

De meldplicht datalekken die op 1 januari 2016 van kracht is geworden, stond hoog op de agenda van security en privacy officers in onderwijs en onderzoek. Toch leek het of niemand zich vooraf realiseerde dat de nieuwe meldplicht zoveel gevolgen zou hebben voor het omgaan met persoonsgegevens en voor de wijze waarop die beschermd moeten worden.

Verder heeft de Autoriteit Persoonsgegevens (voorheen het College Bescherming Persoonsgegevens) sinds 1 januari 2016 de bevoegdheid om flinke boetes uit te delen aan overtreders. In dat opzicht is de Europese Algemene Verordening Gegevensbescherming, die medio 2018 van kracht wordt, de volgende horde die genomen moet worden. Dan gelden nog strengere eisen voor de bescherming van persoonsgegevens en worden bij overtreding van de verordening nog zwaardere boetes uitgedeeld.

Tegelijkertijd hebben we in de sector onderwijs en onderzoek een enorme stijging van het aantal ransomwareaanvallen gezien, die tot een datalek kunnen leiden. Datalekken moeten gemeld worden aan de Autoriteit Persoonsgegevens, maar dit gebeurt volgens diezelfde autoriteit nog veel te weinig, gezien het aantal verwerkers van persoonsgegevens in Nederland.

Cybersecurity staat volop in het nieuws en ook de bij SURF aangesloten instellingen ontkomen er niet aan goed na te denken over wat zij moeten doen om hun cyberweerbaarheid op een hoger peil te brengen en zo de kans op reputatie- en financiële schade zo laag mogelijk te houden. De cybercrisisoefening Ozon die SURF in oktober heeft gehouden, laat zien dat onderwijs en onderzoeksinstellingen serieus bezig zijn met cybersecurity. Meer dan 200 medewerkers van 30 aangesloten instellingen namen deel aan de oefening. De oefening toont aan dat de instellingen goed zijn voorbereid op aanvallen en dat de betrokkenen binnen hun eigen organisatie snel weten op te schakelen tot het bestuurlijk niveau. Instellingen realiseren zich door de oefening meer dan ooit dat een cybercrisis realistisch is en een grote impact op het primaire proces kan hebben.

Om onderwijs- en onderzoeksinstellingen inzicht te geven in de belangrijkste bedreigingen voor de sector, en om duidelijk te maken welke maatregelen u zou kunnen nemen om genoemde bedreigingen tegen te gaan is het voor u liggende Cyberdreigingsbeeld samengesteld.

Erik Fledderus
Algemeen directeur SURF

SAMENVATTING

Meer aandacht voor cybersecurity

De maatschappij heeft steeds meer aandacht voor cybersecurity. Naast het op 5 september 2016 verschenen Cybersecuritybeeld Nederland van het Nationaal Cyber Security Centrum (NCSC) zijn er het afgelopen jaar diverse rapporten verschenen die het belang van weerbaarheid op het gebied van cybersecurity benadrukken. Ook bij de bestuurders van onderwijs- en onderzoeksinstellingen leeft het onderwerp. Dit komt mede door de invoering van de meldplicht datalekken (artikel 34a, Wbp) op 1 januari 2016.

Weerbaarheid vergroten

Dit rapport laat zien welke dreigingen in het cyberdomein, onze digitale wereld, relevant zijn voor de onderwijs- en onderzoeksinstellingen en biedt zo handvatten voor de instellingen om hun weerbaarheid te vergroten.

Risico's zo klein mogelijk maken

De reputatieschade of financiële schade veroorzaakt door een cyberaanval kan zeer ingrijpend zijn en het is dan ook van belang de risico's zo klein mogelijk te maken. In figuur 1 staan de dreigingen die relevant zijn voor onderwijs- en onderzoeksinstellingen:

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	MIDDEN
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

Meest voorkomende dreigingen

Onderwijs

Voor het onderwijsproces is de kans op manifestatie van de volgende dreigingen het grootst:

- *Manipulatie van digitaal opgeslagen data*
  Hierbij gaat het vooral om studieresultaten en toetsmateriaal. Maatregelen om manipulatie tegen te gaan maken gebruik van cryptografische technieken, om de integriteit en vertrouwelijkheid van de gegevens te waarborgen.

- *Identiteitsfraude*
  Met het toenemen van digitale vormen van onderwijs en toetsing wordt het steeds belangrijker om iemands identiteit onomstotelijk vast te kunnen stellen. Als daarover geen grote mate van zekerheid is, kan ongeautoriseerde toegang worden verkregen, waardoor het bijvoorbeeld mogelijk wordt cijfers aan te passen of tentamens te ontvreemden. Sterke authenticatie is een van de maatregelen om identiteitsfraude tegen te gaan.

Onderzoek

Voor het onderzoeksproces is de kans op manifestatie van de volgende dreigingen het grootst:

- *Verkrijging en openbaarmaking van data*
  Tijdens onderzoeken worden vaak gevoelige data verwerkt en opgeslagen. Ook kunnen bepaalde onderzoeken maatschappelijk gevoelig liggen. Maatregelen om het verkrijgen en openbaar maken van dit soort data te voorkomen en van gevoelige onderzoeken, omvatten het gebruik van cryptografie, goede toegangscontrole tot de data en een hoog cyberbewustzijn.

- *Spionage*
  Onderzoeksinstellingen beschikken over potentieel waardevolle data en kennis waarvoor zowel criminelen als staten grote belangstelling hebben. Hoewel enigszins ongrijpbaar omdat hierover weinig informatie publiek beschikbaar komt, is volgens het jaarverslag van de AIVD en het Cyberdreigingsbeeld Nederland van het NCSC bevestigd dat in Nederland spionage plaatsvindt. Maatregelen richten zich in de eerste plaats op het detecteren van pogingen tot spionage en van het exfiltreren van data. Ze omvatten logging van systemen en netwerken en loganalyse om patronen te herkennen.

Bedrijfsvoering

Voor de bedrijfsvoering is de kans op manifestatie van de volgende dreigingen het grootst:

- *Verkrijging en openbaarmaking van data*
  Allerlei gevoelige data, waaronder persoonsgegevens, worden ten behoeve van de bedrijfsvoering verwerkt. Als deze data op straat komen te liggen is er sprake van ernstige reputatieschade en kan de toezichthouder zware boetes opleggen. Maatregelen om het verkrijgen en openbaar maken van gevoelige data te voorkomen, omvatten het gebruik van cryptografie, goede toegangscontrole tot de data en een hoog cyberbewustzijn.

Weerbaarheid

Dit rapport maakt deel uit van het SURF-innovatieprogramma *Betrouwbare en veilige omgeving*. De ambitie van dit innovatieprogramma is dat SURF en de aangesloten instellingen in 2018 immuun zijn voor beveiligingsincidenten en cyberaanvallen. Immuun betekent dat, hoewel zich incidenten voordoen, de beschikbaarheid en betrouwbaarheid van informatie en systemen op hoog niveau gegarandeerd blijven en de herstel- en schadekosten laag zijn. Het gevolg is een snel herstel, dat niet ten koste gaat van een open en vrij toegankelijk internet.

Om dat te bereiken moeten instellingen maatregelen nemen om hun cyberweerbaarheid te verhogen. Traditionele beschermingsconstructies met firewalls werken niet meer, omdat de gebruikers zich in veel gevallen niet binnen de perimeter bevinden. Bovendien worden data meer en meer in de cloud verwerkt en opgeslagen, wat ook invloed heeft op de maatregelen die nodig zijn. Dataclassificatie is belangrijk om te bepalen welke maatregelen adequaat zijn ter bescherming van data vóórdat uitwisseling daarvan plaatsvindt tussen gebruikers onderling en met gebruikers van andere instellingen of partijen.

Voorbereidingen

Voor het invoeren van maatregelen moet het bestuur van de instelling allereerst een goed beeld hebben van welke bedreigingen er zijn, welke bedreigingen relevant zijn voor de organisatie, wat de kroonjuwelen van de organisatie zijn en welke data in de cloud worden verwerkt of opgeslagen.

Verder is het belangrijk dat het bestuur weet wat de status is van de cyberweerbaarheid van de eigen instelling en hoe die zich verhoudt tot die van andere, vergelijkbare instellingen.

SURFaudit voorziet in deze laatste doelstellingen. De self-assessment op basis van het Normenkader Informatiebeveiliging Hoger Onderwijs en het Normenkader Informatiebeveiliging MBO voor mbo-instellingen, is een goed instrument om te bepalen hoe ‘cyberweerbaar’ de instelling is. SURFaudit voorziet ook in een tweejaarlijkse benchmark waarmee instellingen hun cyberweerbaarheid kunnen spiegelen aan die van collega-instellingen.

1. INLEIDING

1.1 Meer aandacht voor cybercrime

De maatschappij als geheel krijgt steeds meer aandacht voor cybersecurity. Zo besteedt de AIVD er aandacht aan in zijn jaarverslag [1], het NCSC doet dat al sinds 2011 in zijn Cybersecuritybeeld Nederland [2]. De WRR publiceerde in 2015 het rapport ‘De publieke kern van het internet’ [3], waarin aandacht is voor cybersecurity en op 6 oktober 2016 publiceerde de Cyber Security Raad ‘De economische en maatschappelijke noodzaak van meer cybersecurity’ [4]. Dit is een onafhankelijk publiek-privaat advies over het belang van cybersecurity voor de Nederlandse economie en maatschappij. Kortom, adviezen en rapporten te over. Ook bestuurders van de instellingen die zijn aangesloten bij SURF krijgen meer aandacht voor cybersecurity en het onderwerp staat hoger op de agenda dan in het verleden.

1.2 Gevolgen van cyberdreigingen

Als een aanvaller toegang weet te krijgen tot IT-systemen of het netwerk, kunnen de gevolgen ingrijpend zijn:

- **Datalek** – gevoelige informatie is gelekt of verloren gegaan. Dit kan bijvoorbeeld om persoonsgegevens gaan of intellectueel kapitaal. In het geval van persoonsgegevens kunnen er boetes volgen.
- **Verstoring van ICT** – online services zijn (tijdelijk) niet meer beschikbaar, als gevolg van sabotage door interne medewerkers of (externe) cybercriminelen, activisten of cybervandalen.
- **Externe reputatieschade** – gelekte informatie heeft langdurige gevolgen voor het imago van de instelling, haar personeel of een derde partij, zoals een leverancier of partnerinstelling.
- **Interne reputatieschade** – informatie lekt waardoor personeel schade lijdt en gaat twijfelen aan de integriteit van de organisatie.
- **Doorgifte van malware** – malware wordt onbewust doorgegeven waardoor schade bij anderen optreedt.
- **Dataverlies door afpersing** – data zijn ontoegankelijk gemaakt of gevoelige informatie wordt pas vrijgegeven wanneer losgeld wordt betaald.
- **Dataverlies door spionage** – een aanvaller heeft toegang gekregen tot gevoelige informatie, bijvoorbeeld intellectueel kapitaal, waardoor economische schade wordt geleden.

1.3 Trends

In deze periode vallen in de onderwijs- en onderzoekssector een aantal trends op:

- Phishing, spearphishing en whaling1 neemt sterk toe.
- Het aantal ransomware-incidenten neemt sterk toe.
- DDoS-aanvallen gaan onverminderd door en worden geavanceerder.
- Aantal kwetsbaarheden in software neemt toe.
- Responsible disclosure beleid wordt ingevoerd.
- Het belang van ketenbeveiliging wordt onderkend.

[1] Vorm van phishing waarbij de aanvaller probeert een hooggeplaatste medewerker in een bedrijf ertoe te bewegen om informatie af te staan of bijvoorbeeld geld over te maken.

NIEUWSITEM

VERPLEEGKUNDIGE GESCHORST OM PLAATSEN FACEBOOKFOTO'S

De verpleegkundige uit het Isala-ziekenhuis in Zwolle plaatste foto's van medische ingrepen.

Maarten Back| 20 april 2016

Een verpleegkundige uit het Isala-ziekenhuis in Zwolle is geschorst, vanwege het plaatsen van foto's van medische ingrepen op Facebook. Volgens het ziekenhuis is met het plaatsen van de foto's het medisch beroepsgeheim geschonden en mogelijk is de plaatsing ook in strijd met de wet Bescherming Persoonsgegevens.

Het ziekenhuis laat in een reactie weten "erg geschrokken" te zijn en dat het de zaak "heel hoog" opneemt. De zaak kwam aan het licht doordat de Volkskrant via een anonieme tipgever de betreffende foto's gekregen en ingezien heeft.

De krant schrijft dat op de foto's onder meer "operatief verwijderde voorwerpen, inwendige opnamen van patiënten en röntgenfoto's" te zien zijn. Isala heeft de zaak doorgegeven aan de Autoriteit Persoonsgegevens, de opvolger van het College bescherming persoonsgegevens. Het ziekenhuis heeft preventief melding gedaan van een vermoedelijk datalek bij de Autoriteit Persoonsgegevens. Dit wordt op dit moment door Isala onderzocht.

Bron: https://www.nrc.nl/nieuws/2016/04/20/verpleegkundige-geschorst-om-plaatsen-facebookfotos-a1407779

ROTTERDAMSE STUDENTEN BETALEN COLLEGEGELD HOGESCHOOL NA NEPMAIL

Zo'n honderd studenten van de Hogeschool Rotterdam (HR) hebben onlangs een phishingmail ontvangen waarin hen gevraagd wordt hun collegegeld over te maken. De afzender deed zich voor als het Studenten Service Center van de hbo-instelling. Voor zover bekend hadden negen studenten niet in de gaten dat ze te maken hadden met een oplichter. Zij hebben collegegeld betaald aan deze persoon. De HR heeft inmiddels alle studenten geïnformeerd over de phishingmail. Dit meldt het studentenblad Profielen van de HR.

De nepmail werd verstuurd een dag nadat de hogeschool zelf via een e-mail aan alle studenten meldde dat het collegegeld op de reguliere wijze zou worden afgeschreven. De phishingmail had als onderwerp 'Let op gewijzigd Inning collegegeld studiejaar 2015/2016' en werd verstuurd vanaf een adres dat erg lijkt op het e-mailadres van het servicecentrum. In de mail werd de studenten gevraagd om het collegegeld handmatig over te maken.

Bron: https://www.nationaleonderwijsgids.nl/hbo/nieuws/31336-rotterdamse-studenten-betalen-collegegeld-hogeschool-na-nepmail.html

1.4 Doel van dit rapport

Dit rapport laat zien welke dreigingen in het cyberdomein, onze digitale wereld, relevant zijn voor de onderwijs- en onderzoeksinstellingen en biedt zo handvatten voor de instellingen om hun weerbaarheid te vergroten.

1.5 Over deze uitgave

Dit is de derde uitgave van het 'Cyberdreigingsbeeld – sector onderwijs en onderzoek'. Deze uitgave is tot stand gekomen op basis van interviews met van security officers en (IT-)medewerkers bij een groot aantal onderwijs- en onderzoeksinstellingen en op basis van publieke bronnen. Het rapport bouwt voort op de vorige uitgaven en beslaat ongeveer de periode oktober 2015 tot oktober 2016.

1.6 Relatie met SURF-diensten

1.6.1. Innovatieprogramma Betrouwbare en Veilige Omgeving

Het opstellen van het 'Cybersecuritybeeld – sector onderwijs en onderzoek' is een van de activiteiten in het innovatieprogramma *Betrouwbare en veilige omgeving*. Met dit innovatieprogramma streeft SURF naar een vrij toegankelijk en open internet als fundament van een betrouwbare en veilige leef- en werkomgeving. De doelstelling van het innovatieprogramma is dat eind 2018 90% van de bij SURF aangesloten instellingen bekwaam is op het gebied van Security, Privacy en Trust.

1.6.2. Normenkader Informatiebeveiliging Hoger Onderwijs

De in het Cyberdreigingsbeeld gesignaleerde dreigingen vormen input voor het onderhouden van het Normenkader Informatiebeveiliging Hoger Onderwijs (Normenkader IBHO). Dit normenkader is gebaseerd op de internationale standaard ISO/IEC 27002:2013 *Code of practice for information security controls*, de meest gebruikte standaard op het gebied van informatiebeveiliging. Het bevat bovendien alle privacy-aspecten die genoemd zijn in het CPB[2]-richtsnoer *Beveiliging van Persoonsgegevens* [5].

1.6.3. SURFaudit

SURFaudit biedt instellingen de mogelijkheid op basis van het Normenkader IBHO een scan uit te voeren op het gebied van informatiebeveiliging, voor de hele organisatie of voor onderdelen. Zo kan de instelling in kaart brengen hoe goed zij informatiebeveiliging onder controle heeft en waar de prioriteiten liggen voor verbetering.

1.7 Leeswijzer

In hoofdstuk 2 van het Cyberdreigingsbeeld leest u welke trends in het algemeen zijn waargenomen en welke specifiek zijn voor onderwijs, onderzoek en bedrijfsvoering van onderwijs en onderzoeksinstellingen. Dit wordt het dreigingslandschap genoemd. Hoofdstuk 3 gaat in op de dreigingen per proces en laat per dreiging zien wie de actoren zijn (degenen die ICT-voorzieningen in onderwijs en onderzoek aanvallen). Hoofdstuk 4 bespreekt per proces de maatregelen die genomen kunnen worden tegen de belangrijkste dreigingen.

[2] College Bescherming Presoonsgegevens, nu Autoriteit Persoonsgegevens

2. DREIGINGSLANDSCHAP

2.1 Inleiding: algemene dreigingen

2.1.1 Data beschermen is complex

Zoals in voorgaande versies van dit rapport al is opgemerkt, kenmerkt de sector onderwijs en onderzoek zich door de openheid van zijn netwerken en toenemende connectiviteit met andere netwerken. Het is een steeds complexere uitdaging om de data (en dan bedoelen we informatie, niet de bits & bytes op een computer) die uitgewisseld worden, te beschermen. Dit komt onder andere door de steeds uitgebreidere samenwerking tussen instellingen onderling, maar ook met private partijen, door de nog steeds toenemende uitwisseling van data tussen studenten onderling en met docenten, en tussen onderzoekers in binnen- en buitenland.

Dataclassificatie steeds belangrijker

Het inwerkingtreden van de meldplicht datalekken op 1 januari 2016 en de inwerkingtreding van de algemene verordening gegevensbescherming (AVG) op 25 mei 2018 [6] [7] maakt dat dataclassificatie, nog meer dan voorheen, nodig is om te bepalen welke maatregelen genomen moeten worden ter bescherming van data voordat uitwisseling daarvan plaatsvindt.

Op basis van dataclassificatie kunnen de juiste beschermingsmaatregelen genomen worden en kan eventueel anonimisatie of pseudonimisatie (zie kader Anonimisatie en Pseudonimisatie) worden toegepast om te voldoen aan de verordening. Niet voldoen aan de meldplicht datalekken, of te zijner tijd de AVG, kan leiden tot zeer hoge boetes. Speciale aandacht vereisen data bij de universitair medische centra (UMC's), omdat daar sprake is van zeer gevoelige informatie die onder geen beding in verkeerde handen mag vallen. Vooral het elektronisch patiëntendossier en koppelingen naar de buitenwereld moeten goed beschermd worden om ongeautoriseerde toegang tot die data te voorkomen.

Governance

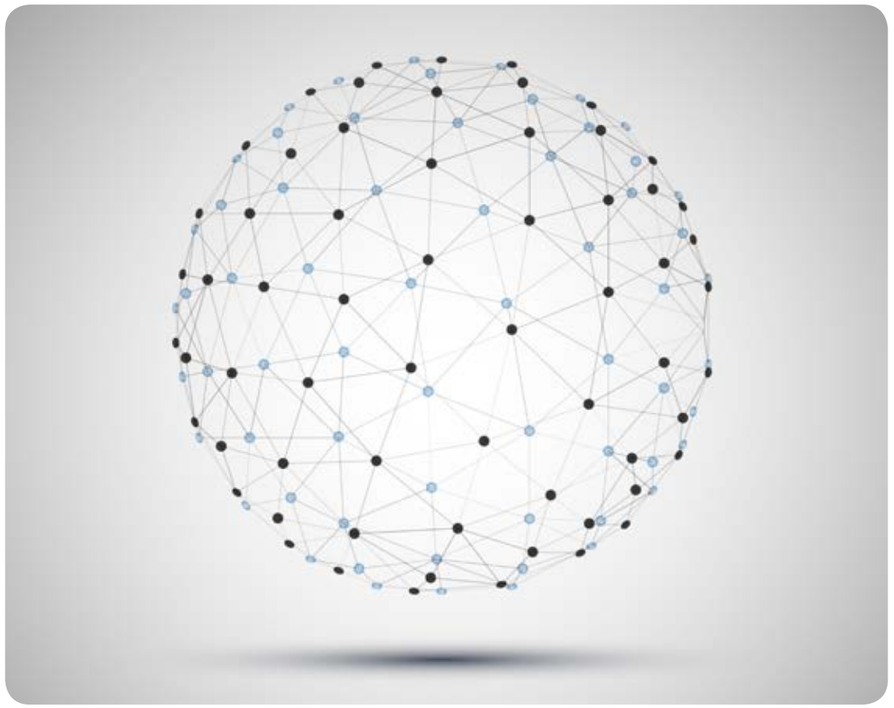
Om dataclassificatie te kunnen invoeren is het van belang dat de governance van de organisatie op orde is. Dan is er vanuit de doelstellingen van de organisatie gekeken naar welke informatie er is, wie de eigenaar of verantwoordelijke van die informatie is en wat de gevolgen zijn als die informatie gelekt, gemanipuleerd of door ongeautoriseerde personen gezien wordt.

2.1.2 Toename van clouddiensten

Verder zien we een sterke toename van clouddiensten in de vorm van cloudopslag en van diverse as-a-service-oplossingen. Bekend zijn opslagdiensten zoals SURFdrive, Dropbox, Google Drive en OneDrive, maar ook het gebruik van online diensten zoals Blackboard, OSIRIS, leerlingregistratiesystemen en online HR-toepassingen neemt sterk toe.

Op tijd beschermingsmaatregelen vaststellen

Daarvoor geldt dat het steeds belangrijker wordt om vóór het in gebruik nemen van een dergelijke dienst te bepalen welke data onder welke voorwaarden de cloud in mogen en welke beschermingsmaatregelen dan nodig zijn. Al was het maar om te voldoen aan wet- en regelgeving, juridische normenkaders en normenkaders voor informatiebeveiliging waar een instelling zich aan gecommitteerd heeft.



Data én gebruikers verspreid over de hele wereld
Data kunnen verspreid zijn over verschillende locaties van instellingen en andere partijen of zijn opgeslagen bij clouddiensten waardoor niet bekend is waar de data zich precies bevinden.

En niet alleen de data zijn verspreid, ook de gebruikers van die data bevinden zich op allerlei plekken in de wereld, niet noodzakelijkerwijs bij een instelling voor onderwijs of onderzoek, maar wellicht thuis of ergens op een openbaar wifi netwerk, netwerken die niet onder controle van de instelling vallen.

2.1.3 Veel verschillende apparaten

De diversiteit van apparatuur neemt steeds toe; waren in het verleden alleen desktops en laptops gangbaar, nu zijn allerlei apparaten online en die worden gebruikt om onderwijs-, onderzoeks- en bedrijfsgegevens te verwerken. Denk bijvoorbeeld aan tablets, smartphones en wearables[3]. Al die apparaten waren nog niet zo lang geleden een nieuwtje, maar zijn langzamerhand gemeengoed geworden. Er zijn allerlei apps beschikbaar voor e-mail en tekstberichten, en er zijn al productiviteitsapps die op een smartwatch kunnen draaien. Veel van die apps verzamelen privédata, contactinformatie en informatie over surfgedrag [7] zonder dat de gebruiker daar weet van heeft, en voor al die apparaten en software wordt malware ontwikkeld om data en identiteitsinformatie van de eigenaar te ontvreemden. Kortom, werken op een grote variëteit aan apparaten wordt steeds gemakkelijker, maar daarmee nemen ook de mogelijkheden toe voor aanvallers om gevoelige gegevens te stelen of te manipuleren.

[3] miniature electronic devices that are worn under, with or on top of clothing [9]

2.2 Dreigingen voor sector onderwijs en onderzoek

In dit hoofdstuk komen het actuele dreigingslandschap en de trends van het afgelopen jaar aan bod.

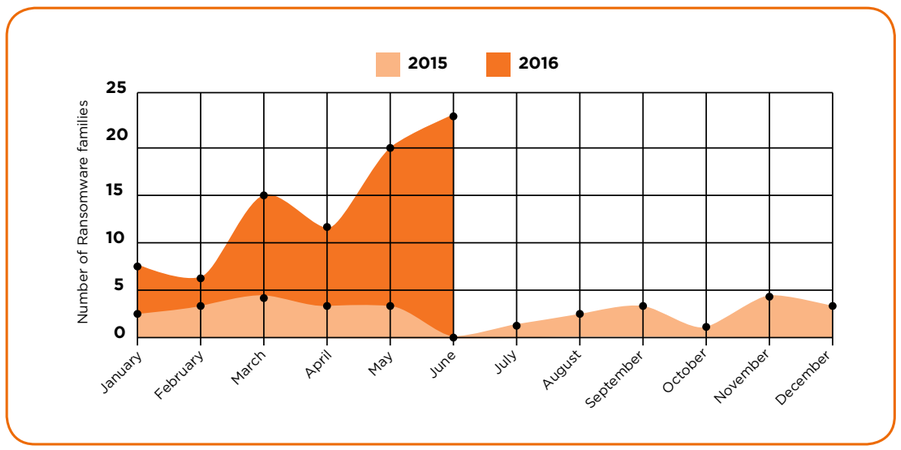
2.2.1 Trends

Het afgelopen jaar zijn in onze sector een aantal trends op te merken:
- Phishing, spearphishing en whaling neemt sterk toe.
- Het aantal ransomware incidenten neemt sterk toe.
- DDoS aanvallen gaan onverminderd door en worden geavanceerder.
- Aantal kwetsbaarheden in software neemt toe.
- Responsible disclosure beleid wordt ingevoerd.
- Het belang van ketenbeveiliging wordt onderkend.

Phishing, spearphishing en whaling[4] nemen sterk toe
Dit jaar is het aantal phishing- en whalingaanvallen flink toegenomen. (zie kader Phishing, spearphishing en whaling).

Terwijl phishing-e-mails redelijk makkelijk te herkennen zijn door mail-/spamfilters, zijn whaling-e-mails vrijwel niet te detecteren, omdat er niet altijd een link of bijlage in zit. Een voorbeeld van whaling is de CEO-fraude die de laatste maanden in opkomst is. In de e-mail, die gericht is aan een specifieke persoon bij de afdeling financiën, wordt gevraagd geld zo snel mogelijk over te maken, vaak naar het buitenland. Het bericht is ondertekend door de directeur van de geadresseerde en er wordt benadrukt dat de betaling zo snel mogelijk moet worden uitgevoerd. Dit soort e-mailberichten wordt steeds geraffineerder, in het bedrijfsleven hebben al diverse succesvolle CEO-fraudeaanvallen plaatsgevonden [8].

Het aantal ransomware-incidenten neemt sterk toe
In 2015 zijn er al een flink aantal incidenten met ransomware gemeld, waaronder het incident bij de VU. Het aantal incidenten is in 2016 verder toegenomen. Verschillende instellingen hebben dit jaar last gehad van ransomware-aanvallen, waarbij de gebruikte ransomware steeds geavanceerder wordt en daardoor moeilijker is tegen te gaan.



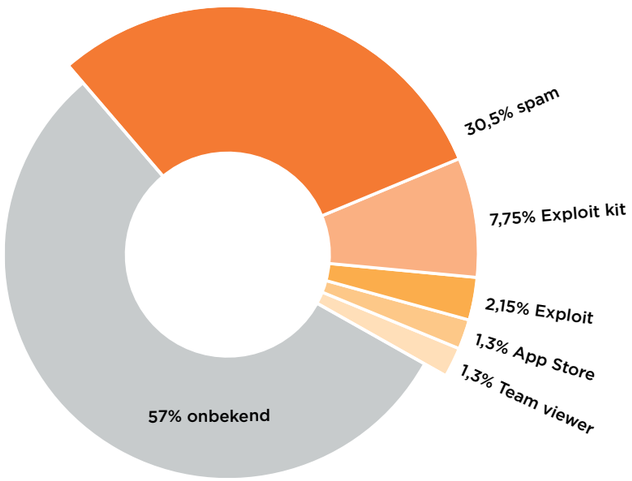
Figuur 1: Toename aantal ransomware families 2015-2016 (bron: Trend Micro [9])

[4] Vorm van phishing waarbij de aanvaller probeert een hooggeplaatste medewerker in een bedrijf ertoe te bewegen om informatie af te staan of bijvoorbeeld geld over te maken.

Bekend waren al incidenten waarbij bestanden niet kunnen worden ontsleuteld (Cryptolocker). Nieuw is de opkomst van incidenten waarbij bestanden verwijderd worden als er geen losgeld betaald wordt (Jigsaw), en incidenten waarbij het losgeld steeds verhoogd wordt als er niet betaald wordt voor de deadline (Surprise) [9].

Figuur 2: Losgeld dat verhoogd wordt als niet op tijd betaald wordt (Bron: Fortinet [10])

De meest gebruikte methode voor het verspreiden van ransomware is het sturen van een phishing-e-mail met een link die de ransomware op het systeem van de gebruiker installeert, zodra het slachtoffer de link aanklikt. Dit is ook de methode die we in de onderwijs- en onderzoekssector vaak zien.



Figuur 3: Aanvalsvectoren ransomware (Bron: Trend Micro [11])

Daarnaast wordt ransomware veel verspreid door allerlei exploit kits[5], die gebruikmaken van specifieke kwetsbaarheden om hun lading af te leveren. Met een exploit kit kan iedereen op een gebruiksvriendelijke manier malware verspreiden, zonder dat daar veel kennis voor nodig is. Bekende en veelgebruikte exploit kits zijn Angler, Neutrino en Nuclear [9].

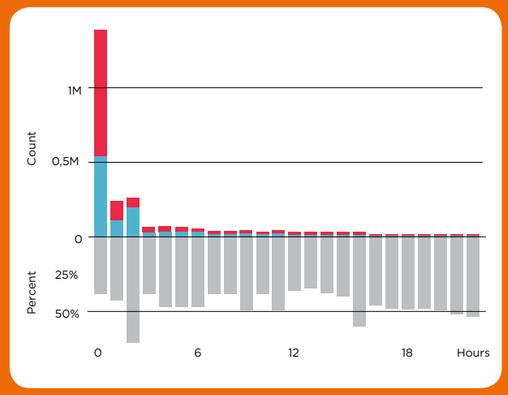
Een nieuwe chantagevariant is de *DDoS-chantage*. Hierbij ontvangt het slachtoffer een e-mailbericht waarin gedreigd wordt met een DDoS-aanval, tenzij losgeld betaald wordt (zie kader DDoS chantage).

[5] Zie bijvoorbeeld: https://zeltser.com/what-are-exploit-kits/ voor een definitie (geraadpleegd op 26 september 2016)

UITGELICHT

PHISHING, SPEARPHISHING EN WHALING

Phishing
Bij phishing wordt een e-mail naar een grote groep gebruikers gestuurd, met als doel om informatie, bijvoorbeeld inloggegevens, op te vragen of om ongemerkt malware op het systeem van de gebruiker te installeren. Dit gebeurt door de gebruiker te verleiden een link of een attachment in de e-mail te openen. Uit onderzoek van Verizon[6] blijkt dat ongeveer 30% van de ontvangers een phishing-e-mail opent en ongeveer 12% van de gebruikers de (kwaadaardige) link of bijlage aanklikt:



Kortom, wanneer de doelgroep groot genoeg is zijn er altijd wel gebruikers die de link aanklikken of de bijlage openen. Zo verzamelt de aanvaller inloggegevens of slaagt erin kwaadaardige software te installeren op het systeem van de gebruiker. De software kan ransomware zijn, of andere malware, die bijvoorbeeld het systeem onderdeel maakt van een botnet.

Spearphishing en whaling
Een meer gerichte vorm van phishing is spearphishing of whaling. Bij deze vorm van phishing worden specifieke personen benaderd. De aanvaller heeft dan van tevoren onderzocht wie het beste benaderd kan worden. Dit kan via e-mail, maar ook telefonisch. Een voorbeeld is de CEO-fraude[7] die de laatste tijd veel voorkomt. Daarbij wordt in een e-mail gevraagd om een groot bedrag over te maken. De e-mail is gericht aan iemand die daartoe in gemachtigd is en die gevoelig is voor de uitgeoefende druk. De e-mail is bijvoorbeeld ondertekend door de algemeen of financieel directeur van de organisatie en verstuurd vanaf een e-mailadres dat bijna niet te onderscheiden is van een valide adres. In september 2016 hebben een aantal instellingen te maken gekregen met CEO-fraude.

DDOS-CHANTAGE[8]

Voorbeeld van een DDoS-chantagemail:

From: "Armada Collective" armadacollective@openmailbox.org
To: abuse@victimdomain; support@victimdomain; info@victimdomain
Subject: Ransom request: DDOS ATTACK!

FORWARD THIS MAIL TO WHOEVER IS IMPORTANT IN YOUR COMPANY AND CAN MAKE DECISION!

We are Armada Collective.

All your servers will be DDoS-ed starting Friday if you don't pay 20 Bitcoins @ XXX

When we say all, we mean all - users will not be able to access sites host with you at all.

Right now we will start 15 minutes attack on your site's IP (victims IP address). It will not be hard, we will not crash it at the moment to try to minimize eventual damage, which we want to avoid at this moment. It's just to prove that this is not a hoax. Check your logs!

If you don't pay by Friday , attack will start, price to stop will increase to 40 BTC and will go up 20 BTC for every day of attack.

If you report this to media and try to get some free publicity by using our name, instead of paying, attack will start permanently and will last for a long time.

This is not a joke.

Our attacks are extremely powerful - sometimes over 1 Tbps per second. So, no cheap protection will help.

Prevent it all with just 20 BTC @ XXX

Do not reply, we will probably not read. Pay and we will know its you. AND YOU WILL NEVER AGAIN HEAR FROM US!

Bitcoin is anonymous, nobody will ever know you cooperated.

Een bekend voorbeeld is het ProtonMail-incident uit 2015, waarbij ProtonMail, een e-maildienst, heeft besloten in te gaan op de chantage om te voorkomen dat andere bedrijven die bij dezelfde ISP zaten als ProtonMail, last zouden houden van de DDoS-aanval[9].

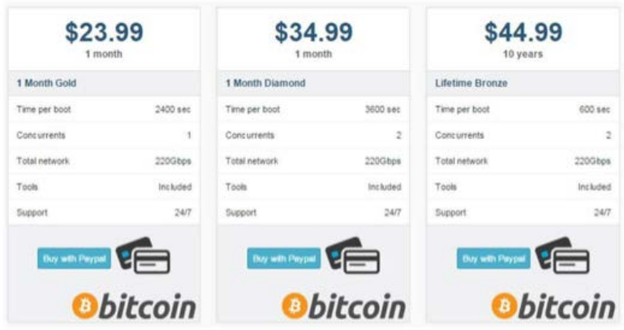
[6] Verizon DBIR 2016 - http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf (opgehaald op 26 september 2016)
[7] https://www.abnamro.nl/nl/grootzakelijk/over-abnamro/veiligheid/slachtoffer-van-ceo-fraude.html (geraadpleegd op 26 september 2016)
[8] https://www.grahamcluley.com/armada-collective-ddos/ (geraadpleegd op 30 november 2015)
[9] http://www.forbes.com/sites/thomasbrewster/2015/11/09/armada-bitcoin-crooks-go-big/#739906c41689 (geraadpleegd op 30 november 2015)

DDoS-aanvallen gaan onverminderd door en worden geavanceerder
Op 20 september 2016 lag de website *KrebsOnSecurity* van onderzoeker en publicist Brian Krebs onder vuur van een denial-of-service-aanval [12]. De aanval was zo intens (meer dan 600 Gigabits per seconde aan verkeer) dat de ISP de site enige tijd afgesloten heeft om zichzelf te beschermen en uiteindelijk de hosting van *KrebsOnSecurity* heeft gestaakt.

Deze aanval was bijzonder, omdat in tegenstelling tot de 'normale' technieken die gezien worden bij denial-of-service-aanvallen (zie kader DDoS-aanval), de aanval nu van heel veel gehackte apparaten leek te komen, een *Attack of Things* [13]. De aanval werd waarschijnlijk uitgevoerd met hulp van een botnet bestaande uit een groot aantal Internet of Things-systemen, zoals thuisrouters en -modems, en camera's en digitale videorecorders die aan het internet gekoppeld zijn. Deze devices hebben vaak ingeprogrammeerde of makkelijk te kraken wachtwoorden.

Ook ENISA[10] [7] signaleert een verschuiving van botnets die bestaan uit een aantal krachtige systemen, naar botnets die bestaan uit heel veel simpele thuissystemen. Doordat steeds meer systemen met het internet verbonden zijn, kunnen we dan ook veel meer van dit soort aanvallen tegemoet zien.

Ook is voor het uitvoeren van DDoS-aanvallen steeds minder kennis en kunde nodig, waardoor bijvoorbeeld studenten ze inzetten tegen scholen . Er zijn diensten (*booters* of *stressers*) beschikbaar om DDoS-aanvallen uit te voeren tegen lage kosten [14] [15]. Een maandabonnement op DDoS-aanvallen tot 60 minuten per keer, kost 20 tot 40 dollar, zodat een aanval met grote impact tegen lage kosten kan worden uitgevoerd [16].



Figuur 4: Voorbeeld van kosten voor booter service (Bron: Incapsula [16])

Naar schatting 40% van al het DDoS-verkeer wordt gegenereerd door booters [7].

SURFcert heeft in 2015 en 2016 een groot aantal alarmmeldingen gehad voor denial-of-service-aanvallen. Tijdens vakantieperiodes daalt het aantal meldingen steeds significant, wat erop wijst dat studenten deze aanvallen uitvoeren.

[10] European Network and Information Security Agency (https://www.enisa.europa.eu/)

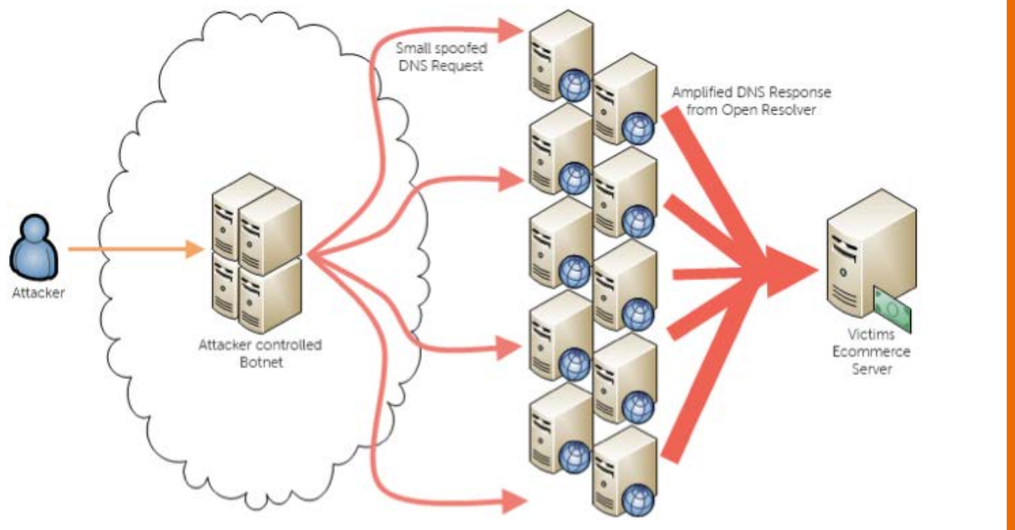
UITGELICHT

DDOS-AANVAL

Bij een denial of service-aanval wordt een website of een internetaansluiting met zoveel verkeer bestookt dat legitiem verkeer de site niet meer kan bereiken. Hierdoor kunnen bijvoorbeeld de website, een e-mailserver of een van buitenaf toegankelijk database server niet meer bereikt worden. Een veel toegepaste variant is de Distributed Denial of Service-aanval of-tewel DDoS-aanval. Voor DDoS worden verschillende technieken gebruikt, waarvan reflectie en amplificatie de meestgebruikte zijn. Bij een reflectieaanval worden andere systemen dan die van de aanvaller getriggerd om netwerkpakketjes naar een doelwit te sturen. Bij amplificatie zijn de pakketten die het andere systeem verstuurt aanmerkelijk groter dan het oorspronkelijke pakketje, waardoor de aanval veel effectiever is.

Voor deze typen aanvallen worden vaak kwetsbare protocollen zoals NTP (Network Time Protocol) en DNS (Domain Name Service) gebruikt.

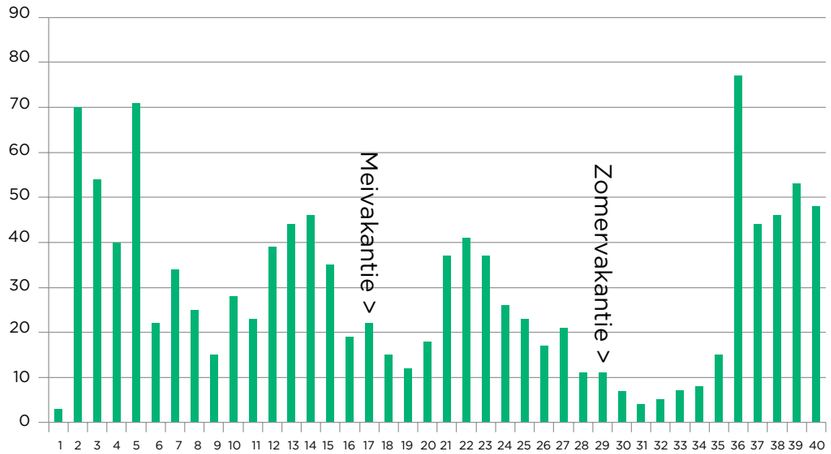
Veel DDoS-aanvallen worden met zogenaamde booters uitgevoerd. Een booter is een on-demand DDoS-service die cybercriminelen tegen betaling aanbieden. Ze worden vooral gebruikt door script kiddies die zo tegen betaling van een laag bedrag een geavanceerde DDoS-aanval kunnen (laten) doen.[11]



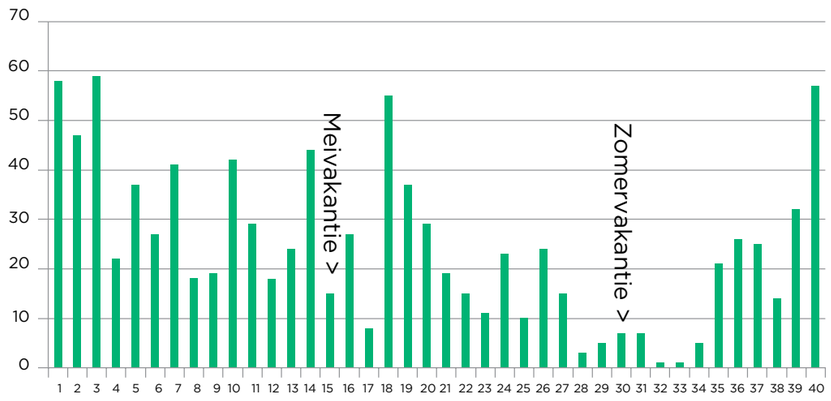
Figuur 2: DNS-amplificatieaanval

(Bron: http://www.evilsec.net/2015/04/drdos-denial-of-service-on-steroids/)

[11] Zie bijvoorbeeld http://www.eweek.com/security/how-do-booters-work-inside-a-ddos-for-hire-attack (geraadpleegd op 30 september 2016)

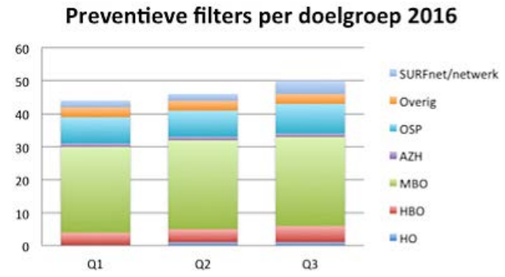


Figuur 5: SURFcert - aantal alarmmeldingen per week Q1-3 2015



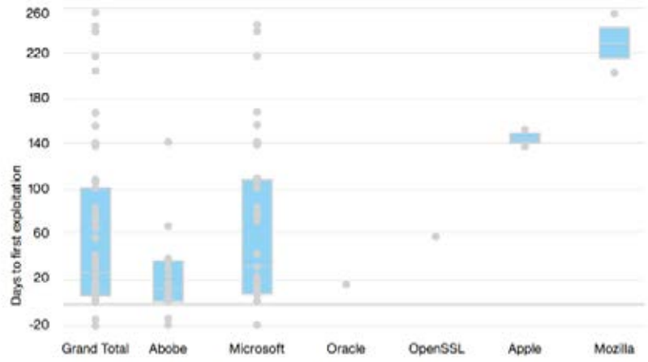
Figuur 6: SURFcert - aantal alarmmeldingen per week Q1-3 2016

Begin 2016 is SURFcert begonnen met het implementeren van preventieve rate-limitingfilters (zie kader rate-limiting), die de meest gangbare aanvallen tegengaan. Het effect daarvan lijkt dat het gemiddeld aantal alarmmeldingen in 2016 iets lager ligt daar in 2015 (zie figuur 5 & 6), wellicht omdat die aanvallen minder effect sorteren.



Figuur 7: Aantal instellingen met preventieve filters per doelgroep (2016)

Aantal kwetsbaarheden in software neemt toe
Het aantal kwetsbaarheden in software neemt nog steeds toe, vooral bij producten van Adobe en Microsoft [17] [18]. Daarbij valt op dat de tijd tussen de publicatie van een kwetsbaarheid en de eerst beschikbare exploit tussen de 10 en 100 dagen ligt (mediaan[12] 30 dagen).



Figuur 8: Beschikbaarheid van exploit na bekend worden van kwetsbaarheid. (bron: Verizon DBIR 2016 [18])

Er is dus niet veel tijd om systemen te patchen, zeker als je bedenkt dat kwetsbaarheden, voordat die bekend worden, al enige tijd bestaan en dan ook misbruikt kunnen worden. Dit bleek maar weer uit de publicatie van data van Hacking Team (juli 2015). Hacking Team beschikte over diverse zero-day exploits, die gebruik maken van (toen) nog onbekende kwetsbaarheden [19].

Instellingen voeren beleid voor responsible disclosure in
Al enige tijd geleden heeft SURF een modelbeleid en procedures voor responsible disclosure aan hogeronderwijsinstellingen beschikbaar gesteld. SURF en een flink aantal instellingen hebben dit inmiddels ingevoerd. Het geeft derden de mogelijkheid om gesignaleerde kwetsbaarheden eenvoudig te melden.

Bovendien heeft SURF met circa 30 andere organisaties op 12 mei 2016 tijdens de EU High Level Meeting on Cyber Security in Amsterdam het Coordinated Vulnerability Disclosure Manifesto [20] ondertekend. Hiermee onderschrijft SURF het belang van de inspanningen van onderzoekers en de hackergemeenschap om het internet en de samenleving veiliger te maken.

Het belang van ketenbeveiliging wordt onderkend
Doordat applicaties en opslag naar de cloud verplaatst worden, wordt ketenbeveiliging steeds belangrijker. Er zijn allerlei risico's die moeten worden afgedekt door een andere organisatie dan de instelling zelf, terwijl de instelling wel verantwoordelijk blijft voor de gevolgen. Veel organisaties gaan ervan uit dat clouddiensten betrouwbaar zijn, ook al hebben ze niet in kaart gebracht welke dreigingen er zijn voor data die bij een clouddienst worden opgeslagen of verwerkt, en hebben ze ook niet geverifieerd of bestaande maatregelen nog de juiste zijn [7]. Maar vaak is niet duidelijk hoe informatie beschermd is bij de clouddienst en wat de gevolgen zijn voor de instelling als die informatie voor ongeautoriseerde derden toegankelijk is.

[12] De mediaan is de middelste waarde in een geordende reeks getallen. De helft van de waardes ligt dus onder de mediaan, de andere helft erboven.

NIEUWSITEM

FBI KLAAGT NEDERLANDSE TIENER VAN HACKERGROEP LIZARD SQUAD AAN

Foto: 123RF
Gepubliceerd: 06 oktober 2016 12:42
Laatste update: 06 oktober 2016 16:35

De FBI heeft twee tieners van de hackergroep Lizard Squad aangeklaagd, onder wie een 19-jarige Nederlander.

De jongen uit Leiden wordt beschuldigd van belaging, cyberaanvallen, het verkopen van ddos-aanvallen, het verkopen van credit card-gegevens en deelname aan een criminele organisatie.

Hij werd afgelopen maand in zijn woonplaats gearresteerd. De zwaarste aanklacht, deelname aan een criminele organisatie, kan leiden tot een celstraf van maximaal tien jaar.

“Ze werkten samen met anderen om om verwoestende cyberaanvallen over de hele wereld in gang te zetten”, aldus de FBI. “Daarnaast verhandelden ze online betaalaccounts die waren gestolen van slachtoffers uit onder andere Illinois.”

Lizard Squad was verantwoordelijk voor meerdere aanvallen op grote diensten en websites. Zo slaagde de groep er in om de servers van Playstation Network en Xbox Live tijdens de feestdagen in 2014 plat te leggen.

In juli 2015 werd één van de Lizard Squad-hackers veroordeeld tot een voorwaardelijke celstraf in Finland. Er zijn meerdere leden van de online groep opgepakt.

Bron: http://www.nu.nl/internet/4332342/fbi-klaagt-nederlandse-tiener-van-hackergroep-lizard-squad.html (opgehaald op 7 oktober 2016)

HACKING TEAM ZOU VIA LEK IN NETWERK-APPARAAT ZIJN GEHACKT

maandag 18 april 2016, 13:51 door Redactie

Het Italiaanse bedrijf Hacking Team dat vorig jaar door een omvangrijke hack werd getroffen zou zijn gehackt via een zero day-lek in een netwerkapparaat in het netwerk, zo claimt de vermeende hacker. Bij de inbraak wist de hacker 400 gigabytes aan data te stelen, waaronder broncode en gevoelige e-mails. Hacking Team ontwikkelt allerlei spyware voor overheden. Volgens de hacker, met het alias Phineas Fisher, had het bedrijf weinig aan het internet blootgesteld. Dat laat hij in een uitleg op Pastebin weten. Voor de supportpagina was een certificaat vereist en op de hoofdwebsite, een Joomla-blog, werden ook geen grote problemen ontdekt. Verder werden een mailserver, een aantal routers, twee vpn-apparaten en een spamfilter gevonden. Hierdoor had de hacker naar eigen zeggen drie opties, namelijk het vinden van een zero day-lek in Joomla, Postfix of één van de netwerkapparaten.

Hij besloot voor de laatste optie te kiezen. Na twee weken van reverse engineering had hij naar eigen zeggen een kwetsbaarheid gevonden waarmee het apparaat op afstand kon worden overgenomen. De hacker zou vervolgens zijn exploit bij verschillende andere bedrijven hebben getest om te voorkomen dat er iets mis zou gaan en Hacking Team de aanval zou ontdekken. Om welke bedrijven en welk netwerkapparaat het gaat heeft de hacker niet laten weten, aangezien het probleem nog steeds niet is opgelost.

Nadat hij toegang tot het apparaat had gekregen wist de hacker uiteindelijk toegang tot het interne netwerk en verschillende databases te krijgen. Hacking Team bleek de back-ups niet te versleutelen, wat de aanvaller meer informatie over het netwerk verstrekte. Uiteindelijk wist hij het ‘domain admin’ wachtwoord te verkrijgen en documenten over het interne netwerk. Hieruit bleek dat Hacking Team ook nog een geïsoleerd netwerk had met de broncode van de spyware. Via de computers van de systeembeheerders wist de hacker uiteindelijk toegang tot dit netwerk te krijgen. Volgens de hacker laat zijn operatie zien dat via hacking zelfs de underdog een kans om te winnen heeft.

Bron: https://www.security.nl/posting/468098/Hacking+Team+zou+via+lek+in+netwerkapparaat+zijn+gehackt

Gelukkig zijn instellingen zich steeds meer bewust van de risico’s in de keten en worden maatregelen daar meer op toegespitst. Bovendien stimuleert SURF het gebruik van het Juridisch normenkader cloudservices hoger onderwijs [21] om normen bij leveranciers (ketenpartners) af te dwingen. Ook in andere onderwijssectoren wordt beter gekeken naar ketenbeveiliging: met het privacyconvenant in het po/vo en met afspraken met uitgevers in het mbo.

2.2.2 Toenemende complexiteit

Bovengenoemde ontwikkelingen maken het dreigingslandschap voor de instellingen steeds complexer. Voor het ontsluiten van data moet bepaald worden wat de gevoeligheid van de data is, wie bij de data mag, vanaf welke locaties, en wat voor toegang wordt toegestaan.

Datatypen per bedrijfsproces

Daarbij is er onderscheid tussen data die van belang zijn voor de bedrijfsvoering, voor onderwijs of voor onderzoek (of een combinatie daarvan):

Informatie	Toelichting	Onderwijs	Onderzoek	Bedrijfsvoering
Studieresultaten	Gegevens die aangeven of een studieactiviteit is behaald en met welke score. Denk aan cijfers voor tentamens, opdrachten en presentaties. Deze vormen de basis voor externe verantwoording en bekostiging.	•		
Onderzoeks-gegevens & Intellectueel eigendom	Resultaten van onderzoek leiden vaak tot nieuwe technologieën, innovaties en methodes. Onder intellectueel eigendom kan ook het lesmateriaal, niet-ontwikkelde methodes, papers en rapporten worden verstaan.		•	
CBRN+ gegevens	Gevoelige chemische, biologische, radiologische en nucleaire informatie die voortkomt uit onderzoek.		•	
Bedrijfsvoering data	Informatie die wordt gebruikt voor de algemene bedrijfsvoering. Hierbij kan worden gedacht aan managementinformatie & financiële gegevens van de instelling.			•
Persoonsgegevens	Instellingen beschikken over een grote hoeveelheid persoonsgegevens van onder meer werknemers, studenten en proefpersonen.	•	•	•
Commercieel & Juridisch	Informatie over bijvoorbeeld aanbestedingen en projectplannen, maar ook over mogelijke juridische zaken die spelen bij de instelling.			•
Gegevens van (onderzoeks) partners	Informatie over partnerinstellingen, onderaannemers en andere derde partijen.		•	•
Gegevens over toetsen	Informatie over de inhoud van tentamens en de correcte antwoorden.	•		

Tabel 2: Informatie en processen

Datatypen naar aspecten beschikbaarheid, integriteit, vertrouwelijkheid en privacy
Voor al deze informatie zijn bovendien de aspecten *beschikbaarheid* (B), *integriteit* (I), *vertrouwelijkheid* (V) en *privacy* (P) van toepassing:

Informatie	Toelichting	B	I	V	P
Studie-resultaten	Gegevens die aangeven of een studieactiviteit is behaald en met welke score. Denk aan cijfers voor tentamens, opdrachten en presentaties. Deze vormen de basis voor externe verantwoording en bekostiging.		•	•	•
Onderzoeks-gegevens & Intellectueel eigendom	Resultaten van onderzoek leiden vaak tot nieuwe technologieën, innovaties en methodes. Onder intellectueel eigendom kan ook het lesmateriaal, niet-ontwikkelde methodes, papers en rapporten worden verstaan.	•	•	•	•
CBRN+ gegevens	Gevoelige chemische, biologische, radiologische en nucleaire informatie die voortkomt uit onderzoek.			•	
Bedrijfs-voering data	Informatie die wordt gebruikt voor de algemene bedrijfsvoering. Hierbij kan worden gedacht aan managementinformatie & financiële gegevens van de instelling.	•	•	•	
Persoons-gegevens	Instellingen beschikken over een grote hoeveelheid persoonsgegevens van onder meer werknemers, studenten en proefpersonen.		•	•	•
Commercieel & Juridisch	Informatie over bijvoorbeeld aanbestedingen en projectplannen, maar ook over mogelijke juridische zaken die spelen bij de instelling.		•	•	
Gegevens van (onderzoeks) partners	Informatie over partnerinstellingen, onderaannemers en andere derde partijen.			•	•
Gegevens over toetsen	Informatie over de inhoud van tentamens en de correcte antwoorden.		•	•	

Tabel 3: Informatie en aspecten

Risicoanalyse
Om te bepalen welke maatregelen nodig zijn om informatie adequaat te beschermen, kan een risicoanalyse worden uitgevoerd. Hiervoor zijn verschillende methodes en softwarepakketten in omloop.

Anderzijds zijn er veel overeenkomsten tussen de instellingen voor onderwijs en onderzoek, zodat het denkbaar is dat instellingen vergelijkbare maatregelen invoeren om risico's af te dekken. Daarvoor is het Normenkader Informatiebeveiliging Hoger Onderwijs (Normenkader IBHO) een goed hulpmiddel. Dit normenkader bevat praktijkrichtlijnen op het gebied van informatiebeveiliging en privacy.

3. BEDREIGINGEN PER PROCES

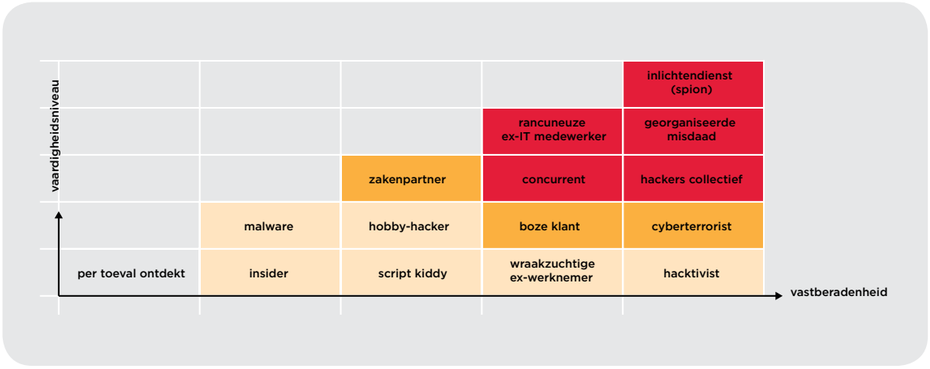
3.1 Inleiding

In dit hoofdstuk brengen we per bedrijfsproces in kaart welke risico's relevant zijn voor instellingen voor onderwijs en onderzoek. De schaal die we gebruiken, is gebaseerd op de schaal die in het Cybersecuritybeeld Nederland 2015 [21] is geïntroduceerd:

LAAG	MIDDEN	HOOG
"Er zijn geen nieuwe trends of fenomenen waar de dreiging van uitgaat. *OF* Er zijn (voldoende) maatregelen beschikbaar om de dreiging weg te nemen. *OF* Er deden zich geen noemenswaardige incidenten voorgedaan in de rapportageperiode."	"Er zijn nieuwe trends en fenomenen waargenomen waar de dreiging van uitgaat. *OF* Er zijn (beperkte) maatregelen beschikbaar om de dreiging weg te nemen. *OF* Incidenten deden zich voor buitenNederland, enkele kleine in Nederland."	"Er zijn duidelijke ontwikkelingen die de dreiging opportuun maken. *OF* Maatregelen hebben beperkt effect, zodat de dreiging aanzienlijk blijft. *OF* Incidenten deden zich voor in Nederland."

Figuur 9: Betekenis risicoschaal

Per proces staan de dreigingen met het grootste risico bovenaan.
Bij ieder risico is er sprake van zogenaamde actoren. Een actor is in dit verband iemand die een aanval uitvoert op een instelling. Op grond van vastberadenheid en vaardigheidsniveau kunnen we een aantal verschillende actoren onderscheiden:



Figuur 10: Vaardigheden en vastberadenheid van aanvallers

Voor de sector onderwijs en onderzoek worden de volgende actoren onderscheiden:

Actor	Vaardigheids-niveau	Toelichting
Studenten	Laag/gemiddeld	Studenten zijn gebaat bij een goede studievoortgang; het manipuleren van studieresultaten kan voor hen interessant zijn. Ze hebben al toegang tot veel systemen en netwerken en zijn in een aantal gevallen zeer vaardig. Studenten zijn zich vaak niet bewust van dreigingen op het gebied van cybersecurity, waardoor ze slordig omgaan met gevoelige informatie.
Medewerkers	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 hebben al toegang tot systemen en netwerken. Medewerkers zijn zich vaak niet bewust van de 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.
Cybercriminelen	Gemiddeld/hoog	Cybercriminelen zijn in het algemeen vooral gedreven door financieel gewin. Ze verkopen gestolen data of proberen losgeld te innen door data tijdelijk ontoegankelijk te maken. Cybercriminelen organiseren zich in toenemende mate, zodat hun kans van slagen groter wordt.
Cyberonderzoekers	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.
Staten	Zeer hoog	Kennis en vaardigheid zijn zeer hoog bij inlichtingen- en politiediensten. In het kader van terrorisme- en misdaadbestrijding worden veel data verzameld. Buitenlandse diensten zijn gedreven door bedrijfseconomische motieven (geïnteresseerd in intellectueel eigendom en innovatieve kennis) en zeer kundig.
Commerciële bedrijven en partnerinstellingen	Laag/gemiddeld	Commerciële partijen zijn gebaat bij het vroegtijdig verkrijgen van informatie van concurrenten. Hetzelfde kan gelden voor rivaliserende partnerinstellingen die onderzoeksdata van elkaar willen hebben. Kennis en kunde zijn aanwezig, maar zal in het algemeen niet gauw worden ingezet tegen collega-instellingen.
Activisten	Laag/gemiddeld	Activisten beschikken over 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	Laag	Cybervandalen zijn op zoek naar erkenning binnen hun eigen groep en zoeken vooral een groot publiek om hun acties te laten zien. Nieuw zijn cyberjihadisten die gevoelige data proberen te vergaren om die vervolgens te publiceren uit propaganda overwegingen. Hun kennis en kunde wisselt, maar is in het algemeen laag.

3.2 Onderwijsproces

Hieronder leest u welke dreigingen relevant zijn voor het onderwijsproces.

	Type dreiging	Manifestatie van dreiging	Risico
1	Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Tentamens of antwoorden worden aangepast	HOOG
2	Identiteitsfraude	• Student laat iemand anders examen maken • Student doet zich voor als andere student of medewerker om inzage te krijgen in tentamens • Student doet zich voor als medewerker en manipuleert studieresultaten	HOOG
3	Verkrijging en openbaarmaking van data	• Privacygevoelige informatie wordt gelekt en gepubliceerd • Fraude door verkrijgen van data over toetsen en opgaven • DDoS-aanval legt IT-infrastructuur plat	MIDDEN
4	Verstoring ICT	• Kritieke examendata worden vernietigd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	MIDDEN
5	Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	LAAG
6	Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	LAAG
7	Spionage	• Studenten beschikken over concurrentiegevoelige informatie via stages bij het bedrijfsleven, waardoor de student doelwit wordt • Controleren van buitenlandse studenten door staten	LAAG

Tabel 4: Dreigingen voor het onderwijsproces

Actor	Vaardigheidsniveau	Dreiging
Studenten	Laag tot Gemiddeld	Identiteitsfraude
		Manipulatie van data
		Verstoren ICT
		Bewust beschadigen imago
Cybercriminelen	Gemiddeld tot Hoog	Verkrijging en openbaarmaking van data
Cyberonderzoekers	Hoog	Verkrijging en openbaarmaking van data
		Verstoren ICT
Activisten	Laag tot Gemiddeld	Verstoren ICT
		Bewust beschadigen imago
Cybervandalen	Laag	Bewust beschadigen imago

Tabel 5: Dreigingen per actor voor het onderwijsproces

3.2.1 Manipulatie van digitaal opgeslagen data

risico

Het vastleggen van studieresultaten is een van de belangrijkste processen voor een onderwijsinstelling. Als dit niet correct gebeurt of wanneer studenten kans zien om de antwoorden van tentamens of examens achteraf aan te passen, zijn de resultaten niet betrouwbaar. De instelling verliest aantrekkingskracht en diploma's van de instelling worden niet meer als waardevol gezien. Niet alleen de instelling zelf, maar ook de afgestudeerden kunnen daar onder lijden. De negatieve impact hiervan is enorm.

Voornaamste actoren: studenten.

NIEUWSITEM

PRIVÉLAPTOP PATIËNTGEGEVENS ISALA GESTOLEN

Auteur Onbekend | 6 oktober 2016

De gegevens van 504 patiënten van het Isala-ziekenhuis in Zwolle zijn ontvreemd. Ze stonden op een privélaptop van een co-assistent die is gestolen. Het voorval is gemeld bij de Autoriteit Persoonsgegevens. De patiënten zijn onder behandeling van de afdeling plastische chirurgie. Het gaat om onder meer patiëntnamen, -nummers en geboortedata. Volgens het ziekenhuis is het niet toegestaan zulke gegevens op een privéapparaat te plaatsen. (ANP)

Bron: https://www.nrc.nl/nieuws/2016/10/06/privelaptop-patientgegevens-isala-gestolen-4671659-a1525304

HACKERS WILLEN WACHTWOORDEN STELEN BIJ AVANS

31 maart 2016

Hackers liggen overal op de loer, ook in het hoger onderwijs. Bij Avans Hogeschool zijn recent twee zogeheten keyloggers ontdekt. Met een keylogger kunnen hackers de aanslagen op het toetsenbord bijhouden en zo wachtwoorden, gebruikersnamen en creditcardgegevens stelen. Het kan om hardware gaan, maar ook om software.

Bij Avans was het kennelijk hardware, want volgens nieuwswebsite Punt vraagt de Brabantse hogeschool iedereen alert te zijn op verdacht gedrag: "Zie je bijvoorbeeld dat iemand aan de achterkant van een pc bezig is met de bekabeling? Meld dit dan bij de ict-helpdesk op de locatie waar je je bevindt", aldus een bericht op de interne website.Het is bij Avans al eens eerder gebeurd, weet Punt. In 2012 werd een student van de opleiding weggestuurd die een keylogger zou hebben geplaatst om inloggegevens van docenten te stelen. De student ging ertegen in beroep en kreeg gelijk: er was niet genoeg bewijs.

Martin Romijn, chief information security officer aan de TU/e, stelt "met 99 procent zekerheid" dat de universiteit het gebruik van hardwarematige key-loggers de afgelopen tien jaar op de Eindhovense campus in elk geval niet is tegengekomen. Volgens hem zijn de apparaatjes die hackers hiervoor gebruiken vorige week tijdens een overleg nog ter sprake gekomen, "toen werd niet gezegd dat zoiets ooit bij de TU/e is aangetroffen", aldus Romijn, hier zelf pas driekwart jaar werkzaam.Een dergelijk bericht vanuit een collega-instelling in het hoger onderwijs maakt de TU/e volgens hem wél extra alert "en geeft aanleiding voor een eigen interne waarschuwing hierover." Maar, zo zegt hij ook: "Gebruikers vragen dagelijks te controleren of er geen vreemde apparaatjes achter het werkstation verstopt zitten, is ook geen haalbare zaak. PC's hebben helaas geen lampje zoals het dashboard van de auto waaraan je snel kunt zien dat de motor onvoldoende olie heeft".

Romijn en Dienst ICT waarschuwden onlangs al voor de toenemende cybercriminaliteit wereldwijd, die ook de TU/e kan treffen. Romijn liet toen weten dat de universiteit in sommige opzichten misschien wel wat minder open moet worden.

Bron: https://www.cursor.tue.nl/nieuwsartikel/artikel/hackers-willen-wachtwoorden-stelen-bij-avans/

3.2.2 Identiteitsfraude

risico 

Voor onderwijsinstellingen is identiteitsfraude een van de belangrijkste problemen. In het algemeen wordt identiteitsfraude vooral ingezet voor financieel gewin; binnen de onderwijssector is het vooral een middel om ongeautoriseerde toegang tot systemen en applicaties te verkrijgen. Wanneer een student zich voordoet als iemand anders tijdens tentamens of examens, is de integriteit van alle studieresultaten in het geding. Wanneer een student de identiteit van een docent of medewerker overneemt, kan die misbruikt worden om gegevens in te zien of te manipuleren. Dit kan grote gevolgen hebben voor de reputatie van de instelling.

Voornaamste actoren: studenten, ontevreden medewerkers of docenten.

3.2.3 Verkrijging en openbaarmaking van data

risico 

Iedere onderwijs- en onderzoeksinstelling verzamelt gevoelige data ten behoeve van onderwijs. Die variëren van persoonsgegevens tot de behaalde studieresultaten. Doordat in het algemeen het cyberbewustzijn bij de instellingen laag is (zoals bijvoorbeeld is gebleken uit de resultaten van de SURFaudit-benchmark 2015) is de kans op lekken van die data aanzienlijk. Ook technische kwetsbaarheden, of ze nu zero-day (zie kader Zero-day) zijn of al langer bekend, kunnen misbruikt worden om toegang tot systemen te verkrijgen en gegevens te verzamelen. Dit kan aanzienlijke reputatieschade opleveren.

Voornaamste actoren: cybercriminelen.

3.2.4 Verstoring ICT

risico 

De beschikbaarheid van netwerken en systemen is van cruciaal belang, vanwege de eerder beschreven openheid van instellingsnetwerken, het gebruik van online leermiddelen, intranetten en het nog steeds toenemende gebruik van online opslagdiensten. Uit gegevens van SURFcert blijkt dat DDoS-aanvallen onverminderd doorgaan, maar in het algemeen goed zijn tegen te gaan. In de afgelopen periode was er een sterke toename van ransomwarebesmettingen. Hierdoor kunnen bestanden, bijvoorbeeld toetsresultaten, lesstof en opdrachten, verloren gaan en het onderwijsproces verstoren. De schade kan aanzienlijk zijn.

Voornaamste actoren: activisten, studenten en medewerkers.

3.2.5 Overname en misbruik ICT

risico 

Wanneer kwaadwillenden toegang verkrijgen tot systemen en het netwerk die nodig zijn voor het onderwijsproces, kunnen deze verstoord worden. De kans hierop is echter klein.

Voornaamste actoren: cybercriminelen.

3.2.6 Bewust beschadigen imago

risico 

Het bewust beschadigen van imago gebeurt meestal door de website van een instelling te manipuleren (defacing), omdat die vaak makkelijk toegankelijk is en een groot bereik heeft. Dit is echter ook gemakkelijk te herstellen, waardoor de schade in het algemeen meevalt.

Voornaamste actoren: studenten, activisten.

3.2.7 Spionage

risico 

Studenten beschikken over concurrentiegevoelige informatie doordat ze een stageopdracht bij een bedrijf uitvoeren of participeren in een wetenschappelijk onderzoek. Die informatie kan interessant zijn voor derde partijen. De kans dat studenten gevoelige informatie doorspelen is klein, maar kan wel enige impact hebben.

Voornaamste actoren: studenten

3.3 Onderzoeksproces

In dit hoofdstuk wordt beschreven welke dreigingen relevant zijn voor het onderzoeksproces.

Type dreiging		Manifestatie van dreiging	Risico
1	Verkrijging en openbaarmaking van data	• Onderzoeksgegevens worden gestolen • Privacygevoelige informatie wordt gelekt en gepubliceerd • Blauwdruk van opstelling onderzoeksinstellingen komt in verkeerde handen	HOOG
2	Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	HOOG
3	Identiteitsfraude	• Activist doet zich voor als onderzoeker	MIDDEN
4	Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata worden vernietigd • Opzet van onderzoeksinstellingen wordt gesaboteerd	MIDDEN
5	Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	MIDDEN
6	Manipulatie van digitaal opgeslagen data	• Manipulatie van onderzoeksgegevens	LAAG

Tabel 6: Dreigingen voor het onderzoeksproces

Actor	Vaardigheidsniveau	Dreiging
Studenten	Laag tot Gemiddeld	Verstoren ICT
Medewerkers	Laag	Identiteitsfraude
		Manipulatie van data
		Verstoren ICT
Cybercriminelen	Gemiddeld tot Hoog	Verkrijging en openbaarmaking van data
		Overname en misbruik ICT
		Spionage
Cyberonderzoekers	Hoog	Verkrijging en openbaarmaking van data
		Verstoren ICT
Staten	Zeer Hoog	Verkrijging en openbaarmaking van data
		Spionage
		Overname en misbruik ICT
Commerciële bedrijven & Partner-instellingen	Laag tot Gemiddeld	Spionage
Activisten	Laag tot Gemiddeld	Verstoren ICT
		Bewust beschadigen imago
		Overname en misbruik ICT
Cybervandalen	Laag	Bewust beschadigen imago

Tabel 7: Dreigingen per actor voor het onderzoeksproces

3.3.1 Verkrijging en openbaarmaking van data

risico ● ■ ■

Bij het doen van onderzoek kunnen allerlei gevoelige gegevens worden verwerkt en opgeslagen. Dat kan opgedane kennis zijn of intellectueel eigendom, maar ook informatie over gevoelige onderzoeken, bijvoorbeeld in de medische sector of over nucleair onderzoek. Het openbaar maken van dit soort gevoelige informatie kan grote maatschappelijke onrust veroorzaken en zelfs leiden tot aansprakelijkheidsclaims. Uit onderzoek blijkt dat in het algemeen cyberbewustzijn bij onderzoekers laag is en vooral gedacht wordt vanuit gemak en efficiëntie. Het gebruik van online opslagdiensten verdient hierbij extra aandacht.

Voornaamste actoren: cybercriminelen, staten, activisten, onderzoekers

3.3.2 Spionage

risico ● ■ ■

Onderzoeksinstellingen kunnen beschikken over gevoelige informatie waar niet alleen criminelen, maar ook staten veel belangstelling voor hebben. Omdat bij veel onderzoeksprojecten samengewerkt wordt tussen verschillende instellingen, en soms ook met private partijen, is bescherming van gevoelige onderzoeksdata een heikel punt. Zelfs wanneer de beveiliging op orde is en de data op zorgvuldige wijze worden opgeslagen, kan informatie gestolen worden wat kan leiden tot claims van derden. Verder zijn volgens de AIVD de Nederlandse topsectoren, waaronder high tech, chemie, energie, water en life sciences & health een populair doelwit in het kader van economische spionage [1]. Daarbij constateert de AIVD tevens dat de complexiteit van digitale spionageaanvallen alsmaar toeneemt en dat detectie daarvan erg moeilijk is. De aanvallers zorgen er bovendien voor dat ze de slachtoffers op afstand blijven volgen om te weten wanneer hun aanval wordt gedetecteerd en welke maatregelen worden genomen, zodat ze tegenmaatregelen kunnen nemen om toegang te blijven houden. De impact van spionage kan dan ook zeer hoog zijn, bijvoorbeeld doordat intellectueel eigendom (de kroonjuwelen) wordt weggesluisd, er verlies van innovatievoorsprong is, reputatieschade optreedt en de kosten van (complexe) mitigatie zeer hoog kunnen zijn. Tegelijkertijd is het inschatten van de kans ervan lastig, omdat er geen gedocumenteerde historie beschikbaar is.

Voornaamste actoren: cybercriminelen, staten, commerciële bedrijven.

3.3.3 Identiteitsfraude

risico ● ■ ■

Voor onderzoeksinstellingen is identiteitsfraude een belangrijk probleem. Terwijl het in de maatschappij veelal ingezet wordt voor financieel gewin, is het binnen de onderzoekssector vooral een middel om toegang tot data te krijgen. Wanneer bijvoorbeeld activisten zich voordoen als onderzoeker kunnen ze bij gevoelige data komen die niet publiek toegankelijk zijn. Dit kan gevolgen hebben voor de reputatie van de instelling en de privacy van de medewerkers en onderzoekers..

Voornaamste actoren: activisten, cybercriminelen.

3.3.4 Verstoring ICT

risico ● ■ ■

De eerder beschreven openheid van instellingsnetwerken en het nog steeds toenemende gebruik van online opslagdiensten, maakt dat beschikbaarheid van systemen en het netwerk ook voor onderzoekers van cruciaal belang is. Uit gegevens van SURFcert blijkt dat DDoS aanvallen weliswaar onverminderd doorgaan [22], maar in het algemeen goed zijn tegen te gaan. Verder laat de rapportage periode een sterke toename van ransomware besmettingen zien. Hierdoor kunnen bestanden, bijvoorbeeld onderzoeksdata, verloren gaan. De schade kan aanzienlijk zijn.

Voornaamste actoren: activisten, studenten en medewerkers.

3.3.5 Overname en misbruik ICT

risico ● ■ ■

Veel onderzoek is afhankelijk van systemen en netwerkconnectiviteit, bijvoorbeeld voor het uitvoeren van berekeningen. Dit soort systemen vormen een aantrekkelijk doelwit voor derden die zulke rekenkracht voor eigen, al dan niet illegaal, gebruik willen aanwenden. Allereerst kan dat invloed hebben op de capaciteit die overblijft voor legitieme doeleinden, maar ook kan de instelling verantwoordelijk worden gehouden voor illegale activiteiten die op haar systemen en netwerken plaatsvinden. Ook kunnen activisten proberen de processen te verstoren. Daarnaast kunnen systemen bij Nederlandse universiteiten misbruikt worden als springplank voor illegale of spionage activiteiten in andere landen. Dit heeft onder andere te maken met de hoge kwaliteit van het ‘Nederlandse internet’. De impact kan dan ook aanzienlijk zijn.

Voornaamste actoren: activisten, studenten, cybercriminelen, staten.

NIEUWSITEM

ONDERZOEKERS VINDEN 500.000 KWETSBARE IOT-APPARATEN

maandag 10 oktober 2016, 10:57 door Redactie,

Beveiligingsonderzoekers hebben meer dan 500.000 kwetsbare Internet of Things-apparaten van een Chinese fabrikant ontdekt die via een standaard-wachtwoord kunnen worden gehackt en gebruikt voor het uitvoeren van bijvoorbeeld ddos-aanvallen, zo waarschuwt beveiligingsbedrijf Flashpoint.

Het gaat om apparaten zoals digitale videorecorders, netwerkvideorecorders en ip-camera's van de Chinese fabrikant XiongMai Technologies. De fabrikant ontwikkelt de hardware die allerlei andere bedrijven vervolgens als hun eigen product doorverkopen. De apparaten maken echter gebruik van een standaard wachtwoord en gebruikersnaam waarmee een aanvaller via Telnet kan inloggen. Onlangs werden verschillende grote ddos-aanvallen waargenomen die via gehackte IoT-apparaten werden uitgevoerd.

De apparaten waren geïnfecteerd door malware die via de standaard inloggegevens binnenkwam. Vervolgens werden de besmette IoT-apparaten gebruikt voor het vinden van nieuwe kwetsbare apparaten en het platleggen van websites. Volgens onderzoekers van Forcepoint is het probleem dat het standaard wachtwoord en gebruikersnaam niet eenvoudig zijn te veranderen. Zo is het wachtwoord 'hardcoded' in de firmware en zijn er geen tools voorhanden om het wachtwoord uit te schakelen. Daarnaast is het via de webinterface van de apparaten niet duidelijk dat er een dergelijk standaard wachtwoord is.

De onderzoekers ontdekten daarnaast ook een tweede kwetsbaarheid in de apparatuur van Xiong-Mai Technologies waarop de "CMS" or "NetSurveillance" software draait. De inlog-url voor het apparaat vraagt om een gebruikersnaam en wachtwoord. Zodra de gebruiker inlogt wordt een tweede pagina geladen. Deze pagina blijkt ook direct benaderbaar zonder inloggegevens te zijn. Via de zoekmachine Shodan vonden de onderzoekers in totaal 515.000 apparaten op internet die met beide beveiligingslekken te maken hebben.

Bron: https://www.security.nl/posting/488313/Onderzoekers+vinden+500_000+kwetsbare+IoT-apparaten

FBI: HACK VS LIEP VIA NEDERLAND

De FBI slaat alarm nadat hackers zijn binnengedrongen in Amerikaanse verkiezingssystemen. Ze hebben gebruikgemaakt van Nederlandse internetservers, die vanwege hun snelheid populair zijn bij het hackersgilde.

Koen Voskuil 13-09-16, 07:43 Laatste update: 14-09-16, 06:01

Paniek in de Verenigde Staten. Vermoedelijk Russische hackers hebben sinds juli aanvallen gepleegd op de zogeheten State Board of Election Systems, waar databases met alle kiesgerechtigden worden bijgehouden.

"Maar liefst vier van de acht gebruikte servers staan in Nederland", zegt oud-hacker Rickey Gevers. Die servers worden aangestuurd vanuit Rusland. Het is dus waarschijnlijk dat hier een Russische hackersgroep achter zit."

Internetknooppunt

Het is niet ongewoon dat Russische hackers zich bedienen van Nederlandse internetservers, zegt securityconsultant Roel van der Valk van beveiligingsbedrijf Pinewood. „Nederland is een belangrijk internetknooppunt met een goede infrastructuur. Daar komen helaas ook hackers op af.

Bron: http://www.ad.nl/dossier-nieuws/fbi-hack-vs-liep-via-nederland-aa8db113/

3.3.6 Manipulatie van digitaal opgeslagen data

risico ■ •

Het vastleggen van onderzoeksdata wordt steeds meer gezien als een belangrijke taak van onderzoeksinstellingen om de transparantie en controleerbaarheid van onderzoeken te waarborgen. Er zijn een aantal gevallen geweest van onderzoekers die hun onderzoeksdata gemanipuleerd lijken te hebben om gewenste resultaten te kunnen tonen. Opslag van ruwe onderzoeksdata wordt dan ook meer een kerntaak van de instellingen. De kans op manipulatie is echter niet groot.

Voornaamste actoren: onderzoekers, medewerkers.

3.4 Bedrijfsvoering

Hieronder leest u welke dreigingen relevant zijn voor de bedrijfsvoering.

Type dreiging		Manifestatie van dreiging	Risico
1	Verkrijging en openbaarmaking van data	• Privacygevoelige informatie wordt gelekt en gepubliceerd • Andere gevoelige informatie, bijvoorbeeld financiële informatie, wordt gelekt en gepubliceerd	HOOG
2	Verstoring ICT	• DDoS-aanval legt IT-infrastructuur plat • Kritieke onderzoeksdata of examendata worden vernietigd • Onderwijsmiddelen worden onbruikbaar door malware (bijvoorbeeld eLearning of het netwerk)	MIDDEN
3	Overname en misbruik ICT	• Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	MIDDEN
4	Identiteitsfraude	• Medewerker verkrijgt toegang tot personeelsgegevens en manipuleert die.	LAAG
5	Manipulatie van digitaal opgeslagen data	• Medewerker verkrijgt toegang tot personeelsgegevens en manipuleert die.	LAAG

Tabel 8: Dreigingen voor bedrijfsvoering

Actor	Vaardigheidsniveau	Dreiging
Studenten	Laag tot Gemiddeld	Verstoren ICT
Cybercriminelen	Gemiddeld tot Hoog	Verkrijging en openbaarmaking van data
		Identiteitsfraude
Cyberonderzoekers	Hoog	Verkrijging en openbaarmaking van data
		Verstoren ICT
Activisten	Laag tot Gemiddeld	Verstoren ICT

Tabel 9: Dreigingen per actor voor bedrijfsvoering

3.4.1 Verkrijging en openbaarmaking van data

risico

Bij de bedrijfsvoering worden allerlei gevoelige data verwerkt en opgeslagen, bijvoorbeeld personeelsgegevens en financiële data. Sinds de invoering van de meldplicht datalekken en de aanstaande inwerkingtreding van de AVG (mei 2018) is het beschermen van persoonsgegevens zeer belangrijk en lekken van dat soort data kan tot flinke financiële en reputatieschade leiden.

Voornaamste actoren: cybercriminelen, activisten, medewerkers.

3.4.2 Verstoring ICT

risico

De eerder beschreven openheid van instellingsnetwerken en het nog steeds toenemende gebruik van online applicaties en opslagdiensten, maakt dat beschikbaarheid van systemen en het netwerk ook voor de bedrijfsvoering van belang is. De sterke toename van ransomwarebesmettingen van de laatste tijd maken de kans groter dat bestanden, zoals personeelsgegevens en financiële gegevens, verloren gaan. De impact daarvan kan aanzienlijk zijn, vooral in verband met de dit jaar ingevoerde meldplicht datalekken en eventuele sancties die daarop kunnen volgen.

Voornaamste actoren: activisten, medewerkers.

3.4.3 Overname en misbruik ICT

risico

De bedrijfsvoering is afhankelijk van systemen en netwerkconnectiviteit, vooral door de steeds grotere toepassing van online applicaties. Net als bij ‘verstoring ICT’ kan de impact van overname en misbruik van ICT aanzienlijk zijn.

Voornaamste actoren: activisten, medewerkers.

3.4.4 Identiteitsfraude

risico

Voor bedrijfsvoering wordt identiteitsfraude niet als een acute dreiging gezien. De kans dat het voorkomt is zeer laag, hoewel het denkbaar is dat een ontevreden medewerker zich via identiteitsfraude toegang verschaft tot bijvoorbeeld personeelsdossiers. Dit kan gevolgen hebben voor de reputatie van de instelling, de privacy van de medewerkers en de integriteit van dossiers.

Voornaamste actoren: medewerkers.

3.4.5 Manipulatie van digitaal opgeslagen data

risico

Voor informatievoorziening en financiën is het belangrijk dat de integriteit van gegevens gewaarborgd is. Deze processen zijn echter al volwassen en goed ingebed in de organisatie. De kans op manipulatie van data wordt dan ook als zeer laag beschouwd.

Voornaamste actoren: medewerkers.

VOORBEELDINCIDENTEN

ANONIMISATIE EN PSEUDONIMISATIE

Volgens de Nederlandse Praktijk Richtlijn NPR-ISO/TS 25237:2009 ‘Health informatics — Pseudonymization’[13] zijn zowel anonimisatie als pseudonimisatie vormen van de-identificatie.

Anonimisatie is het proces dat de koppeling tussen een identificerende dataset en het datasubject verbreekt en *geanonimiseerde data* zijn data waaruit de patiënt niet kan worden geïdentificeerd door de ontvanger.

Pseudonimisatie is een specifieke vorm van anonimisatie. Hierbij wordt ook de koppeling tussen een identificerende dataset en het datasubject verbroken, maar wordt er ook een associatie gecreëerd tussen een specifieke set karakteristieken gerelateerd aan het datasubject en een of meer pseudoniemen. Een *pseudoniem* is een persoonlijke identificatiecode die verschilt van een normale persoonlijke identificatiecode.

Pseudonimiseren onderscheidt zich van anonimiseren doordat bij anonimiseren het koppelen van gegevens uit verschillende bronnen niet mogelijk is, terwijl dat bij pseudonimiseren wel mogelijk is.

De Autoriteit Persoonsgegevens (voorheen CBP) heeft criteria opgesteld waaraan voldaan moet worden bij de toepassing van pseudonimisatie[14]:

1. Er wordt vakkundig gebruik gemaakt van pseudonimisering, waarbij de eerste encryptie plaatsvindt bij de aanbieder van de gegevens.
2. Er zijn technische en organisatorische maatregelen genomen om herleidbaarheid van de versleuteling (replay attack) te voorkomen.
3. De verwerkte gegevens zijn niet indirect identificerend.
4. In een onafhankelijk deskundig oordeel (audit) wordt voor aanvang van de verwerking en daarna periodiek vastgesteld dat aan de voorwaarden 1, 2 en 3 is voldaan.
5. De pseudonimiseringsoplossing moet op heldere en volledige wijze worden beschreven in een openbaar document, zodat iedere betrokkene kan nagaan welke garanties de gekozen oplossing biedt.

ZERO-DAY AANVALLEN

Een zero-day aanval (zero-day exploit) is een aanval die misbruikt maakt van een onbekende kwetsbaarheid in software of een applicatie. Zo’n kwetsbaarheid heet dan ook een zero-day kwetsbaarheid (zero-day vulnerability).

Het is niet mogelijk een zero-day aanval te detecteren, althans niet met traditionele middelen als antivirussoftware en websitereputatiedatabases, simpelweg omdat de betreffende kwetsbaarheid nog niet bekend is. Traditionele beschermingssoftware werkt op basis van patroonherkenning en van een zero-day aanval is het patroon nog niet bekend.

Tot nog toe zijn in 2016 negen zero-day exploits ontdekt en in heel 2015 waren het er dertien[15]. Volgens eerder onderzoek van FireEye duurt het circa 310 dagen voordat kwetsbaarheden die door cybercriminelen zijn ontdekt, bekend worden[16].

Dit soort kwetsbaarheden worden voor grote bedragen openlijk verkocht:
“Researchers from Trustwave’s SpiderLabs team have uncovered a zero-day exploit on Russian underground malware forum exploit.in, affecting all versions of Microsoft Windows OS from Windows 2000 all the way up to a fully patched version of Windows 10.” [17]

De prijs is van deze kwetsbaarheid is 90.000 dollar...

[13] https://www.nen.nl/NEN-Shop/Norm/NPRISOTS-252372009-en.htm
[14] https://www.zorgttp.nl/userfiles/Downloads/Facsheet_pseudonimisatie_algemeen_201307.pdf (geraadpleegd op 26 september 2016)
[15] https://www.fireeye.com/current-threats/recent-zero-day-attacks.html (geraadpleegd op 30 september 2016)
[16] https://www2.fireeye.com/rs/848-DID-242/images/wp-zero-day-danger.pdf (opgehaald op 30 september 2016)
[17] https://thehackernews.com/2016/06/windows-zero-day-exploit.html (geraadpleegd op 7 oktober 2016)

4. WEERBAARHEID

4.1 Inleiding

Zoals in hoofdstuk 1.6 al is vermeld, maakt dit rapport deel uit van het SURF innovatieprogramma *Betrouwbare en veilige omgeving.* De ambitie van dit innovatieprogramma is dat SURF en de aangesloten instellingen in 2018 immuun zijn voor beveiligingsincidenten en cyberaanvallen. Immuun betekent dat, hoewel zich incidenten voordoen, de beschikbaarheid en betrouwbaarheid van informatie en systemen op hoog niveau gegarandeerd blijven en de herstel- en schadekosten laag zijn. Het gevolg is een snel herstel, dat niet ten koste gaat van een open en vrij toegankelijk internet.

4.2 Maatregelen nemen

Om dat te bereiken moeten instellingen maatregelen nemen om hun cyberweerbaarheid te verhogen. In het Cyberdreigingsbeeld 2015 [22] hebben we gesignaleerd dat de-perimeterization de manier van beschermen van data verandert. Dit vertaalt zich in andersoortige maatregelen: traditionele beschermingsconstructies met firewalls werken niet meer, omdat de gebruikers zich in veel gevallen niet binnen de perimeter bevinden. Bovendien worden data meer en meer in de cloud verwerkt en opgeslagen, wat ook invloed heeft op de maatregelen die nodig zijn. En, zoals eerder genoemd, is dataclassificatie belangrijk om te bepalen welke maatregelen adequaat zijn ter bescherming van data vóórdat uitwisseling daarvan plaatsvindt tussen gebruikers onderling en met gebruikers van andere instellingen of partijen.

4.2.1 Voorbereidingen

Voor het invoeren van maatregelen moet het bestuur van de instelling allereerst een goed beeld hebben van welke bedreigingen er zijn, welke bedreigingen relevant zijn voor de organisatie, wat de kroonjuwelen van de organisatie zijn en welke data in de cloud worden verwerkt of opgeslagen.

Verder is het belangrijk dat het bestuur weet wat de status is van de cyberweerbaarheid van de eigen instelling en hoe die zich verhoudt tot die van andere, vergelijkbare instellingen.

SURFaudit voorziet in deze laatste doelstellingen. De self-assessment op basis van het Normenkader IBHO is een goed instrument om te bepalen hoe ‘cyberweerbaar’ de instelling is. SURFaudit voorziet ook in een tweejaarlijkse benchmark waarmee instellingen hun cyberweerbaarheid kunnen spiegelen aan die van collega-instellingen.

4.2.2 Maatregelen tegen belangrijke bedreigingen voor het onderwijsproces

Manipulatie van digitaal opgeslagen data
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het aspect *integriteit*:

- Dataclassificatie – Er is een classificatiesysteem, zodat gebruikers kunnen bepalen welke data gevoelig zijn en hoe ze er mee om moeten gaan.
- Identiteitscontrole – Er is een systeem om de identiteit van gebruikers vast te stellen. Daarbij wordt onderscheid gemaakt tussen de initiële identificatie en het controleren van de identiteit op momenten dat die vastgesteld moet worden om toegang te verlenen (dit kan digitale toegang zijn, maar ook fysieke toegang).

- Toegangscontrole – Er is een systeem voor identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen tot welke data, vanaf welke locaties en met welke apparaten.
- Versleuteling – Voor het beschermen van de integriteit en vertrouwelijkheid van gegevens wordt versleuteling van de data toegepast, zowel bij opslag als tijdens transport (bijvoorbeeld via e-mail of file transfer).
- Logging – Toegang tot de data wordt gelogd, zodat vastgesteld kan worden (real-time of achteraf) op welke manier de data zijn verwerkt en door wie.
- Back-up en restore – Er is een back-upprocedure zodat data na een incident hersteld kan worden.

Identiteitsfraude
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het aspect *integriteit*:
- Identiteitscontrole – Er is een systeem om de identiteit van gebruikers vast te stellen. Daarbij wordt onderscheid gemaakt tussen de initiële identificatie en het controleren van de identiteit op momenten dat die vastgesteld moet worden om toegang te verlenen (dit kan digitale toegang zijn, maar ook fysieke toegang).
- Toegangscontrole – Er is een systeem om aan de hand van de identiteit te bepalen of, en welke, toegang verleend wordt.
- Bewustzijn – Gebruikers moeten zich bewust zijn van aanvalstechnieken om identiteiten te achterhalen als (spear)phishing en social engineering, zodat zij daarvan niet het slachtoffer worden.

4.2.3 Maatregelen tegen belangrijke bedreigingen voor het onderzoeksproces

Verkrijging en openbaarmaking van data
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het aspect *vertrouwelijkheid*:
- Fysieke beveiliging – Er is (bijvoorbeeld) een pasjessysteem voor ruimtes en locaties waar systemen zijn gehuisvest. Voor het toekennen van toegangsrechten tot de ruimtes en externe locaties is een proces ingericht. Voor datacenters geldt dat de toegang strak wordt gecontroleerd.
- Dataclassificatie – Er is een classificatiesysteem, zodat gebruikers kunnen bepalen welke data gevoelig zijn en hoe ze er mee om moeten gaan, en zodat bepaald kan worden welke gebruikers toegang krijgen.
- Toegangscontrole – Er is een systeem voor identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen tot welke data, vanaf welke locaties en met welke apparaten.
- Versleuteling – Voor het beschermen van de vertrouwelijkheid en integriteit van gegevens wordt, afhankelijk van de classificatie, versleuteling van de data toegepast, zowel bij opslag als tijdens transport (bijvoorbeeld via e-mail of file transfer). Versleutelingsprotocollen en algoritmes voldoen aan de huidige stand der techniek.
- Zonering – Voor de opslag van gevoelige data wordt zonering toegepast, bijvoorbeeld gebruikmakend van het ‘Defense-in-depth’-principe, zodat de data bij een eventuele inbraak niet zomaar benaderd kan worden of naar buiten gebracht kan worden.
- Bewustzijn – Gebruikers weten dat er dataclassificatie is en welke maatregelen ze moeten nemen om gevoelige data te beschermen.
- Informatiebeveiligingscontinuïteit – Wanneer zich een incident voordoet moeten maatregelen effectief blijven, zodat bescherming van de gevoelige data gewaarborgd blijft.

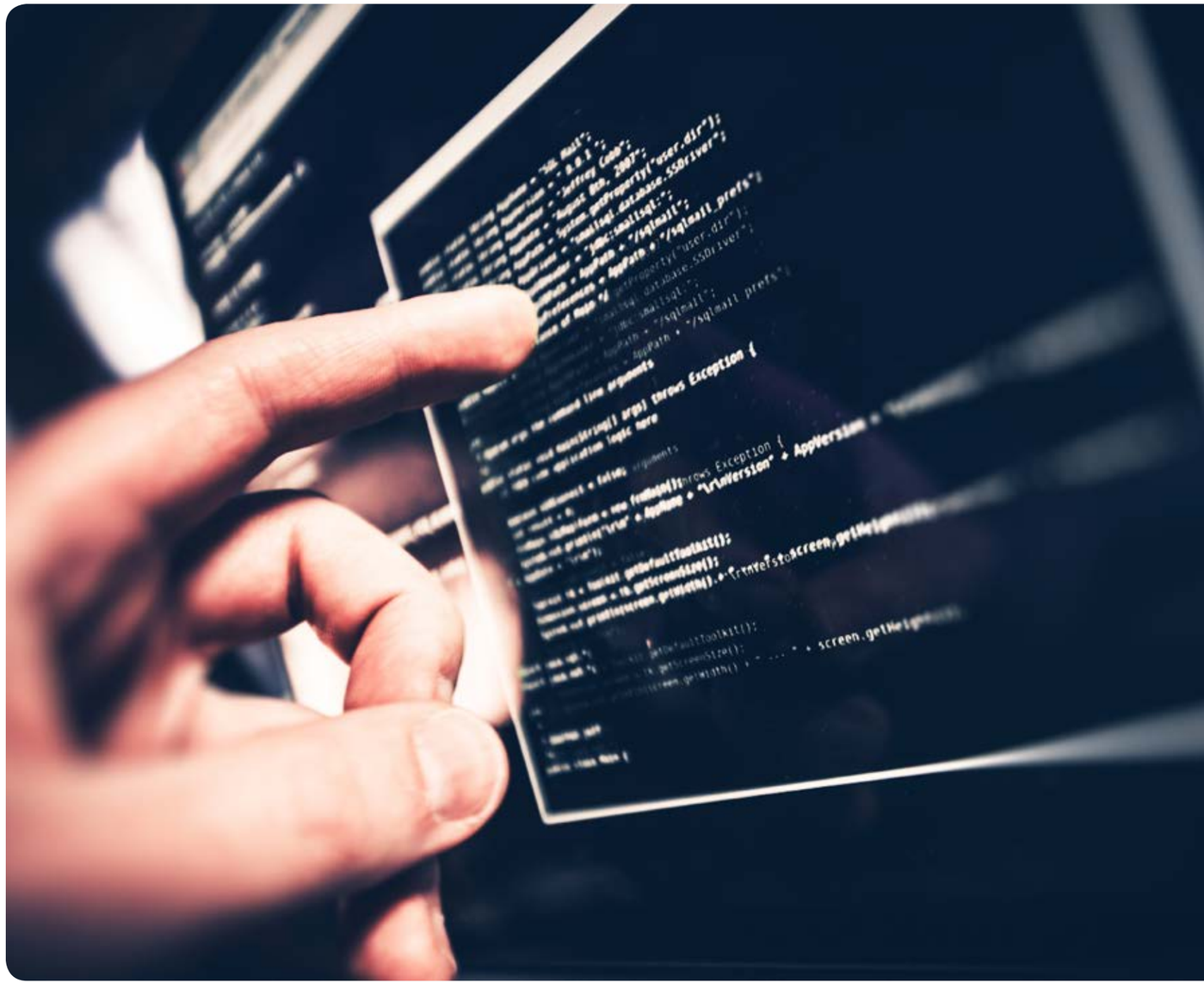
Spionage
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het aspect *vertrouwelijkheid*:
- Bewustzijn – Gebruikers weten dat er dataclassificatie is en welke maatregelen ze moeten nemen om gevoelige data te beschermen.
- Toegangscontrole – Er is een systeem voor identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen tot welke data, vanaf welke locaties en met welke apparaten.
- Versleuteling – Voor het beschermen van gegevens wordt, afhankelijk van de classificatie, versleuteling van de data toegepast, zowel bij opslag als tijdens transport (bijvoorbeeld via e-mail of file transfer). Versleutelingsprotocollen en algoritmes voldoen aan de huidige stand der techniek.
- Zonering – Voor de opslag van gevoelige data wordt zonering toegepast, bijvoorbeeld gebruikmakend van het ‘Defense-in-depth’-principe, zodat de data bij een eventuele inbraak niet zomaar benaderd kan worden of naar buiten gebracht kan worden.
- Netwerkmonitoring – Het interne netwerk en de koppeling naar het publieke netwerk worden gemonitord om ongebruikelijke patronen over langere tijd te detecteren.
- Logging – Gegevens over het inkomende en uitgaande verkeer worden bewaard voor periodieke analyse om ongebruikelijke patronen over langere periodes te signaleren. Logbestanden worden op adequate wijze beschermd tegen manipulatie.
- Systeemmonitoring – Systemen worden gemonitord om ongebruikelijke activiteit te detecteren die over langere tijd plaatsvindt. Opgeslagen monitoringdata worden op adequate wijze beschermd tegen manipulatie.
- Informatiebeveiligingscontinuïteit – Beveiligingsmaatregelen worden gehandhaafd wanneer zich een incident voordoet en de data niet op de normale manieren verwerkt kunnen worden ten gevolge van het incident.

4.2.4 Maatregelen tegen dreigingen voor de bedrijfsvoering

Verkrijging en openbaarmaking van data
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het aspect *vertrouwelijkheid*:
- Fysieke beveiliging – Er is (bijvoorbeeld) een pasjessysteem voor ruimtes en locaties waar systemen zijn gehuisvest. Voor het toekennen van toegangsrechten tot de ruimtes en externe locaties is een proces ingericht. Voor datacenters geldt dat de toegang strak wordt gecontroleerd.
- Dataclassificatie – Er is een classificatiesysteem, zodat gebruikers kunnen bepalen welke data gevoelig zijn en hoe ze er mee om moeten gaan, en zodat bepaald kan worden welke gebruikers toegang krijgen.
- Toegangscontrole – Er is een systeem voor identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen tot welke data, vanaf welke locaties en met welke apparaten.
- Versleuteling – Voor het beschermen van de vertrouwelijkheid en integriteit van gegevens wordt, afhankelijk van de classificatie, versleuteling van de data toegepast, zowel bij opslag als tijdens transport (bijvoorbeeld via e-mail of file transfer). Versleutelingsprotocollen en algoritmes voldoen aan de huidige stand der techniek.
- Zonering – Voor de opslag van gevoelige data wordt zonering toegepast, bijvoorbeeld gebruikmakend van het ‘Defense-in-depth’-principe, zodat de data bij een eventuele inbraak niet zomaar benaderd kan worden of naar buiten gebracht kan worden.
- Bewustzijn – Gebruikers weten dat er dataclassificatie is en welke maatregelen ze moeten nemen om gevoelige data te beschermen.
- Informatiebeveiligingscontinuïteit – Wanneer zich een incident voordoet moeten maatregelen effectief blijven, zodat bescherming van de gevoelige data gewaarborgd blijft.

Verstoring ICT
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op de aspecten *beschikbaarheid* en *integriteit*:
- Antivirus software – Antivirussoftware is op alle systemen geïnstalleerd om malware-infecties tegen te gaan.
- Netwerkmonitoring – Het interne netwerk en de koppeling naar het publieke netwerk worden gemonitord om ongebruikelijke patronen te detecteren.
- Systeemmonitoring – Systemen worden gemonitord om ongebruikelijke activiteit te detecteren. Opgeslagen monitoringdata worden op adequate wijze beschermd tegen manipulatie.
- Logging – Gegevens over het inkomende en uitgaande verkeer worden bewaard voor analyse (real-time of achteraf). Logbestanden worden op adequate wijze beschermd tegen manipulatie.
- Back-up en restore – Er is een back-upprocedure zodat data na een incident hersteld kunnen worden.

Overname en misbruik ICT
De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op de aspecten *beschikbaarheid* en *integriteit*:
- Fysieke beveiliging – Er is (bijvoorbeeld) een pasjessysteem voor ruimtes en locaties waar systemen zijn gehuisvest. Voor het toekennen van toegangsrechten tot de ruimtes en externe locaties is een proces ingericht. Voor datacenters geldt dat de toegang strak wordt gecontroleerd.
- Toegangscontrole – Er is een systeem voor Identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen tot welke data, vanaf welke locaties en met welke apparaten.
- Netwerkmonitoring – Het interne netwerk en de koppeling naar het publieke netwerk worden gemonitord om ongebruikelijke patronen te detecteren.
- Systeemmonitoring – Systemen worden gemonitord om ongebruikelijke activiteit te detecteren. Opgeslagen monitoringdata worden op adequate wijze beschermd tegen manipulatie.
- Logging – Gegevens over het inkomende en uitgaande verkeer worden bewaard voor periodieke analyse om ongebruikelijke patronen te signaleren. Logbestanden worden op adequate wijze beschermd tegen manipulatie.



5. BIBLIOGRAFIE

[1] AIVD, Jaarverslag 2015, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2015.
[2] NCSC, Cyberdreigingsbeeld Nederland, [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland. [Geopend 30 september 2016].
[3] Wetenschappelijke Raad voor het Regeringsbeleid, De publieke kern van het internet, Amsterdam University Press, Amsterdam, 2015.
[4] C. P. Herna Verhagen, De economische en maatschappelijke noodzaak van meer cybersecurity, Cyber Security Raad, 2016.
[5] Autoriteit Persoonsgegevens, Richtsnoer Beveiliging van Persoonsgegevens,AP, 2013.
[6] Autoriteit Persoonsgegevens, Europese Privacywetgeving, [Online]. Available: https://autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/europese-privacywetgeving. [Geopend 26 september 2016].
[7] ENISA, Enisa Threat Landscape 2015, ENISA, 2016.
[8] Fraude Helpdesk, DUITS BEDRIJF € 40 MILJOEN KWIJT DOOR CEO-FRAUDE, [Online]. Available: https://www.fraudehelpdesk.nl/nieuws/duits-bedrijf-e-40-miljoen-kwijt-door-ceo-fraude-2. [Geopend 6 september 2016].
[9] Trend Micro, 2016 Midyear Security Roundup, [Online]. Available: http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup. [Geopend 26 september 2016].
[10] Fortinet, Take it Easy, and Say Hi to This New Python Ransomware, [Online]. Available: https://blog.fortinet.com/2016/09/01/take-it-easy-and-say-hi-to-this-new-python-ransomware. [Geopend 30 september 2016].
[11] Trend Micro, The Reign of Ransomware, TrendLabs, 2016.
[12] B. Krebs. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Geopend 30 september 2016].
[13] Flashpoint, Attack of Things, [Online]. Available: https://www.flashpoint-intel.com/attack-of-things/. [Geopend 30 september 2016].
[14] Top10booters, Top 10 Booters - The Booter Ranking Site, [Online]. Available: http://top10booters.com. [Geopend 30 september 2016].
[15] SafeSkyHacks, Top 10 DDoser's (Booters/Stressers), [Online]. Available: https://www.safeskyhacks.com/Forums/showthread.php?39-Top-10-DDoser-s-%28Booters-Stressers%29. [Geopend 30 september 2016].
[16] Incapsula, DDoS Global Threat Landscape Report Q2-2015, Incapsula, 2016.
[17] Verisign, Verisign iDefense 2016 Cyberthreats and Trends Report, Verisign, 2016.
[18] Verizon, Verizon Data Breach Incident Report 2016, Verizon, 2016.
[19] Symantec, Third Adobe Flash zero-day exploit (CVE-2015-5123) leaked from Hacking Team cache, [Online]. Available: http://www.symantec.com/connect/blogs/third-adobe-flash-zero-day-exploit-cve-2015-5123-leaked-hacking-team-cache. [Geopend 30 november 2015].
[20] GFCE, Launch manifesto on responsible disclosure, Global Forum on Cyber Expertise, [Online]. Available: http://www.thegfce.com/news/news/2016/05/12/launch-manifesto-on-responsible-disclosure. [Geopend 30 september 2016].
[21] SURFnet, Juridisch normenkader cloudservices hoger onderwijs, 09 02 2016. [Online]. Available: https://www.surf.nl/kennisbank/2013/juridisch-normen kader-cloud-services-hoger-onderwijs.html. [Geopend 31 10 2016].
[22] NCSC, Cybersecuritybeeld Nederland 2015, NCSC, 2016.
[23] SURFcert, Kwartaalrapportage Q3 security exploitatie & innovatie, SURFnet, Utrecht, 2016.
[24] SURFnet, Cyberdreigingsbeeld 2015, SURF, Utrecht, 2015.
[25] Wikipedia, [Online]. Available: https://en.wikipedia.org/wiki/Wearable_computer. [Geopend 26 september 2016].

NIEUWSITEM

STUDENT ONTDEKT LEK IN STUDENTEN-INFORMATIE-SYSTEEM HVA EN UVA

Door Olaf van Miltenburg, maandag 20 juni 2016 15:08

Een Nederlandse student heeft in het Student Information System dat de UvA en de HvA gebruiken, een lek ontdekt waarmee hij op eenvoudige wijze persoonsgegevens en foto's van meer dan 500.000 medestudenten kon binnenhalen.
De student software-engineering Nelson Berg liep tegen de kwetsbaarheid aan toen hij zich wilde aanmelden voor een examen. Hij ontdekte door simpelweg naar de bron te kijken dat alle namen en studentnummers te scrapen waren via een url in een verborgen div op de site https://sis.hva.nl. Door vervolgens de parameter {StudentIdentifier} aan te passen, bleken ook de foto's en telefoonnummers van de studenten geautomatiseerd binnengehaald te kunnen worden.
Via het lek kon hij 385.000 namen en studentnummers, 200.000 telefoonnummers en 130.000 foto's van HvA-studenten downloaden. Via het systeem van de UvA lukte dat voor 237.000 namen en id-nummers, 131.000 telefoonnummers en 63.000 foto's. Berg vermoedt dat meer universiteiten van de kwetsbare SIS-implementatie gebruikmaken.
Na de melding tijdens Pinksteren aan het CERT-UvA zijn de kwetsbaarheden op 17 mei, een dag later, verholpen. De UvA bevestigt de lezing van Berg, maar meldt dat SIS de kwetsbaarheid niet meer bevat. "Wij nemen inderdaad SIS af en hebben de leverancier op dezelfde dag dat we de melding kregen op de hoogte gesteld. Daarnaast hebben we ook de overige universiteiten ingelicht en ook daar is het lek gedicht", zegt een woordvoerster tegen Tweakers. Vooralsnog heeft de UvA studenten en medewerkers niet ingelicht over het lek. De UvA zegt geen aanwijzingen te hebben dat het lek misbruikt is, zodat een melding niet nodig leek.
"Alleen van mijn ip-adres ging het om miljoenen requests bij het binnenhalen en er zijn geen alarmbellen afgegaan", zegt Berg tegen Tweakers. "Je zou denken dat ze het monitoren. Waarschijnlijk zit het lek er al vanaf het begin in. Ze kunnen niet met zekerheid zeggen dat het niet is misbruikt, denk ik."
Berg is parttime pentester. "Ik heb een iets grotere achtergrond wat dit soort zaken betreft, maar in tien minuten had ik de twee lekken gevonden, terwijl ik me alleen in wilde schrijven. Ik zag een nummer in een parameter van een url dat sterk op mijn studentnummer leek. Daarna kon ik een scraper in Python schrijven om de gegevens te downloaden." Volgens de student is het onverantwoordelijk dat het systeem een dergelijk lek kon bevatten. "Normaal zie je dit alleen in systemen die nog niet live staan."

Bron: https://tweakers.net/nieuws/112697/student-ontdekt-lek-in-studenteninformatiesysteem-hva-en-uva.html

RENT A DENIAL-OF-SERVICE BOOTER FOR $60, WREAK $720K IN DAMAGE

Or $7.2 million a day, by some measures

4 Mar 2016 at 06:30, Darren Pauli

Criminals can pay distributed-denial-of-service attackers less than US$60 to inflict as much as US$720,000 in damage to an organisation per day, researcher Dennis Schwarz says.

The so-called booter or stresser services are commonly sold as would-be legitimate tools for security professionals. These tools are supposedly used to test the resilience of corporate networks by flooding them offline with junk network traffic. But in reality many booters are used for illegal DDoS and use hacked and stolen router and machine resources to power the attacks.

Schwarz examined one booter service sold on a Russian crime forum by a user known as Forceful comparing the cost to rent per day with the average damage of DDoS and analysing an acquired malware binary.

Bron: http://www.theregister.co.uk/2016/03/04/rent_a_denial_of_service_booter/

COLOFON

Auteur
Bart Bosma

Redactie
Jan Michielsen

Coördinatie
Nanda Bazuin

Ontwerp
Vrije Stijl, Utrecht

Fotografie
iStock

November 2016

Met dank aan:
Hans Alfons, *Vrije Universiteit Amsterdam*
Ronald Boontje, *Universiteit van Amsterdam*
Ludo Cuijpers, *Kennisnet*
Margot van Ditmarsch, *Leids Universitair Medisch Centrum*
Frank Haak, *Universiteit van Amsterdam – Hogeschool van Amsterdam*
Bart van den Heuvel, *Universiteit Maastricht*
Karel van Houten, *TNO*
Xander Jansen, *SURFcert*
Een analist van de AIVD
Elma Middel, *Hanze Hogeschool*
Alf Moens, *SURFnet*
Menno Nonhebel, *KNAW*
Wouter Oosterbaan, *NCSC*
Martijn Plijnaer, *Hogeschool Inholland*
Anita Polderdijk-Rijntjes, *Windesheim*
Remco Poortinga-van Wijnen, *SURFnet*
Jean Popma, *Radboud Universiteit*
René Ritzen, *Universiteit Utrecht*
Martin Romijn, *Technische Universiteit Eindhoven*
Raoul Vernède, *Wageningen University & Research*

SURF

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