SAMENVATTING

CYBERDREIGINGSBEELD 2019/2020
ONDERWIJS EN ONDERZOEK

SURF

INHOUD

VOORWOORD
OPENHEID, ALERTHEID EN VERTROUWEN

Het nieuwe decennium is net begonnen. Terugkijkend zien we dat ieder decennium zijn eigen mondiale spanningen en veiligheidsissues kent. Denk aan de wereldoorlogen in de eerste helft van de vorige eeuw, de Koude Oorlog die daarop volgde, en niet te vergeten de terroristische aanslagen van en na 9/11. De geschiedenis herhaalt zich, maar nooit op dezelfde manier.

Dat geldt ook in de ICT: van DDoS-aanvallen hadden we 15 jaar geleden nog nooit gehoord, bijvoorbeeld. En nu die een bekend verschijnsel zijn, dient de volgende categorie van cyberaanvallen zich aan: veel organisaties worden geconfronteerd met ransomware-aanvallen, zoals recent de Universiteit Maastricht.

ICT biedt steeds meer mogelijkheden en is sterk verweven met primaire processen, ook in onderwijs en onderzoek. Cyberaanvallen worden steeds vernuftiger en complexer. Het zijn niet meer alleen whizzkids en nerds die erachter zitten. Cyberaanvallen zijn inmiddels ook een instrument van statelijke actoren, die deze aanvallen op zijn minst toelaten. Tegen zulke actoren moeten we als sector samen optreden. Dit begint bij onderlinge kennisuitwisseling, zodat we structureel van elkaar kunnen leren. Het cyberdreigingsbeeld is daar een voorbeeld van.

Maar met het uitbrengen van een cyberdreigingsbeeld zijn we als sector niet klaar. We moeten ermee aan de slag! We moeten elkaar meer opzoeken, binnen de gebruikelijke netwerken maar ook daarbuiten. Incidenten zoals de aanval op de Universiteit Maastricht laten namelijk zien dat iedere instelling zijn huiswerk in vredestijd op orde moet brengen, door risico's en impact van cyberaanvallen te doorgronden en kwetsbaarheden te verhelpen. En als het spannend wordt, moeten we direct aan de slag met de informatie die op dat moment beschikbaar komt. Dat vereist openheid van de instelling die op dat moment wordt aangevallen. Het vereist de alertheid van collega-instellingen om niet achterover te leunen, maar de eigen systemen te blijven monitoren. En van ons allemaal vereist het dat we vertrouwen hebben in de afspraken die we met elkaar hebben gemaakt.

Als we dit cyberdreigingsbeeld allemaal als leidraad gebruiken, hebben we bij het maken van ons huiswerk in elk geval een goede start!

Jan Bogerd
Voorzitter College van Bestuur Hogeschool Utrecht

Erwin Bleumink
Lid bestuur SURF

1. INLEIDING

Voor u ligt een samenvatting van het *Cyberdreigingsbeeld 2019/2020 – onderwijs en onderzoek*, waarin we de hoofdpunten uit het volledige rapport[1] op een rij zetten. We kijken terug op 2019 en vooruit naar 2020. Welke trends zagen we in 2019 in de sector onderwijs en onderzoek? Welke dreigingen hebben zich gemanifesteerd in de sector? Wat verwachten we voor 2020 en wat is er opgenomen in de jaarplannen[2] van instellingen en organisaties?

Doel van het rapport

Het Cyberdreigingsbeeld heeft als doel om een globaal beeld te schetsen van de staat van informatieveiligheid en bescherming van persoonsgegevens. Het is tot stand gekomen op basis van vrijwillige deelname aan een survey en niet noodzakelijk op basis van officiële cijfers van de participerende instellingen.

Werkwijze

Om inzicht te krijgen in welk soort incidenten daadwerkelijk hebben plaatsgevonden en welke risico's voor onderwijs- en onderzoeksinstellingen het meest relevant zijn in vergelijking met 2018, hebben we in het najaar van 2019[3] een survey onder instellingen uitgevoerd.

Verder hebben we trends in kaart gebracht door verschillende publieke rapporten te raadplegen, waaronder het jaarverslag van de AIVD [1], het jaarlijkse Cybersecuritybeeld Nederland [2], het Cyberkompas 2019 van het NCSC [3], publicaties van de Wetenschappelijke Raad voor het Regeringsbeleid [4], maar ook van internationale rapporten zoals het Verizon Data Breach Investigations Report [5], het ENISA Threat Landscape Report [6] en "The cyber threat to Universities" van het NCSC (UK) [7].

Leeswijzer

In het volgende hoofdstuk gaan we kort in op de resultaten van de survey, in hoofdstuk drie noemen een aantal cybersecuritytrends, in hoofdstuk vier gaan we in op de weerbaarheid van instellingen en in hoofdstuk vijf komen we tot een afronding met enkele aanbevelingen. Tot slot vindt u in hoofdstuk zes een viertal aandachtspunten voor de bestuurstafel.

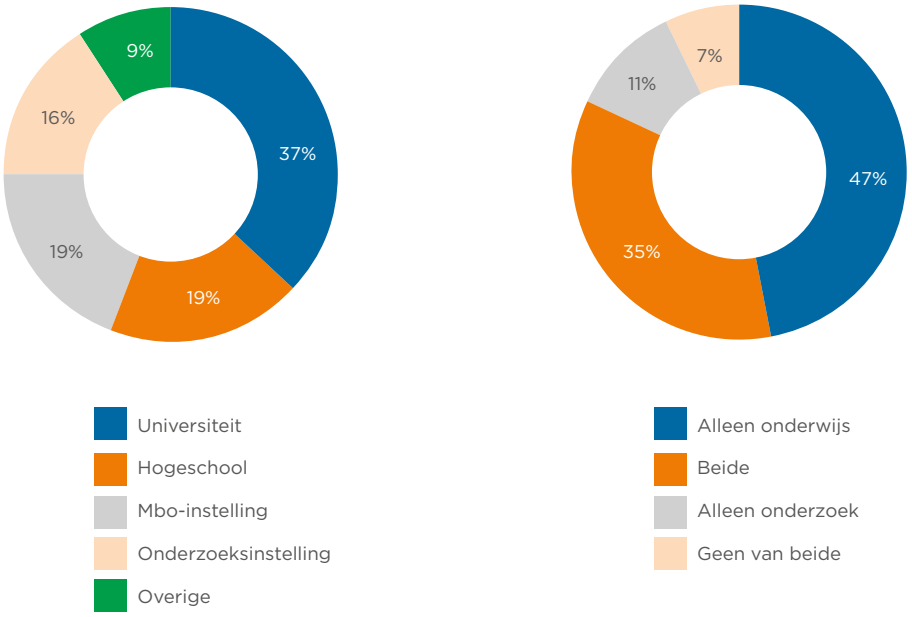
[1] *https://www.surf.nl/files/2020-02/surf-cyberdreigingsbeeld-2019-2020.pdf*
[2] *In het jaarplan van een instelling staan de geplande activiteiten voor het betreffende jaar die zijn opgenomen in het budget*
[3] *Van 5 tot 25 november 2019*

2. SURVEY – RESPONS EN RESULTATEN

We hebben 178 instellingen aangeschreven om de survey in te vullen. Daarvan hebben 57 instellingen de survey volledig ingevuld. Verder behandelen we een deel van resultaten uit het cyberdreigingsbeeld, te weten de resultaten op het gebied governance, awareness en de risico-perceptie voor 2020.

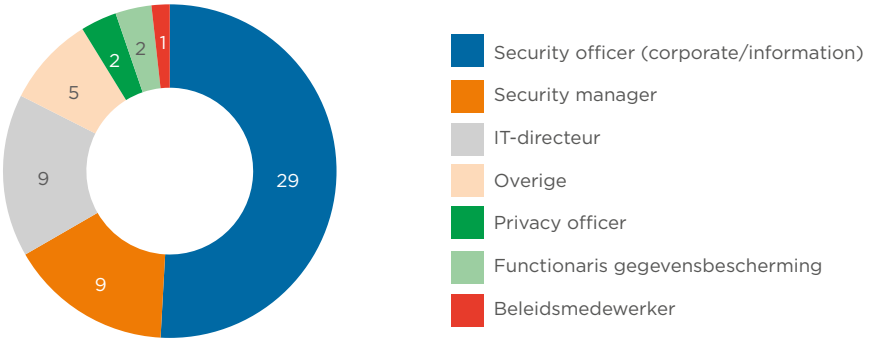
2.1 Respons

De verdeling over het type instelling is als volgt:



Figuur 1: Respondenten per type instelling en verdeling tussen onderwijs- en onderzoeksinstellingen

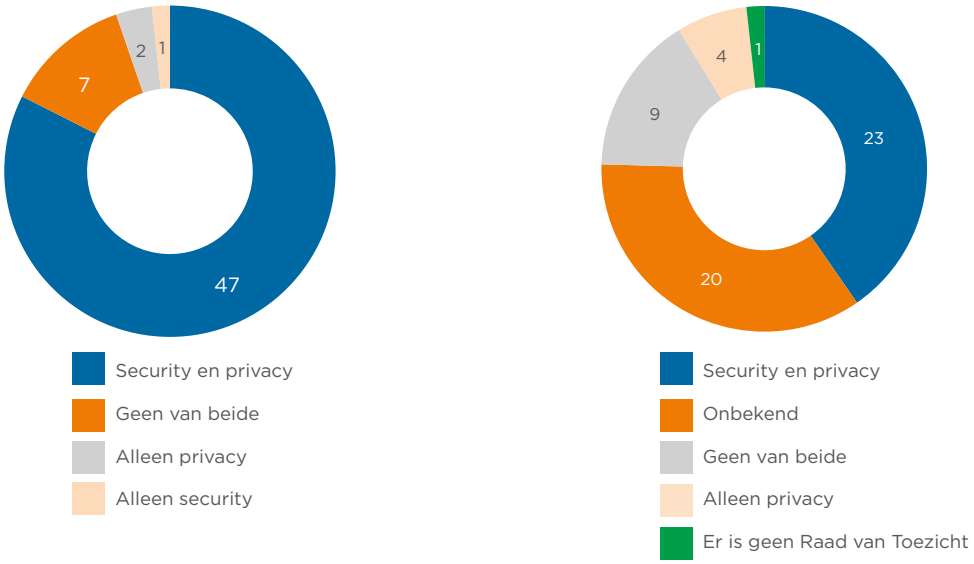
Van degenen die de survey hebben ingevuld valt het merendeel (ca. 70%) in de categorie security officer:



Figuur 2: Rol van de respondenten

2.2 Resultaten

Governance

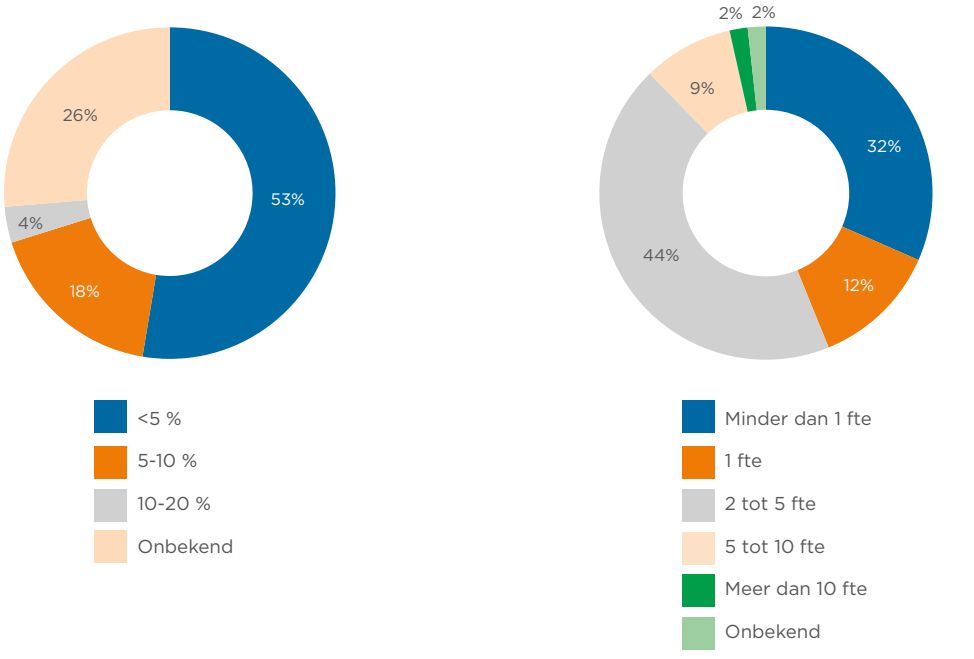


Figuur 3: Periodieke rapportage aan bestuur (links) en aan de raad van toezicht (rechts)

Figuur 3 laat zien dat het bestuur periodiek op de hoogte wordt gehouden van zowel security- als privacy-incidenten. Wanneer er sprake is van een ernstig incident, wordt bij een groot deel van de instellingen (93%) het bestuur direct ingelicht.

Ook de raad van toezicht wordt bij een behoorlijk aantal instellingen periodiek op de hoogte gehouden over incidenten. Een deel van de responses over de raad van toezicht is echter ook 'onbekend'. De meeste instellingen hebben zowel een security officer als een functionaris gegevens-bescherming. Ruim 20% heeft daarbij ook nog een privacy officer.

Middelen[4]



Figuur 4: Percentage van IT-budget (links) en aantal fte beschikbaar (rechts) voor informatiebeveiliging

[4] *Gebaseerd op door de respondenten ingevulde schattingen*

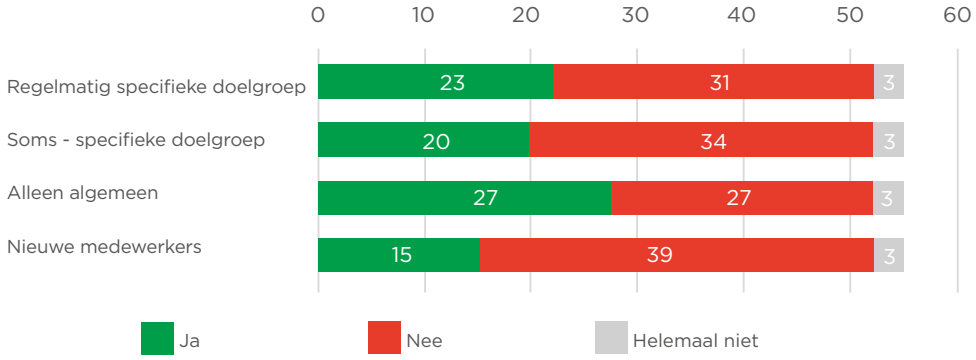
Sinds vorig jaar zijn er meer middelen beschikbaar gekomen voor informatiebeveiliging. Een grote groep instellingen heeft 2-5 fte beschikbaar voor informatiebeveiliging (zie Figuur 4). Het aantal beschikbare fte's hangt ook samen met de grootte van de instelling:

fte's	aantal medewerkers	aantal studenten
meer dan 5 fte	3.500 - 7.000	25.000 - 45.000
2 - 5 fte	1.000 - 6.500	8.500 - 45.000
1 fte	400 - 3.000	4.000 - 30.000
minder dan 1 fte	100 - 850	1.000 - 8.000

Tabel 1: Relatie tussen fte's en grootte van de instelling

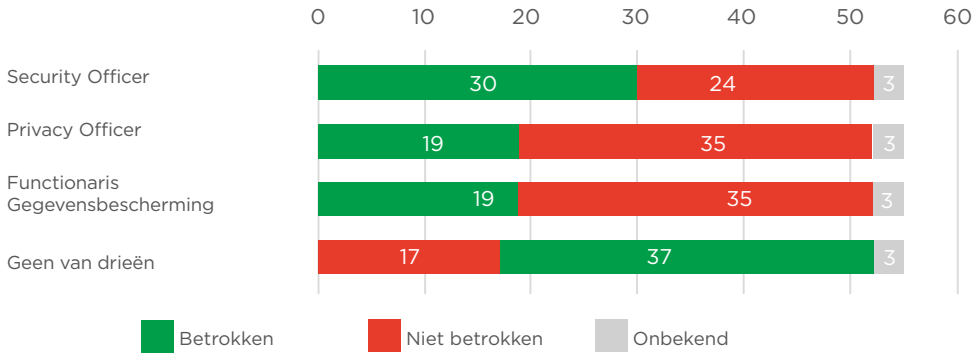
Awareness

Figuur 5 illustreert dat nieuwe medewerkers, docenten en onderzoekers bij het in dienst treden in veel gevallen geen awareness-training krijgen (bij bijna 70% van de instellingen) en dat bij minder dan de helft van de instellingen structureel algemene of op specifieke groepen gerichte awareness-trainingen plaatsvinden:



Figuur 5: Awareness-campagnes

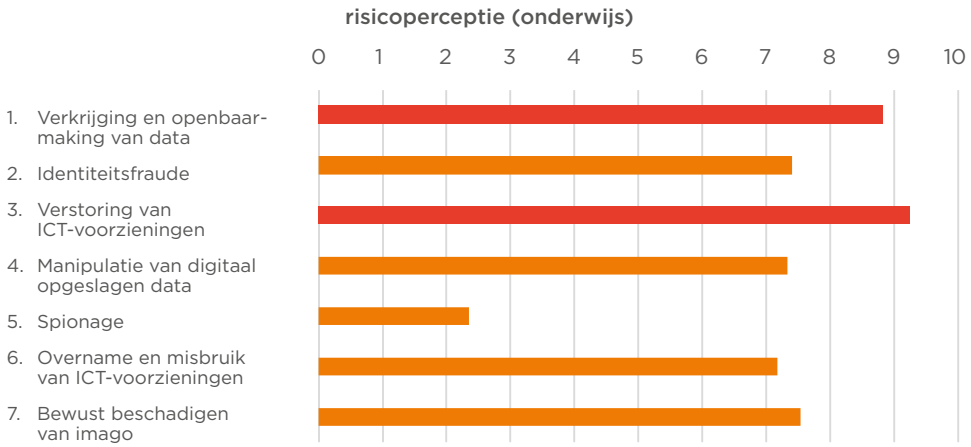
Uit Figuur 6 blijkt dat bij ongeveer 70-75% van de instellingen aandacht is voor informatie-beveiliging en bescherming van persoonsgegevens bij projecten, inkoop en aanbestedingen:



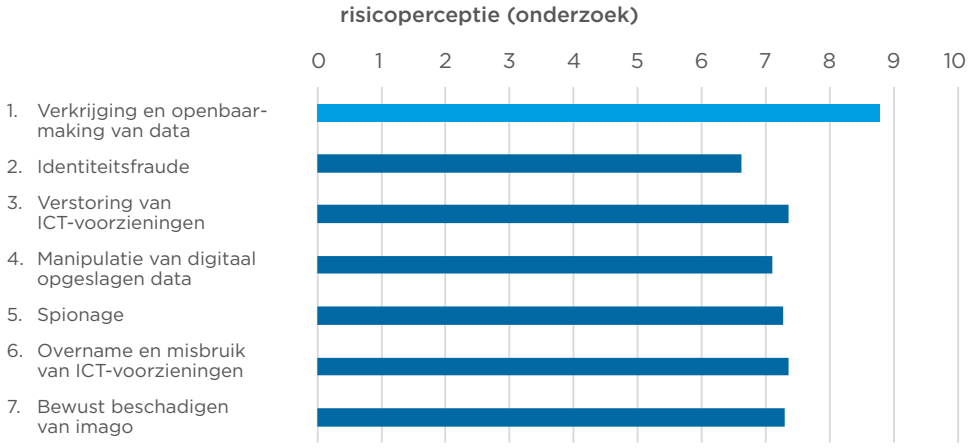
Figuur 6: Aandacht voor informatiebeveiliging en privacy

Risicoperceptie

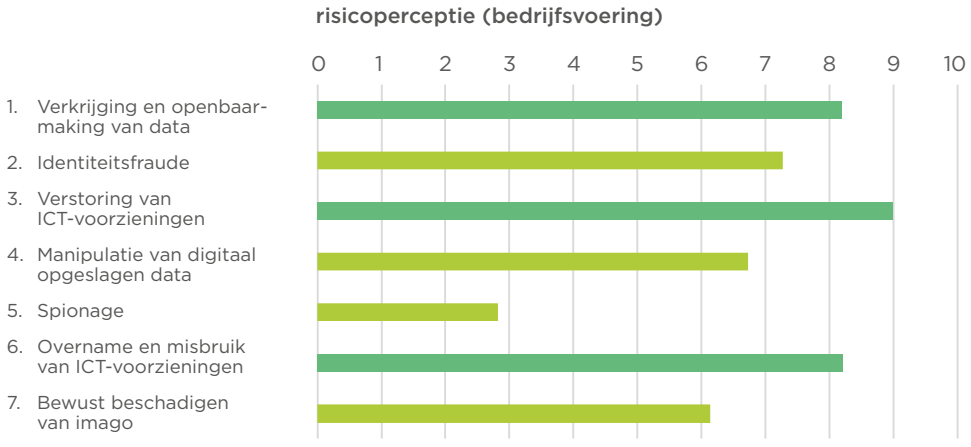
De standaardmethode voor het bepalen van de hoogte van het risico is het product van de kans op schade en de gevolgen van de schade: risico = kans * impact. In de survey hebben de respondenten kans en impact ingeschat. De resultaten daarvan staan in onderstaande grafieken (zie Figuur 7 - 9).



Figuur 7: Perceptie van de risicocategorieën (onderwijs)



Figuur 8: Perceptie van de risicocategorieën (onderzoek)



Figuur 9: Perceptie van de risicocategorieën (bedrijfsvoering)

Hieruit blijkt dat:

- voor het onderwijsproces *Verkrijging en openbaarmaking van data en Verstoring van ICT-voorzieningen* worden gezien als het grootste risico,
- voor onderzoek *Verkrijging en openbaarmaking van data* als grootste risico wordt gezien,
- voor bedrijfsvoering V*erstoring van ICT-voorzieningen, Verkrijging en openbaarmaking van data en Overname en misbruik van ICT-voorzieningen* als grootste risico worden gezien en dat,
- behalve bij onderzoek, *Spionage* **niet** als een hoog risico wordt gezien.

3. CYBERSECURITYTRENDS

Dit hoofdstuk geeft een kort overzicht van de belangrijkste cybersecuritytrends van het afgelopen jaar. Ook zetten we de trends voor het komende jaar op een rij.

Trends in onderwijs en onderzoek

Op basis van de survey worden ten opzichte van 2018 geen grote verschuivingen in het type dreigingen gesignaleerd. Evenals in 2018 was er ook in 2019 een lichte toename bij *Verkrijging en openbaarmaking van data, identiteitsfraude en verstoring van ICT-voorzieningen*. Dit beeld wijkt niet veel af van de dreigingen die door de publieke bonnen voor de andere sectoren worden genoemd.

Toename van dreigingen

De verwachting voor 2020 is een verdere toename van dreigingen, niet alleen voor onderwijsinstellingen, maar ook voor onderzoeksinstellingen, waarbij ransomware en phishing veel gebruikte middelen zullen zijn.

Actoren

Als alle dreigingstypen worden samengevoegd dan laat de survey zien (zie Figuur 10) dat instellingen (h)activisten/cybervandalen als belangrijkste actoren zien, gevolgd door beroepscriminelen en de eigen medewerkers. Dit beeld wijkt iets af van het landelijke beeld in het Cybersecuritybeeld Nederland 2019 [2] waarin statelijke actoren en beroepscriminelen als voornaamste actoren worden genoemd. Dezelfde actoren worden door het Britse NCSC als belangrijkste actoren voor universiteiten genoemd [7]. Waarom deze situatie afwijkt van de cijfers uit de survey, vereist nader onderzoek.

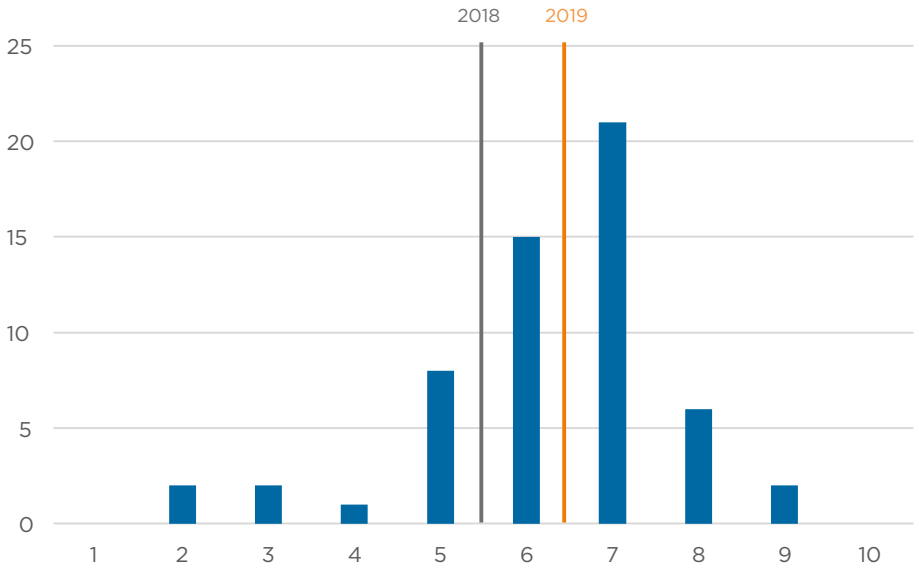
Figuur 10: Actoren voor alle risico-categorieën

4. WEERBAARHEID ONDERWIJS- EN ONDERZOEKSINSTELLINGEN

De digitale weerbaarheid van onderwijs- en onderzoekinstellingen is nog niet overal op voldoende niveau. Daarin staat de sector niet alleen. Zowel het NCSC [2] als de WRR [4] geven aan dat de cyberweerbaarheid in Nederland nog onder de maat is. Dit geldt voor alle sectoren. De Algemene Rekenkamer rapporteert bijvoorbeeld in haar verantwoordingsonderzoek over 2018 [8] dat de rijksoverheid de informatiebeveiliging niet op orde heeft. De toenemende complexiteit en connectiviteit van het ICT-landschap zet de weerbaarheid verder onder druk.

Beoordeling eigen cyberweerbaarheid sector onderwijs en onderzoek

Respondenten beoordelen de cyberweerbaarheid van de eigen organisatie gemiddeld met een voldoende (score 6,3 op een schaal van 0-10). Dit is een lichte stijging ten opzichte van 2018 waar de score 5,5 bedroeg. Op basis van deze uitkomsten kan worden gesteld dat er, ondanks vooruitgang, bij onderwijs- en onderzoeksinstellingen nog ruimte is voor verdere verhoging van de cyberweerbaarheid.



Figuur 11: Eigen inschatting van de cyberweerbaarheid van instellingen

Om risico's te verminderen is het absoluut noodzakelijk om de weerbaarheid te vergroten. Connectiviteit en complexiteit bij organisaties nemen nog steeds toe terwijl basismaatregelen soms ontbreken. Het businessmodel van cybercriminelen is nog steeds lucratief. Zij gebruiken relatief eenvoudig te verkrijgen middelen om grote schade aan organisaties toe te brengen. Voor sommige criminelen is geld de grote drijfveer. Bij statelijke actoren is het verkrijgen van kennis of economische voorsprong de drijfveer om organisaties aan te vallen. Het vergroten van de weerbaarheid is het belangrijkste instrument om deze dreigingen te bestrijden.

5. CONCLUSIES EN AANBEVELINGEN

Globaal gezien wijkt het Cyberdreigingsbeeld 2019/2020 onderwijs en onderzoek niet veel af van het Cyberdreigingsbeeld uit 2018. Het aantal incidenten stijgt echter verder waardoor de dreiging per saldo toeneemt. Dit vereist onverminderde inzet van organisaties om de weerbaarheid te verhogen. Dit hoofdstuk bevat conclusies en aanbevelingen voor de sector onderwijs en onderzoek om de weerbaarheid te verhogen.

Bewustwording belangrijke pijler voor weerbaarheid

Door gebrek aan kennis en vanwege misleiding blijft de mens een zwakke schakel. Instellingen moeten daarom veel energie in bewustwording en opleiding van gebruikers steken.

Risicoprofiel cloudgebruik up-to-date brengen

Doordat instellingen steeds meer cloudtoepassingen gebruiken die door een klein aantal niet-Europese grote spelers worden geleverd, ontstaan nieuwe dreigingen voor de beschikbaarheid en vertrouwelijkheid van gegevens. Door afwijkende wetgeving of geopolitieke spanningen kan het voorkomen dat deze leveranciers hun plichten tegenover de afnemers niet meer na kunnen komen. Bovendien kan een onderbreking in hun dienstverlening grote gevolgen hebben voor de primaire processen van de afnemers.

Instellingen moeten samen optrekken om de risico's in kaart te brengen en gezamenlijk oplossingen te vinden.

Hoge investeringen, hooggekwalificeerde expertise noodzakelijk

Weerstandverhogende maatregelen vergen grote investeringen. Budgetten voor informatiebeveiliging staan echter altijd onder druk. Deze gaan immers altijd ten koste van het primaire proces, onderwijs en onderzoek.

Voldoende hooggekwalificeerde expertise is noodzakelijk om de dreigingen adequaat te kunnen weerstaan. In de survey wordt het tekort aan capaciteit als één van de belangrijkste kwetsbaarheden genoemd. De vraag naar goed gekwalificeerde expertise is echter hoog en het aanbod laag. Ook hier kan samenwerking en pooling soelaas bieden.

Samenwerking uitbreiden

Om de toenemende dreigingen het hoofd te bieden, is samenwerking cruciaal. In SURFverband wordt er al veel samengewerkt en kennis gedeeld, bijvoorbeeld in community's als SCIPR en SCIRT[5], via de dienst SURFcert[6] en bij het Platform Integrale Veiligheid Hoger Onderwijs[7].
Om de sector onderwijs en onderzoek in zijn geheel weerbaarder te maken tegen cybercriminaliteit is samenwerking op onderstaande onderwerpen een vereiste:

- het delen van informatie en dreigingen,
- het delen van expertise op het gebied van cybersecurity,
- het inrichten van security monitoring en logging (SIEM), mogelijk uit te breiden tot volwaardige SOC-functionaliteit (Security Operations Center),
- samenwerking bij cybersecurityoefeningen (zoals NOZON/OZON) of Red teaming

Samenwerking tussen instellingen helpt om efficiënter te werken en de gesignaleerde tekorten aan capaciteit en expertise te overkomen.

[5] *SCIPR – SURF Community voor Informatiebeveiliging en Privacy, SCIRT – SURFnet Community van Incident Response Teams (zie: https://www.surf.nl/beveiligingscommunitys-werk-samen-aan-beveiliging-en-privacy)*
[6] *Zie: https://www.surf.nl/en/surfcert-247-support-in-case-of-security-incidents*
[7] *Zie: https://www.integraalveilig-ho.nl/*

6. REFLECTIE VOOR DE BESTUURDER

Op basis van de resultaten van de survey en de gesignaleerde trends hebben we voor bestuurders een aantal reflectievragen op een rijtje gezet (zie ook Figuur 12). Ze helpen om deze thema's te bespreken en er conclusies aan te verbinden voor het beleid en de inrichting van de organisatie:

- Wat is uw ambitieniveau op het gebied van digitale weerbaarheid en integrale veiligheid?
- Hoe is uw informatiepositie over cyberincidenten en hoe houdt u zicht op cyberdreigingen?
- Hoe ziet het cyberrisicoprofiel van uw organisatie eruit, welke risico's bent u bereid te accepteren, in welke mate en past dat bij uw verantwoordingsplicht?
- Heeft uw instelling een integraal veiligheidsbeleid en in hoeverre sluit het informatie-beveiligingsbeleid daarbij aan?

Figuur 12: Reflectievragen voor bestuurders

GERAADPLEEGDE BRONNEN

#	Auteur(s)	Titel	Uitgever	Jaar	URL	opgehaald
[1]	Algemene Inlichtingen en Veiligheidsdienst	**Jaarverslag AIVD 2018**	AIVD	2019	https://www.aivd.nl/documenten/jaarverslagen/2019/04/02/jaarverslag-aivd-2018	16-10-2019
[2]	National Coördinator Terrorisme en Veiligheid	**Cybersecuritybeeld Nederland 2019**	NCTV	2019	https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland/nieuws/2019/juni/12/csbn-2019-ontwrichting-ligt-op-de-loer	20-09-2019
[3]	Nationaal Cybersecurity Centrum Nederland	**Cyberkompas 2019**	NCSC	2019	https://www.ncsc.nl/aan-de-slag/cyberkompas	16-12-2019
[4]	Wetenschappelijke Raad voor het Regeringsbeleid	**Voorbereiden op digitale ontwrichting**	WRR	2019	https://www.wrr.nl/onderwerpen/digitale-ontwrichting/documenten/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting	10-09-2019
[5]	Verizon Business	**Verizon Data Breach Investigations Report 2019**	Verizon	2019	https://enterprise.verizon.com/resources/reports/dbir/	13-08-2019
[6]	European Union Agency for Cybersecurity	**ENISA Threat Landscape Report**	ENISA	2019	https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018	05-09-2019
[7]	National Cyber Security Centre UK	**The cyber threat to Universities**	NCSC (UK)	2019	https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities	16-12-2019
[8]	Algemene Rekenkamer	**Rijksoverheid heeft informatiebeveiliging en IT beheer nog niet op orde**	Algemene Rekenkamer	2019	https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/nieuws/2019/05/15/rijksoverheid-heeft-informatiebeveiliging-en-it-beheer-nog-niet-op-orde	10-01-2020

COLOFON

Auteurs
Bart Bosma *(SURF)*
René Ritzen (*SURF*)

Redactie
Yvonne Klaassen (*SURF*)

Coördinatie
Nanda Bazuin (*SURF*)

Vormgeving
Vrije Stijl, Utrecht

Fotografie
Istock

April 2020

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

Bas Roset	*Kennisnet*
Dietmar Timmerman	*Hogeschool Saxion*
Eric van den Beld	*Hogeschool Saxion*
Maarten Veldhuis	*Rijn IJssel*
Marcel van der Kolk	*Hogeschool Utrecht*
Martijn Bijleveld	*SaMBO-ICT*
Pamela Mercera	*Vrije Universiteit Amsterdam*
Peter Berndsen	*RIVM*
Raoul Vernède	*Universiteit Utrecht*
Rienk de Vries	*Albeda*
Roeland Reijers	*Universiteit van Amsterdam*
Sebastiaan Kamp	*Erasmus universiteit*

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