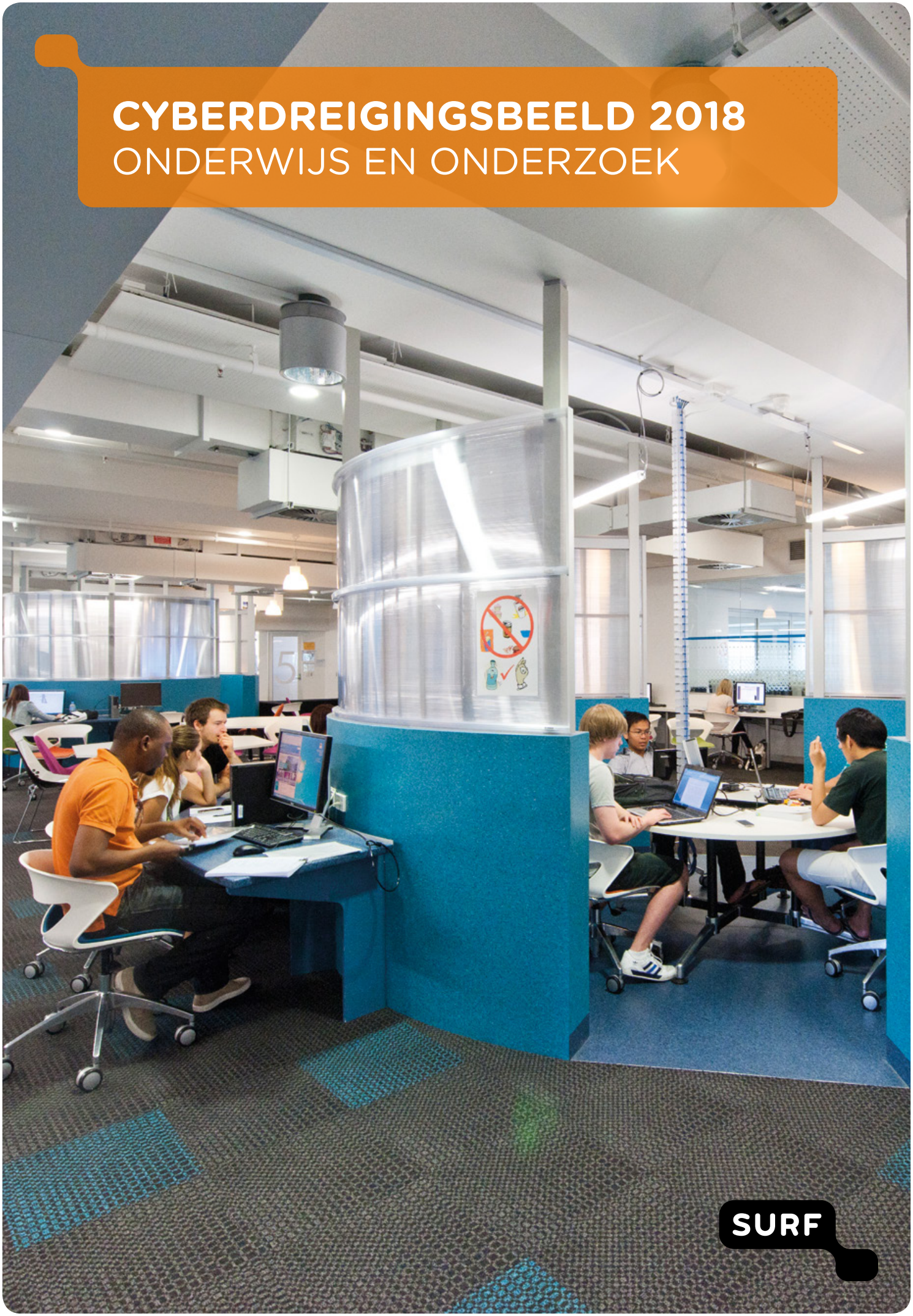
CYBERDREIGINGSBEELD 2018
ONDERWIJS EN ONDERZOEK



INHOUD

VOORWOORD

ICT is van levensbelang voor onderwijs en onderzoek. We zien een snelle groei van digitale leermethoden, de digitale samenwerking met partners neemt toe en we wisselen steeds meer digitale data grensoverschrijdend uit. Digitalisering is wijdverspreid en biedt ongekende mogelijkheden voor onderwijs en onderzoek. SURF voorziet bijvoorbeeld in high-performance computing, big-dataprocessing en clouddiensten voor zijn leden. Dat draagt bij aan een florerende en innovatieve kennisinfrastructuur. Om die mogelijkheden ook op langere termijn te benutten, moet er vertrouwen zijn in dergelijke digitale oplossingen. Tegelijkertijd nemen de dreigingen rond digitalisering toe en raken zo direct het hart van ons onderwijs en onderzoek.

Voor u ligt alweer de 5e editie van het Cyberdreigingsbeeld voor onderwijs en onderzoek, waarmee wij inzicht willen bieden in ontwikkelingen die relevant zijn voor onze sector. De basis voor deze analyse is gelegd door een survey uit te voeren bij instellingen die aangesloten zijn bij SURF. De survey heeft als belangrijkste conclusie dat de informatiepositie over cyberrisico's verbeterd moet worden vanwege de verwevenheid met het primair proces en daarmee de impact als een cybersecurity-incident zich voordoet. Het rapport geeft daarnaast een actueel beeld van de cyberrisico's die instellingen ervaren. Dat beeld zal in praktijk per instelling verschillen en roept vragen op over de situatie bij de instellingen.

Deze vragen moeten indringend op tafel bij de bestuurders van de instellingen. Dit rapport daagt bestuurders uit met prikkelende vragen en aandachtspunten. Hoe is uw instelling voorbereid op cyberdreigingen? Wat zijn uw ambities? Wat weet u over cyberincidenten bij uw instelling? Wat ons betreft allemaal uitermate relevante vragen. Het nemen van basismaatregelen en aanbieden van veilige producten en diensten is namelijk nog niet altijd vanzelfsprekend. Ook beoordelen instellingen hun eigen weerbaarheid als onvoldoende of, wellicht erger, ze weten niet eens hoe ze ervoor staan. Het is aan de bestuurders van instellingen een visie te ontwikkelen met betrekking tot cybersecurity ofwel hun visie een plaats te geven in het bredere kader van integrale veiligheid zoals dat onder andere is beschreven door het 'Programma Integrale Veiligheid Hoger Onderwijs'.

Concreet vraagt dat bijvoorbeeld om het verder ontplooien van veelbelovende initiatieven als 'security-by-design' en 'privacy-by-design' en om mee te doen aan cybercrisisoefeningen zoals OZON, die SURF iedere twee jaar organiseert, om de eigen weerbaarheid te bevorderen. Deze oefening was dit jaar weer een enorm succes, waarbij veel geleerd is en instellingen onderling kennis en ervaringen uitwisselden. Een geslaagd voorbeeld van gezamenlijk optrekken om als sector onze weerbaarheid te bevorderen.

Terugkijkend op vijf jaar Cyberdreigingsbeeld zien we voortdurend veranderingen in de dreigingen die op ons af komen en een verdere toename van de complexiteit van het applicatielandschap bij instellingen. Instellingen zijn in toenemende mate afhankelijk van digitalisering, dus waakzaamheid is geboden en het belang van proactieve maatregelen wordt steeds groter.

Samen met de tweejaarlijkse SURFaudit-benchmark draagt dit rapport bij aan de bewustwording op alle niveaus over de staat van informatiebeveiliging in de sector onderwijs en onderzoek, zodat de instellingen weten wat ze kunnen doen om weerbaarder te worden, dreigingen het hoofd te bieden en digitalisering ten volle te benutten.

Erwin Bleumink, *Lid bestuur SURF*
Marjolein Jansen, *Vice-voorzitter Vrije Universiteit Amsterdam*
en *Ambassadeur Cybersecurity SURF*

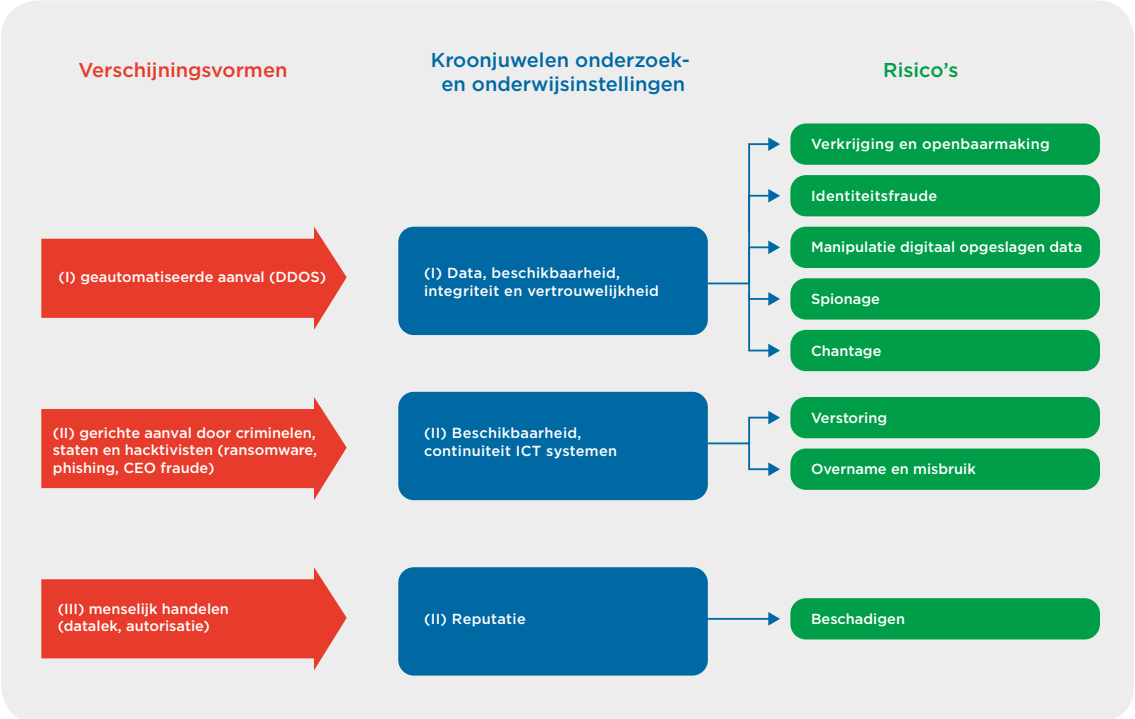
SAMENVATTING

Algemeen

Dit Cyberdreigingsbeeld informeert bestuurders, security en privacy officers van Nederlandse onderzoeks- en onderwijsinstellingen over ontwikkelingen op het vlak van cybersecurity die hebben plaatsgevonden in 2018. Daarnaast hebben we een survey gehouden om de risicoperceptie van de instellingen in kaart te brengen en een beeld te krijgen van incidenten die zich hebben voorgedaan in de volgende risicocategorieën:

1. Verkrijging en openbaarmaking van data
2. Identiteitsfraude
3. Verstoring ICT
4. Manipulatie van digitaal opgeslagen data
5. Spionage
6. Overname en misbruik ICT
7. Bewust beschadigen imago

De volgende figuur illustreert de de verschijningsvormen van dreigingen, de risico's en welke kroonjuwelen ze beïnvloeden:



Algemene trends die we waargenomen hebben in 2018 op het vlak van cyberdreigingen

Kwaadwillenden maken net als in voorgaande jaren gebruik van malware om hun doelen te bereiken. Ransomware is een veel gebruikt middel en verschillende instellingen zijn getroffen door besmettingen. Verder vinden denial-of-serviceaanvallen regelmatig plaats, met wisselend effect, en worden nog steeds hackingaanvallen uitgevoerd om toegang te krijgen tot interne systemen. De effectiviteit van phishing blijft kennelijk groot genoeg om regelmatig voor te komen.

Criminelen zijn vooral geïnteresseerd in geldelijk gewin: data zijn geld. Ook onderzoeks- en onderwijsinstellingen zijn in het bezit van waardevolle data, variërend van persoonsgegevens tot onderzoekdata. Daarbij geldt enerzijds dat wanneer de basis beveiligingsmaatregelen niet op orde zijn, criminelen zich makkelijk toegang kunnen verschaffen tot interne systemen. Anderzijds geldt dat wanneer controle en logging niet goed zijn ingericht, moeilijk valt te achterhalen wat er gebeurt op het netwerk en op interne systemen. Naast externen kunnen ook interne medewerkers problemen veroorzaken, al dan niet opzettelijk.

Cyberdreigingen die instellingen hebben ondervonden in 2018

De perceptie van het risico dat instellingen lopen is behoorlijk veranderd: de risico's worden veel hoger ingeschat dan tot nog toe het geval was. Waar in voorgaande jaren risico's laag werden ingeschat zijn nu de meeste risico's middelhoog ingeschat. Wellicht hangt dat samen met de invoering van de AVG op 25 mei 2018. In de aanloop hiernaar hebben instellingen veel aandacht besteed aan het beveiligen van persoonsgegevens. Ook hebben ze procedures ingericht om datalekken, mochten die zich voordoen, tijdig te melden bij de autoriteit persoonsgegevens. Daardoor hebben instellingen meer aandacht gekregen voor de governance van informatiebeveiliging en voor de noodzaak van maatregelen om informatie af te schermen.

De top 3 cyberdreigingen verschilt per sector. Voor onderwijs en bedrijfsvoering is de verstoring van ICT-voorzieningen het belangrijkste risico. Die dreiging heeft dan ook vrij direct effect op de continuïteit van het primaire (onderwijs)proces. Voor de sector onderzoek is de verkrijging en openbaarmaking van data het belangrijkste risico. Ook die dreiging raakt direct aan een kroonjuweel van instellingen, namelijk het intellectueel eigendom/integriteit van onderzoeks- en persoonsgegevens. Ook het beschadigen van imago wordt als een belangrijk risico gezien.

Bij de beantwoording van de vraag naar de frequentie waarmee incidenten hebben plaats gevonden valt op dat veel respondenten van de survey aangeven dat dit niet bekend is. Dit onderstreept een van de conclusies uit het SURFaudit-benchmarkrapport dat 'controle en logging' laag scoort. Bij een risico als 'verstoring van ICT-voorzieningen' is het aantal 'niet bekend'-responses juist laag, waarschijnlijk omdat alle instellingen een incidentregistratie-systeem hebben en een verstoring snel gemeld zal worden.

Actuele trends die de volle aandacht hebben zijn het voortdurend optreden van denial-of-serviceaanvallen, het gebruik van BYOD en het gebruik van internet of things (IoT).

Maatregelen die instellingen nemen ter bevordering van hun cyberweerbaarheid

Bij de meeste instellingen die hebben meegedaan aan de survey staat informatiebeveiliging op de agenda van het college van bestuur en is er, in mindere mate, ook aandacht voor bij de raad van toezicht. Alle instellingen hebben een goedgekeurd informatiebeveiligingsbeleid, maar soms schort het aan het evalueren en up-to-date houden daarvan.

De weerbaarheid van instellingen scoort goed in de survey:

- de mbo-instellingen scoren bovengemiddeld,
- de hbo-instellingen laten een wisselend beeld zien met enkele uitschieters naar beneden (score 2 & 3 op een schaal van 1 – 10) en
- universiteiten en onderzoeksinstellingen scoren iets boven het gemiddelde (5,5).

De mate waarin de deelnemers aan de survey dreigingen als onder controle beoordelen is ‘redelijk’, zij het dat ‘spionage’ en ‘bewust beschadigen van imago’ beduidend lager worden beoordeeld.

Bestuurlijke dialoog

Ten behoeve van de bestuurlijke dialoog over cybersecurity hebben we, gevoed door de resultaten van dit Cyberdreigingsbeeld, vijf vragen opgenomen voor de thema’s cyberrisicoprofiel, ambities, informatiepositie, cybersecuritybeleid en evaluatie. Deze vragen kunnen bestuurders gebruiken om – in samenspraak met hun Corporate (Information) Security Officer, diensten en faculteitsdirecteuren, Raad van Toezicht – het gesprek te voeren over cyberrisico’s en cyberweerbaarheid van hun eigen instelling.

INLEIDING

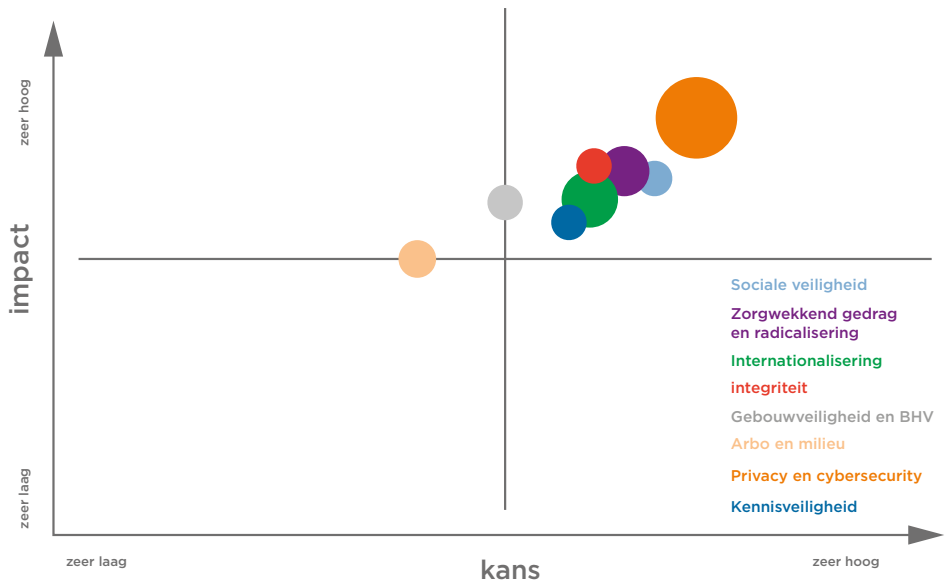
1.1 Achtergrond

Sinds 2014 brengt SURF jaarlijks de belangrijkste ontwikkelingen in cyberdreigingen voor onderzoek- en onderwijsinstellingen in beeld. Het SURF Cyberdreigingsbeeld geeft een actueel beeld van trends en dreigingen. Deze versie bouwt voort op de eerdere edities van het Cyberdreigingsbeeld, maar legt de nadruk op ontwikkelingen die in de afgelopen periode (van januari 2018 tot januari 2019) plaatsvonden.

Met het Cyberdreigingsbeeld informeert SURF bestuurders, security en privacy officers van Nederlandse onderzoeks- en onderwijsinstellingen op ontwikkelingen die zich voordoen, zodat zij hun eigen informatiebeveiliging en privacybescherming verder kunnen verbeteren.

Instellingen hebben te maken met verschillende veiligheidsthema's. Het Programma Integrale Veiligheid Hoger Onderwijs (IV-HO) onderscheidt acht veiligheidsthema's variërend van sociale veiligheid en zorgwekkend gedrag tot internationalisering. [1] Cybersecurity en privacy worden door instellingen gezien als de belangrijkste dreigingen, zo blijkt uit het Dreigingsbeeld Hoger Onderwijs 2018. Concreet gaat het om datalekken, manipulatie van data en identiteitsfraude, verlies van intellectueel eigendom en reputatie-schade. [2]

Het SURF Cyberdreigingsbeeld zoomt in op cybersecurity, onderdeel van het thema 'Privacy en cybersecurity' in het IV-HO Dreigingsbeeld.



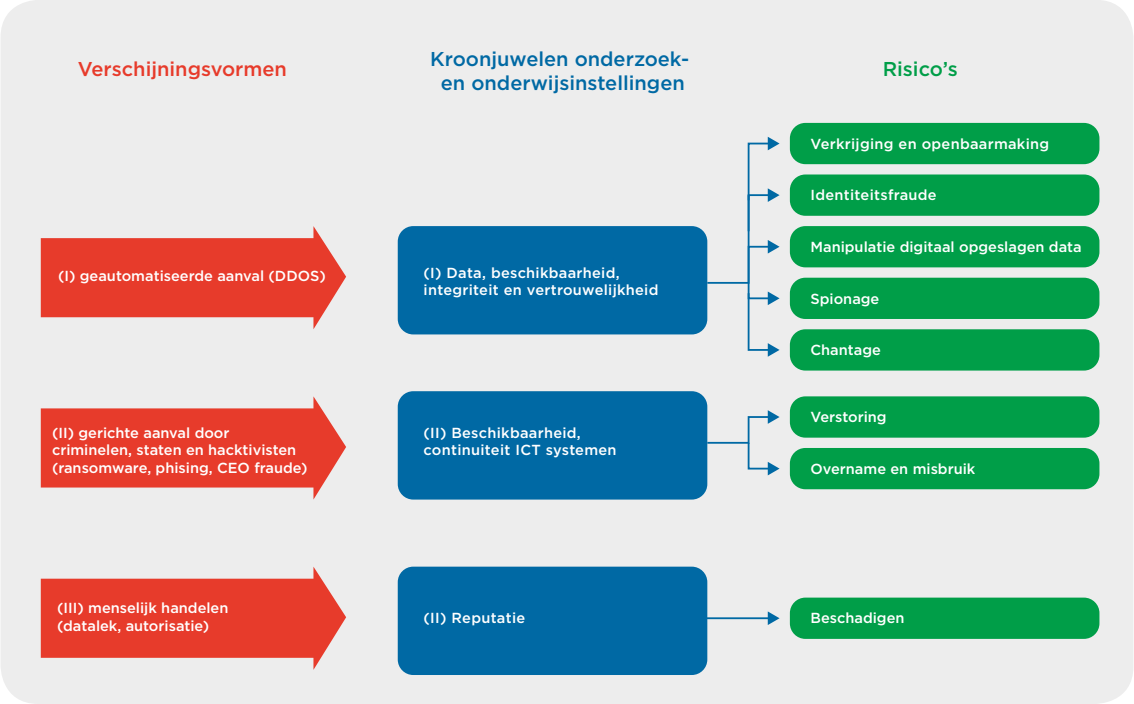
Figuur 1: Dreigingsmatrix uit het Dreigingsbeeld Hoger Onderwijs van IV-HO [3]

De nieuwe editie: cybersurvey onder onderwijsinstellingen

Waar voorgaande edities in belangrijke mate gebaseerd waren op publieke bronnen zoals rapportages van het Nationaal Cyber Security Centrum (NCSC) en Verizon en gesprekken met security officers van instellingen, hebben we in deze editie gevraagd naar cyberdreigingen onder medewerkers van onderzoeks- en onderwijsinstellingen die zich bezighouden met privacy en ICT. Daarnaast hebben we meer dan voorheen, de mbo-instellingen betrokken in het Cyberdreigingsbeeld.

1.2 Cyberdreigingen, kroonjuwelen en verschijningsvormen

Als analysekader gebruiken we het onderstaande model:



Figuur 2: Verschijningsvormen, kroonjuwelen en risico's

Dit diagram illustreert de effecten van de verschijningsvormen van dreigingen en van de risico's op de kroonjuwelen. Verder gaan we kort in op maatregelen die de weerbaarheid van instellingen tegen deze cyberrisico's beïnvloeden.

Kroonjuwelen

Instellingen beschouwen beschikbaarheid, integriteit en vertrouwelijkheid van data, de continuïteit van onderwijs, onderzoek en bedrijfsvoering, en reputatie als hun kroonjuwelen:

	Kroonjuwelen	Voorbeelden
1	Data (beschikbaarheid, integriteit, vertrouwelijkheid)	Persoonsgegevens (studenten, medewerkers)
		Persoonsgegevens in kader onderzoek/databases, waaronder bijzondere persoonsgegevens zoals etniciteit, religie en medische gegevens.
		Intellectueel eigendom
2	ICT-voorzieningen (continuïteit van onderwijs, onderzoek en bedrijfsvoering)	Osiris, e.d.
		Studentenadministratie
		Websites (algemeen, faculteiten, evenementen)
		Beveiliging
		Klimaatbeheersing gebouwen
3	Reputatie (imagoschade)	Reputatie is een afgeleide van het ongestoord en veilig functioneren van ICT-voorzieningen en van de integriteit en beschikbaarheid van data. De reputatie komt in het geding bij (grootschalige) incidenten, waarbij mogelijk sprake is van nalatigheid, bijvoorbeeld niet voldoen aan de AVG, gebrekkige informatiebeveiliging of incidentrespons.

Tabel 1: Risico's

Risico's die zich manifesteren kunnen effect hebben op de beschikbaarheid, integriteit en vertrouwelijkheid van data, de continuïteit van onderwijs, onderzoek en bedrijfsvoering en op de reputatie van instellingen. In dit rapport gebruiken we de zeven categorieën van risico's die in eerdere edities van het Cyberdreigingsbeeld zijn gedefinieerd (zie ook bijlage 1):

1. Verkrijging en openbaarmaking van data
2. Identiteitsfraude
3. Verstoring ICT
4. Manipulatie van digitaal opgeslagen data
5. Spionage
6. Overname en misbruik ICT
7. Bewust beschadigen imago

Verschijningsvormen

Cyberrisico's voor mbo's, hogescholen en universiteiten kunnen zich op verschillende manieren manifesteren (zie Figuur 2):

- geautomatiseerde aanvallen (zoals DDoS)
- gerichte aanvallen door criminelen, staten en andere personen en groeperingen (zoals gijzelingssoftware en spionage)
- menselijk handelen- bewust of onbewust (resulterend in verlies van data).

Effecten

Effecten treden bijvoorbeeld op doordat data worden verkregen (diefstal), gemanipuleerd of onrechtmatig worden ingezien (spionage), identiteitsfraude wordt gepleegd of doordat instellingen worden gechanteerd. Maar ook doordat ICT-voorzieningen worden overgenomen en/of verstoord.

Weerbaarheid

Instellingen kunnen zich op verschillende manieren beschermen tegen digitale aanvallen en verstoringen, afhankelijk van het risicoprofiel van de betreffende instelling. Voor informatiebeveiliging zijn onder meer ambitieniveaus beschikbaar die als richtlijn voor informatiebeveiliging en privacy gelden (zie ook: SURFaudit-benchmark).[51] Naast preventie, gericht op het voorkomen van cyberincidenten, kunnen instellingen investeren in detectie, incidentrespons en crisismanagement.

1.3 Werkwijze

Voor dit Cyberdreigingsbeeld heeft SURF een survey uitgevoerd onder medewerkers van mbo-instellingen, hogescholen, universiteiten en andere bij SURF aangesloten instellingen, die beroepsmatig in aanraking komen met informatiebeveiliging, zoals security & privacy officers. De survey is uitgezet onder leden van SCIPR en SCIRT en via de regiegroep IBP in het mbo.

SCIRT is de community van leden van Computer Security Incident Response Teams (CSIRT's) van op SURF aangesloten instellingen. Doel van SCIRT is om synergie te behalen binnen het veld van beveiligingsexperts van de bij SURF aangesloten instellingen. SCIRT is dé plek waar operationele security-experts actuele security-uitdagingen bespreken en de laatste tips & trucs uitwisselen.

SCIPR is een *community of practice* waarin informatiebeveiligers en privacy officers uit de SURF-doelgroep samenwerken aan het verbeteren van professionele informatiebeveiliging en privacy. SCIPR staat voor SURF Community voor Informatiebeveiliging en Privacy. Het doel is de informatiebeveiliging en privacy bij onderwijs- en onderzoeksinstellingen te verbeteren. Dit doet SCIPR onder andere door beleid en leidraden te ontwikkelen.

De platforms werken met elkaar samen. SCIPR houdt zich bezig met securitybeleid en governance, SCIRT met meer operationele zaken.

De regiegroep ibp in het mbo is een samenwerkingsverband onder de vlag van saMBO-ICT, waarin ook Kennisnet en SURF deelnemen. Het doel van de regiegroep is het ontwikkelen van kennis en delen van ervaringen.

De survey bevatte vragen over de belangrijkste cyberdreigingen en over maatregelen om de cyberweerbaarheid te bevorderen. In totaal hebben 35 respondenten de survey ingevuld, verdeeld over 28 instellingen. Het betreft zowel kleinere als grote instellingen. Verder namen instellingen deel die alleen onderzoek doen, instellingen die alleen onderwijs aanbieden en instellingen die beide doen. Niet alle respondenten hebben alle vragen beantwoord.

Mbo	3
Hbo	14
Wo	7
Onderzoek	3
Onbekend	1

Tabel 2: Aantal instellingen per sector

Security officer/-manager	17
Privacy officer	5
Hoofd IT	4
Beleidsmedewerker/adviseur	4
Overig	5

Tabel 3: Aantal respondenten per functie

Om de opzet en uitkomsten van de survey te valideren, hebben we een klankbordgroep samengesteld van geïnteresseerde medewerkers van onderzoeks- en onderwijsinstellingen. De input van de klankbordgroep hebben we meegenomen in de survey en verwerkt in deze rapportage.

Om trends in kaart te brengen hebben we gezaghebbende publicaties geraadpleegd en informatie opgehaald uit de eigen datasets van SURF, zoals die van SURFcert.

1.4 Cyberdreigingsbeeld 2017

Cyberdreigingsbeeld 2017: hoofdpunten

In het Cyberdreigingsbeeld 2017 kwamen de volgende trends naar voren:

1. Beroepscriminelen en statelijke actoren vormen nog altijd de grootste dreiging en richten de meeste schade aan.
2. Weerbaarheid van individuen en organisaties blijft achter bij de groei van de dreiging.
3. Toenemende digitalisering van burgers (en dus van studenten, docenten, onderzoekers en andere medewerkers van onderwijs- en onderzoeksinstellingen) verandert het dreigingslandschap.
4. Denial-of-serviceaanvallen blijven voortduren maar zijn wel onder controle.
5. Kwaadwillenden maken nog steeds misbruik van kwetsbaarheden, ook op mobiele apparaten, om toegang tot kritieke systemen te verkrijgen. [4]

Cyberdreigingsbeeld 2018: vergeleken met voorgaande edities

De bovenstaande trends hebben zich ook in 2018 onverkort voortgezet. Een belangrijk verschil met de voorgaande editie van het Cyberdreigingsbeeld is de invoering van de Algemene Verordening Gegevensbescherming (AVG) medio 2018. De AVG heeft tot veel aandacht geleid bij instellingen en het afgelopen jaar hebben instellingen maat-regelen getroffen om te voldoen aan de AVG. De aandacht voor de AVG is een mogelijke verklaring voor een andere perceptie van cyberdreigingen: het is voorstelbaar dat deelnemers dreigingen hierdoor hoger inschatten dan voorgaande jaren. Verder hebben we in 2018 een andere werkwijze gehanteerd. De zeven dreigingen uit de eerdere edities hebben we vanuit het oogpunt van continuïteit gehandhaafd.

Cyberdreigingen zijn niettemin uitermate dynamisch. De ‘kleur’ van het Cyberdreigings-beeld zal per jaar verschillen. We merken op dat in deze editie voor de eerste keer een meer kwantitatieve beoordeling van dreigingen heeft plaatsgevonden. De beoordeling van dreigingen verschilt daardoor van eerdere edities. In deze editie is een bredere doelgroep geraadpleegd. Naast onderzoeksinstellingen, hogescholen en universiteiten hebben mbo-instellingen deelgenomen aan de survey.

1.5 Leeswijzer

Hoofdstuk 2 geeft een beeld van de belangrijkste actuele cybertrends.
Hoofdstuk 3 zoomt in op de belangrijkste cyberdreigingen voor onderzoeks- en onderwijs-instellingen. De focus ligt zowel op de *perceptie* van dreigingen als op het daadwerkelijke plaatsvinden van cyberincidenten.
Hoofdstuk 4 is gewijd aan de cyberweerbaarheid van instellingen, dus de mate waarin zij zijn voorbereid op de preventie en respons op cyberdreigingen.
Hoofdstuk 5 bevat de belangrijkste highlights uit dit rapport en punten voor reflectie die bestuurders kunnen gebruiken voor de dialoog over cyberrisico’s en –weerbaarheid binnen hun eigen instelling.

2. TRENDS

Dit hoofdstuk geeft een beeld van de belangrijkste actuele cybertrends. Ze zijn afgeleid uit gezaghebbende rapportages en informatie van SURF. Aan bod komen: werkwijzen, motieven, actoren en digitale weerbaarheid. Daarnaast wordt een beeld geschetst van datalekken en incidentregistraties bij SURF.

2.1 Werkwijzen: gijzelingssoftware, DDoS en hacking

- Hoewel cybercriminelen nog steeds succes hebben met beproefde en bewezen aanvalstechnieken [5], neemt de complexiteit van aanvallen steeds toe. [6]
- Gijzelingssoftware (ransomware) is de meest voorkomende vorm van kwaadaardige software; voor cybercriminelen is er in dat geval geen noodzaak om data te ontvreemden, zij zetten enkel in op het blokkeren van het gebruik van data en systemen. Belangrijkste reden waarom het vaak voorkomt: het is simpel in te zetten, weinig risicovol voor de aanvaller en blijkt erg effectief [8]. Hoewel de exacte schade niet duidelijk is, nadert de geschatte schadesom door ransomware in 2017 5 miljard Amerikaanse dollar. [9]
- Cyberaanvallen kunnen eenvoudig worden uitgevoerd. Er is een levendige onlinehandel, waarin infrastructuur, hulpmiddelen en technieken voor het uitvoeren van aanvallen tegen betaling worden aangeboden. Hierdoor is het, ook voor andere actoren dan bijvoorbeeld staten, relatief eenvoudig om een aanval uit te voeren. [7] Dat leidt volgens het Nationaal Cyber Security Centrum tot intensivering van het dreigingsbeeld. Die aanvallen hebben een grote mate van willekeur, waardoor ze burgers en diverse andere (bedrijfs) sectoren treffen. De verwachting is dat de willekeur van aanvallen afneemt en aanvallen gerichter plaatsvinden, om winsten te optimaliseren. [10]
- Website defacements blijven zich voordoen, hoewel de impact van dergelijke aanvallen minimaal is. [11]
- Ransomware blijft een prominente dreiging, hoewel de groei lijkt af te nemen. Een nieuw verdienmodel voor criminelen, en daarom een mogelijke toekomstige dreiging, vormt ‘cryptojacking’, het misbruiken van bandbreedte en computerresources voor cryptomining die tot verstoring van ICT-voorzieningen kan leiden. [12]
  Dit is volgens deskundigen wel afhankelijk van de koers van cryptomunten die recent gedaald is; een hogere koers maakt dit interessanter als verdienmodel.
- Veel inbreuken gebeuren met gestolen credentials [13]. Het vergaren van login informatie (credential-harvesting) vindt steeds vaker plaats in cloudapplicaties, die ook vaker gebruikt worden door instellingen.
- Cyberactoren maken momenteel veelvuldig gebruik van e-mail als een instrument voor het verspreiden van kwaadaardige software of voor phishing doeleinden. [14]
- In bijna de helft van incidenten waarbij data is gestolen, wordt hacking als methode gebruikt [15]

2.2 Motieven: geldelijk gewin, data als handelswaar

- Driekwart van inbraken wordt gepleegd voor financieel gewin. [16] Dat betekent dat in feite alle gegevens waarover instellingen beschikken waarde hebben. Data zijn geld waard, dat is belangrijk om te beseffen.

- De interesse in persoonsgegevens onder verschillende typen actoren is groot. Voor het verwerven van die gegevens worden cyberaanvallen uitgevoerd. De gegevens worden onder meer gebruikt voor creditcard en identiteitsfraude. [17]
- Binnen de sector onderwijs vinden aanvallen volgens het Data Breach Investigations Report van Verizon [18] overwegend plaats vanuit financiële overwegingen (70%), gevolgd door spionage (20%) en plezier (11%). [19] Het illustreert dat ook onderwijs- en kennisinstanties over gegevens beschikken van bijvoorbeeld medewerkers en studenten of onderzoekdatabases die financieel aantrekkelijk zijn voor cybercriminelen.
- De meest voorkomende gegevens die worden gecompromitteerd zijn persoonsgegevens, gevolgd door betalingsgegevens en medische data. [20]
- Cyberaanvallen richten zich op instanties en personen die slecht beveiligd en voorbereid zijn. [21] Doordat cyberaanvallen in een groot aantal gevallen vrij willekeurig plaatsvinden, kunnen zij iedereen raken. Dat maakt partijen die zich niet voorbereiden dan ook uitermate kwetsbaar. [22]
- Cyberaanvallen zijn en blijven een profijtelijke manier om specifieke (persoonlijke, economische of ideologische) doelen te realiseren. De impact en de opbrengst van cyberaanvallen groeit onder invloed van toenemende digitalisering. [23]

2.3 Actoren: criminelen en staten/personen

- Een ruime meerderheid van de digitale aanvallen (73%) wordt gepleegd door zogenaamde outsiders, zoals criminelen en staten. Bijna een derde van aanvallen wordt door insiders gepleegd. [24] Denk aan IT-administrators, tijdelijke werknemers en gebruikers die toegang tot gevoelige data hebben. De risico's die hier een rol spelen zijn onder anderen datalekken door onachtzaamheid of nalatigheid en opzettelijk lekken van gegevens [25]. Hierbij geldt dat dit risico lastig is te detecteren en tegen te gaan, doordat insiders vaak legitiem toegang tot vertrouwelijke gegevens hebben. De 'insider threat' wordt vaak onderschat en is ook moeilijker te detecteren.
- Vooral commerciële instellingen en overheidsinstanties zijn doelwit van statelijke actoren. [26]
- Naast criminelen en staten kunnen hacktivisten, cybervandalen en insiders zorgen voor verstoring van bedrijfsprocessen en diefstal van informatie. [27]

De Nederlandse ICT-beveiliger Fox-IT waarschuwt voor gijzelsoftware SamSam. Die nieuwe vorm van ransomware saboteert eerst de back-ups en vergrendelt daarna de originele bestanden. Inmiddels zouden al tientallen bedrijven in Nederland door de ransomware getroffen zijn. Er zijn vooralsnog geen Belgische slachtoffers bekend bij Fox-IT. [28]

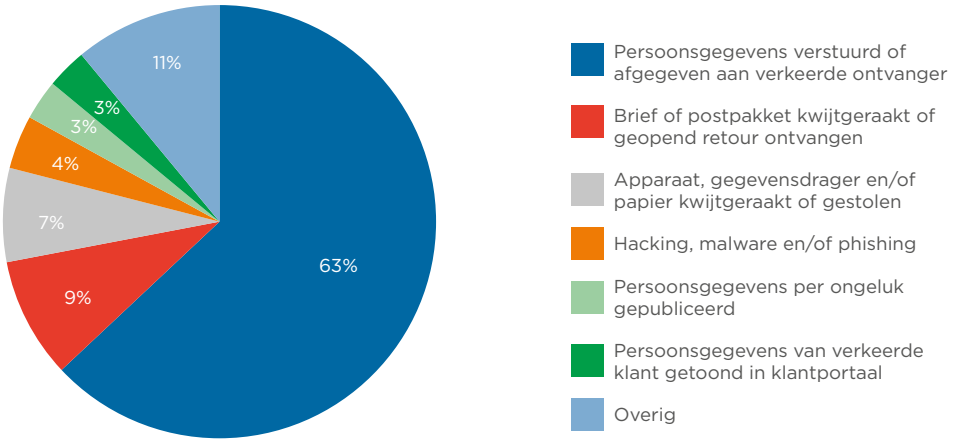
2.4 Digitale weerbaarheid: basismaatregelen en onveilige producten en diensten

- Het Nationaal Cyber Security Centrum (NCSC) waarschuwt dat de digitale weerbaarheid van Nederland onder druk staat. Organisaties zijn kwetsbaar, zelfs voor aanvallen met eenvoudige middelen. Het NCSC meldt dat incidenten voorkomen hadden kunnen worden door het treffen van basismaatregelen, zoals het tijdig implementeren van beveiligingsupdates. Verder leiden toenemende complexiteit en connectiviteit in het ICT-landschap tot kwetsbaarheden. [29]
- Het Nationaal Cyber Security Centrum waarschuwt voor digitaal onveilige producten en diensten. Zij vormen volgens het cybercentrum een fundamentele oorzaak van veel cyberincidenten. Dan gaat het bijvoorbeeld over het niet (langer) beschikbaar stellen door leveranciers van updates en het niet, of niet eenvoudig, kunnen installeren van updates. [30]

- Bij de meeste organisaties is er niet voldoende kennis en kunde om dreigingen effectief af te weren. [31] Een bijkomende risico is dat cybersecurity door medewerkers vooral als verantwoordelijkheid van de afdeling IT wordt gezien, hoewel cyberincidenten regelmatig samenhangen met menselijke fouten, zoals het openen van spammails of het veelvuldig gebruik van dezelfde wachtwoorden. Ook opereert IT nog teveel onafhankelijk en te weinig in verbinding met andere (staf)diensten en gebruikers, waardoor zij elkaar onvoldoende versterken. [32]
- Een zorg onder experts is het onvermogen van instellingen om voldoende gekwalificeerd en specialistisch IT-personeel aan zich te binden. [33] Door de toegenomen complexiteit van het werkveld en de grote vraag in de markt voor dergelijk personeel is er een hevige concurrentiestrijd om goede specialisten te werven en te houden.
- Er is een sterke toename van het gebruik van clouddiensten. [34] Ook bij SURF zien we die toename, getuige het aantal afnemers van clouddiensten zoals SURFcumulus (ca. 100 afnemers) en Microsoft Office 365 via SURFmarket (van ca. 100 eind 2017 naar ruim 200 eind 2018). Hierdoor vormen deze diensten een interessant doelwit voor hackers. [35]
- Het ICT-landschap van organisaties wordt steeds ingewikkelder, onder invloed van groeiende connectiviteit, organische groei en lange levensduur van ICT-systemen. Tel daarbij het toegenomen gebruik van clouddiensten op en duidelijk is dat het moeilijker wordt om overzicht en regie op het ICT-landschap te houden. [36] Het gebrek binnen instellingen aan een goed begrip van eigen ICT-systemen wordt door sommige experts dan ook als een onderschat risico gezien. Het gaat dan over vragen als: waar bevinden zich onze meest precaire data? en hoe is ons netwerk opgebouwd? [37] Volgens Fox-IT is het monitoren van netwerken en endpoints steeds belangrijker, doordat aanvallers gebruik maken van bestaande tools op netwerken en computers. Dat vraagt inzicht in de vraag welke tools en gedragingen afwijkend zijn en welke niet. [38]
- Beveiligingsmaatregelen kosten tijd en geld en de directe opbrengst van dergelijke preventieve maatregelen is niet of lastig aantoonbaar. Dat kan leiden tot belangentegenstellingen tussen bijvoorbeeld meer weerbaarheid en het gebruiksgemak voor individuele gebruikers, of tussen de continuïteit van processen en het uitvoeren van maatregelen en security-updates. Die belangentegenstellingen kunnen een rem vormen op digitale weerbaarheid van instellingen. [39]
- Als een aanval effectief is, is er slechts weinig tijd voor het nemen van preventieve maatregelen. Dat betekent dat vertrouwelijke data binnen enkele seconden of minuten gecompromitteerd kunnen zijn. [40]

2.5 Meldingen dataleken

Op 25 mei 2018 werd de Algemene Verordening Gegevensbescherming van kracht. De AVG verplicht organisaties een datalek te melden bij de Autoriteit Persoonsgegevens (AP). In 2018 werden er bij de Autoriteit in totaal 20.881 meldingen gedaan; een forse stijging ten opzichte van voorgaande jaren. Onderstaande figuur geeft een beeld van het type datalekken.



Figuur 3: Type datalekken [41]

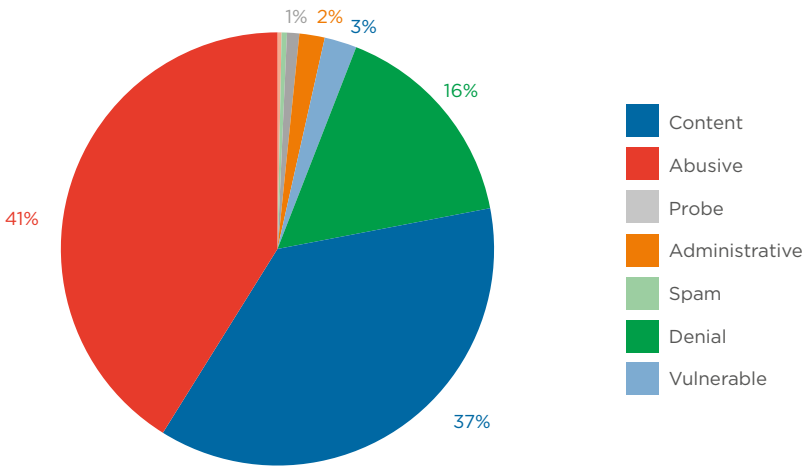
In de meeste gevallen gaat het om het versturen of afgeven van persoonsgegevens aan de verkeerde ontvanger, bijvoorbeeld het versturen van een email met gevoelige persoonsgegevens aan een verkeerde ontvanger. Naam, geslacht en contactgegevens zijn de meest gelekte gegevens. De AP kreeg ruim 6000 meldingen over gelekte medische gegevens en het BSN. Datalekken door hacking en phishing komen met name voor in de zorg. Dan kan het bijvoorbeeld gaan om organisaties die bestookt worden met nep e-mails die afkomstig lijken van een betrouwbare partij zoals een zakelijke relatie. Door het aanklikken van links of het openen van nep-e-mails bestaat het risico dat een virus zoals ransomware wordt geïnstalleerd, waarmee betaling wordt geëist. [42]

2.6 Bij SURF waargenomen trends

SURFcert

SURFcert biedt aangesloten instellingen 24 x 7 ondersteuning bij beveiligingsincidenten. Meldingen die binnenkomen worden geregistreerd en in categorieën ingedeeld. Wanneer SURFcert een melding in behandeling neemt is er sprake van een incident. Sommige meldingen worden automatisch gegenereerd wanneer bepaalde drempelwaardes worden overschreden.

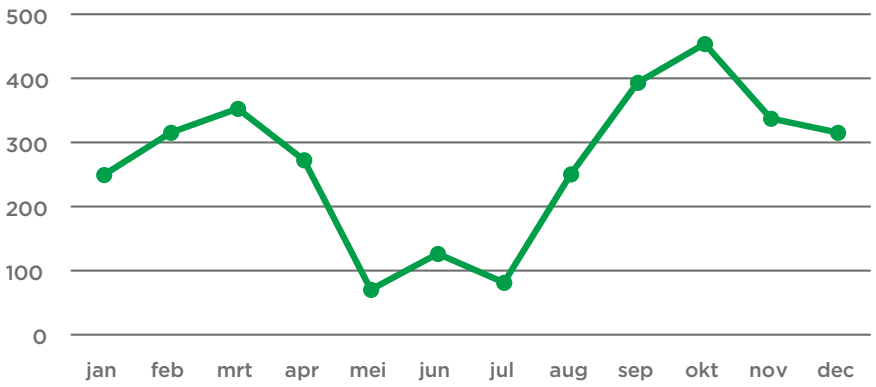
Alle bij SURFcert in behandeling genomen meldingen worden als volgt onderscheiden (zie bijlage 2):



Figuur 4: SURFcert type incidenten

Bijna 80% van de incidenten heeft betrekking op systemen bij instellingen die bij SURFcert bekende kwetsbaarheden bevatten (vulnerable – 37%) en op systemen die contact zoeken met IP-adressen waarvan bekend is dat ze geassocieerd zijn met malware (infected – 41%). De derde grote categorie incidenten (denial – 16%) heeft betrekking op systemen die betrokken zijn bij een DDoS-aanval, meestal als slachtoffer, soms als dader, bijvoorbeeld doordat ze booter[1] services opzoeken.

De volgende grafiek laat zien hoeveel DDoS-meldingen bij SURFcert in 2018 zijn binnengekomen:

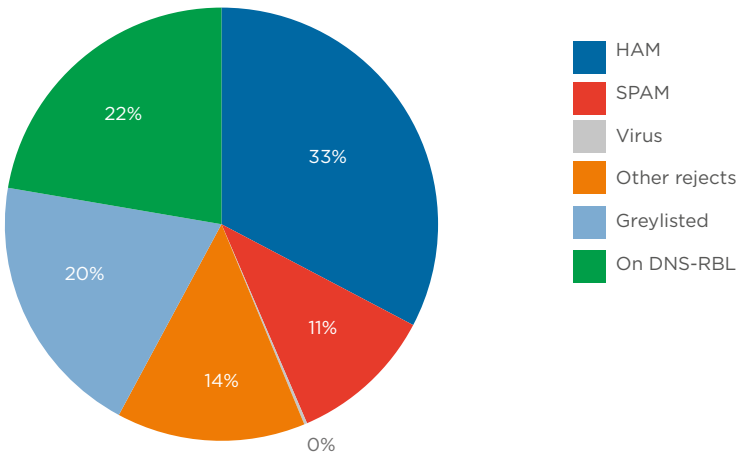


Figuur 5: SURFcert; binnengekomen DDoS-meldingen (per maand)

Bovenstaande figuur illustreert dat er een dip is in de zomermaanden, terwijl van januari tot april meer meldingen binnenkomen, en van augustus tot december veel meer. Over het hele jaar genomen blijft het aantal meldingen van DDoS-aanvallen hoog.

SURFmailfilter

De dienst SURFmailfilter controleert en filtert alle binnenkomende en uitgaande e-mail op virussen, phishing en spam. Minimaal 95% van de spam wordt gedetecteerd. Een vijftigtal bij SURF aangesloten instellingen maakt gebruik van SURFmailfilter.



Figuur 6: SURFmailfilter; categorieën gefilterde e-mail

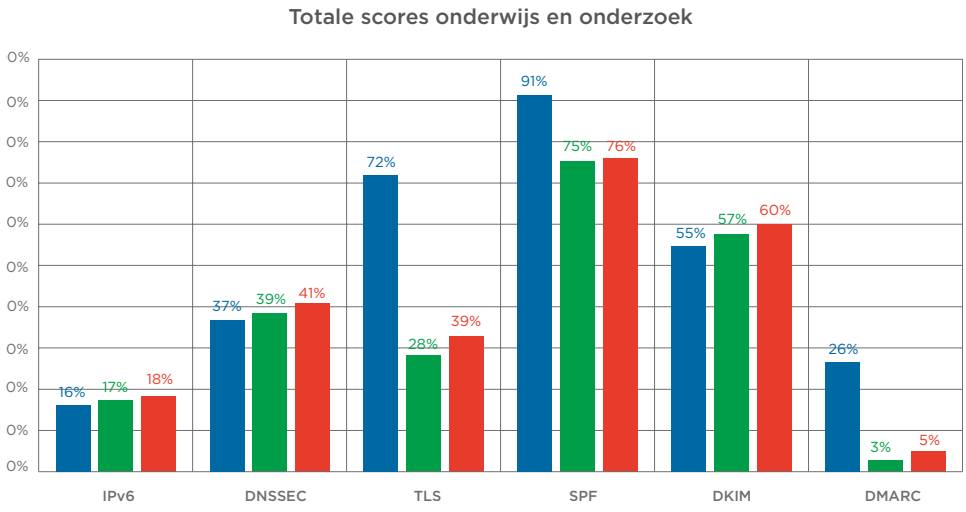
[1] Een booter of stresser service, ook wel DDoS-for-Hire genoemd, biedt denial-of-serviceaanvallen aan. Veel worden als legitieme testtool via het internet aangeboden voor lage kosten (zie bijv. https://www.booter.pw/#pricing).

Meer dan de helft van de mail (56%: On DNS-RBL, Greylisted en Other rejects) wordt tegengehouden. De hoeveelheid mail die SURFmailfilter per dag afhandelt zit normaliter tussen de 2 en 5 miljoen berichten (met in december 2018 een uitschieter naar 20 miljoen berichten op een dag ten gevolge van een spam run).

IV-metingen

Het Forum standaardisatie [43] doet voor de overheid halfjaarlijkse metingen naar een aantal Informatie Veiligheid standaarden, de zogenaamde IV-metingen. De standaarden zijn vastgesteld door het Forum Standaardisatie en staan op de PTOLU (Pas Toe Of Leg Uit) lijst, de lijst van standaarden waaraan de (semi-)overheid zich moet houden bij aanschaf en inrichting van ICT-systemen. SURF participeert in het forum standaardisatie en spin-offs zoals de Veilige E-mail Coalitie (VEC).

In dat kader voert SURF sinds april 2018 ieder kwartaal IV-metingen voor de sector onderwijs en onderzoek uit. In de meting wordt gekeken naar IPv6-adoptie, DNSSEC, TLS (conform richtlijnen NCSC), SPF, DKIM en DMARC (de laatste 3 zijn standaarden voor veilige e-mail). Onderstaande grafiek geeft aan dat er ruimte is voor verbetering, maar dat ook een stijgende lijn* zichtbaar is:



Figuur 7: IV-metingen 2018 (vanaf april 2018)

*Noot: Internet.nl heeft de metingen en de berekening van de score na de Q2-meting aangepast. Hierdoor lijken de resultaten van de TLS-meting en de DMARC-meting achteruitgegaan.

3. CYBERDREIGINGEN ONDERWIJS EN ONDERZOEK

In de survey hebben we een aantal aspecten van informatiebeveiliging uitgevraagd. In dit hoofdstuk gaan we in op de risicoperceptie van instellingen, hoe vaak dreigingen zich daadwerkelijk hebben voorgedaan, in hoeverre er verandering is ten opzichte van 2017 en hoeveel aandacht voor een aantal ontwikkelingen bestaat.

3.1 Percepties van dreigingen

In de survey hebben we gevraagd naar de kans dat een dreiging zich manifesteert en naar de impact van een dreiging als die zich zou manifesteren, beide op een schaal van 1 – 5. Verder is onderscheid gemaakt tussen de drie kolommen onderwijs, onderzoek en bedrijfsvoering. In Tabel 5: Risicoperceptie 2018 is de risicoperceptie bepaald door de waardes voor kans en impact met elkaar te vermenigvuldigen. Om onderscheid te maken tussen Hoog, Middelhoog en Laag risico is de volgende risicomatrix vastgesteld na discussie in de klankbordgroep:

Impact:	1	2	3	4	5
K1	1	2	3	4	5
K2	2	4	6	8	10
K3	3	6	9	12	15
K4	4	8	12	16	20
K5	5	10	15	20	25

< 5 = Laag **5-10** = Middelhoog **> 10** = Hoog

Tabel 4: Risicomatrix

Risicoperceptie 2018: Kans * impact	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	9,6	11,6	8,4
2. Identiteitsfraude	10	8,1	9,2
3. Verstoring van ICT-voorzieningen	12,2	9,5	10
4. Manipulatie van digitaal opgeslagen data	8,2	9,7	8,4
5. Spionage	2,8	8,7	3,1
6. Overname en misbruik van ICT-voorzieningen	10	9,1	9,9
7. Bewust beschadigen van imago	10,3	9,9	7,2

Tabel 5: Risicoperceptie 2018

Voor onderwijs zijn de **top 3 risico's** (op basis van de numerieke score):

1. verstoring van ICT-voorzieningen (hoog)
2. bewust beschadigen imago (hoog)
3. identiteitsfraude/overname en misbruik van ICT-voorzieningen (middelhoog)

Het risico dat het laagst scoort (en beduidend lager dan de andere dreigingen in de sector onderwijs) is spionage.

Voor onderzoek zijn de **top 3 risico's** (op basis van de numerieke score):

1. verkrijging en openbaarmaking data (hoog)
2. beschadigen imago (middelhoog)
3. manipulatie van digitaal opgeslagen data (middelhoog)

Waar spionage als risico laag scoort voor de sectoren onderwijs en bedrijfsvoering, is dit niet het geval voor de sector onderzoek. Spionage wordt in deze sector als middelhoog risico beoordeeld. De dreigingen liggen allemaal dicht tegen de hoogste risicocategorie.

Voor bedrijfsvoering zijn de **top 3 risico's** (op basis van de numerieke score):

1. verstoring ICT-voorzieningen (middelhoog)
2. overname en misbruik ICT-voorzieningen (middelhoog)
3. identiteitsfraude (middelhoog)

Het risico dat het laagst scoort (en beduidend lager dan de andere dreigingen in de sector bedrijfsvoering) is spionage.

Risicoperceptie verschillende sectoren

Kijken we naar de risicoperceptie van verschillende sectoren, dan valt op dat mbo-instellingen de onderzochte dreigingen over de gehele linie lager inschatten dan hogescholen en universiteiten. Dat kan verband houden met de inschatting van de eigen cyberweerbaarheid, maar ook met het idee dat mbo-instellingen geen gewild doelwit van cyberactoren zijn. Nadere duiding is hier wenselijk. De sector onderzoek (hogescholen en universiteiten) komt over de volle breedte van de dreigingen tot een hogere inschatting van de risico's.

Risicoperceptie ten opzichte van eerdere jaren

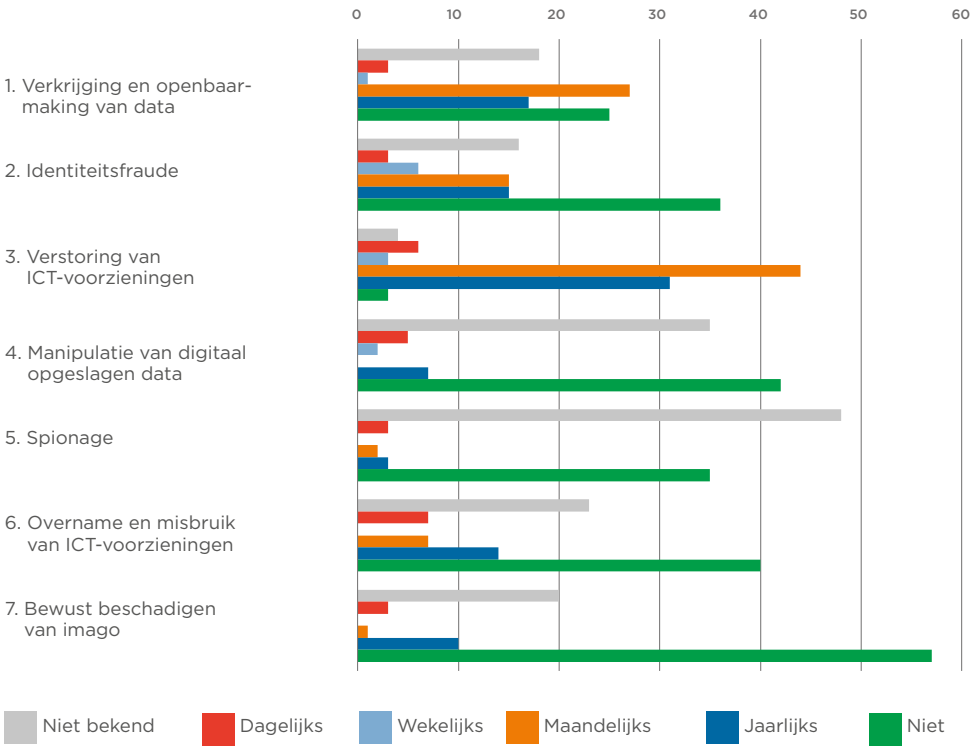
De risicoperceptie van de dreigingen is in 2018 duidelijk hoger dan in voorgaande jaren. Opvallend is dat in voorgaande edities de dreiging van imagoschade voor alle sectoren laag scoorde. De invoering van de AVG, met de kans op boetes bij niet naleven, heeft bij instellingen in 2018 mogelijk tot een hogere perceptie van de risico's geleid.

Risicoperceptie 2017	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	M	H	H
2. Identiteitsfraude	H	M	L
3. Verstoring van ICT-voorzieningen	M	M	M
4. Manipulatie van digitaal opgeslagen data	H	L	L
5. Spionage	L	H	L
6. Overname en misbruik van ICT-voorzieningen	L	M	M
7. Bewust beschadigen van imago	L	L	L

Tabel 7: Risicoperceptie 2017

3.2 Daadwerkelijk voorkomen van dreigingen

In deze paragraaf geven we een beeld van het daadwerkelijke voorkomen van dreigingen: de frequentie waarmee zich incidenten hebben voorgedaan in de afgelopen 12 maanden.



Figuur 8: Incidenten per dreiging (som van onderwijs, onderzoek en bedrijfsvoering)

Wat opvalt in Figuur 8 is het grote aantal respondenten dat aangeeft dat een aantal dreigingen zich niet heeft gemanifesteerd, waaronder beschadigen van imago, manipulatie van digitaal opgeslagen data en overname en misbruik ICT-voorzieningen. Kennelijk zijn deze risico's goed afgedekt. Dreigingen als verstoring van ICT-voorzieningen en verkrijging en openbaarmaking van data doen zich maandelijks voor. Er bestaan dan ook goede mechanismen om ze te melden, bijvoorbeeld incident-registratiesystemen zijn wijdverbreid en iedere instelling heeft procedures om datalekken te kunnen melden.

Verder valt op dat een behoorlijk hoog aantal respondenten aangeeft niet te weten hoe vaak incidenten zich voordoen. Dat geldt met name voor spionage en manipulatie van digitaal opgeslagen data. Het beperkte zicht op incidenten sluit aan bij de resultaten van de SURFaudit-benchmark 2017 [44], waaruit bleek dat 'controle en logging' veel lager scoort dan het door SCIPR aanbevolen ambitieniveau.

Hierbij past de kanttekening dat het detecteren van dreigingen zoals spionage of manipulatie van data ingewikkeld kan zijn (en wellicht alleen aan het licht komt bij een heterdaad of gerichte controle van databestanden). Dit in tegenstelling tot verstoring van ICT-voorzieningen die eerder gevolgen zal hebben in de fysieke realiteit: het disfunctioneren van e-mailverkeer en websites en beperkte bereikbaarheid van systemen. De kans op detectie is groter.

Nieuwsitem: spionage

Nederlandse universiteiten slachtoffer Iraanse hackers

In maart wordt bekend dat de Verenigde Staten negen Iraanse hackers hebben aangeklaagd voor digitale spionage op universiteiten. Ook Nederlandse universiteiten zouden slachtoffer zijn geworden (welke universiteiten is niet bekend). De hackers hebben volgens de Verenigde Staten in totaal voor 31 terabyte aan documenten en data gestolen: het betreft voornamelijk wetenschappelijke documenten en ander intellectueel eigendom. [45]

Nieuwsitem: menselijk handelen

Datalek Saxion Hogeschool

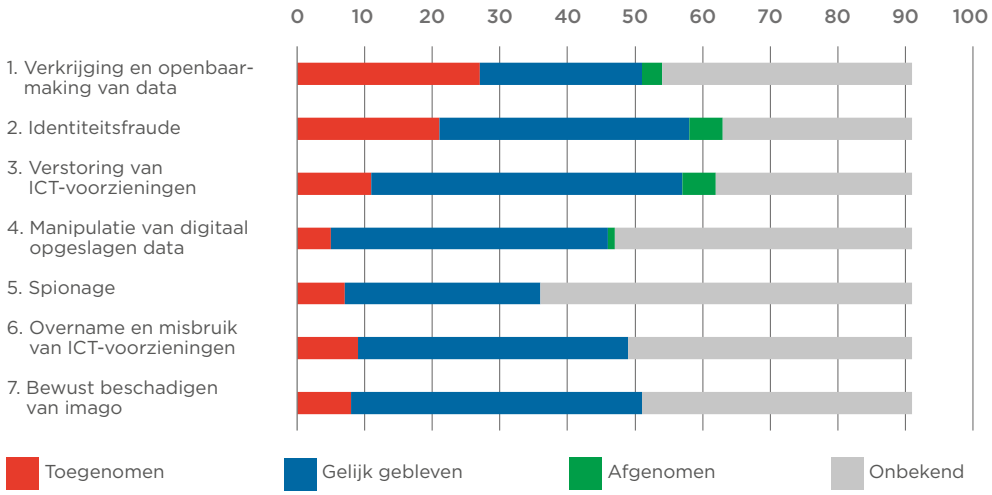
In mei zijn de gegevens van 5100 studenten van Saxion Hogeschool zeker 24 uur openbaar geweest. Het gaat om de naam, adres, woonplaats en mailadres van de studenten, plus de boeken die ze hadden besteld. Tijdens mailcontact is per ongeluk een tabblad met de persoonsgegevens van de studenten meegestuurd, waarna deze gegevens openbaar zijn gemaakt. [46]

3.3 Veranderingen van cyberdreigingen ten opzichte van 2017

Hieronder staan de resultaten op de vraag of cyberdreigingen in vergelijking met 2017 zijn **toegenomen**, **afgenomen**, **gelijk gebleven** of dat dit **niet bekend** is. Hierbij valt op dat

- de dreiging van verkrijging en openbaarmaking van data én
- identiteitsfraude het sterkst zijn toegenomen
- en dat manipulatie van opgeslagen data
- en spionage het minst sterk zijn toegenomen.

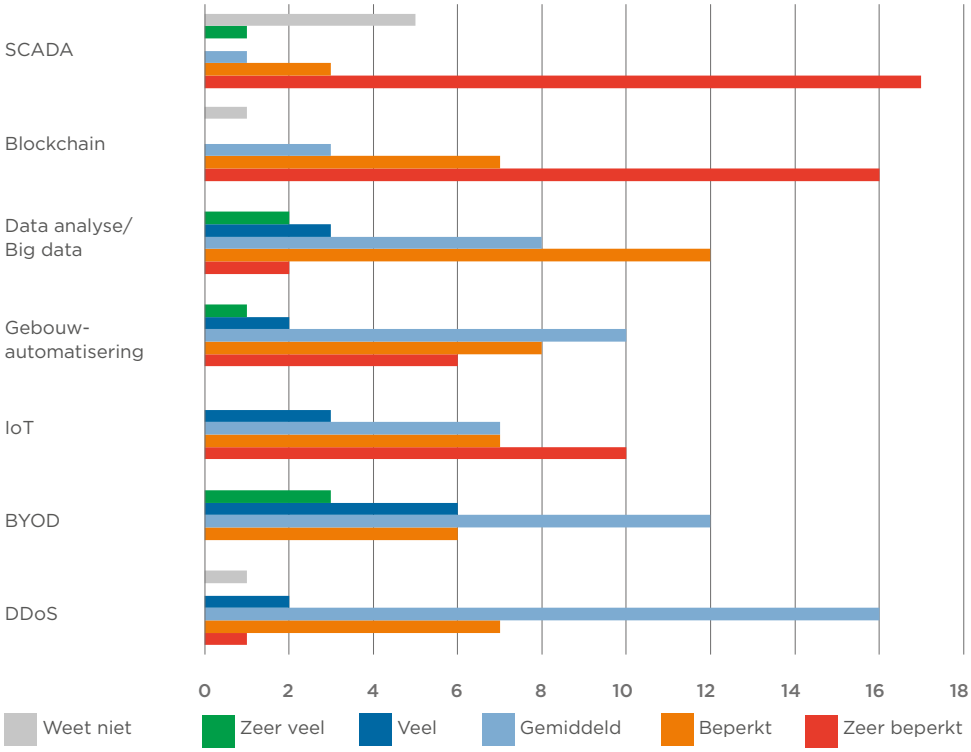
Verder valt op dat de ontwikkeling van cyberdreigingen veelal niet duidelijk of bekend is voor de instellingen.



Figuur 9: Veranderingen van cyberdreigingen ten opzichte van 2017

3.4 Aandacht voor actuele trends

Bij instellingen is er ook aandacht voor actuele trends op het gebied van ICT, omdat die op termijn gevolgen kunnen hebben voor informatiebeveiliging. In de survey geven de deelnemers aan met name aandacht te hebben voor DDoS-aanvallen, Bring Your Own Device (BYOD) en internet of things (IoT). Beperkte aandacht is er voor ontwikkelingen als Supervisory Control and Data Acquisition (SCADA)[2] en Blockchain.[3]



Figuur 10: Aandacht voor ontwikkelingend.

Nieuwsitem: menselijk handelen

Mailbom Avans Hogeschool

Een student van de Avans Hogeschool stuurt een mail met een enquête per ongeluk aan een grote groep, waardoor een mailbom ontstaat: veel mensen reageren op elkaar waardoor al die mails bij alle duizenden ontvangers terecht komen. De mailadressen zijn voor alle deelnemers zichtbaar. [47]

Nieuwsitem: menselijk handelen

Persoonsgegevens per abuis verspreid op Universiteit Twente

In mei wordt een kieslijst abusievelijk toegevoegd aan een e-mail aan alle studenten van de faculteit ITC. In het document staan persoonlijke en vertrouwelijke gegevens. Het incident is direct gemeld bij de Autoriteit Persoonsgegevens. [48]

[2] SCADA is het verzamelen, verwerken en visualiseren van meet- en regelsystemen van machines in grote industriële systemen.
[3] Blockchain is een systeem dat gebruikt kan worden om gegevens zoals overschrijvingen en eigendomsaktes vast te leggen.

4. CYBERWEERBAARHEID

In dit hoofdstuk gaan we in op de organisatie van informatiebeveiliging en hoeveel aandacht ervoor is in de organisatie.

4.1 Governance: bestuurlijke aandacht voor informatiebeveiliging

Een meerderheid van de respondenten geeft aan dat informatiebeveiliging op de agenda van het college van bestuur staat en expliciet als bestuurlijke portefeuille is belegd. Dat sluit aan bij de resultaten van de SURFaudit-benchmark 2017 aangaande het cluster 'organisatie en beleid'. Voor het hebben van door de directie goedgekeurd beleid scoren instellingen in het algemeen goed. Wel scoren ze minder op het regelmatig (her)beoordelen van informatiebeveiligingsbeleid op doeltreffendheid en adequaatheid. [49] Dat is belangrijk gelet op de dynamiek en veranderingen die zich voordoen in dreigingen en de omgeving waarbinnen instellingen opereren.

Informatiebeveiliging op agenda college van bestuur

Ja	20
Nee	5
Onbekend	2

Informatiebeveiliging als portefeuille college van bestuur

Ja	15
Nee	9
Onbekend	3

Bij ongeveer de helft van de instellingen is cybersecurity ook een onderwerp op de agenda van de raad van toezicht, hoewel een vergelijkbaar aantal respondenten eveneens aangeeft niet te weten of dit het geval is.

Informatiebeveiliging op agenda raad van toezicht

Ja	12
Nee	2
Onbekend	13

4.2 Organisatie van informatiebeveiliging

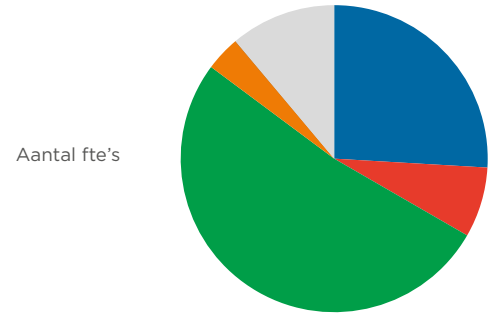
Capaciteit

Hieronder staan de resultaten op de vraag over hoeveel capaciteit de eigen instelling beschikt voor informatiebeveiliging in fte's. Geen instelling beschikt over meer dan 10 fte voor informatiebeveiliging; één instelling beschikt over 5-10 fte, gevolgd door 14 instellingen met 2-5 fte. Hoewel de benodigde capaciteit afhangt van diverse variabelen (omvang, complexiteit, belangen) valt op dat zeven instellingen aangeven over minder dan 1 fte te beschikken voor informatiebeveiliging.

Uit de feedback van de klankbordgroep komt naar voren dat de awareness en kennis op tactisch en operationeel niveau binnen de instellingen als zorg wordt gezien. Daarin wordt de organisatorische inrichting van de instelling als belemmerende factor ervaren voor het uitvoeren van informatiebeveiligingsbeleid.

Beschikbare capaciteit voor informatiebeveiliging (in fte's):

< fte	7
1 fte	2
2 – 5 fte	14
5 – 10 fte	1
> 10 fte	0
Onbekend	3



Figuur 11: Aantal fte's voor informatiebeveiliging

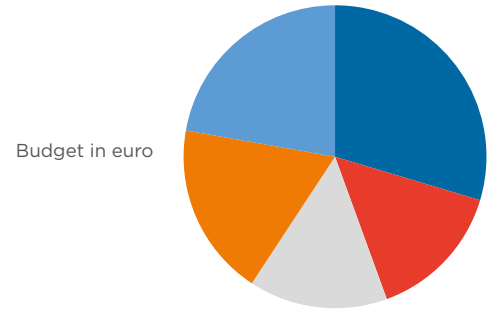
Noot: De hier gemelde lage investering in de cybercrisisoefening OZON lijkt niet in overeenstemming met de feitelijke deelname aan OZON, waarbij 40 van de 50 deelnemende instellingen op niveau zilver/goud hebben ingeschreven wat een significante investering in tijd en mensen heeft gevergd.

Budget

Hieronder staan de resultaten op de vraag over het beschikbare budget binnen de eigen instelling voor informatiebeveiliging:

- vijf instellingen geven op jaarbasis méér dan 200.000 euro uit aan informatiebeveiliging.
- bij acht instellingen is er op jaarbasis minder dan 50.000 euro beschikbaar voor informatiebeveiliging.
- voor zes deelnemers is het onbekend welk budget er beschikbaar is.

< €50k per jaar	8
€50k - €100k per jaar	4
€100k - €200k per jaar	4
> €200k per jaar	5
Onbekend	6



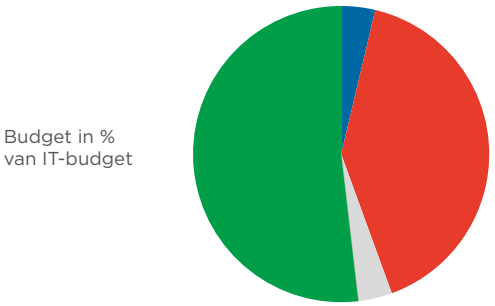
Figuur 12: Beschikbaar budget voor informatiebeveiliging

Het budget voor informatiebeveiliging (als onderdeel van het totale ICT-budget) van de instellingen ligt voor elf instellingen tussen 1 tot 5%. Voor veertien deelnemers is het onbekend welk budget er verhoudingsgewijs beschikbaar is voor informatiebeveiliging.

Deze bedragen liggen ruim onder de zogenaamde '10-procentmaatstaf' waar de Cyber Security Raad in het rapport Nederland droge voeten voor pleit. Uit een landenanalyse blijkt dat gemiddeld 10 procent van het IT-budget besteed wordt aan cybersecurity en privacy maatregelen. De commissie adviseert deze maatstaf als richtlijn over te nemen voor overheden en andere publieke instellingen. [50]

Beschikbaar budget voor informatiebeveiliging (als percentage van het totale ICT-budget):

< 1 %	1
1 - 5%	11
5 - 10%	1
10 - 20%	0
> 20%	0
Onbekend	14



Figuur 13: Investering in informatiebeveiliging

Corporate (Information) Security Officer

6 instellingen geven aan niet over een CISO (of CSO) te beschikken. Als reden wordt de omvang van de eigen organisatie genoemd. Op de vraag of de CISO (of CSO) over voldoende mandaat en capaciteit beschikt om onafhankelijk te controleren en adviseren, zijn de meningen verdeeld:

Voldoende capaciteit en mandaat CISO/CSO?

Eens	10
Oneens	11
Geen CISO	6

Waar is informatiebeveiliging belegd?

Vijftien instellingen geven aan dat informatiebeveiliging niet alleen de taak is van de afdeling of medewerker IT. Elf instellingen geven echter aan dat dit wel het geval is: informatiebeveiliging is binnen die instellingen primair de taak van IT. Dit onderschrijft het trendbeeld in hoofdstuk 2, waarin deskundigen erop wijzen dat informatiebeveiliging door medewerkers als een 'IT-feestje' wordt gezien. Maar ze wijzen er ook op dat IT nog erg onafhankelijk en te weinig in verbinding met andere diensten opereert. [51]

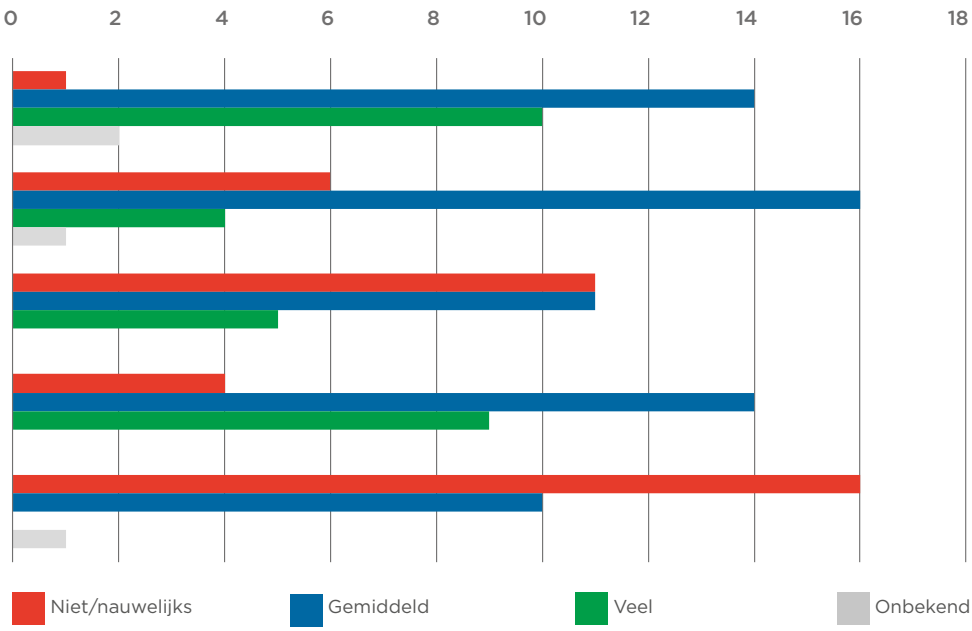
Informatiebeveiliging primair taak van IT:

Ja	11
Nee	15
Onbekend	1

4.3 Cyberweerbaarheid

Investeringen in cyberweerbaarheid

Instellingen investeren met name in firewalls en in awareness van eigen medewerkers. Maar ook in het versterken van de awareness van medewerkers, wat gunstig is gezien de lage score daarop van instellingen in de recente SURFaudit-benchmark [52]. Kennelijk hebben de instellingen meer aandacht voor bijscholing van hun medewerkers over beleidsregels en procedures, en instructies voor contractanten. Daarentegen worden vrijwel geen investeringen gedaan in de awareness van externen, deelname aan de landelijke cybercrisisoefening OZON* en het zogeheten 'Computer Emergency Respons Team' (CERT).



Figuur 14: Investering in cyberweerbaarheid

*Noot: De hier gemelde lage investering in de cybercrisisoefening OZON lijkt niet in overeenstemming met de feitelijke deelname aan OZON, waarbij 40 van de 50 deelnemende instellingen op niveau zilver/goud hebben ingeschreven wat een significante investering in tijd en mensen heeft gevergd.

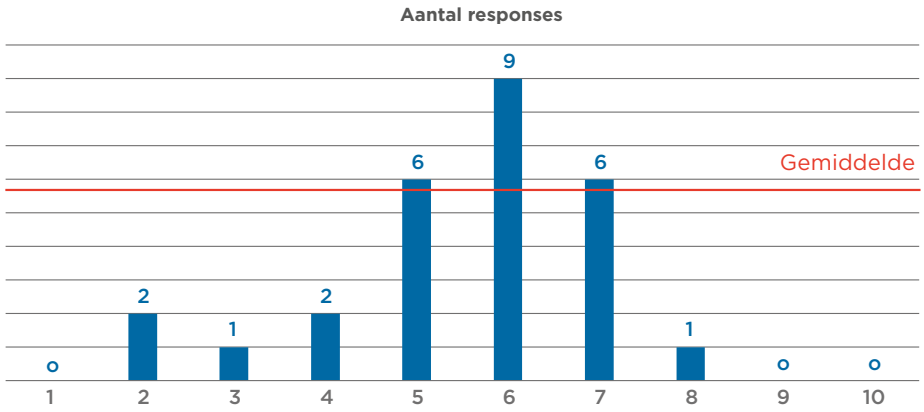
Verder geven instellingen aan te investeren in:

- controles of het beleid dat vastgesteld is ook wordt uitgevoerd (SURFaudit),
- het uitvoeren van Pentesten, die geven inzicht geven in de status waar een IT-organisatie zich bevindt,
- zonering en centrale logging/monitoring,
- nieuwe CISO,
- governance,
- ondersteuning in middelen van een programma om weerbaarheid te verhogen en awareness te verbeteren.

Beoordeling eigen cyberweerbaarheid

Respondenten beoordelen de cyberweerbaarheid van de eigen organisatie gemiddeld met een krappe voldoende (score 5,5 op een schaal van 0-10). Dat is conform de uitkomsten uit de benchmark, waarin instellingen in 2017 voor alle clusters onder het streefniveau uitkomen. [53] Afgaande op deze uitkomsten is er binnen instellingen ruimte voor verdere verbetering van informatiebeveiliging.

Eén instelling beoordeelt de eigen weerbaarheid met een cijfer 8, zes instellingen geven zichzelf een score 7 en negen instellingen een score 6:



Figuur 15: Aantal responses per weerbaarheidsniveau (survey)

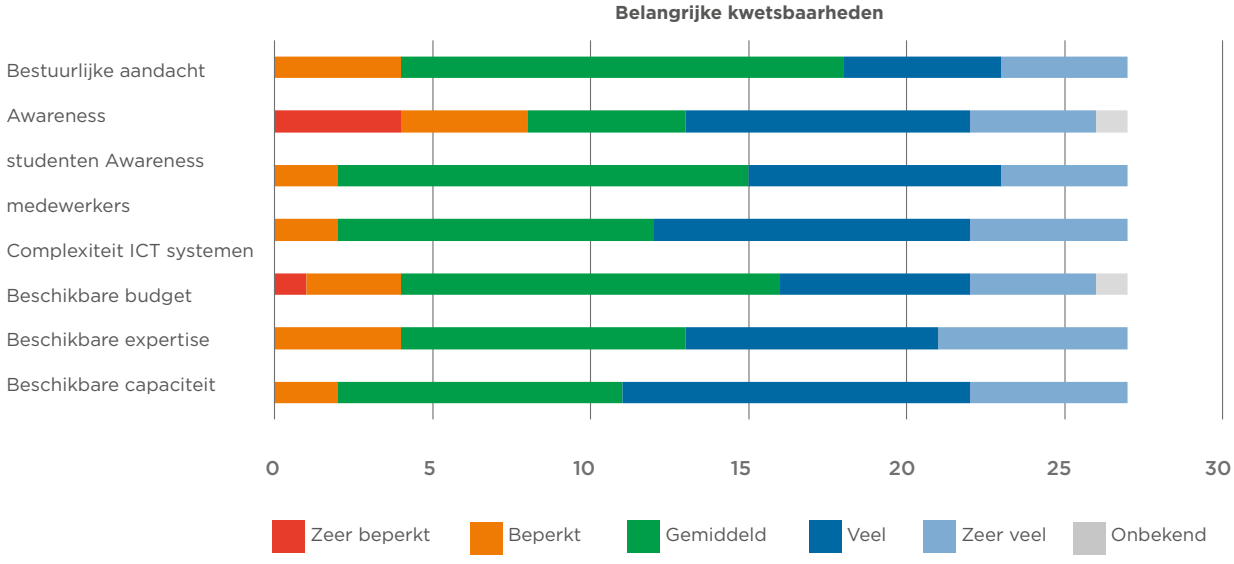
Opvallend is verder dat de mbo-instellingen die deze vraag hebben beantwoord, hun weerbaarheid relatief hoog inschatten (7). Dat houdt mogelijk verband met hun risico-perceptie: de mbo-instellingen schatten de risico's voor hun eigen instelling laag in.

Kwetsbaarheden

Als belangrijke kwetsbaarheden noemen de respondenten onder meer de beschikbare capaciteit en expertise, de complexiteit van ICT-systemen en de awareness van studenten. Het gaat dan onder andere over:

- benodigde specialistische kennis en opleiding van personeel,
- de inhuur daarvan,
- eigenaarschap van informatie en gebruikersspelregels (autorisatie) en
- bewustwording door de invoering van de AVG.

Dit sluit aan bij het trendbeeld uit hoofdstuk 2, waarin de zorg werd gedeeld dat het veel organisaties ontbreekt aan voldoende kennis en kunde om dreigingen effectief af te weren. [54]



Figuur 16: Relevantie van kwetsbaarheden

Nieuwsitem: phishing mails

Phishing mails op Universiteit Groningen

Op nieuwjaarsdag ontvangen medewerkers en studenten van de Universiteit Groningen een mail met als onderwerp 'VEILIGHEIDSINFORMATIE!!' De mail lijkt afkomstig van de ICT-afdeling en bevat een link naar een website waar ter verificatie de gebruikersnaam en het wachtwoord van het universiteitsaccount moeten worden ingevuld. [55]

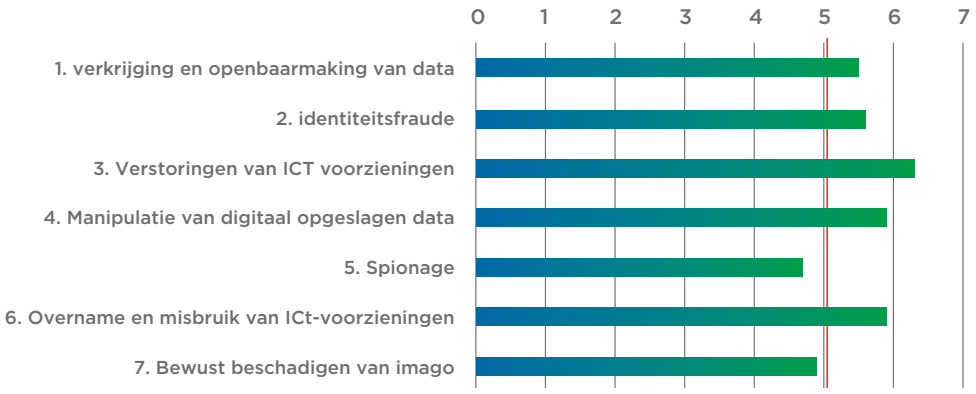
Phishing mails op Universiteit Twente

Maandag 19 maart komen er bij de Universiteit Twente meldingen binnen van phishing mails gericht aan medewerkers van de universiteit. Het onderwerp van de mail is 'Migreer,' wat de phishing extra verleidijk maakt gezien de universiteit op dat moment bezig is met de migratie van de Exchange/outlook omgeving. [56]

Dreigingen die onder controle zijn

De dreigingen die volgens respondenten het best onder controle zijn, zijn:

- verstoring van ICT-voorzieningen (score 6,3)
- overname en misbruik van ICT-voorzieningen (score 5,9)
- manipulatie van digitaal opgeslagen data (score 5,9)



Figuur 17: Mate waarin dreigingen onder controle zijn (op een schaal van 1 – 10)

Spionage en het bewust beschadigen van imago worden door de instellingen gezien als dreigingen die het minst onder controle zijn. Zij scoren lager dan 5 op een schaal van 10.

5. HIGHLIGHTS EN REFLECTIE VOOR DE BESTUURDER

In dit afsluitende hoofdstuk belichten we enkele highlights uit het cyberdreigingsbeeld (voortkomend uit hoofdstukken 2 t/m 4). Doel is het informeren van bestuurders over actuele cybertrends en risico's. Tot slot geven we vijf punten voor reflectie die bestuurders kunnen gebruiken voor de dialoog over cyberrisico's en –weerbaarheid in hun eigen instelling.

5.1 Bestuurlijke highlights

1. **De risicoperceptie van cyberdreigingen in 2018 is duidelijk hoger dan in voorgaande jaren.** Opvallend is dat in voorgaande edities de dreiging van imagoschade voor alle sectoren laag scoorde. De invoering van de AVG, met de kans op boetes bij niet naleving, leidt bij instellingen in 2018 mogelijk tot hogere perceptie van het risico.

2. **De top 3 cyberdreigingen verschilt per sector.** Voor onderwijs en bedrijfsvoering is de verstoring van ICT-voorzieningen de belangrijkste dreiging. Die dreiging heeft vrij direct effect op de continuïteit van het primaire (onderwijs)proces, een kroonjuweel. Voor de sector onderzoek is de verkrijging en openbaarmaking van data de belangrijkste dreiging. Ook die dreiging raakt direct aan een kroonjuweel van instellingen, namelijk het intellectueel eigendom/integriteit van onderzoeks- en persoonsgegevens. Ook het beschadigen van imago wordt als een belangrijke dreiging gezien.

Risicoperceptie 2018: Kans * impact	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	M	H	M
2. Identiteitsfraude	M	M	M
3. Verstoring van ICT-voorzieningen	H	M	M
4. Manipulatie van digitaal opgeslagen data	M	M	M
5. Spionage	L	M	L
6. Overname en misbruik van ICT-voorzieningen	M	M	M
7. Bewust beschadigen van imago	H	M	M

Tabel 7: Risicoperceptie 2018

3. **Verstoring van ICT-voorzieningen, overname en misbruik van ICT-voorzieningen, en de manipulatie van digitaal opgeslagen data zijn dreigingen die het best onder controle zijn.** Spionage en het bewust beschadigen van imago worden door de instellingen gezien als dreigingen die het minst onder controle zijn.

4. **Naast criminelen en staten kunnen hacktivisten, cybervandalen en insiders zorgen voor verstoring van bedrijfsprocessen en diefstal van informatie.** Hoewel de complexiteit van aanvallen groeit, profiteren cybercriminelen van beproefde en bewezen aanvalstechnieken, zoals gijzelingssoftware, DDoS en hacking.

5. **De informatiepositie over cyberincidenten is zeer beperkt.** Wat opvalt is de beperkte informatiepositie van instellingen over cyberincidenten. Een aanzienlijk deel van de instellingen heeft geen zicht op het aantal incidenten dat plaatsvindt. Dat is zorgelijk. Het kan zijn dat de betreffende respondent hier geen zicht op heeft, maar het kan evengoed zijn dat incidenten niet worden geregistreerd of, zorgelijker, niet worden opgemerkt. Dat maakt ICT-voorzieningen en data van instellingen kwetsbaar. Een betere informatiepositie kan instellingen bovendien helpen risico gestuurde maatregelen te treffen.

6. **Er zijn zorgen over het op orde zijn van basismaatregelen en over digitaal onveilige producten en diensten.** De eerder geuite zorgen over de digitale weerbaarheid van organisaties [57] zijn nog steeds actueel. Het Nationaal Cyber Security Centrum wijst ook dit jaar op de kwetsbaarheid van instellingen en roept op tot het treffen van basismaatregelen, zoals het tijdig implementeren van beveiligingsupdates. Dat is nodig, gelet op toenemende complexiteit en onderlinge verbondenheid van ICT-voorzieningen.

7. **Overzicht én regie op eigen ICT-landschap zijn voor organisaties steeds lastiger.** Door toenemende connectiviteit, organische groei van ICT-systemen en het groeiend gebruik van clouddiensten is het hebben en behouden van overzicht en regie ICT-systemen en voorzieningen steeds ingewikkelder.

8. **Instellingen beoordelen eigen cyberweerbaarheid gemiddeld met een onvoldoende.** Deelnemers beoordelen de digitale weerbaarheid van de eigen instelling gemiddeld met een 5,5 (op een schaal van 0-10). Dat is conform de uitkomsten uit de SURFaudit-benchmark, waarin instellingen in 2017 voor alle clusters onder het streefniveau uitkomen. Als belangrijke kwetsbaarheden noemen de instellingen onder meer de beschikbare capaciteit en expertise, de complexiteit van ICT-systemen en de *awareness* van studenten en medewerkers. Het budget voor informatiebeveiliging als onderdeel van het totale ICT-budget, ligt ruim onder de zogenaamde ‘10 procent maatstaf’ van de commissie Verhagen [58].

5.2 Punten voor reflectie

Cybersecurity vergt een gemeenschappelijke inspanning van ICT-specialisten, juristen en privacymedewerkers. Reguliere medewerkers, docenten en studenten kunnen bijdragen door het zich eigen maken van best practices en instructies rond autorisatie, privacy, wachtwoordbeheer en software-updates. Maar gelet op de mogelijke impact van cyberrisico's op instellingen[4] is bestuurlijke betrokkenheid een must. Ten behoeve van de bestuurlijke dialoog over cybersecurity hebben we, gevoed door de resultaten van dit Cyberdreigingsbeeld, vijf vragen opgenomen voor de bestuurstafel.

Deze vragen kunnen bestuurders gebruiken om (in samenspraak met hun Corporate (Information) Security Officer, diensten en faculteitsdirecteuren, Raad van Toezicht) het gesprek te voeren over cyberrisico's en –weerbaarheid van hun eigen instelling.

Thema	Toelichting	Bestuurlijke reflectie
Cyberrisicoprofiel	De impact van cyberdreigingen is afhankelijk van het risico-profiel van instellingen.	Hoe ziet uw cyberrisicoprofiel eruit?
Ambities	Instellingen kunnen zich op verschillende manieren voor-bereiden op cyberdreigingen. Hiervoor zijn richtlijnen en een ambitieniveau beschikbaar via SCIPR/SURFaudit.	Wat is uw ambitieniveau op het gebied van digitale weerbaarheid?
Informatiepositie	Er is beperkt zicht op aantallen en impact van cyberincidenten bij onderwijsinstellingen.	Hoe is uw informatiepositie over cyberincidenten?
Cybersecuritybeleid	Naast informatiebeveiliging loont investeren in detectie en incidentrespons. Dit uitgaande van het gegeven dat 100% voorkomen van cyberinciden-ten weinig realistisch is.	Hoe ziet het cybersecurity-beleid van uw instelling eruit en hoe is de balans tussen preventie en incidentrespons?
Evaluatie	Dynamiek in cyberdreigingen vraagt om tussentijdse evaluatie en herbeoordeling.	Hoe houdt u zicht op cyberdreigingen?

Tabel 8: Reflectievragen

4 Het COT evalueerde samen met de Erasmus Universiteit Rotterdam de afwikkeling van een datalek in 2016. Eén van de bevindingen betrof het bestuurlijke karakter van dergelijke incidenten. [59]

BIJLAGE 1
CYBERDREIGINGEN

De zeven dreigingen en mogelijke manifestaties die in eerdere edities van het Cyberdreigingsbeeld zijn gedefinieerd:

	Type dreiging	Manifestatie van dreiging
#	Type dreiging	Gebeurtenis
1	Verkrijging en openbaar-making 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
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
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 e-learning of het netwerk)
4	Manipulatie van digitaal opgeslagen data	→ Studieresultaten worden vervalst
		→ Manipulatie van onderzoeksgegevens
		→ Aanpassing van bedrijfsvoering data
5	Spionage	→ Onderzoeksgegevens worden afgetapt
		→ Via een derde partij wordt intellectueel eigendom gestolen
		→ Controleren van buitenlandse studenten door staten
6	Overname en misbruik ICT	→ Opstelling van onderzoeksinstellingen overgenomen
		→ Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)
7	Bewust beschadigen imago	→ Website wordt beklad
		→ Socialmedia-account wordt gehackt

Tabel 9: Dreigingen voor onderwijs en onderzoek

BIJLAGE 2
SURFCERT TYPE INCIDENTEN

#	Categorieën	Toelichting
1	content	verkeer dat wordt gefilterd vanwege illegale content, zoals illegale downloads
2	abusive	instellingsverkeer dat overlast veroorzaakt
3	probe	verkeer van een instelling om informatie te verzamelen
4	administrative	niet technische kwesties, hieronder vallen bijvoorbeeld opsporingsverzoeken
6	spam	spamverkeer
7	denial	meldingen over systemen die betrokken zijn bij een DDoS-aanval
8	vulnerable	meldingen over systemen bij instellingen waarop bij SURFcert bekende kwetsbaarheden zijn gevonden
9	infected	systemen die contact zoeken met IP adressen waarvan bekend is dat ze geassocieerd zijn met malware

BIBLIOGRAFIE

[1] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/over-ons/. [Geopend 01 2019].

[2] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/wp-content/uploads/COT-Dreigingsbeeld-Onderwijs-2018.pdf. [Geopend 01 2019].

[3] Integraal Veilig Hoger Onderwijs, [Online]. Available: https://integraalveilig-ho.nl/). [Geopend 01 2019].

[4] B. Bosma, „SURF Cyberdreigingsbeeld 2017," [Online]. Available: https://www.surf.nl/kennisbank/2017/cyberdreigingsbeeld-2017-publicatie.html. [Geopend 01 2019].

[5] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[6] ENISA, „Threat Landscape 2017," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. [Geopend 01 2019].

[7] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[8] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[9] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].

[10] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[11] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[12] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[13] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[14] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].

[15] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[16] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[17] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].

[18] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[19] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].

[20] Europol, „Internet Organised Crime Threat Assessment 2018," [Online]. Available: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018. [Geopend 01 2019].
[21] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].
[22] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].
[23] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecurity beeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[24] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].
[25] Crowd Research Partners, „Insider Threat Report 2018," [Online]. Available: https://crowdresearchpartners.com/portfolio/insider-threat-report/. [Geopend 01 2019].
[26] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[27] Computable, „Fox-IT waarschuwt voor ransomware SamSam," [Online]. Available: https://www.computable.nl/artikel/nieuws/security/6524994/250449/fox-it-waarschuwt-voor-ransomware-samsam.html. [Geopend 01 2019].
[28] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[29] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[30] ENISA, „Threat Landscape 2017," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. [Geopend 01 2019].
[31] Verdict Encrypt, „What Cybersecurity Risks Are Companies Currently Underestimating the Most?," 03 2018. [Online]. Available: http://verdict-encrypt.nridigital.com/verdict_encrypt_mar18/what_cybersecurity_risks_are_companies_currently_underestimating_the_most_34_experts_have_their_say. [Geopend 01 2019].
[32] Verdict Encrypt, „What Cybersecurity Risks Are Companies Currently Underestimating the Most?," 03 2018. [Online]. Available: http://verdict-encrypt.nridigital.com/verdict_encrypt_mar18/what_cybersecurity_risks_are_companies_currently_underestimating_the_most_34_experts_have_their_say#_blank. [Geopend 01 2019].
[33] CBS, „CBS Cybersecuritymonitor 2018," [Online]. Available: https://www.cbs.nl/nl-nl/publicatie/2018/38/cybersecuritymonitor-2018. [Geopend 01 2019].
[34] Fox-IT, „De dreigingen van 2017 en de trends van 2018," [Online]. Available: https://www.fox-it.com/nl/insights/blogs/blog/dreigingen-2017-en-trends-2018/. [Geopend 01 2019].
[35] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[36] Verdict Encrypt, „What Cybersecurity Risks Are Companies Currently Underestimating the Most?," 03 2018. [Online]. Available: http://verdict-encrypt.nridigital.com/verdict_encrypt_mar18/what_cybersecurity_risks_are_companies_currently_underestimating_the_most_34_experts_have_their_say#_blank. [Geopend 01 2019].

[37] Fox-IT, „De dreigingen van 2017 en de trends van 2018," [Online]. Available: https://www.fox-it.com/nl/insights/blogs/blog/dreigingen-2017-en-trends-2018/. [Geopend 01 2019].
[38] NCSC, „Cybersecuritybeeld Nederland 2018: Digitale dreiging in Nederland neemt toe," [Online]. Available: https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2018.html. [Geopend 01 2019].
[39] Verizon Business, „2018 Data Breach Investigations Report," [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf. [Geopend 01 2019].
[40] Autoriteit Persoonsgegevens, „Meldplicht datalekken: facts & figures 2018," [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2018.pdf. [Geopend 01 2019].
[41] Autoriteit Persoonsgegevens, „Meldplicht datalekken: facts & figures 2018," [Online]. Available: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2018.pdf. [Geopend 01 2019].
[42] Forum Standaardisatie, „Forum Standaardisatie," [Online]. Available: https://www.forumstandaardisatie.nl/. [Geopend 01 2019].
[43] B. Bosma, „Rapport SURFaudit benchmark 2017," [Online]. Available: https://www.surf.nl/kennisbank/2018/rapport-surfaudit-benchmark-2017.html. [Geopend 01 2019].
[44] NU, „Nederlandse universiteiten slachtoffer van Iraanse staatshackers," 23 03 2018. [Online]. Available: https://www.nu.nl/internet/5191589/nederlandse-universiteiten-slachtoffer-van-iraanse-staatshackers.html. [Geopend 01 2019].
[45] NOS, „Gegevens studenten hogeschool Saxion op straat door datalek," 01 05 2018. [Online]. Available: https://nos.nl/artikel/2229926-gegevens-studenten-hogeschool-saxion-op-straat-door-datalek.html. [Geopend 01 2019].
[46] Brabants Dagblad, „Mailbom bij Avans Hogeschool: honderden onzinberichten, duizenden e-mailadressen bereikt, maar niet zichtbaar," 24 05 2018. [Online]. Available: https://www.bd.nl/den-bosch-e-o/mailbom-bij-avans-hogeschool-honderden-onzinberichten-duizenden-e-mailadressen-bereikt-maar-niet-zichtbaar~af4f7d43/. [Geopend 01 2019].
[47] Tubantia, „UT mailt persoonlijke gegevens van 500 studenten rond," 29 05 2018. [Online]. Available: https://www.tubantia.nl/enschede/ut-mailt-persoonlijke-gegevens-van-500-studenten-rond~ab17c443/. [Geopend 01 2019].
[48] B. Bosma, „Rapport SURFaudit benchmark 2017," [Online]. Available: https://www.surf.nl/kennisbank/2018/rapport-surfaudit-benchmark-2017.html. [Geopend 01 2019].
[49] Cybersecurityraad, „De economische en maatschappelijke noodzaak van meer cybersecurity, 2016," 09 2016. [Online]. Available: https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf. [Geopend 01 2019].
[50] Verdict Encrypt, „What Cybersecurity Risks Are Companies Currently Underestimating the Most?," 03 2018. [Online]. Available: http://verdict-encrypt.nridigital.com/verdict_encrypt_mar18/what_cybersecurity_risks_are_companies_currently_underestimating_the_most_34_experts_have_their_say. [Geopend 01 2019].
[51] B. Bosma, „Rapport SURFaudit benchmark 2017," [Online]. Available: https://www.surf.nl/kennisbank/2018/rapport-surfaudit-benchmark-2017.html. [Geopend 01 2019].
[52] B. Bosma, „Rapport SURFaudit benchmark 2017," [Online]. Available: https://www.surf.nl/kennisbank/2018/rapport-surfaudit-benchmark-2017.html. [Geopend 01 2019].
[53] ENISA, „Threat Landscape 2017," [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends. [Geopend 01 2019].
[54] Computable, „RUG scherpt beveiliging aan na phishing," 03 01 2018. [Online]. Available: https://www.computable.nl/artikel/nieuws/security/6273951/250449/rug-scherpt-beveiliging-aan-na-phishing.html. [Geopend 01 2019].
[55] University of Twente, „Phishing mail waarschuwing," 19 03 2018. [Online]. Available: https://www.utwente.nl/nieuws/!/2018/3/201267/phishing-mail-waarschuwing. [Geopend 01 2019].

[56] Cybersecurityraad, „De economische en maatschappelijke noodzaak van meer cybersecurity," 09 2016. [Online]. Available: https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf. [Geopend 01 2019].
[57] Cybersecurityraad, „De economische en maatschappelijke noodzaak van meer cybersecurity," 09 2016. [Online]. Available: https://www.cybersecurityraad.nl/binaries/Rapport_Verhagen_NED_DEF_tcm107-314468.pdf. [Geopend 01 2019].
[58] SURF, „Cybercrisisoefening OZON," [Online]. Available: https://www.surf.nl/diensten-en-producten/surfcert/cybercrisisoefening-ozon/index.html. [Geopend 01 2019].
[59] Tweakers, „OZON 2018 - Een kijkje achter de schermen bij een grote 'cyberincidentoefening," 06 10 2018. [Online]. Available: https://tweakers.net/reviews/6605/ozon-2018-een-kijkje-achter-de-schermen-bij-een-grote-cyberincidentoefening.html. [Geopend 01 2019].
[60] L. v. d. Varst, „Dynamiek rond een nieuw crisistype: lessen uit de respons op een datalek bij Erasmus Universiteit Rotterdam," 04 12 2017. [Online]. Available: https://www.linkedin.com/pulse/dynamiek-rond-een-nieuw-crisistype-lessen-uit-de-op-van-der-varst/. [Geopend 01 2019].

COLOFON

Auteurs
Bart Bosma
(SURFnet)
Laurens van der Varst
(COT Instituut voor Veiligheids- en Crisismanagement-an Aon Company)

Redactie
Jan Michielsen

Vormgeving
Vrije Stijl, Utrecht

Drukwerk
Drukkerij Libertas Pascal

Fotografie
QUT Science and Engineering

Februari 2019

Dit rapport is mede tot stand gekomen dankzij bijdragen van de klankbordgroep bestaande uit:

Maarten Veldhuis	*Rijn IJssel*
Roeland Reijers	*Universiteit van Amsterdam*
Marcel van der Kolk	*Hogeschool Utrecht*
Hendrik Jan Buist	*Hogeschool Utrecht*
Rob van Duin	*Haagse Hogeschool*
Edwin Hubers	*Hogeschool Leiden*
Rienk de Vries	*Albeda College*
Remon Klein Tank	*Wageningen University & Research*
Bart van den Heuvel	*Universiteit Maastricht*
Eric van den Beld	*Hogeschool Saxion*
Matto Franssen	*Rijksuniversiteit Groningen*
René Ritzen	*Universiteit Utrecht*
Dubravka Marović	*Universiteit Leiden*

Samen aanjagen van vernieuwing

Universiteiten, hogescholen, mbo-instellingen, onderzoeks-instellingen en universitaire medische centra werken binnen SURF aan ICT-voorzieningen en -innovaties. Met als doel: beter en flexibeler onderwijs en onderzoek. Dat doen we door de best mogelijke digitale diensten te leveren, kennisdeling en -uitwisseling te stimuleren en vooral door steeds te blijven innoveren! Hiermee dragen we bij aan een sterke en duurzame Nederlandse kenniseconomie.

SURF