CYBERDREIGINGSBEELD 2015

SECTOR ONDERWIJS EN ONDERZOEK

SURF

VOORWOORD

De wereld om ons heen verandert in snel tempo. Toenemende digitalisering raakt alle aspecten van ons leven. Privé- en zakelijke activiteiten zijn niet meer strikt gescheiden: werkdocumenten staan op onze eigen tablet of smartphone, worden doorgestuurd naar ons privé-e-mailadres, en privébestanden staan op werkcomputers. Dat levert veel gemak op, maar ook zorgen over de veiligheid van die gegevens. In de sector onderwijs en onderzoek is er sprake van omvangrijke gegevensuitwisseling tussen medewerkers van instellingen onderling, tussen docenten en studenten, en tussen medewerkers en externe partijen. Voor de instellingen, voor een deel verantwoordelijk voor die gegevens, is het een grote uitdaging om al die gegevens op een efficiënte en veilige manier te behandelen.

Het mbo heeft het afgelopen jaar een inhaalslag gemaakt om informatiebeveiliging naar een hoger niveau te tillen. Maar voor alle instellingen geldt dat ze de beveiliging van gegevens continu verbeteren en steeds meer aandacht hebben voor privacy-vraagstukken. Samenwerkingsverbanden zijn uitgebreid en geïntensiveerd, en houden zich nu ook met privacy bezig. Instellingen maken zo steeds meer gebruik van de middelen en voorbeelden die gedeeld worden.

Dat neemt niet weg dat door de toenemende digitalisering kwaadwillenden ook meer aanvalsmogelijkheden krijgen. We moeten dus steeds blijven nadenken over vragen als: “Hoe kunnen we kennis en informatie op een veilige manier delen en welke maatregelen moeten we nemen om dat te realiseren?” Voorwaarde daarvoor is wel dat informatiebeveiliging en privacy binnen de instellingen hoog op de agenda blijven staan op uitvoerend, facilitair én bestuurlijk niveau.

SURF richt zich op verschillende thema’s die het gebruik van geavanceerde ICT-diensten in het hoger onderwijs en onderzoek stimuleren. *Beveiliging en privacy* is een van die thema’s. SURF helpt onderwijsinstellingen bij het vinden van een balans tussen beveiliging, waarborgen van de privacy, toegankelijkheid en gebruiksgemak. Het Cyberdreigingsbeeld geeft inzicht in de belangrijkste bedreigingen voor de onderwijs- en onderzoeksinstellingen en laat zien welke maatregelen genomen kunnen worden om die bedreigingen tegen te gaan.

Erik Fledderus
Algemeen directeur SURF

INHOUDSOPGAVE

Voorwoord **3**

Managementsamenvatting **6**

1 Inleiding **10**
1.1 Achtergrond: digitale dreigingen nemen toe 10
1.2 Doel: weerbaarheid van de instellingen vergroten 11
1.3 Leeswijzer 11
1.4 Doelgroep: managers en securityprofessionals in hoger onderwijs en mbo 12
1.5 Totstandkoming 12

2 Dreigingslandschap **14**
2.1 Inleiding 14
2.2 Trends 14
2.2.1 Toenemende connectiviteit 14
2.2.2 Voortzettende groei van digitale data 15
2.2.3 Meer geavanceerde cyberdreigingen 16
2.2.4 Toenemende digitalisering in het onderwijs en in het onderzoek 16
2.2.5 Veiligstellen van data 16
2.3 Bedreigde informatietypen 16
2.4 Actoren 18
2.5 Kwetsbaarheden 19

3 Dreigingen en maatregelen **24**
3.1 Inleiding 24
3.2 Veranderende dreigingen 24
3.3 Veranderende aanpak beveiligingsmaatregelen 25
3.4 Van high-level naar concrete maatregelen 26
3.5 Concrete maatregelen 27
3.5.1 Verkrijging en openbaarmaking van data 28
3.5.2 Identiteitsfraude 30
3.5.3 Verstoring ICT 30
3.5.4 Manipulatie van data 31
3.5.5 Spionage 31
3.5.6 Overname en misbruik ICT 32
3.5.7 Bewust beschadigen imago 32

4 incidenten met lessons learned **36**
4.1 Inleiding 36
4.2 Ransomware 36
4.2.1 Het incident 36
4.2.2 Lessons learned 37
4.2.3 Verdere stappen 37
4.2.4 Geschatte kosten 37
4.3 Distributed Denial of Service (DDoS) 38
4.3.1 Het incident 38
4.3.2 Lesson learned 40
4.3.3 Geschatte kosten 40
4.4 Spionage 40

Referenties **43**

MANAGEMENT-SAMENVATTING

Snelle digitalisering

Onze maatschappij is al in hoge mate gedigitaliseerd. Vergaande digitalisering biedt niet alleen meer mogelijkheden voor gebruikers, maar ook voor kwaadwillenden. Zo hebben onderwijs- en onderzoeksinstellingen steeds meer systemen en diensten buiten de deur geplaatst, waardoor het aantal aanvalsmogelijkheden is toegenomen.

Iedereen met iedereen verbonden

Ook de sector onderwijs en onderzoek heeft te maken met de gevolgen van deze vergaande digitalisering. Gebruikers hebben steeds meer apparaten die met elkaar en met het internet verbonden zijn. Docenten, studenten en onderzoekers communiceren onderling en met elkaar via allerlei apparaten en vragen toegang tot data vanaf allerlei locaties. Daarbij vervaagt het onderscheid tussen het vertrouwde netwerk binnen de instelling en het publieke netwerk buiten de instelling. Gebruikers werken zowel op hun werkplek in de instelling als vanuit huis en benaderen nu eens data binnen de instelling, dan weer data die zich bij een andere instelling of een clouddienst bevinden. Toegang moet dan ook verleend worden op basis van de identiteit van de gebruiker, zijn locatie, welke data hij wil benaderen en welke rechten hij daarvoor heeft.

Uitdaging: beschikbaarheid én bescherming

Het is aan de instellingen om veilige, laagdrempelige en geïntegreerde systemen aan te bieden, zodat in deze complexe omgeving data beschikbaar zijn voor degenen die ze nodig hebben, en tegelijkertijd beschermd zijn tegen kwaadwillenden. Waarbij dan ook voldaan moet worden aan wet- en regelgeving zoals de privacywetgeving.

Weerbaarheid vergroten

Het Cyberdreigingsbeeld wil een bijdrage leveren aan het vergroten van de weerbaarheid van de instellingen door aan te geven welke dreigingen het meest relevant zijn voor de sector onderwijs en onderzoek en welke maatregelen genomen kunnen worden om die dreigingen tegen te gaan en de impact ervan tot een minimum te beperken.

Dreigingen

Voor dit Cyberdreigingsbeeld zijn diverse medewerkers van instellingen en overheidsinstanties geïnterviewd. Uit de interviews komen drie significante dreigingen naar voren:

- Identiteitsfraude – Toenemende digitalisering van het onderwijs vereist goede identificatie van studenten en medewerkers. Wanneer studenten een digitale toets maken, moet zeker zijn dat de juiste student die toets maakt. Wanneer iemand toetsresultaten invoert, moet diegene daartoe gerechtigd zijn, zodat bijvoorbeeld een student resultaten niet kan aanpassen. Toetsen en de bijbehorende antwoorden

zijn vertrouwelijke informatie en mogen alleen toegankelijk zijn voor geautoriseerde medewerkers. Bijvoorbeeld diefstal van identiteitsgegevens van een docent kan leiden tot het uitlekken van toetsen of manipulatie van cijfers.
- Verstoring van ICT – DDoS-aanvallen zijn een blijvend probleem. Vooral tijdens tentamenperiodes en aan het begin van het schooljaar worden veel DDoS-aanvallen gedaan vanuit en gericht op de instellingsnetwerken. De landelijke trend is een toename van besmettingen met ransomware en cryptoware gesignaleerd, een trend die ook bij de onderwijs en onderzoeksinstellingen zichtbaar is.
- Spionage – Cyberspionage blijft voorkomen, maar is moeilijk te detecteren. Veel pogingen om gevoelige data te bemachtigen, beginnen met gerichte aanvallen op specifieke personen. Bijvoorbeeld met een e-mail die met malware besmette bijlagen of links naar websites met malware bevat. Wat er vervolgens gebeurt blijft onder de radar en is daardoor nauwelijks merkbaar, waardoor spionage ongrijpbaar blijft. We weten niet wat er gebeurt en weten ook niet wat er niet gebeurt.

Maatregelen

Om deze dreigingen tegen te gaan zijn allereerst maatregelen op strategisch niveau nodig. Bestuur en directie bepalen welke processen belangrijk zijn voor de instelling, welke risico's aanvaardbaar zijn en welke mate van bescherming nodig is. Idealiter gebeurt dat op basis van een risicoanalyse die regelmatig herhaald wordt. Deze risicomanagementcyclus geeft bestuur en directie voortdurend inzicht in de status van de risico's voor de hele instelling en biedt de verantwoordelijken de mogelijkheid de juiste maatregelen op tactisch en operationeel niveau in te regelen. Daarbij speelt de security officer als coördinator met voldoende mandaat en middelen van het bestuur een belangrijke rol in het afstemmen van het informatiebeveiligingsbeleid tussen de verschillende geledingen, het aanreiken van ideeën en het vergroten van bewustzijn. Het idee dat het instellingsnetwerk afgeschermd kan worden van de buitenwereld gaat niet meer op, omdat de gebruikers zich niet noodzakelijkerwijs binnen de instelling bevinden en ook de gegevens voor een groot deel buiten de instellingsgrenzen staan. Daarnaast moet er gekeken worden naar de hele keten van gebruiker tot gegevens, moeten afhankelijkheden in kaart worden gebracht, moeten afspraken met derde partijen goed worden doordacht en gedocumenteerd, en moet worden toegezien op de naleving daarvan, bijvoorbeeld door het hanteren van gestandaardiseerde service level agreements (SLA's).

Een aantal standaard maatregelen zijn meer preventief van aard:

- Netwerkverkeer en toegang tot systemen moet gemonitord worden om ongebruikelijke toegang of ongebruikelijke patronen te detecteren. De beveiligingsstatus van systemen moet regelmatig gecontroleerd worden en relevante technische dreigingen moeten bekend zijn om zo misbruik van bekende kwetsbaarheden tegen te gaan.
- Back-up moet goed ingeregeld zijn. Wanneer er sprake is van 'verstoring van ICT' waarbij data verloren is gegaan, is een recente back-up het meest probate middel om die data te herstellen. Bijvoorbeeld bij een cryptowarebesmetting is de keuze om het losgeld niet te betalen makkelijker als er een recente back-up is, en blijft eventueel dataverlies binnen de perken.

MANIPULATIE VAN DATA: HAAGSE HOGESCHOOL DOET AANGIFTE OM FRAUDE

De Haagse Hogeschool gaat aangifte doen naar aanleiding van de tentamenfraude die er vrijdag aan het licht kwam.

Omroep West onthulde afgelopen vrijdag dat er tentamens op bestelling te krijgen zijn bij de hogeschool. De omroep had zelf op donderdag al de vragen op zak van een tentamen Financiële Analyse, terwijl dat tentamen pas vrijdag werd afgenomen.

(Algemeen Dagblad, 14 juli 2014)

HACKEN: UZ LEUVEN DIENT KLACHT IN TEGEN 'KOPPEN' WEGENS HACKING GEGEVENS

De KU Leuven zal een strafklacht indienen bij de onderzoeksrechter tegen de poging tot hacken van haar servers. 'Het is immers niet aan journalisten om (te proberen om) gegevens van patiënten te identificeren en te verwerken', redeneert de universiteit. 'Daar bestaan geëigende en veilige procedures voor.'

De reportage die VRT vanavond zal uitzenden, toont hoe makkelijk het is om gegevens van duizenden patiënten binnen een halfuur te achterhalen. Het UZ Leuven benadrukt expliciet dat er geen patiëntendossiers gehackt werden. De firewall die de dossiers beschermt tegen hackers heeft die 'aanval' verijdeld.

(De Standaard, 16 oktober 2014)

1. INLEIDING

1.1 Achtergrond: digitale dreigingen nemen toe

Kenmerkend voor onderwijs- en onderzoeksinstellingen is hun open karakter. Er vindt veel uitwisseling van informatie en kennis plaats tussen studenten en docenten of tussen onderzoekers. Dit gebeurt binnen instellingen, maar ook tussen instellingen onderling. Deze uitwisseling verloopt vooral digitaal, wat veel voordelen heeft, maar ook extra dreigingen met zich meebrengt. Het lekken van data, de schending van privacy en cybercrime zijn onderwerpen die dagelijks het nieuws halen. Het is dus van belang dat de beschikbaarheid van systemen en verbindingen hoog is en interrupties tot een minimum beperkt blijven.

Naast de toegenomen informatie-uitwisseling via internet zien we in het onderwijs meer ontwikkelingen die dreigingen veroorzaken: steeds meer studenten en docenten gebruiken hun eigen apparaten om informatie te verwerken; de instelling heeft geen volledige controle over de beveiliging van die apparaten. Verder is er veel informatie die vertrouwelijk is of onderhevig is aan privacywetgeving. Er zijn bijvoorbeeld onderzoeken waarbij grote hoeveelheden persoonsgegevens verwerkt worden, van medische gegevens tot gedragsgegevens. Voor onderzoeken waarbij buitenlandse instituten betrokken zijn, heeft het herroepen van het *EU-U.S. Safe Harbor-verdrag*[1] ook grote gevolgen voor het uitwisselen van persoonsgegevens.

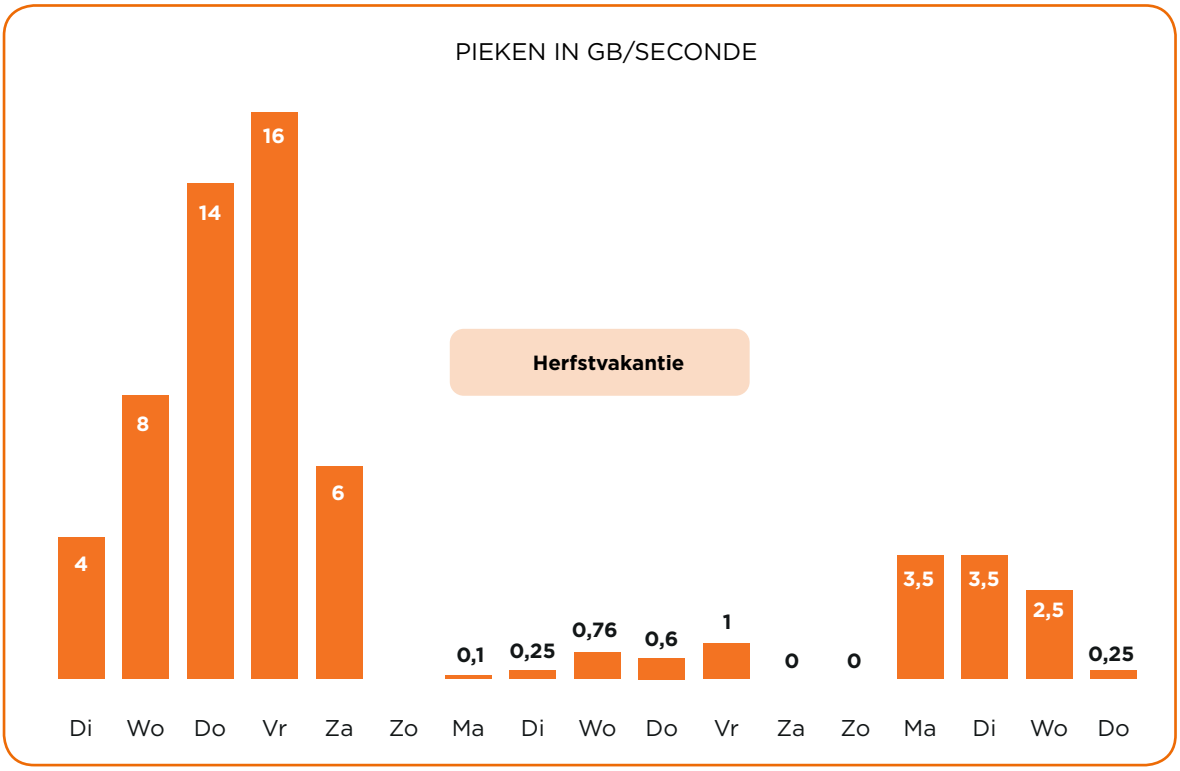
Bij SURFcert[2], de incident-responsedienst van SURF, is er sinds 2013 een sterke toename van geregistreerde *Denial of Service* (DoS) incidenten waargenomen. Terwijl er in 2014 bijvoorbeeld gemiddeld per maand zo'n 20 DoS-aanvallen zijn geregistreerd, is dat aantal in 2015 opgelopen tot zo'n 60 per maand. Opvallend is daarbij dat direct na schoolvakanties, tijdens tentamenperiodes en aan het begin van het schooljaar pieken in de activiteit zijn te zien (zie grafiek pagina 11). Dit jaar valt op dat de activiteit ook langer voortduurt dan vorig jaar.

Om deze dreigingen het hoofd te bieden en toch een goede uitwisseling van data mogelijk te blijven maken, zijn specifieke beveiligingsmaatregelen vereist, anders dan bij het bedrijfsleven waar juist afscherming van data gebruikelijker is.

Anderzijds zijn er op het vlak van beveiliging ook positieve ontwikkelingen zichtbaar in de sector onderwijs en onderzoek:

- In het mbo is gestart met een gestructureerde aanpak van informatiebeveiliging en privacy. Er is bijvoorbeeld een 'Programma Informatiebeveiliging 2015' om de mbo-instellingen te stimuleren en ondersteunen bij het ontwikkelen van een beveiligingsbeleid[3]. Daarnaast organiseert de 'taskforce IBP' in het mbo verschillende masterclasses over informatiebeveiliging en privacy.
- De Vereniging van Samenwerkende Nederlandse Universiteiten (VSNU), de Vereniging Hogescholen en de MBO Raad zijn betrokken bij control en governance: veel instellingen hebben een security en/of privacy officer aangesteld, er wordt actief samengewerkt in allerlei gremia, er is een normenkader en een toetsingskader voor het hoger onderwijs, gebaseerd op internationale standaarden, het mbo heeft zijn eigen normenkader opgesteld op basis van het 'Normenkader Informatiebeveiliging HO 2015' en er wordt op allerlei manieren aan kennisdeling gedaan.
- In de pers en de politiek is veel aandacht voor privacy en datalekken. Dat verhoogt het beveiligingsbewustzijn in de hele maatschappij.

[1] *Zie: https://www.surf.nl/nieuws/2015/10/europees-hof-van-justitie-verklaart-privacyverdrag-safe-harbor-ongeldig.html (opgehaald op 9 oktober 2015)*
[2] *https://www.surf.nl/diensten-en-producten/surfcert/index.html (opgehaald op 9 oktober 2015)*
[3] *Zie: https://www.sambo-ict.nl/2015/02/programma-informatiebeveiliging-2015/ (opgehaald op 9 oktober 2015)*



Toename van aanvalsactiviteit voor, tijdens en na de herfstvakantie 2015 (bron: SURFcert)

1.2 Doel: weerbaarheid van de instellingen vergroten

Het Cyberdreigingsbeeld 2015 laat het belang zien van een goede bescherming van data(systemen). Het biedt u inzicht in de aanwezige cyberdreigingen en dient als startpunt om de nodige maatregelen te nemen. Zo kunt u zelf actief en effectief tegen deze dreigingen optreden om de impact ervan te verminderen en om zo uw instelling weerbaar te maken tegen cyberdreigingen.

1.3 Leeswijzer

In hoofdstuk 2 van het Cyberdreigingsbeeld leest u welke trends in onderwijs, onderzoek en ICT voor dreigingen zorgen, welke processen in het onderwijs bedreigd worden en wie de actoren zijn (degenen die ICT-voorzieningen in onderwijs en onderzoek aanvallen). Dit wordt het dreigingslandschap genoemd.

Hoofdstuk 3 gaat in op een aantal specifieke dreigingen en laat per dreiging zien welke maatregelen genomen kunnen worden. Ook worden er een aantal incidenten beschreven die zich het afgelopen jaar voorgedaan hebben

1.4 Doelgroep: managers en securityprofessionals in hoger onderwijs en mbo

Het Cyberdreigingsbeeld 2015 is bedoeld voor de doelgroep van SURF: de instellingen voor hoger onderwijs en wetenschappelijk onderzoek en de mbo-instellingen. Het eerste deel (hoofdstuk 2) richt zich meer op bestuurders en managers, het tweede deel (hoofdstuk 3) richt zich op securityprofessionals.

1.5 Totstandkoming

Deze versie van het Cyberdreigingsbeeld bouwt voort op het Cyberdreigingsbeeld 2014[4] en interviews die in de periode juli tot oktober 2015 zijn gehouden met diverse medewerkers van onderwijs- en onderzoeksinstellingen, het Nationaal Cyber Security Centrum (NCSC) en de Algemene Inlichtingen- en Veiligheidsdienst (AIVD). Uit de interviews komt naar voren dat veel van de trends die zijn gesignaleerd in het Cyberdreigingsbeeld 2014 zich in 2015 hebben voortgezet en dat er veel incidenten[5] zijn geweest die instellingen hebben geraakt.

Een belangrijke bron van informatie is daarnaast het in oktober 2015 door het NCSC gepubliceerde *Cybersecuritybeeld Nederland 2015*[6]. Dit bevat een aantal trends, de kernbevindingen, die in grote lijnen de dreigingen bevestigen die tijdens interviews met medewerkers van verschillende instellingen als meest relevant zijn genoemd.

[4] *Cyberdreigingsbeeld – Sector Hoger Onderwijs en Wetenschappelijk Onderzoek 2014 (SURFnet, 2014)*
[5] *In 2014 zijn bijna 8000 incidenten bij SURFcert geregistreerd.*
[6] *Cybersecuritybeeld Nederland 2015 (NCSC, 2015)*

SPIONAGE: BRITSE GEHEIME DIENST BESPIONEERDE JARENLANG BELGACOM-KLANTEN

Bij de digitale aanval op Belgacom kon de Britse geheime dienst veel meer communicatie onderscheppen dan tot nu toe werd aangenomen. De geheime dienst GCHQ raakte in 2011 binnen in het netwerk door drie werknemers te hacken. Daarna kon de GCHQ twee en een half jaar lang ongestoord rondsnuffelen in het netwerk van Belgacom en dochterbedrijf BICS. De geheime dienst kon zo de communicatie onderscheppen van de individuele klanten van Belgacom zelf, van de NAVO en de EU, en van de klanten van honderden internationale telecomproviders.

(De Standaard, 13 december 2014)

SPIONAGE: KWAADAARDIGE MALWARE REGIN GEBRUIKT BIJ HACK BELGACOM

De geavanceerde spionagesoftware Regin, waarover computerbeveilingsbedrijf Symantec gisteren rapporteerde, is gebruikt bij de cyberaanval op de Belgische telecomprovider Belgacom. Dat blijkt uit gesprekken met betrokkenen en onderzoek van *NRC Handelsblad*, in samenwerking met *De Standaard* en *The Intercept*.

Vorig jaar september onthulden NRC Handelsblad en De Standaard dat Belgacom slachtoffer was geworden van een grootschalige hack, waarschijnlijk uitgevoerd door de Britse of Amerikaanse inlichtingendienst.

(NRC, 24 november 2014)

2. DREIGINGSLANDSCHAP

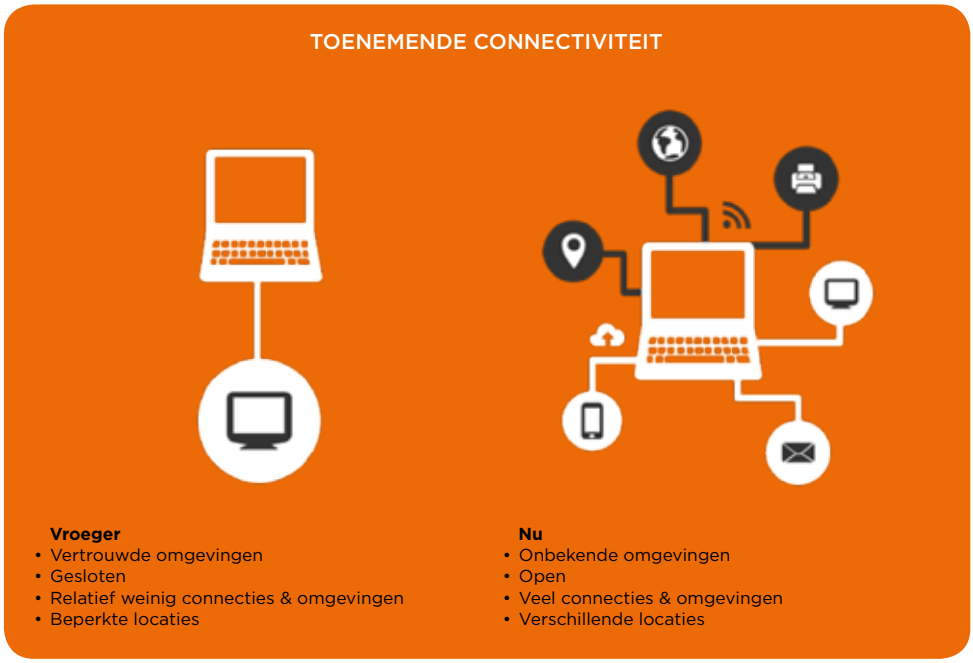
2.1 Inleiding

Dit hoofdstuk beschrijft het dreigingslandschap voor het onderwijs en onderzoek in Nederland. Welke ICT-trends beïnvloeden de dreigingen? (paragraaf 2.2) Welke soorten data worden bedreigd? (paragraaf 2.3) Wie zijn de actoren, dus degenen die ICT-systemen in onderwijs en onderzoek aanvallen? (paragraaf 2.4) En wat zijn de kwetsbare punten waar rekening mee moet worden gehouden bij het nemen van maatregelen? (paragraaf 2.5)

2.2 Trends

2.2.1 Toenemende connectiviteit

Meer gebruikers buiten het instellingsnetwerk online
Onderwijs- en onderzoeksinstellingen zijn steeds meer, en op steeds meer verschillende manieren, met elkaar verbonden. Bijna elk apparaat kan met het internet worden verbonden om verschillende onderwijs- en onderzoeksdiensten (en de bijbehorende data) te benaderen. Hoewel onderwijsinstellingen van oudsher een open karakter hebben, bevonden de data zich vroeger vooral op de locatie zelf. Omdat studenten, onderzoekers en docenten tegenwoordig buiten het netwerk van de instelling zelf online zijn en gegevens zich buiten het campusnetwerk bevinden, is de traditionele beveiliging aan de rand van het netwerk niet meer voldoende om de data veilig te stellen. Het wordt dan ook steeds belangrijker om de data zelf te beveiligingen en toegang te verlenen op basis van kenmerken als: wie is de gebruiker, wat is zijn rol, waarom benadert hij de data en wat wil hij ermee.



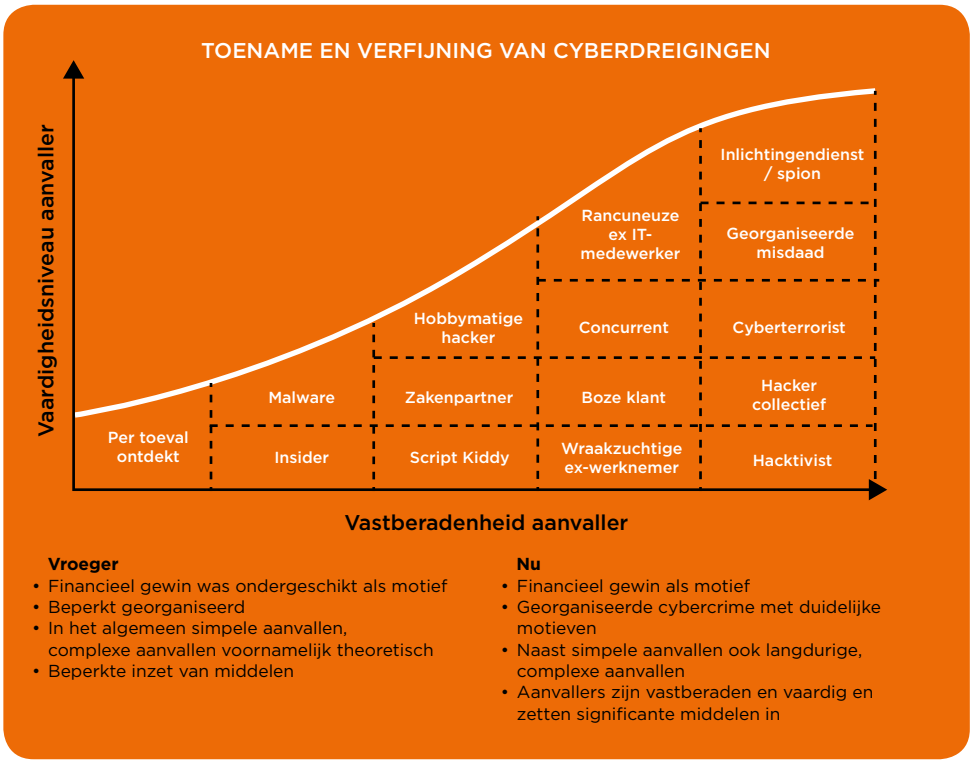
Bron: Cyberdreigingsbeeld 2014

Meer apparaten maken verbinding met instellingsnetwerk
Uit het Threat Landscape 2014 van de European Union Agency for Network and Information Security (ENISA)[7] blijkt dat de groei van interconnected devices nog steeds doorzet. Ook bij onderwijs- en onderzoeksinstellingen worden naast laptops en werkstations steeds meer andere apparaten gebruikt die met het internet verbonden zijn. Denk aan tablets en mobiele telefoons, die steeds vaker worden ingezet bij bijvoorbeeld digitale colleges en soms ook toetsing. De groei in het aantal apparaten en het aantal leveranciers van clouddiensten resulteert ook in een toename van het aantal verbindingen waarover data wordt gedeeld. Deze verbindingen verlopen vaak via onbekende netwerken zoals het thuisnetwerk van de gebruiker of een publiek wifi-netwerk. Dit zijn netwerken die voor de instellingen niet te controleren zijn.

Informatie buiten de instelling opgeslagen
Informatie wordt steeds vaker buiten de instellingen opgeslagen, bijvoorbeeld in de cloud. Soms is dat een bewuste keuze, maar vaak is het onbedoeld het gevolg van een SaaS[8]-oplossing die wordt ingezet. Daarbij is niet altijd duidelijk waar de informatie wordt opgeslagen en wie verantwoordelijk is voor de vertrouwelijkheid, integriteit en beschikbaarheid ervan. Met het verwerpen van EU-U.S. Safe Harbor-verdrag door het Europese Hof van Justitie[9] is dit vraagstuk nog complexer geworden.

2.2.2 Voortzettende groei van digitale data

Naast de exponentiële groei van connectiviteit is er ook een enorme groei van de hoeveelheid data die wordt gedeeld en opgeslagen[10]. In sommige gevallen worden er bewust zo veel mogelijk data verzameld om er later analyse op uit te kunnen voeren (big data). Dit brengt allerlei problemen met zich mee op het gebied van beveiliging en privacy.



Bron: Cyberdreigingsbeeld 2014

[7] *ENISA Threat Landscape 2014 (ENISA, 2014)*
[8] *SaaS – Software as a Service*
[9] *https://www.surf.nl/nieuws/2015/10/europees-hof-van-justitie-verklaart-privacyverdrag-safe-harbor-ongeldig.html (opgehaald op 10 oktober 2015)*
[10] *Big Data – for better or worse (SINTEF, 2013)*

2.2.3 Meer geavanceerde cyberdreigingen

Door bovengenoemde ontwikkelingen binnen de sector onderwijs en onderzoek, zijn ook de mogelijkheden en motieven voor cybercriminelen gegroeid. Er zijn immers meer data om te stelen, wat de verleiding alleen maar groter maakt, en er zijn meer (via internet toegankelijke) gebruikersomgevingen om bij deze data te komen.

De markt voor cybercrime is sterk gegroeid. Het afgelopen jaar liet diverse incidenten zien waarbij grote hoeveelheden data zijn gestolen[11]. Er valt veel meer informatie te halen en door deze op de juiste manier te combineren, is de waarde van data sterk toegenomen. De financiële prikkel om de data te stelen, wordt dan ook steeds groter.

De professionalisering van cybercrime zet gestaag door: cybercriminelen leren van elkaar, waardoor ze in staat zijn om uiterst geavanceerde aanvallen te orkestreren[12]. Daarbij misbruiken ze langdurig verschillende kwetsbaarheden in systemen, software en processen om langzaam maar zeker tot hun doel te komen (vaak zijn dat grote sets van gevoelige data). Deze zogenaamde Advanced Persistent Threats (APT's, zie kader op pagina 29), gericht op systeembeheerders, onderzoekers of bestuurders, kunnen maanden of soms wel jaren in beslag nemen. Ze zijn zodanig opgezet dat ze onzichtbaar blijven en het is niet altijd direct duidelijk voor het slachtoffer welke informatie het doel van de aanval is, laat staan welke impact deze kan hebben, totdat het te laat is.

2.2.4 Toenemende digitalisering in het onderwijs en in het onderzoek

Naast de bovengenoemde algemene veranderingen hebben onderwijs- en onderzoeksinstellingen te maken met veranderingen in de eigen sector, zoals de verdere digitalisering van het onderwijs. Niet alleen neemt het gebruik van internet in de klaslokalen toe, maar er wordt ook steeds meer gebruik gemaakt van volledig digitale lesvormen als online colleges, opdrachten en tentaminering, waarbij de student vanuit iedere willekeurige locatie kan deelnemen aan het onderwijs. Hiermee wordt de toegankelijkheid van onderwijs enorm vergroot, maar het brengt ook een aantal nieuwe uitdagingen op het gebied van cybersecurity met zich mee, bijvoorbeeld op het gebied van identiteitscontrole.

2.2.5 Veiligstellen van data

Na een aantal incidenten met het manipuleren van onderzoeksdata in het wetenschappelijk onderzoek zijn internationale standaarden en protocollen aangescherpt en treedt de universiteit steeds meer op als een controlerende entiteit. Bovendien hebben universiteiten als taak om ruwe onderzoeksdata veilig te stellen en toegankelijk te maken, zodat andere onderzoekers die data kunnen gebruiken voor vervolgonderzoek of om resultaten te kunnen verifiëren. Ook dit draagt bij aan een verdere digitalisering.

2.3 Bedreigde informatietypen

Terwijl de hoeveelheid data sterk is gegroeid en de digitalisering binnen de sectoren razendsnel voortschrijdt, zijn dreigingen voor de beschikbaarheid, integriteit en vertrouwelijkheid van data de laatste jaren sterk toegenomen.

Bij de instellingen voor onderwijs en onderzoek kunnen we onderscheid maken tussen data die betrekking hebben op drie verschillende processen binnen de sector:
- onderwijs
- onderzoek
- bedrijfsvoering

[11] *Verizon Data Breach Investigations Report 2015 (Verizon, 2015)*
[12] *Mandiant M-Trends 2015 (Mandiant, 2015)*

Onderwijs – Onderwijsinstellingen hebben van nature een open karakter, delen van informatie staat centraal. Daarbij is het de primaire taak van onderwijsinstellingen om studenten af te leveren met een betrouwbaar diploma. De maatschappij moet het onderwijsproces kunnen vertrouwen.

Onderzoek – Ook bij het doen van onderzoek staat kennisdeling centraal en wordt er intensief samengewerkt tussen verschillende onderzoekers, studenten en – in het kader van derdegeldstromen – met bedrijfsleven en overheden. Grote onderzoeksprojecten kunnen bovendien grensoverschrijdend zijn. Onderzoek en de bijbehorende informatievoorziening is dan ook vaak sterk decentraal georganiseerd. Zowel het open karakter van de instellingen als het decentraal beheer van onderzoeksgegevens zijn kenmerkend voor de sector. Samen kan dit gemakkelijk leiden tot een tekort aan dataveiligheid en privacybescherming.

Bedrijfsvoering – Behalve organisaties die faciliteiten voor onderwijs en onderzoek bieden, zijn instellingen voor (hoger) onderwijs en onderzoek organisaties met personeel. De instelling moet ervoor zorgen dat de privacy van haar medewerkers (en studenten) gewaarborgd blijft en dat de continuïteit van het onderwijsproces gegarandeerd is. Om te voldoen aan privacywetgeving en andere wet- en regelgeving, moeten gegevens op de juiste manier beschermd worden.

In de onderstaande tabel zijn de verschillende informatietypen op een rijtje gezet en daarbij op welk proces ze betrekking hebben[13].

Informatie		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.	■		
Onderzoeksgegevens & 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.	■		

Data en processen (bron: Cyberdreigingsbeeld 2014)

[13, 14] *Overgenomen uit Cyberdreigingsbeeld - Sector Hoger Onderwijs en Wetenschappelijk Onderzoek 2014 (SURFnet, 2014)*

Alle genoemde informatietypen zijn ook onderhevig aan de securityaspecten beschikbaarheid, integriteit en vertrouwelijkheid en aan privacywetgeving. Dit is weergegeven in onderstaande tabel.

Informatie		Beschikbaarheid	Integriteit	Vertrouwelijkheid	Privacy
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.		■	■	

Data en beveiligingsaspecten

2.4 Actoren

De personen of organisaties die aanvallen uitvoeren, de actoren, kunnen allerlei motieven hebben, bijvoorbeeld financieel gewin, verhoging van sociale status of versterking van politieke of economische status van een staat (spionage).

De tabel[14] op pagina 19 illustreert welke actoren een rol spelen voor de sector onderwijs en onderzoek:

Uit de interviews blijkt dat slechts een aantal van de hierboven genoemde actoren als relevant worden gezien. Opvallend is dat buitenlandse geheime diensten (statelijke actoren) door onderwijsinstellingen niet worden gezien als een hoog risico. Anderzijds blijkt dat juist onderzoeksinstellingen de statelijke actoren wel beschouwen als een hoog risico. Actoren die door alle typen instellingen als relevant worden gezien, zijn:

- Studenten – Hun interesse ligt voornamelijk bij het manipuleren van resultaten om hun positie binnen de opleiding te verbeteren.
- Medewerkers – Zijn vooral geïnteresseerd in het manipuleren van gegevens over hun functioneren of eigen gewin.
- Cybercriminelen – Dit zijn beroepscriminelen die gebruik maken van geavanceerde digitale technieken om hun doel te bereiken.
- Cybervandalen – Voeren aanvallen uit met beperkte middelen en kennis, vaak omdat het kan of om status binnen hun ‘peer group’ te verhogen.

DREIGINGEN PER ACTOR		DREIGING		
Actor	Vaardigheidsniveau	Onderwijs	Onderzoek	Bedrijfsvoering
Studenten	Laag tot Gemiddeld	Identiteitsfraude		
		Manipulatie van data		
		Verstoren ICT		
		Bewust beschadigen imago		
Medewerkers	Laag		Identiteitsfraude	
			Manipulatie van data	
			Verstoren ICT	
		Verkrijging en openbaar-making van data	Verkrijging en openbaar-making van data	Verkrijging en openbaar-making van data
Cybercriminelen	Gemiddeld tot Hoog		Overname en misbruik ICT	Identiteitsfraude
			Spionage	
Cyberonderzoe-kers	Hoog	Verkrijging en openbaar-making van data	Verkrijging en openbaar-making van data	Verkrijging en openbaar-making van data
		Verstoren ICT	Verstoren ICT	Verstoren ICT
Statelijke actoren	Zeer Hoog		Verkrijging en openbaar-making van data	
			Spionage	
			Overname en misbruik ICT	
Commerciële bedrijven & part-nerinstellingen	Laag tot Gemiddeld		Spionage	
Activisten	Laag tot Gemiddeld	Verstoren ICT	Verstoren ICT	Verstoren ICT
		Bewust beschadigen imago	Bewust beschadigen imago	
			Overname en misbruik ICT	
Cybervandalen	Laag	Bewust beschadigen imago	Bewust beschadigen imago	

Dreigingen sector onderwijs en onderzoek

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 buiten Nederland, 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."

Legenda relevantie - *Bron: Cybersecuritybeeld Nederland (Nationaal Cyber Security Centrum, 2015)*

2.5 Kwetsbaarheden

Hoewel de instellingen steeds meer aandacht besteden aan informatiebeveiliging, meer samenwerkingsverbanden opzetten en kennis delen, blijven kwetsbaarheden een heikel punt. Het verhelpen ervan duurt te lang, waardoor kwaadwillenden kwetsbaarheden waarvoor patches al beschikbaar zijn, toch kunnen blijven misbruiken. Verder moeten we niet alleen kwetsbaarheden in hardware en software onderkennen, waarvan er steeds weer nieuwe ontdekt worden, maar ook kwetsbaarheden op het menselijk vlak en in de bedrijfsprocessen. Om de ICT-omgeving veiliger te maken moet gekeken worden naar maatregelen in deze drie categorieën[15]:

- mens
- proces
- technologie

[15] *SANS – People, Process, and Technologies Impact on Information Data Loss (Janes, 2012)*

2.5.1 Mens

De gebruiker zelf is een van de grootste kwetsbaarheden waardoor veel datalekken ontstaan en dan vooral door phishing-aanvallen (zie kader op pagina 22). Volgens het Verizon Data Breach Investigations Report 2015[16], opent 23% van de respondenten uit hun onderzoek phishing-e-mails en 11% ook nog de bijlage. Daarvan doet 50% dat binnen een uur na ontvangst van de e-mail en de eerste klik vindt al plaats binnen een minuut!

Andere voorbeelden van menselijke fouten zijn het gebruiken van clouddiensten als Dropbox voor gevoelige data, of het opslaan daarvan op een onbeveiligde USB-stick, het gebruik van onveilige wachtwoorden (te kort, te simpel of te vaak hetzelfde), het installeren van onveilige, soms illegale software (freeware, shareware enzovoort) en het delen van gebruikersaccounts.

Verhogen van bewustzijn, zodat men zich beter realiseert wat de gevolgen kunnen zijn van ondoordacht handelen, is een belangrijk middel om menselijke fouten te voorkomen. Cybersecurity krijgt in het onderwijs en onderzoek zeker aandacht, maar dit onderwerp blijft vaak onderbelicht, omdat het buiten de kernactiviteit van instellingen valt en nog te vaak wordt onderschat. Het is van cruciaal belang dat bestuurders en andere leidinggevenden het belang van cybersecurity uitdragen en zelf het juiste voorbeeld geven.

2.5.2 Proces

Allerlei processen hebben invloed op de staat van beveiliging. Te denken valt aan processen als identiteits- en toegangsbeheer, dataclassificatie, patching en softwareontwikkeling. Hoe volwassener die processen zijn, des te beter de staat van de informatiebeveiliging is.

Onderwijs- en onderzoeksinstellingen hebben te maken met grote aantallen gebruikersidentiteiten, die bovendien vaak wisselen. Het beheren en bewerken van identiteiten en bijbehorende toegangsrechten (uitdelen, aanpassen en intrekken) is een complex proces dat goed ingericht moet zijn.

Dataclassificatie is belangrijk om te kunnen bepalen hoe gebruikers met data om moeten gaan. Om te beginnen moeten gevoelige data op een veilige manier worden opgeslagen (encryptie, segmentering van het netwerk, adequate toegangscontrole), daarnaast moet het voor gebruikers duidelijk zijn hoe zij gevoelige data veilig moeten opslaan en transporteren. Daarnaast moet gemonitord worden wat er gebeurt met gevoelige data (wie benadert ze, welke data wordt benaderd, wat gebeurt er met de data en waarom).

Het verhelpen van kwetsbaarheden is een blijvend probleem. Uit onderzoek[17] blijkt dat de tijd om de helft van alle gevonden kwetsbaarheden te patchen (de half-lifetijd) gemiddeld bijna 30 dagen is, terwijl 80% van die kwetsbaarheden misbruikt wordt binnen 48 uur. Bovendien hebben de instellingen een grote diversiteit aan systemen, wat het onderhoudsproces moeilijker maakt. En deze systemen mogen vaak niet zomaar uit de lucht gehaald worden, denk bijvoorbeeld aan roostersystemen, e-mail en netwerkconnectiviteit.

Bij het ontwikkelen van nieuwe systemen ontbreekt vaak de tijd en kennis, om vanaf het begin beveiligingsaspecten mee te nemen. Vooral webapplicaties moeten vaak snel beschikbaar gesteld worden.

[16] *Verizon Data Breach Investigations Report 2015 (Verizon, 2015)*
[17] *http://www.csoonline.com/article/2899169/cyber-crime/measuring-the-effectiveness-of-your-vulnerability-management-program.html (opgehaald op 10 oktober 2015)*

Hulpmiddelen als de *OWASP Top 10*[18] en het *OWASP Top 10 Privacy Risks Project*[19] ondersteunen bij het ontwikkelen van veilige webapplicaties. Daarnaast is het belangrijk om scans op kwetsbaarheden en penetratietesten uit te voeren op nieuwe webapplicaties en deze regelmatig te herhalen als de webapplicatie in de lucht is.

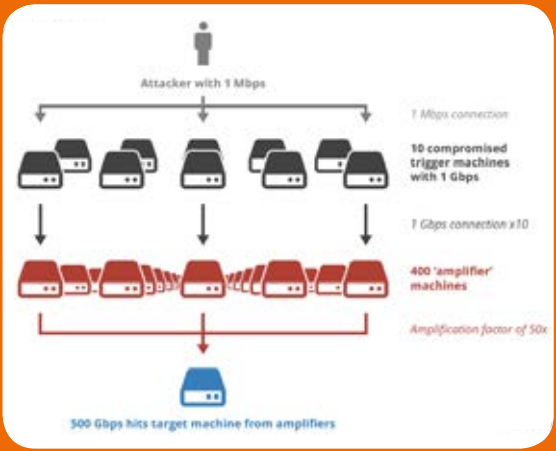
2.5.3 Technologie

Kwetsbaarheden in ICT-systemen kunnen zich voordoen op verschillende lagen, van besturingssysteem (en zelfs BIOS/UEFI[20]) tot applicaties. Bijvoorbeeld *Rootkit:W32/Whistler* is een bootsector virus dat het Master Boot Record (MBR) van een harde schijf infecteert en tijdens het bootproces kwaadaardige bestanden in het systeem laadt. Een ander voorbeeld is het *Driver Update*-programma dat ervoor lijkt te zorgen dat alle drivers up-to-date blijven, maar intussen allerlei malwaretoepassingen installeert. Vooral de sterke toename van het aantal webapplicaties en de focus van veel ontwikkelaars op het 'zo snel mogelijk werkend' opleveren van applicaties maakt dat beveiliging vaak achteraf wordt toegepast, als dat al gebeurt. Dit leidt ertoe dat er allerlei kwetsbaarheden in de applicaties voorkomen die misbruikt kunnen worden. Veel systemen bij de instellingen zijn verouderd. Oude systemen bevatten meer kwetsbaarheden dan nieuwe systemen, maar vaak kunnen ze niet zomaar up-to-date worden gebracht, bijvoorbeeld omdat er applicaties op draaien die niet werken op nieuwe versies van het besturingssysteem, of omdat er voor bepaalde hardware geen drivers meer beschikbaar zijn op een nieuw besturingssysteem.

Ook kwetsbaarheden in de infrastructuur manifesteren zich op verschillende manieren: een draadloos netwerk dat niet goed beveiligd of verouderd is of netwerkswitches die geen toegangscontrole op de netwerkpoorten ondersteunen, waardoor het voor kwaadwillenden makkelijker is om in te breken op het netwerk.

[18] OWASP Top Ten Project (OWASP Top Ten Project, 2013) (OWASP Top Ten Privacy Risks Project, 2014)
[19] OWASP Top Ten Privacy Risks Project (OWASP Top Ten Privacy Risks Project, 2014)
[20] Basic Input/Output System, Unified Extensible Firmware Interface

DDOS



Schema van een reflectie aanval (bron: Cloudflare)

Een DDoS-aanval (Distributed Denial of Service) is een kwaadaardige poging om een systeem plat te leggen. In tegenstelling tot een DoS (Denial of Service) aanval, waarbij één systeem en één internetconnectie wordt gebruikt om het doelwit te bestoken met verkeer, wordt bij een DDoS- aanval gebruik gemaakt van meerdere systemen en internetconnecties, die vaak wereldwijd verspreid zijn. Traditioneel werd bij DDoS-aanvallen veel gebruikgemaakt van botnets, maar nu worden ook allerlei andere methodes gebruikt waarvan reflectie en amplificatie het meest populair zijn*. Ook belangrijk is dat eigen systemen misbruikt kunnen worden om andere instellingen aan te vallen. Bijvoorbeeld NTP-servers en DNS-servers die niet goed geconfigureerd zijn: deze kunnen misbruikt worden als reflector.

* *Akamai's [state of the internet] / security (Akamai, 2014; Akamai, 2014)*
** *http://www.rijnmond.nl/nieuws/13-10-2015/waarschuwing-voor-phishingmail-inholland (opgehaald op 10 november 2015)*

PHISHING

Phishing is een vorm van fraude waarbij een gebruiker verleid wordt om een nepwebsite te bezoeken en daar gevoelige informatie achter te laten, zoals persoonsgegevens, bankgegevens of logingegevens. Die worden vervolgens misbruikt door de fraudeur. In veel gevallen gaat het om een e-mail die er legitiem uitziet en waarin gedreigd wordt met bijvoorbeeld het opheffen van de bankrekening. Een recent voorbeeld is de waarschuwing die Hogeschool Inholland en de politie Rotterdam uitgaven. Kennelijk waren 7000 phishingmails uit naam van de onderwijsinstelling verstuurd. Studenten werden opgeroepen de e-mails met als onderwerp 'verificatie gegevens' niet te openen en er niet op te reageren**.

Bron: https://twitter.com/Politie_Rdam

Bron: https://www.fraudehelpdesk.nl/ (opgehaald op 16 november 2015)

Spear-phishing is een vorm van phishing die specifiek gericht is op een bepaalde persoon of functieniveau binnen een organisatie. In de regel is hieraan social engineering vooraf gegaan om die persoon te identificeren en om mogelijke afzenders te identificeren waardoor de ontvanger de e-mail vertrouwt. Er zijn drie aspecten waardoor spear-phishing werkt: de (schijnbare) afzender is vertrouwd, de informatie in het bericht is correct en past bij de afzender, en het verzoek dat wordt gedaan lijkt logisch.

3 DREIGINGEN EN MAATREGELEN

3.1 Inleiding

Hoofdstuk 2 gaf een overzicht van het dreigingslandschap. Dit hoofdstuk gaat concreter in op de vraag hoe de dreigingen die uit het onderzoek en recente incidenten naar voren komen, zich kunnen manifesteren en wat de relevantie is voor de verschillende processen (onderwijs, onderzoek en bedrijfsvoering). Daarnaast leest u in meer detail hoe deze dreigingen zich voordoen en welke maatregelen genomen kunnen worden om de dreigingen tegen te gaan of de impact ervan zo klein mogelijk te houden.

3.2 Veranderende dreigingen

Uit het onderzoek van 2014[21] zijn dreigingen naar voren zijn gekomen die nog steeds bestaan; met name identiteitsfraude wordt veel genoemd. Uit de interviews die in 2015 zijn gehouden, komen wel een aantal accentverschuivingen naar voren:

- Het meest opvallend is de sterke toename van incidenten met ransomware en cryptoware (zie kader op pagina 29), waarbij detectie in veel gevallen tekortschiet en maatregelen vooral in de preventieve sfeer moeten worden gezocht.
- Het valt op dat ook het aantal DDoS[22]-aanvallen (zie kader op pagina 22) blijft toenemen en dat kwetsbaarheden in software nog steeds een groot probleem vormen. Door de grote hoeveelheid updates en patches, loopt het invoeren daarvan vaak achter. Cybercriminelen kunnen zo nog steeds gebruikmaken van kwetsbaarheden, ook al zijn patches al beschikbaar. En dan zijn er ook nog de kwetsbaarheden waarvoor nog geen patches beschikbaar zijn of die zelfs nog niet bekend zijn bij de softwarefabrikant (zero-day vulnerabilities).
- Aanvallen worden steeds geavanceerder, waardoor het voor organisaties steeds lastiger is om dreigingen te herkennen en ermee om te gaan.

Uit het jaarverslag 2014 van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD)[23] blijkt verder dat niet alleen spionageaanvallen op Nederlandse organisaties plaatsvinden, maar dat ook de Nederlandse digitale infrastructuur wordt gebruikt voor aanvallen elders in de wereld. De Nederlandse infrastructuur is namelijk goed toegankelijk en heeft veel bandbreedte.

In het voorwoord zegt minister Plasterk:

> *"Veel andere mogendheden zijn geïnteresseerd in onze technische, hightech, economische en wetenschappelijke kennis en proberen die onder andere via digitale kanalen te bemachtigen. Ons land kent een van de best ontwikkelde ICT-infrastructuren ter wereld. Dat is een kracht, maar dat geeft ook verantwoordelijkheid. Misbruik van deze netwerken moet bestreden worden."*

Volgens het jaarverslag "kunnen via digitale spionage in een kort tijdsbestek grote hoeveelheden informatie op grotendeels anonieme en simultane wijze verzameld worden bij doelwitten die geografisch verspreid liggen. Een digitale spionageaanval

[21] *Cyberdreigingsbeeld – Sector Hoger Onderwijs en Wetenschappelijk Onderzoek 2014 (SURFnet, 2014)*
[22] *Distributed Denial-of-Service*
[23] *AIVD – Jaarverslag 2014 (Algemene Inlichtingen- en Veiligheidsdienst, 2014)*

is dan ook zelden gericht op één organisatie, maar meestal op tientallen publieke of private organisaties wereldwijd tegelijkertijd." En "Nederland beschikt over veel bandbreedte, een van 's werelds grootste internetknooppunten en legio mogelijkheden voor het huren van server(ruimte)s. Hierdoor is Nederland een ideale uitvalsbasis of doorvoerhaven voor digitale aanvallen." Vooral de open, stabiele en snelle ICT-infrastructuur van de Nederlandse universiteiten en hogescholen zijn ideaal als potentiële springplanken voor digitale aanvallen elders, wat reputatieschade kan opleveren voor de onderwijsinstellingen.

3.3 Veranderende aanpak beveiligingsmaatregelen

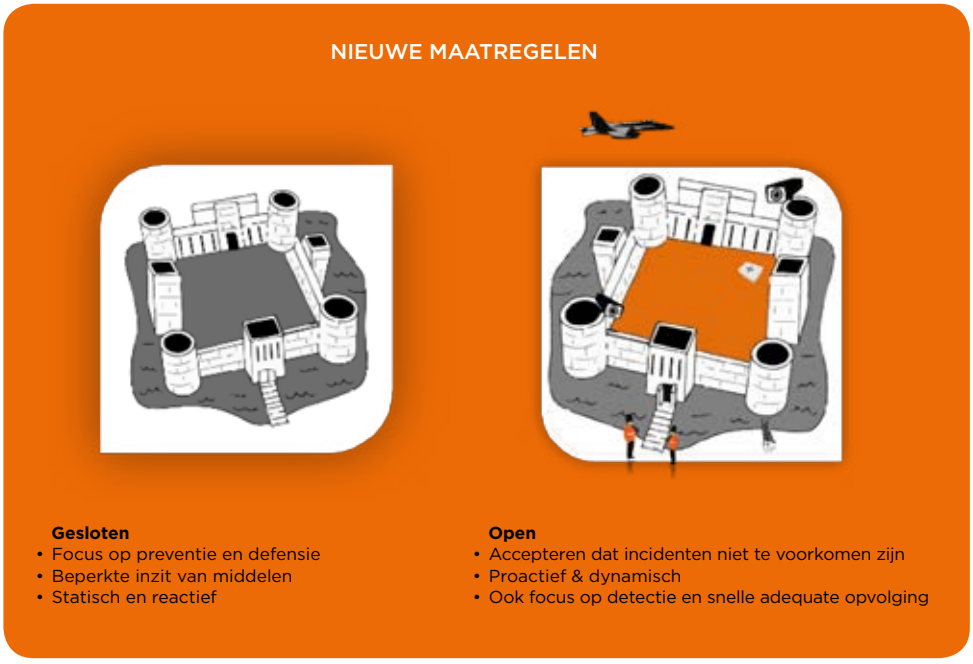
3.3.1 Van preventief naar reactief

In het verleden waren beveiligingsmaatregelen vooral preventief en defensief, volgens het concept van 'perimeter defense', ook wel kasteelconcept genoemd. Tegenwoordig ligt de nadruk steeds vaker op detectie en reactieve maatregelen ('de-perimeterization', of hotelconcept)[24]. Dit is zeker het geval in een omgeving waarin toegang tot data belangrijker is dan bescherming van data.

3.3.2 Nadruk op identiteit bij beveiliging

In het kasteelconcept wordt een netwerk 'ommuurd' met onder andere een firewall en antivirussoftware. Deze verdediging is vrij statisch en zorgt ervoor dat data moeilijk toegankelijk zijn. In een wereld waar de cloud steeds belangrijker is - gegevens en gebruikers bevinden zich niet meer op een vaste plek - is een andere benadering van netwerkbeveiliging noodzakelijk.

In die benadering is er niet één dikke, goed beschermende muur, maar wordt de identiteit van de gebruiker als uitgangspunt genomen voor toegang tot delen van het netwerk, bijvoorbeeld data. Het is daarbij heel belangrijk dat onomstotelijk kan worden vastgesteld dat de gebruiker is wie hij zegt dat hij is. Rechten worden immers uitgedeeld aan individuen.



[24] *Maak van het kasteel een hotel (Pool, 2008, opgehaald op 29 september 2015)*

Zo wordt het netwerk meer als een hotel: een gebouw met openbare ruimtes, maar ook met ruimtes waar je alleen met een sleutel naar binnen kunt.

Maatregelen toegesneden op gebruiker

Toegang wordt gebruikerafhankelijk en daarom worden ook beveiligingsmaatregelen steeds meer toegesneden op de individuele gebruiker. Ze hangen dan af van zijn identiteit, welke rol hij heeft, waar hij zich bevindt en welke data hij benadert. Studenten en docenten van een mbo-instelling hebben andere eisen dan onderzoekers aan een universiteit. In alle gevallen zijn sommige data openbaar, andere vertrouwelijk en weer andere privacygevoelig of een combinatie daarvan. Welke maatregelen precies nodig zijn, is gebaseerd op een risicoafweging, waarbij de waarde van de informatie leidend is.

3.4 Van high-level naar concrete maatregelen

Bestuur en directie bepalen welke processen belangrijk zijn voor de instelling, welke risico's aanvaardbaar zijn en welke mate van bescherming nodig is. Idealiter wordt als hulpmiddel een risicomanagementcyclus ingericht, zodat bestuur en directie voortdurend inzicht hebben in de status van de risico's voor de hele instelling. Onderdeel van het risicomanagementproces is een risicoanalyse die regelmatig herhaald wordt. De uitkomst hiervan biedt de verantwoordelijken binnen de geledingen de mogelijkheid de juiste maatregelen op tactisch en operationeel niveau in te regelen. De security officer speelt als coördinator met voldoende mandaat van het bestuur, een belangrijke rol in het afstemmen van het informatiebeveiligingsbeleid tussen de verschillende geledingen, het aanreiken van ideeën en het vergroten van bewustzijn.

In het vorige dreigingsbeeld[25] zijn een aantal high-level maatregelen genoemd die als startpunt dienen:

- zorgen dat cybersecurity vanuit het bestuur gedragen wordt;
- cybersecurity integraal onderdeel van het beleid van de instelling maken;
- de juiste balans van maatregelen vinden;
- in staat zijn om dreigingen te detecteren en tijdig en adequaat te handelen;
- voorbereid zijn op een cyberaanval.

Deze richtlijnen passen goed bij het Normenkader Informatiebeveiliging HO 2015[26] dat zowel in de het hoger onderwijs en onderzoek als bij de mbo-instellingen[27] gebruikt wordt als referentie voor informatiebeveiliging.

Om verder te bepalen welke maatregelen concreet genomen moeten worden, zijn de volgende vragen relevant[28]:

- Wat is de impact wanneer we worden getroffen door een cyberaanval (kosten, imago)?
- Kunnen we snel reageren op een cyberaanval?
- Hebben we onze kroonjuwelen geïdentificeerd en begrijpen we de waarde die ze hebben voor anderen?
- Weten we waarin we moeten investeren om de cyber security risico's te verminderen?
- Zijn we veerkrachtig genoeg om een cyberaanval te overleven?

[26] *Normenkader Informatiebeveiliging HO 2015 (Moens, 2015)*
[27] *Normenkader Informatiebeveiliging MBO (Kennisnet / saMBO-ICT, 2015)*
[28] *Global State of Information Security Survey 2015 (PWC, 2015)*

Om deze vragen adequaat te kunnen beantwoorden wordt een risicoanalyse uitgevoerd. Daarbij is input van het bestuur nodig om te bepalen welke processen het belangrijkst zijn voor de instelling, zodat de strategische keuzes goed onderbouwd zijn. Uit de risicoanalyse volgt welke dreigingen, in combinatie met de aanwezige kwetsbaarheden, de grootste impact hebben voor de instelling. Maatregelen worden vervolgens toegespitst op die dreigingen. Maatregelen om de geïdentificeerde dreigingen tegen te gaan omvatten in ieder geval:

- dataclassificatie
- vergroten van bewustzijn
- antivirussoftware
- back-up- en restore-proces
- identiteits- en toegangscontrole
- monitoring, logging en signalering

3.5 Concrete maatregelen

De dreigingen die in het onderzoek van 2014[29] zijn geïdentificeerd als relevant en volledig voor de sector onderwijs en onderzoek, zijn dat nog steeds. Daarom hebben we die als uitgangspunt genomen voor het beschrijven van maatregelen om dreigingen te weerstaan.

Type Dreiging	**Manifestatie van dreiging**		**Relevantie (kans x impact)**		
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

Impact van de dreiging t.o.v. 2014: ↓ = afgenomen, → = gelijk gebleven, ↑ = toegenomen

Dreigingen sector onderwijs en onderzoek

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 buiten Nederland, 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."

Legenda relevantie - *Bron: Cybersecuritybeeld Nederland (Nationaal Cyber Security Centrum, 2015)*

[29] *Cyberdreigingsbeeld – Sector Hoger Onderwijs en Wetenschappelijk Onderzoek 2014 (SURFnet, 2014)*

Algemene maatregelen om deze dreigingen tegen te gaan zijn[30]:

- Informatiebeveiligingsbeleid – Alle maatregelen die worden genomen, komen voort uit het informatiebeveiligingsbeleid dat is vastgesteld door bestuur en directie. Het informatiebeveiligingsbeleid wordt met geplande tussenpozen of als zich significante veranderingen voordoen, beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.
- Taken en verantwoordelijkheden – Alle verantwoordelijkheden bij informatiebeveiliging zijn gedefinieerd en toegewezen. Er is een disciplinair proces vastgelegd voor medewerkers die inbreuk maken op het beveiligings- en/of privacybeleid.
- Wijzigingsbeheer – Veranderingen in de organisatie, bedrijfsprocessen, informatieverwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging, worden beheerst.
- Back-up en restore – Regelmatig worden back-upkopieën van informatie, software en systeemafbeeldingen gemaakt. Gemaakte back-ups worden regelmatig getest conform het back-upbeleid.
- Fysieke beveiliging – Beveiligde gebieden zijn beschermd door passende toegangsbeveiliging, om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.
- Stroomvoorziening – Apparatuur is beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

In de volgende paragrafen gaan we in op specifieke maatregelen die per dreiging genomen kunnen worden.

3.5.1 Verkrijging en openbaarmaking van data

De sector onderwijs en onderzoek is kennisintensief waarin digitale (gevoelige) dataopslag centraal staat. Wanneer dergelijke informatie in verkeerde handen valt, kan dit leiden tot reputatieschade en verlies van vertrouwen in de instelling en/of haar bestuur. Vooral onderzoeksinstellingen beschikken over uiterst gevoelige data, waarbij verlies en openbaarmaking zelfs kunnen leiden tot ingrijpende aansprakelijkheidsclaims. Met als gevolg dat studenten besluiten elders te gaan studeren, derdegeldstroomopdrachten aan anderen worden gegund, of subsidies van bijvoorbeeld het NWO wegvallen.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het beveiligingsaspect *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 moet een systeem voor identiteits- en toegangsbeheer zijn 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[31], zodat de data bij een eventuele inbraak niet zomaar benaderd kan worden of naar buiten gebracht kan worden.

[30] *Uit bijlage III in Baseline Informatiebeveiliging HO (BIHO) (SCIPR (SURFibo), 2015)*
[31] *Zie bijvoorbeeld: Defense in Depth (NSA)*

RANSOMWARE

Ransomware blokkeert een computer en vraagt vervolgens geld van de gebruiker om de computer weer toegankelijk te maken. **Cryptoware** is een vorm van ransomware waarbij bestanden van de gebruiker worden versleuteld en de decryptiesleutel pas na betaling van losgeld wordt overhandigd (althans dat is de veronderstelling). Daardoor helpt alleen het verwijderen van de malware niet meer; er moet betaald worden om de decryptiesleutel te verkrijgen, zodat de versleutelde bestanden weer toegankelijk worden.

Een voorbeeld van cryptoware is **CryptoLocker**. Bij infectie vindt het volgende proces plaats: het programma wordt opgeslagen in het gebruikersprofiel, het maakt een aantal registersleutels aan, beschermt zichzelf tegen verwijdering, versleutelt bestanden na het ophalen van een encryptiesleutel en houdt bij welke bestanden versleuteld zijn. Vervolgens wordt een boodschap getoond, waarin wordt aangegeven dat de gebruiker binnen een bepaalde tijd losgeld moet betalen om de decryptiesleutel te verkrijgen:

Bron: www.virusresearch.org

Na betaling van het losgeld kan de gebruiker de bestanden weer ontsleutelen.

Fox IT* raadt aan om bij besmetting met cryptoware, het systeem niet uit te zetten, omdat de encryptiesleutel zich in het werkgeheugen van de computer bevindt. Fox IT is er in een aantal gevallen in geslaagd om de decryptiesleutel te vinden, doordat ze deze uit het werkgeheugen konden halen. Dit is echter niet meer mogelijk zodra de computer is uitgezet.

Ook bevindt de betaalinformatie zich in het werkgeheugen, dus mocht een gebruiker besluiten om losgeld te betalen, dan kan dat niet meer zodra de computer is uitgezet, omdat dan de betaalinformatie gewist is. Wel is het verstandig de netwerkverbinding te verbreken om het verder versleutelen van bestanden op het netwerk te voorkomen.

De beste manier om het dataverlies tot een minimum te beperken is het hebben van een recente back-up, zodat bestanden die versleuteld zijn, teruggezet kunnen worden. Dat vereist dus een goede back-upprocedure waarbij data regelmatig (dagelijks) geback-upt wordt.

ADVANCED PERSISTENT THREATS

Voor spionageactiviteiten, of die nu door cybercriminelen of door staten worden uitgevoerd, worden vaak zogenaamde Advanced Persistent Threats (APT's) gebruikt. Een APT is langdurige aanval die zoveel mogelijk onder de radar plaatsvindt en een specifiek doel heeft. APT's worden vaak voorbereid door een spear-phishing attack (zie kader op pagina 22) in de vorm van een e-mail met pdf-bijlage, gericht aan bijvoorbeeld een paar managers. In tegenstelling tot een DDoS-aanval richt een APT geen zichtbare schade aan, maar probeert permanente toegang tot gegevens te bewerkstelligen en data te stelen. APT's zijn ook complex en moeilijk te herkennen.

Er zijn echter wel signalen die erop duiden dat een APT gaande is**:

- een toename van logins met superadminaccounts, vooral buiten normale werktijden;
- backdoor Trojans op systemen;
- grote, niet normale datastromen vanaf interne systemen naar externe systemen of andere interne systemen;
- grote, niet normale dataopslag op onverwachte plekken;
- hackingtools op systemen, vooral zogenaamde pass-the-hash (PTH) tools.

* *"The state of Ransomware" (Klijnsma, 2015)*
** *http://www.infoworld.com/article/2615666/security/5-signs-you-ve-been-hit-with-an-advanced-persistent-threat.html (opgehaald op 19 oktober 2015)*

- Bewustzijn – Gebruikers moeten 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.

3.5.2 Identiteitsfraude

Identiteitsfraude is een van de belangrijkste problemen op het gebied van cybercrime. Het wordt vaak ingezet voor financieel gewin, maar kan ook als middel worden gebruikt om bepaalde data te verkrijgen of te manipuleren. Onderwijsinstellingen hebben met identiteitsfraude te maken wanneer gestolen identiteiten misbruikt worden voor spamming of phishing, en wanneer studenten zich voordoen als iemand anders, bijvoorbeeld om zo betere studieresultaten te halen. Vooral door de opkomst van digitale lesvormen en online tentaminering, wordt digitale identiteitsfraude een steeds meer voorkomende dreiging.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het beveiligingsaspect *integriteit*:

- Identiteitscontrole – Er moet een systeem zijn 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.

3.5.3 Verstoring ICT

Verstoring van de ICT kan zich op verschillende manieren voordoen en heeft meestal als doel om het netwerk of systemen van een bedrijf of instelling plat te leggen. Omdat onderwijs- en onderzoeksinstellingen veel gebruik maken van netwerken, met toegang vanaf verschillende locaties, vormt dit een reële bedreiging. De meest voorkomende manieren om een netwerk of systemen plat te leggen zijn een DDoS-aanval of het verspreiden van *malware* (*virus, spyware* of *ransomware*). De mogelijke gevolgen van een dergelijke aanval kunnen aanzienlijk zijn voor de bedrijfscontinuïteit. Het netwerk kan bijvoorbeeld uren – of zelfs dagen – onbereikbaar zijn voor medewerkers en studenten. Vooral de financiële gevolgen van een dergelijke aanval kunnen sterk oplopen.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op de beveiligingsaspecten *beschikbaarheid* en *integriteit*:

- Antivirussoftware – 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.
- Logging – Gegevens over het inkomende en uitgaande verkeer worden bewaard voor analyse (real-time of achteraf).
- Back-up en restore – Er is een back-upprocedure zodat data na een incident hersteld kunnen worden.

3.5.4 Manipulatie van data

Het delen van data is de norm bij instellingen voor hoger onderwijs en wetenschappelijk onderzoek: tussen docent en student, tussen onderzoekers, tussen instellingen en met het bedrijfsleven en de overheid. Als data worden gedeeld, is het van groot belang dat de informatie zodanig wordt vastgelegd dat deze niet naderhand kunnen worden gemanipuleerd. Als vastgelegde informatie is gemanipuleerd of er een reële verdenking van manipulatie is, kan alle in het systeem aanwezige informatie als onbetrouwbaar worden gezien. Dit wordt gezien als grote bedreiging voor de reputatie van de instelling en de waarde van het product dat zij aflevert.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het beveiligingsaspect *integriteit*:

- Dataclassificatie – Er is een classificatiesysteem, zodat gebruikers kunnen bepalen welke data gevoelig zijn en hoe ze ermee 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 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 (realtime 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.

3.5.5 Spionage

Spionage is een meer geavanceerde dreiging voor de sector onderwijs en onderzoek. Bij spionage gaat het vaak om subtiele vormen van informatievergaring gedurende langere tijd. Iemand van buiten de instelling eigent zich op onrechtmatige wijze gevoelige informatie toe en gebruikt deze informatie voor eigen gewin of speelt die eventueel door naar derden. Vooral onderzoeksinstellingen hebben informatie van hoge intellectuele waarde en beschikken vaak over uiterst (privacy)gevoelige informatie, die zeer interessant kan zijn voor concurrerende instellingen en zelfs staten. Cybercriminelen kunnen gegevens via spionagetactieken verkrijgen om deze vervolgens door te verkopen.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het beveiligingsaspect *vertrouwelijkheid*:

- Bewustzijn – Gebruikers moeten 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.
- Systeemmonitoring – Systemen worden gemonitord om ongebruikelijke activiteit te detecteren die over langere tijd plaatsvindt.
- 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.

3.5.6 Overname en misbruik ICT

Als kwaadwillende personen van buitenaf toegang krijgen tot het netwerk van een onderwijs- of onderzoeksinstelling, kunnen zich twee gevaren voordoen: ze kunnen lopende processen binnen het netwerk verstoren (bijvoorbeeld berekeningen die worden gemaakt), maar ze kunnen ook resources van het netwerk misbruiken voor hun eigen doeleinden. Het grootste gevaar van een dergelijke inbraak is dat de onderwijs- of onderzoeksinstelling aansprakelijk kan worden gehouden voor de programma's die draaien binnen hun omgeving. Als deze ongewenst, kwaadwillend of zelfs illegaal zijn, kan het soms lastig blijken om te bewijzen dat de instelling hier geen verantwoordelijkheid voor draagt.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op de beveiligingsaspecten *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.
- Logging – Gegevens over het inkomende en uitgaande verkeer worden bewaard voor periodieke analyse om ongebruikelijke patronen te signaleren.
- Systeemmonitoring – Systemen worden gemonitord om ongebruikelijke activiteit te detecteren.

3.5.7 Bewust beschadigen imago

Het beschadigen van imago, meestal door bekladding van websites, gebeurt door groepen of individuen met verschillende doelen. Sommigen doen het 'voor de kick', anderen doen het omdat ze een bepaalde boodschap willen verspreiden en weer anderen doen het uit protest tegen een bepaalde instelling. Omdat onderwijs- en onderzoeksinstellingen een relatief groot publiek naar hun vaak decentraal beheerde websites trekken, zijn deze sites ook een aantrekkelijk doelwit voor de verschillende groepen. Daarnaast zijn er belangengroepen die er baat bij hebben om deze instellingen in een kwaad daglicht te zetten. Het bereik van een dergelijke aanval is vaak niet heel omvangrijk, omdat er snel kan worden ingegrepen. Maar vertrouwen reist te voet en gaat te paard. Imagoschade kan ook zo groot zijn dat dit toch een onderwerp van belang is.

Maatregelen

De aanpak van deze dreiging omvat in ieder geval de volgende maatregelen, die vooral betrekking hebben op het beveiligingsaspect *integriteit*:

- Beveiliging van webapplicaties – Bij het ontwerp en programmeren van webapplicaties worden beveiligingsprincipes direct meegenomen (bijvoorbeeld op basis van de OWASP top 10[32]).
- Monitoring van webapplicaties – Het regelmatig uitvoeren van scans op kwetsbaarheden en penetratietesten op webapplicaties.
- Toegangscontrole – Er is een systeem voor identiteits- en toegangsbeheer om te bepalen welke gebruikers toegang krijgen voor beheer en onder welke voorwaarden.
- Back-up en restore – Er is een back-upprocedure zodat data na een incident hersteld kunnen worden.

[32] *OWASP Top Ten Project (Open Web Application Security Project, 2013)*

CRYPTOWARE: GIJZELVIRUS HIT ONDER CYBERCRIMINELEN

Virussen die een computer gijzelen blijven onder criminelen in populariteit stijgen. Dat komt doordat het een lucratieve business is, schrijft het Nationaal Cyber Security Center in het jaarlijkse trendrapport over cyberveiligheid in Nederland, dat gisteren naar de Tweede Kamer is gestuurd.

De kwaadaardige software blokkeert de toegang tot de computer of tot bestanden als foto's en documenten op die computer. De criminelen eisen vervolgens losgeld om die blokkade ongedaan te maken. Volgens eerdere schattingen van de politie besluit zo'n vijf procent van de slachtoffers te betalen. Het gaat dan om bedragen variërend van 100 tot 700 euro.

Niet alleen burgers zijn slachtoffer, ook bedrijven en overheden. Zo werden computers van de gemeenten Dronten, Lochem en Den Haag vergrendeld. Vaak is de besmetting mogelijk doordat medewerkers op het werk privémail lezen. De fatale malware wordt veelal meegestuurd in een e-mail die afkomstig lijkt van een bekend bedrijf.

(Trouw, 15 oktober 2015)

4 INCIDENTEN MET LESSONS LEARNED

4.1 Inleiding

In dit hoofdstuk beschrijven we een aantal actuele beveiligingsincidenten. U leest wat de impact van deze incidenten was en welke maatregelen zijn genomen om de schade te beperken en de kans op herhaling te voorkomen.

4.2 Ransomware

4.2.1 Het incident

Begin 2015 werd de Vrije Universiteit Amsterdam getroffen door CryptoLocker, een vorm van ransomware (zie kader op pagina 29). In eerste instantie leek de malware binnengekomen te zijn via e-mail van buiten, maar al snel bleek dat de malware muteerde en zich kennelijk ook aan e-mailberichten van interne gebruikers wist te koppelen. Uiteindelijk zijn zo'n 200 computers besmet geraakt.

Volgens Erwin Eliveld, Information Security Officer van het Security Operations Center van de afdeling Informatiemanagement & Beleid, bleek dat "hoewel veel mensen op de hoogte waren van dit soort narigheid, de crypto-variant die de VU trof niet goed werd gedetecteerd." In feite realiseerden sommige getroffen gebruikers zich pas dat er iets serieus aan de hand was op het moment dat ze hun bestanden niet meer konden openen. Zodra duidelijk was wat er aan de hand was, is een login-mededeling voor alle studenten en medewerkers gemaakt om ze te attenderen op CryptoLocker.

Maatregelen

Allereerst is besloten geen losgeld te betalen om een decryptiesleutel te verkrijgen. Vervolgens heeft de VU een aantal maatregelen genomen om de gevolgen van een infectie zoveel mogelijk te beperken en verdere verspreiding van het virus te voorkomen:

- inzet van een tweede antivirusoplossing voor systemen die onder de invloedsfeer van IT verkeerden;
- het op read-only zetten van de netwerkschijven, omdat bestanden op netwerkschijven werden versleuteld;
- blokkeren van het computeraccount direct na detectie van de malware;
- opnieuw installeren van de computer om de malware te verwijderen;
- terugzetten van de back-up van de vorige avond op de schoon geïnstalleerde computer.

Aanvankelijk zijn de netwerkschijven iedere avond op read-only gezet, later alleen in het weekend. Overdag was er voldoende capaciteit bij de afdeling om ernstige problemen te voorkomen. Op die manier is het dataverlies voor de meeste gebruikers tot een minimum beperkt gebleven. Lokale bestanden die versleuteld waren door CryptoLocker, zijn wel verloren gegaan.

4.2.2 Lessons learned

In dit geval is de schade voor de gebruikers tot een minimum beperkt door een goede back-upprocedure voor de netwerkschijven. Het is belangrijk regelmatig back-ups uit te voeren, omdat het voor veel antivirus- en antimalwaresoftware moeilijk is om cryptoware te detecteren. Met een recente back-up blijft het dataverlies beperkt. Dit incident heeft het gevaar van malware als serieus probleem op de radar gezet bij de VU en zijn er verdere maatregelen gepland om besmettingen te voorkomen, zoals het evalueren van SPF (Sender Policy Framework) voor e-mail. Op dit moment is de soft-fail geactiveerd.

4.2.3 Verdere stappen

Om dit soort besmettingen in de toekomst zoveel mogelijk te voorkomen, zijn naar aanleiding van het incident een aantal maatregelen ingevoerd:

- Op Windows-servers is het screenfilter gebruikt om afwijkende bestandsnamen en extensies te detecteren. Aan die detectie is een actie gekoppeld: het IP-adres van de computer waarop de encryptie plaatsvindt, wordt geblokkeerd. Dit beperkt het aantal bestanden dat wordt geraakt.
- De mechanismen om netwerkschijven snel read-only te maken, staan stand-by.

4.2.4 Geschatte kosten

De gemaakte kosten zijn gebaseerd op de volgende veronderstellingen:

- 200 geïnfecteerde systemen die hersteld zijn
- aanmelding probleem per systeem: 5 minuten (gemiddeld)
- diagnose probleem per systeem: 10 minuten (gemiddeld)
- bepalen oplossing (korte termijn): 2 uur
- bepalen oplossing (lange termijn): 8 uur
- inregelen oplossing: 4 uur
- herstel besmette systemen per systeem: 1 uur
- terugzetten data van back-up per systeem: 3 uur
- kosten per dag: € 500

Op basis hiervan zijn ruim 300 mandagen besteed aan het herstel van getroffen systemen en voor het inregelen van nieuwe procedures. Niet meegenomen in het kostenoverzicht zijn de inhuur van een externe partij voor onderzoek en de aanschaf van nieuwe software om dit soort malware beter te kunnen detecteren:

Kostenraming CryptoLocker-incident

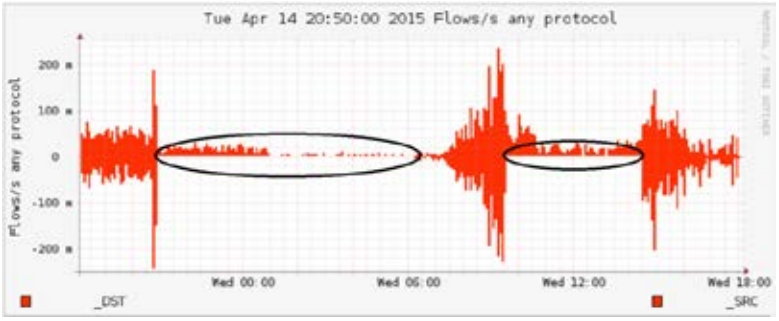
werkzaamheden	tijd/incident	aantal	tijd in uren
aanmelding probleem	5 min.	200	16,67
diagnose probleem	10 min.	200	33,33
bepalen kortetermijnoplossing			2,00
bepalen langetermijnoplossing			8,00
inregelen oplossing			4,00
herstel besmette systemen	1 uur	200	200,00
terugzetten van data	3 uur	200	600,00
verloren werktijd + herstel verloren data	8 uur	200	1600,00
aanpassing procedures			
		Totaal uren	2464,00
		Totaal dagen	308
		Kosten per dag	€500,00
		Totaal kosten	€154.000,00

4.3 Distributed Denial of Service (DDoS)

4.3.1 Het incident

Op 14 en 15 april 2015 zijn een aantal websites van SURF tweemaal getroffen door een DDoS-aanval (zie kader op pagina 22). Doordat de SURF-websites bij een externe partij worden gehost, werden de reguliere SURF-diensten, zoals eduroam en SURFconext, niet getroffen. Maar om diezelfde reden was het ook lastiger om een snelle oplossing toe te passen. Vanwege de hevigheid van de aanval en bijbehorende overlast voor andere klanten op dezelfde hostingomgeving besloot de hostingpartij namelijk de websites uit de lucht te halen door het IP-adres te blokkeren. SURF wilde graag werken aan een oplossing om de websites zo snel mogelijk weer in de lucht te krijgen en heeft toen zelf een aantal maatregelen genomen. Op 16 april vonden weer twee kleinere aanvallen plaats, die door deze oplossing afgeslagen konden worden.

In onderstaande grafiek is duidelijk te zien dat er twee periodes zijn waarin geen uitgaand verkeer meer plaatsvindt.



Symptoom van een DDoS aanval – geen uitgaand verkeer meer (bron: SURFcert)

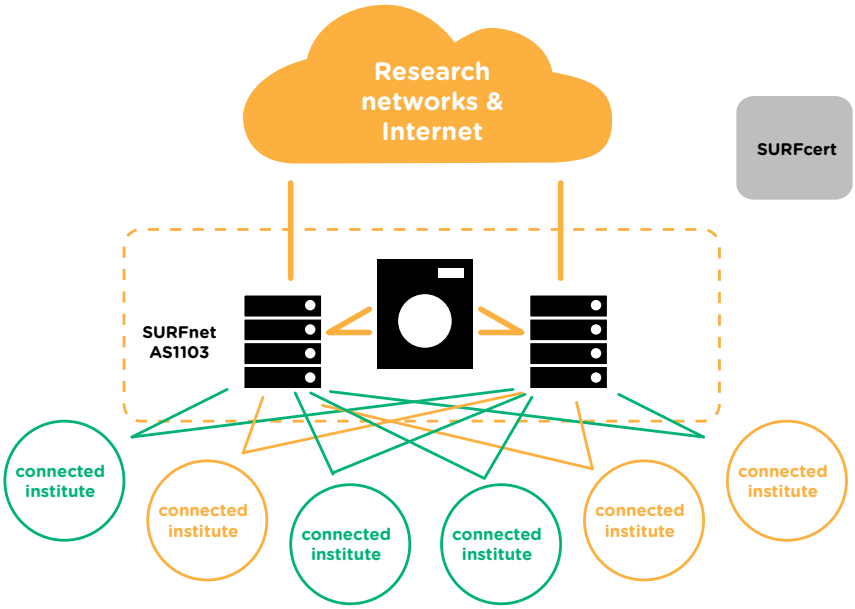
Maatregelen

Controle naar SURF

Omdat de hostingpartij geen maatregelen kon of wilde nemen, heeft SURF besloten zelf de controle over te nemen:

- Er is een reverse proxy geactiveerd die de websites (surf.nl, surfnet.nl, etc.) naar het internet publiceert. De reverse proxy staat in het eigen netwerk van SURF, waarmee SURF zelf de controle over de beschikbaarheid krijgt.
- De reverse proxy heeft een backchannel naar de oorspronkelijke hostingpartij waardoor de gevolgen van de DDoS-aanval op het oorspronkelijke IP-adres omzeild kunnen worden.
- Door een DNS-wijziging wordt verkeer voor de SURF-websites via de reverse proxy geleid.

Op 16 april vonden er weer twee aanvallen plaats die snel en effectief konden worden afgeslagen door het DDoS-verkeer ‘weg te wassen’ met behulp van de wasmachine in het eigen netwerk.

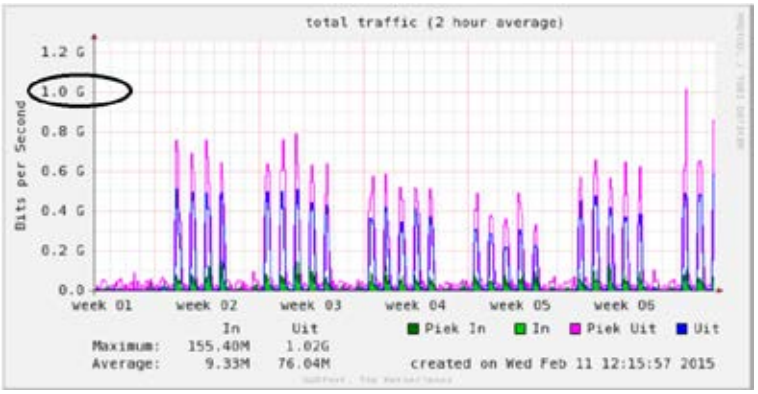


Verkeer voor bijv. SURF wordt door de wasmachine geleid (bron: SURFcert)

Wasmachine
SURFcert kan de wasmachine inschakelen zodra blijkt dat er sprake is van een DDoS-aanval. Dat betekent dat de impact van een aanval snel verminderd kan worden. Hiervoor wordt verkeer naar het aangevallen IP-adres omgeleid naar de wasmachine. Daar wordt het ongewenste verkeer, zoveel mogelijk, verwijderd. Het overige verkeer wordt ongestoord doorgelaten met als gevolg dat overbelasting van de aansluiting wordt gestopt.

Vanwege het karakter van deze werkwijze kan dit niet te lang voortduren. Als een instelling vaker wordt aangevallen, is het verstandig om direct aan de slag te gaan met een meer permanente oplossing.

Netwerkfilters
Netwerkfilters worden op verzoek van de instelling of op advies van SURF in het netwerk opgenomen. Ze beschermen preventief tegen enkele veel voorkomende aanvallen. Ze limiteren de hoeveelheid verkeer dat doorgelaten wordt via een aantal protocollen die bij DDoS-aanvallen veel misbruikt worden.



Netwerkfilters geactiveerd (bron: SURFcert)

4.3.2 Lesson learned

SURF vindt het niet acceptabel dat haar website heel lang niet bereikbaar is. Alleen blokkeren en afwachten tot de aanval voorbij is, is voor SURF daarom geen optie. SURF heeft ervoor gekozen het heft in eigen hand te nemen en zelf een reverse proxy in te richten in het eigen netwerk. Daardoor kan gebruik gemaakt worden van de anti-DDoS-middelen die SURF zelf heeft, terwijl de websites nog steeds door de hostingpartij worden gehost.

4.3.3 Geschatte kosten

De impact voor SURF is op het operationele vlak minimaal geweest. Externe gebruikers hebben wel wat last ondervonden doordat het niet mogelijk was zich in te schrijven voor events en trainingen via de website. Ook is er tijdelijk een omleidingspagina getoond om gebruikers op de hoogte te stellen van het probleem en vragen te kunnen stellen.

Twee SURF-medewerkers hebben naar schatting 2 mandagen gespendeerd aan analyse en rapportage. Daarnaast is er een proxyserver ingericht om zelf de controle te krijgen over de toegang en moesten enkele handelingen worden verricht om configuraties over te zetten.

4.4 Spionage

Volgens het jaarverslag van de AIVD[33] is de spionage (dreigingsbron: staten) voor overheden, private organisaties en burgers nog steeds actueel met een middelhoog tot hoog dreigingsniveau. De offensieve cybercapaciteiten zijn toegenomen sinds 2013/2014: “Het afgelopen jaar stond bijvoorbeeld in het teken van enkele digitale aanvallen door criminelen die opvielen door hun goede organisatie, nauwkeurige uitvoering en technische geavanceerdheid.” In tegenstelling tot ransomware en DDoS-aanvallen richt spionage zich meestal op het verkrijgen van informatie.

Een voorbeeld van digitale spionage is de Gemalto-hack , waarbij volgens Gemalto de Britse en Amerikaanse geheime diensten hebben geprobeerd om encryptiesleutels van simkaarten te verkrijgen. Verder zijn er volgens de AIVD verschillende gevallen van economische spionage geweest, maar omdat bedrijven niet verplicht zijn dergelijke aanvallen te melden, is de totale omvang van deze digitale spionageaanvallen op Nederlandse bedrijven en de economische schade als gevolg hiervan moeilijk vast te stellen[34].

[33] *AIVD – Jaarverslag 2014 (Algemene Inlichtingen- en Veiligheidsdienst, 2014)*
[34] *http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx (opgehaald op 16 november 2015)*
[35] *http://www.volkskrant.nl/binnenland/hoe-russische-spion-in-eindhoven-werd-opgespoord-a4109550/ en https://www.cursor.tue.nl/nieuwsartikel/artikel/vermeende-russische-spion-werkte-aan-tue/ (opgehaald 16 oktober 2015)*

Een voorbeeld van spionage bij een onderwijsinstelling werd op 28 juli 2015 in de Volkskrant beschreven. Op die dag verscheen een artikel over een vermeende Russische spion, de 28-jarige Ivan Agafonov, die als postdoc aan de TU/e werkte. Volgens de AIVD zou de man een "risico voor de veiligheid van Nederland" vormen[35]. De reactie van de TU/e was als volgt:

> *In juli 2014 heeft de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) via een officieel ambtsbericht de TU/e geïnformeerd dat deze onderzoeker contact onderhield met de Russische inlichtingendienst. In de Staatscourant is vervolgens gepubliceerd dat zijn verblijfsvergunning is ingetrokken.*
>
> *Het College van Bestuur heeft naar aanleiding van deze berichten de medewerker onmiddellijk geschorst en op non-actief gesteld. Daarop heeft de TU/e het dienstverband beëindigd. In verband met de wet op de privacy kan de universiteit geen verdere informatie verstrekken.*
>
> *Bron: https://www.tue.nl/universiteit/nieuws-en-pers/nieuws/28-07-2015-oud-medewerker-genoemd-in-spionagezaak/*

DDOS-AANVAL: PROTONMAIL DENKT DAT ‘STAATSHACKERS’ GEAVANCEERDE AANVAL UITVOERDEN

De Zwitserse dienst voor versleuteld mailen ProtonMail kampt met DDoS-aanvallen en wordt door criminelen afgeperst. Het lijkt er volgens ProtonMail echter op dat de dienst onder vuur ligt van een tweede groepering met geavanceerde aanvallen, die aan staatshackers doet denken.

Afgelopen dinsdag ontving ProtonMail een dreigmail van criminelen die claimden achter ddos-aanvallen van de afgelopen weken in Zwitserland te zitten. Daaropvolgend kreeg de webmaildienst voor versleutelde mail twee aanvallen te verduren, die tot kortstondige uitval leidden.

“Binnen de tijdspanne van enkele uren bereikten de aanvallen een geavanceerd niveau zoals we dat nog niet eerder zagen”, claimt de dienst in een verklaring. Bij deze aanval werd de infrastructuur van de upstreampartners van de dienst direct aangevallen. “De gecoördineerde aanval op onze isp overschreed 100 Gbit/s en niet alleen onze datacenters, maar ook routers in Zürich, Frankfurt en andere locaties waar onze isp nodes heeft, lagen onder vuur.”

Deze aanval legde het datacentrum en de provider lam, waardoor veel andere diensten en bedrijven getroffen werden. Hierop besloot ProtonMail het losgeld te betalen. Desondanks duurde de aanval voort, terwijl de criminelen van de eerste aanval ontkenden achter de tweede ddos-aanval te zitten.

ProtonMail redeneert dat twee groeperingen het gemunt hebben op de webmaildienst. “Daarbij vertoonden de tweede aanvallers capaciteiten die worden geassocieerd met daders die door staten gesponsord worden”, claimt ProtonMail, dat erop wijst dat de criminelen bereid waren flinke bijkomende schade voor lief te nemen.

(Tweakers.nl, 6 november 2015)

REFERENTIES

- Algemene Inlichtingen- en Veiligheidsdienst. (2014). AIVD Jaarverslag 2014. Opgehaald van https://www.rijksoverheid.nl/documenten/jaarverslagen/2015/04/01/jaarverslag-aivd-2014
- Cisco. (2015). 2015 Midyear Security Report. Opgeroepen op 10 5, 2015, van http://www.cisco.com/web/offers/lp/2015-midyear-security-report/index.html?keycode=000854836www.cisco.com/go/msr2015
- Dijkstra, A. (2014, 06 14). Risico en gevaar van achterhaalde technologie. Opgeroepen op 10 2, 2015, van computable.nl: https://www.computable.nl/artikel/opinie/datacenters/5112098/4907128/risico-en-gevaar-van-achterhaalde-technologie.html
- ENISA. (2014). ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats (27-01-2015 ed.). ENISA. Opgehaald van https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014
- Janes, P. (2012). People, Process, and Technologies Impact on Information Data Loss. SANS Institute.
- Klijnsma, Y. (2015). The state of Ransomware. Opgehaald van Fox IT: http://blog.fox-it.com/
- Mandiant. (2015). Mandiant M-Trends: A View from the Front Lines. Opgehaald van https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html
- NCSC. (2015). Cybersecuritybeeld Nederland. NCSC.
- NSA. (sd). Opgeroepen op 10 16, 2015, van https://www.nsa.gov/ia/_files/support/defenseindepth.pdf
- OWASP Top Ten Privacy Risks Project. (2014). Open Web Application Security Project. Opgeroepen op 11 9, 2015, van www.owasp.org: https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project
- OWASP Top Ten Project. (2013). Open Web Application Security Project. Opgeroepen op 11 9, 2015, van www.owasp.org: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
- Pool, R. O. (2008). Maak van het kasteel een hotel. Opgeroepen op 09 29, 2015, van https://www.security.nl/posting/18385/Maak+van+het+kasteel+een+hotel
- PWC. (2015). Global State of Information Security® Survey 2015. PWC. Opgehaald van http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html
- SCIPR (SURFibo). (2015, 5 1). Opgeroepen op 10 16, 2015, van https://www.surf.nl/binaries/content/assets/surf/nl/2015/baseline-informatiebeveiliging-ho-2015.pdf
- SINTEF. (2013, 05 22). Opgeroepen op 11 13, 2015, van http://www.sintef.no/en/corporate-news/big-data--for-better-or-worse/
- SURF. (sd). SURF Meerjarenplan 2015-2018. Opgeroepen op 11 20, 2015, van https://www.surf.nl/over-surf/missie-en-strategie/meerjarenplan-surf/index.html
- SURFnet. (2014). Cyberdreigingsbeeld - Sector Hoger Onderwijs en Wetenschappelijk Onderzoek.
- Verizon. (2015). 2015 Data Breach Investigations Report. Verizon. Opgehaald van http://www.verizonenterprise.com/DBIR/2015/

OVERZICHT DREIGINGEN

Type Dreiging	Manifestatie van dreiging				Relevantie (kans x impact)		
Type Dreiging	Gebeurtenis		Actoren	Voorbeeld Incidenten	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en open-baarmaking 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	→	• Cybercriminelen • Activisten • Staten • Medewerkers	• Tentamenfraude door openbaarmaking van tentamenopgaven • Privacygevoelige gegevens over studenten en leerlingen op straat beland • Kamervragen over intranetlek Hogeschool	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	→	• Studenten • Cybercriminelen • Activisten	• Kamervragen naar identiteitsfraude Hogeschool Windesheim • Fraude in toelating examens	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)	↑	• Cyberonderzoekers • Activisten • Studenten • Medewerkers	• Distributed Denial of Service aanval treft SETI project • Dorifelvirus treft ook universiteiten • Server legde netwerk Universiteit Utrecht plat	MIDDEN	MIDDEN	MIDDEN
4. Manipulatie van digitaal opgeslagen data	• Studieresultaten worden vervalst • Manipulatie van onderzoeksgegevens • Aanpassing van bedrijfsvoering data	↓	• Studenten • Medewerkers	• Student krijgt vier jaar celstraf voor het wijzigen van zijn cijfers • Massale fraude economiestudenten • Student hackt website en inleversysteem Informatica	HOOG	LAAG	LAAG
5. Spionage	• Onderzoeksgegevens worden afgetapt • Via een derde partij wordt intellectueel eigendom gestolen • Controleren van buitenlandse studenten door staten	→	• Staten • Bedrijven & commerciële partnerinstellingen • Cybercriminelen	• MI5 waarschuwde Britse universiteiten voor cyberaanvallen • NSA hackt Belgische cyberprofessor • Chinezen bespioneren denk tanks met expertise in Irak	LAAG	HOOG	LAAG
6. Overname en misbruik ICT	• Opstelling van onderzoeksinstellingen overgenomen • Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	→	• Cybercriminelen • Studenten • Medewerkers	• Yahoo blokkeert Universiteit Maastricht wegens spam • Student gebruikt universiteit computers om dogecoin te minen	LAAG	MIDDEN	MIDDEN
7. Bewust beschadigen imago	• Website wordt beklad • Social media account wordt gehackt	→	• Activisten • Studenten • Cyberonderzoekers • Cybervandalen	• Homepage Faculteit Letteren beklad • Hackers bekladden website van MIT	LAAG	LAAG	LAAG

Impact van de dreiging t.o.v. 2014: ↓ = afgenomen, → = gelijk gebleven, ↑ = toegenomen

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 buiten Nederland, 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."

Legenda relevantie - *Bron: Cybersecuritybeeld Nederland (Nationaal Cyber Security Centrum, 2015)*

Informatie	Onderwijs	Onderzoek	Bedrijfsvoering
Studieresultaten	■		
Onderzoeksgegevens & Intellectueel eigendom		■	
CBRN+ gegevens		■	
Bedrijfsvoering data			■
Persoonsgegevens	■	■	■
Commercieel & Juridisch			■
Gegevens van (onderzoeks)partners		■	■
Gegevens over toetsen	■		

COLOFON

Tekst
SURF

Ontwerp
Vrije Stijl, Utrecht

Fotografie
Robert Lagendijk, Kees Rutten

November 2015

SURF

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