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. Dit 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

BESTUURSSAMENVATTING

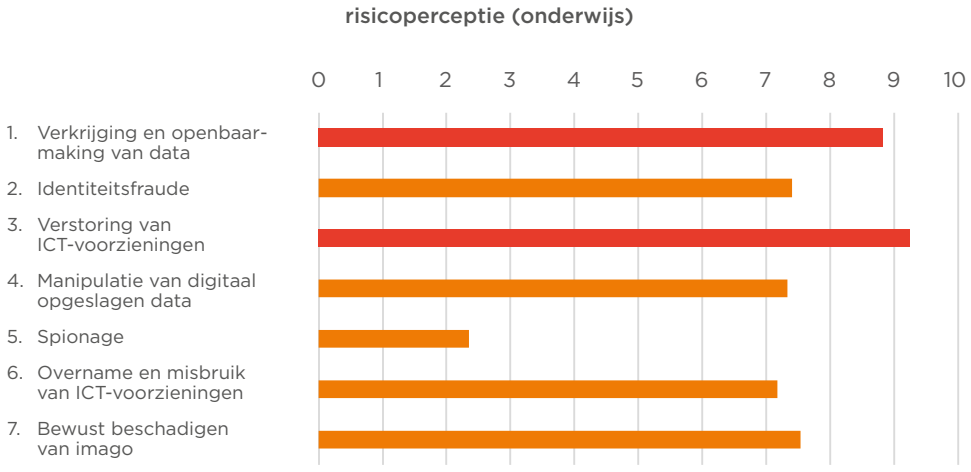
In dit Cyberdreigingsbeeld – onderwijs en onderzoek kijken we terug op 2019 en vooruit naar 2020. We brengen in kaart welke trends er in 2019 in de sector onderwijs en onderzoek waren en welke dreigingen zich hebben gemanifesteerd in de sector. Ook bekijken we welke trends we verwachten in 2020 en wat daarvoor is opgenomen in de jaarplannen van instellingen en organisaties.

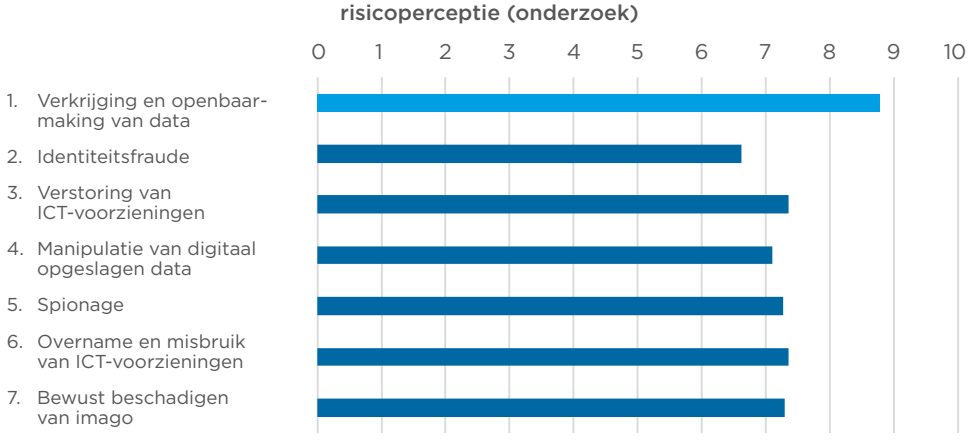
In het najaar van 2019[1] hebben we een survey onder instellingen uitgevoerd om meer inzicht te krijgen in welk soort incidenten daadwerkelijk hebben plaatsgevonden en welke risico's voor onderwijs- en onderzoeksinstellingen het meest relevant zijn in vergelijking met 2018.

Weerbaarheid en risicoperceptie

Uit de survey komt naar voren dat instellingen vinden dat ze er wat beter voorstaan dan in 2018 wat betreft weerbaarheid. Dit blijkt ook uit de risicoperceptie waarvan de scores wat lager liggen dan in 2018.

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





[1] *Van 5 tot 25 november 2019*

Figuur 1: Perceptie van de risicocategorieën per proces

Incidenten

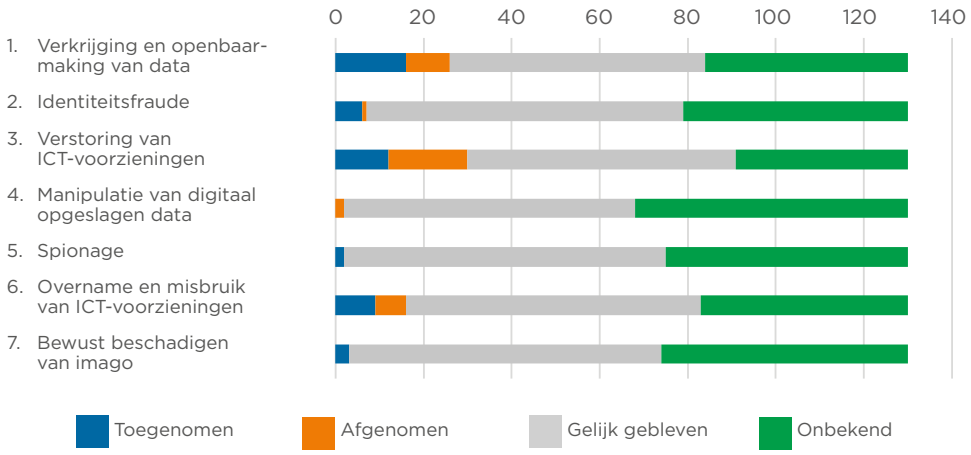
Vergelijken we de aantallen incidenten die zich hebben voorgedaan in 2019 met de risicoperceptie, dan valt op dat bij onderwijs en bedrijfsvoering vooral het risico op incidenten in de categorieën *Verkrijging en openbaarmaking van data* en *Verstoring van ICT-voorzieningen* hoog scoort, terwijl incidenten in 2019 zich vooral hebben voorgedaan bij de categorie *Verstoring van ICT-voorzieningen*.

	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	Gemiddeld	Weinig	Gemiddeld
2. Identiteitsfraude	Veel	Weinig	Gemiddeld
3. Verstoring van ICT-voorzieningen	Veel	Veel	Veel
4. Manipulatie van digitaal opgeslagen data	Weinig	Geen	Weinig
5. Spionage	Weinig	Weinig	Geen
6. Overname en misbruik van ICT-voorzieningen	Gemiddeld	Weinig	Weinig
7. Bewust beschadigen van imago	Weinig	Weinig	Weinig

Veel Gemiddeld Weinig Geen

Tabel 1: Schattingen van de aantallen incidenten per risicocategorie (2019)

Wat betreft de dynamiek van incidenten zien we dat voor alle categorieën het aandeel onbekend vrij hoog is, net als in 2018:



Figuur 2: Toename of afname van aantallen incidenten per risicocategorie voor onderwijs, onderzoek en bedrijfsvoering samen.

Integrale veiligheid

Cybersecurity is onderdeel van het hele veiligheidsbeleid van de organisatie. Uit het rapport 'Dreigingsbeeld HO' van het platform IV-HO [21] uit 2018 is gebleken dat het thema *Privacy en cybersecurity* een van de hoogst scorende thema's is qua kans, impact en dynamiek.

Reflectie voor de bestuurder

In Tabel 2 hebben we een aantal thema's op een rijtje gezet op basis van gesignaleerde trends:

Thema	Toelichting	Bestuurlijke reflectie
Informatiepositie	Dynamiek in cyberdreigingen vraagt om regelmatige tussentijdse evaluatie en herbeoordeling.	Hoe is uw informatiepositie over cyberincidenten? Hoe houdt u zicht op cyberdreigingen?
Cyberrisicoprofiel	De impact van cyberdreigingen is afhankelijk van het risicoprofiel van instellingen.	Hoe ziet uw cyberrisicoprofiel eruit? Welk risico bent u bereid te accepteren, in welke mate en past dat bij uw verantwoordingsplicht?
Integrale veiligheid	Cyberveiligheid is een van de thema's bij integrale veiligheid.	Heeft uw instelling een integraal veiligheidsbeleid en in hoeverre sluit het informatiebeveiligingsbeleid daarbij aan?
Ambities	Instellingen kunnen zich op verschillende manieren voorbereiden op (cyber)dreigingen.	Wat is uw ambitieniveau op het gebied van digitale weerbaarheid en integrale veiligheid?

Tabel 2: Reflectievragen voor bestuurders

1. INLEIDING

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

1.1 Achtergrond

Voor u ligt het zesde Cyberdreigingsbeeld – onderwijs en onderzoek, waarin we terug-kijken op 2019 en vooruitkijken naar 2020. Welke trends zagen we in 2019 in de sector onderwijs en onderzoek? Welke dreigingen hebben zich gemanifesteerd in de sector? En welke trends worden in 2020 verwacht en wat is er opgenomen in de jaarplannen[2] van instellingen en organisaties?

Qua vorm en inhoud bouwt het Cyberdreigingsbeeld voort op de eerdere uitgaven die SURF sinds 2014 jaarlijks publiceert. Naast informatiebeveiliging staan het omgaan met persoons-gegevens en kennisveiligheid op de radar van de onderwijs- en onderzoeksinstellingen.

Net als in voorgaande jaren hebben we gebruik gemaakt van publieke bronnen zoals 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] om diverse trends in kaart te brengen.

In het najaar van 2019[3] hebben we een survey onder instellingen uitgevoerd om meer 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.

1.2 Dreigingen, middelen en risico’s

Risico’s ontstaan doordat beschikbare middelen bedreigd worden door actoren die kwetsbaarheden uitbuiten. Voor informatiebeveiliging bij onderwijs- en onderzoeks-instellingen zijn zeven risicocategorieën in kaart gebracht (zie bijlage 1 voor meer details):

- Verkrijging en openbaarmaking van informatie
- Identiteitsfraude
- Verstoring ICT
- Manipulatie van data
- Spionage
- Overname en misbruik ICT
- Bewust beschadigen imago

Actoren, middelen, kwetsbaarheden en maatregelen

Actoren gebruiken een bepaalde werkwijze, bijvoorbeeld phishing of malware. Omdat onderwijs- en onderzoeksinstellingen over talloze middelen beschikken, focussen zij de bescherming op de belangrijkste middelen, ook wel kroonjuwelen genoemd.

[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*

Figuur 2: Actoren, middelen, kwetsbaarheden en maatregelen

In dit rapport kijken we naar dreigingen en risico's, actoren en hun werkwijze en naar kwetsbaarheden die misbruikt kunnen worden. Aan de hand van de survey kijken we vervolgens naar de stappen die instellingen hebben gezet om die kwetsbaarheden te mitigeren, de mate van investering in en de effectiviteit van maatregelen om hun informatieveiligheid te vergroten.

Instellingen bepalen op grond van een risicoafweging welke maatregelen nodig zijn om hun kroonjuwelen afdoende te beschermen. Dit rapport beoogt een bijdrage te leveren aan de risicoafweging die onderwijs- en onderzoeksinstellingen maken door actuele trends in kaart te brengen. In algemene zin geven we aan welke maatregelen instellingen hebben genomen en als effectief beschouwen.

Incidenten

In 2019 is er aantal high-profile incidenten geweest, waaronder de hack van het leerlingvolgsysteem bij Aventus [10] in februari en de ransomware-aanval op Maastricht University [11] in december, die veel impact hadden. De verwachting voor 2020 is een verdere toename van dreigingen, niet alleen voor onderwijsinstellingen, maar ook voor onderzoeksinstellingen, waarbij ransomware als middel veel gebruikt zal worden [2].

Samenwerken

Samenwerken wordt veel genoemd als manier om samen sterker te staan en gezamenlijk efficiënter te werken. In de sector onderwijs en onderzoek wordt al veel samengewerkt in SURF-community's als SCIPR en SCIRT[4]. En buiten SURF zijn allerlei voorbeelden te vinden waarbij instellingen zelf succesvolle samenwerking opzetten. Bijvoorbeeld in Canada werkt een aantal universiteiten samen om een 'shared security operations center for higher education'[5] te realiseren, in de Verenigde Staten bestaat er al zo'n samenwerking[6]. Dichter bij huis in Nederland werken zorginstellingen samen om een security operations center in te richten[7], terwijl in Denemarken[8] en Zwitserland[9] de incident-responsediensten van de onderwijssector samenwerken met andere sectoren.

1.3 Leeswijzer

In hoofdstuk 2 gaan we in op de resultaten van de survey die in november 2019 is uitgevoerd. In hoofdstuk 3 focussen we op gesignaleerde trends die relevant zijn voor onderwijs- en onderzoeksinstellingen, mede aan de hand van enkele SURF-statistieken. In hoofdstuk 4 kijken we terug op resultaten van de survey met als aandachtspunt weerbaarheid en concluderend staan in hoofdstuk 5 conclusies en aanbevelingen om de sector onderwijs en onderzoek beter voor te bereiden op een cyberveilige toekomst.

[4] *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)*
[5] *Zie: https://canssoc.ca/*
[6] *Zie: https://omnisoc.iu.edu/*
[7] *Zie bijv. https://www.ictmagazine.nl/uitgelicht/beter-beveiligd-implementeer-soc/*
[8] *Zie: https://www.cert.dk/en en https://www.deic.dk/en*
[9] *Zie: https://www.switch.ch/security/*

2. OPZET EN RESPONS VAN DE SURVEY

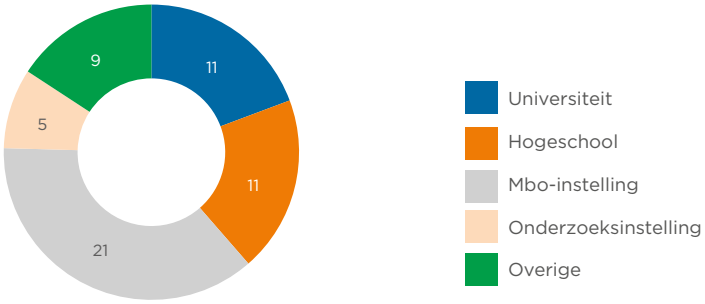
Net als in 2018 heeft SURF in 2019 een survey[10] uitgezet onder de aangesloten onderwijs- en onderzoeksinstellingen om een beeld te krijgen van incidenten die zich hebben voorgedaan, de risicoperceptie van instellingen, hoe informatiebeveiliging is georganiseerd en hoe weerbaar instellingen denken te zijn.

2.1 Werkwijze

Van iedere bij SURFnet aangesloten instelling hebben we de securitycontactpersoon gevraagd de survey in te vullen of in te laten vullen. Van de 178 aangeschreven instellingen hebben 57 instellingen de survey volledig ingevuld. Op basis daarvan hebben we een analyse gemaakt.

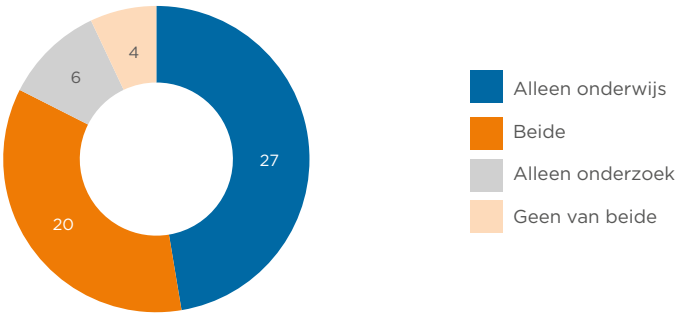
Het Cyberdreigingsbeeld heeft als doel om een globaal beeld te schetsen van de staat van informatieveiligheid en bescherming van persoonsgegevens. Het is tot stand gekomen op basis van vrijwillige deelname en niet noodzakelijk op basis van officiële cijfers van de participerende instellingen.

De verdeling over het type instelling is als volgt:



Figuur 3: Respondenten per type instelling

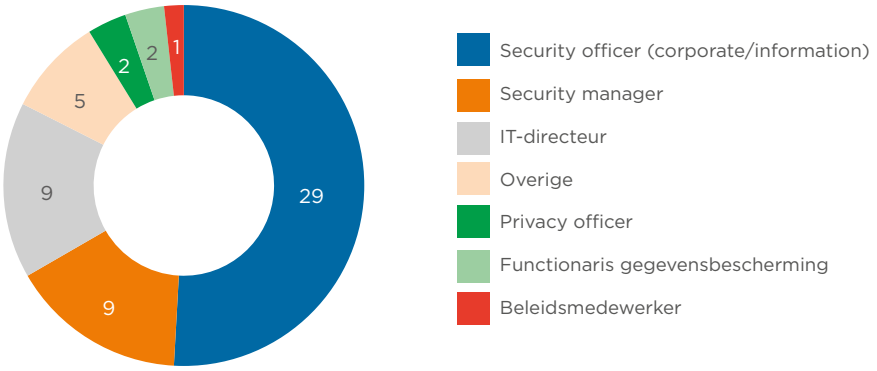
Door de instellingen individueel te benaderen in plaats van via een oproep aan de community is met name het aantal mbo-instellingen dat de survey heeft beantwoord significant toegenomen ten opzichte van 2018. De verdeling tussen onderwijs- en onderzoeksinstellingen ziet er als volgt uit:



Figuur 4: Verdeling onderzoek-onderwijs

[10] *De survey kon worden ingevuld van 5 tot 25 november 2019*

Onder de respondenten zijn functionarissen met een securityrol in de meerderheid (ca. 70%):



Figuur 5: Rol respondenten

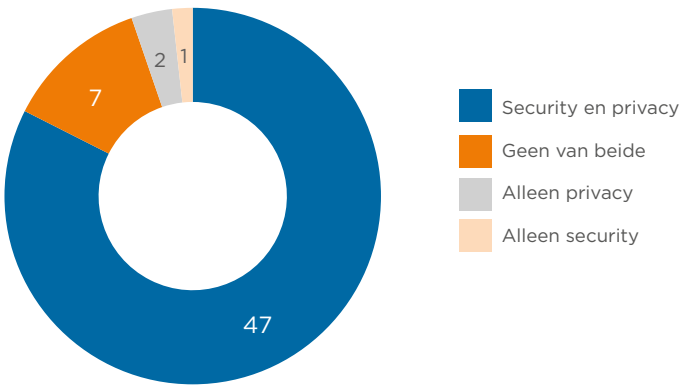
2.2 Resultaten

In dit hoofdstuk gaan we verder in op de vragen over de governance bij de instellingen, aantallen incidenten, in hoeverre aandacht wordt besteed aan awareness, hoeveel wordt geïnvesteerd in maatregelen en kwetsbaarheden in de organisatie.

Governance

Hoe een organisatie informatiebeveiliging en bescherming van persoonsgegevens heeft ingericht, bepaalt mede hoe weerbaar deze organisatie is tegen cyberdreigingen. Onder weerbaarheid verstaan we hier de veerkracht van een organisatie en haar digitale systemen en processen [8]. Een belangrijk aspect is de betrokkenheid van het bestuur bij de inrichting van informatiebeveiliging en de afhandeling van incidenten. Wanneer het bestuur hier niet bij betrokken is en geen ondersteuning biedt, is het moeilijk voor de organisatie om dit op een effectieve manier in te richten.

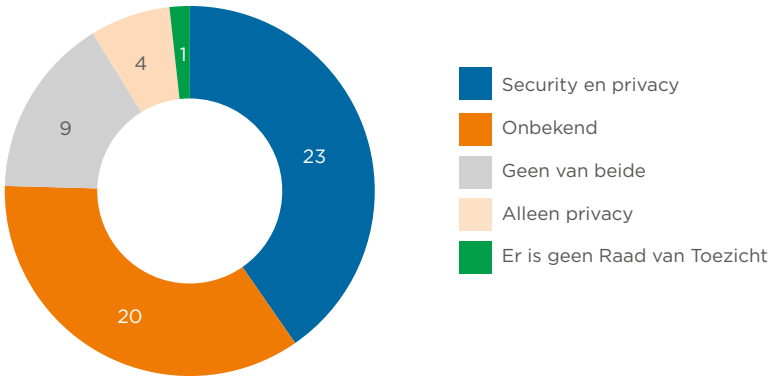
Figuur 6 laat zien bij hoeveel instellingen het bestuur periodiek rapportages ontvangt over de staat van informatieveiligheid inclusief de bescherming van persoonsgegevens:



Figuur 6: Periodieke rapportage aan het bestuur

Hieruit blijkt dat de meeste instellingen over zowel beveiligings- als privacy-incidenten aan het bestuur rapporteren. Anderzijds rapporteert 12% van de instellingen helemaal niet periodiek aan het bestuur.

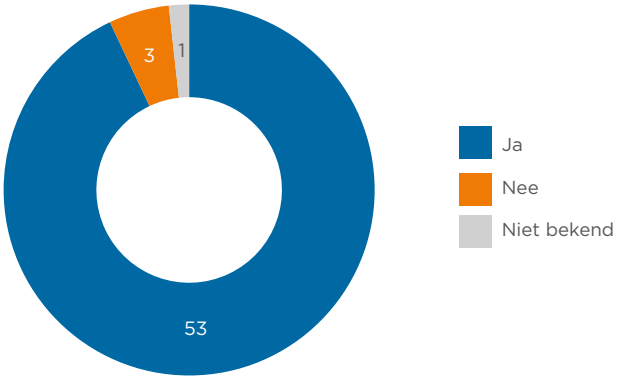
Bij de vraag of instellingen aan de raad van toezicht rapporteren, weet een flink aantal respondenten niet of dit het geval is:



Figuur 7: Periodieke rapportage aan de raad van toezicht

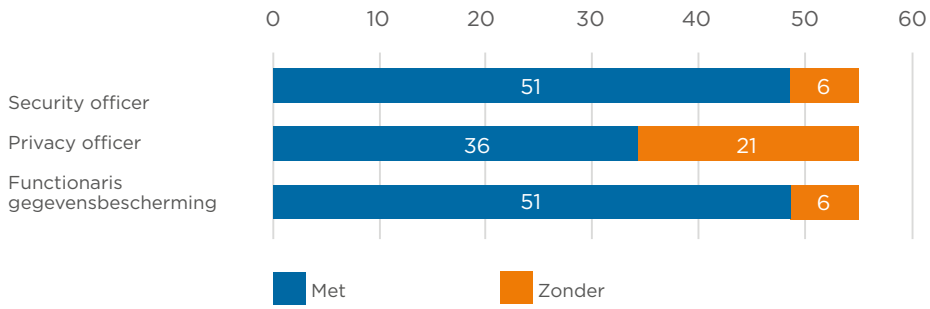
Wanneer dat wel bekend is, wordt in de meeste gevallen over zowel de staat van informatieveiligheid als die van bescherming van persoonsgegevens gerapporteerd, net als bij rapportages aan het bestuur.

Wanneer er sprake is van een ernstig incident wordt bij de meerderheid van de instellingen het bestuur direct ingelicht:



Figuur 8: Instellingen die incident direct melden aan het bestuur

Een groot deel van de instellingen heeft zowel een security officer als een functionaris gegevensbescherming, ruim 20% heeft daarbij ook nog een privacy officer:

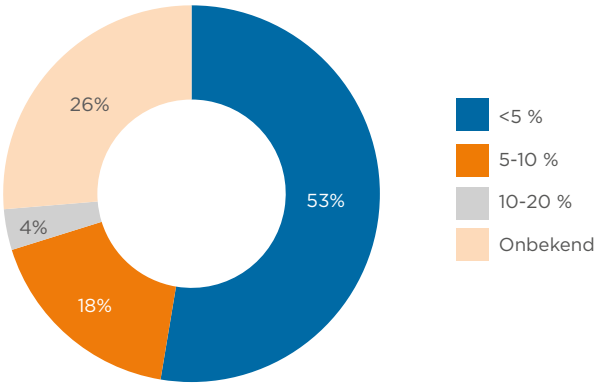


Figuur 9: Functionarissen bij de instellingen

Van de instellingen die geen privacy officer hebben is meer dan de helft een mbo-instelling.

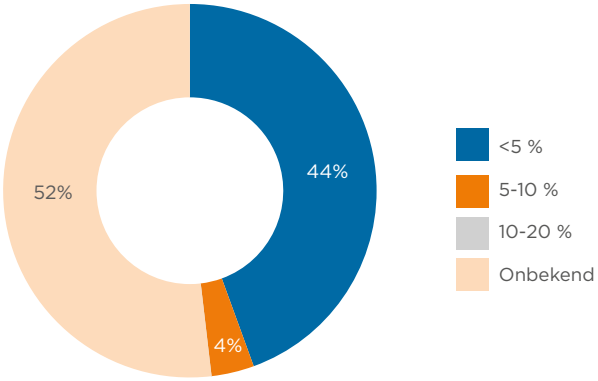
Beschikbaarheid middelen[11]

Een ander aspect is de beschikbaarheid van middelen. Bij meer dan de helft van de instellingen wordt minder dan 5% van het IT-budget besteed aan informatiebeveiligingsmaatregelen:



Figuur 10: Percentage van het IT-budget dat beschikbaar is voor informatiebeveiliging en privacy (2019)

Meest opvallend is de halvering van het percentage 'onbekend' ten opzichte van 2018 (zie Figuur 11). Verder lijkt er in z'n geheel meer van het beschikbare budget aan informatiebeveiliging en privacy te worden besteed.



Figuur 11: Percentage van het IT-budget dat beschikbaar is voor informatiebeveiliging en privacy (2018)

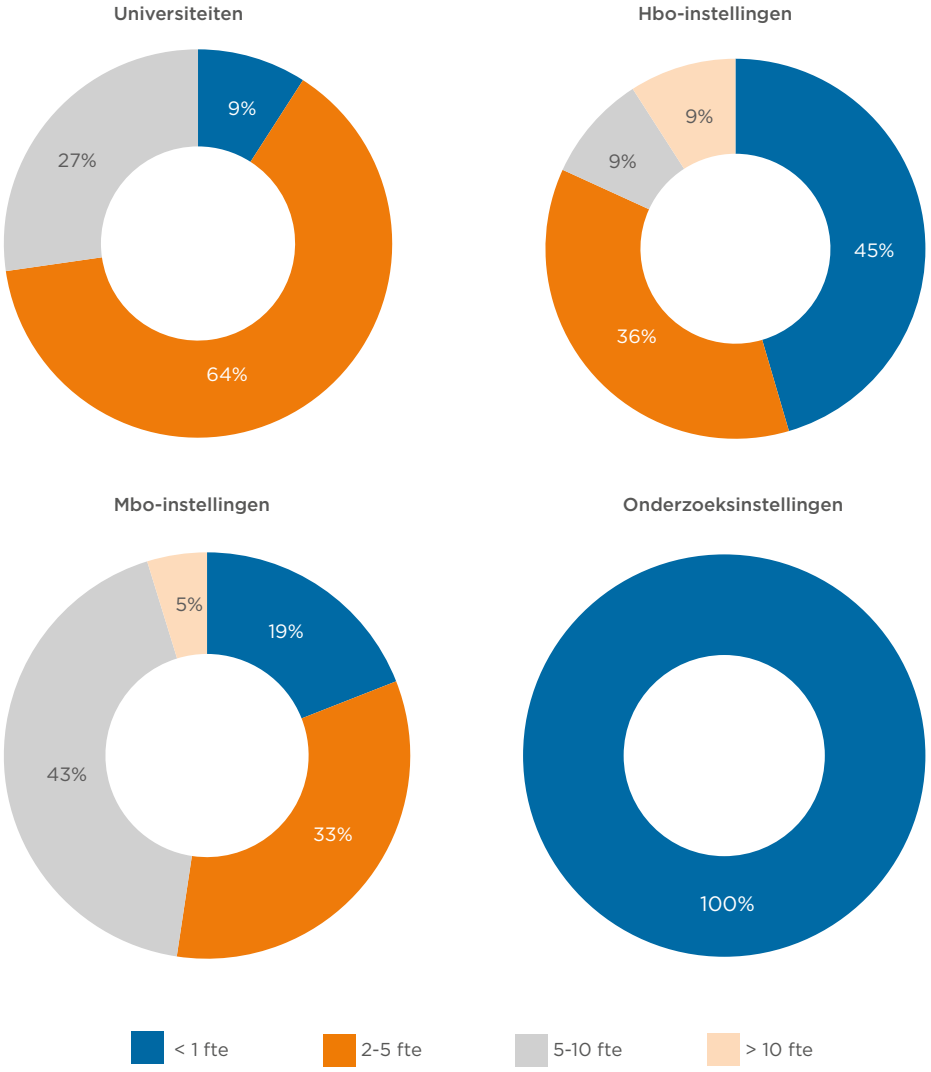
Wanneer we de instellingen naar grootte indelen, blijkt er een relatie te zijn met het aantal fte's dat beschikbaar is voor informatiebeveiliging en privacy:

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 3: fte's naar grootte van de instelling

[11] *Deze gegevens zijn geen officiële data, maar door de respondenten opgegeven schattingen, zowel voor 2019 als 2018.*

Kijken we naar de verdeling van fte's bij het type instelling, dan valt op dat bij alle onderzoeksinstellingen minder dan 1 fte beschikbaar is voor informatiebeveiliging. Verder heeft 45% van de hbo-instellingen minder dan 1 fte beschikbaar, de overige hbo-instellingen hebben meer dan 2 (de meeste 2-5) fte beschikbaar. De meerderheid van universiteiten en mbo-instellingen heeft 2-5 fte beschikbaar voor informatiebeveiliging:

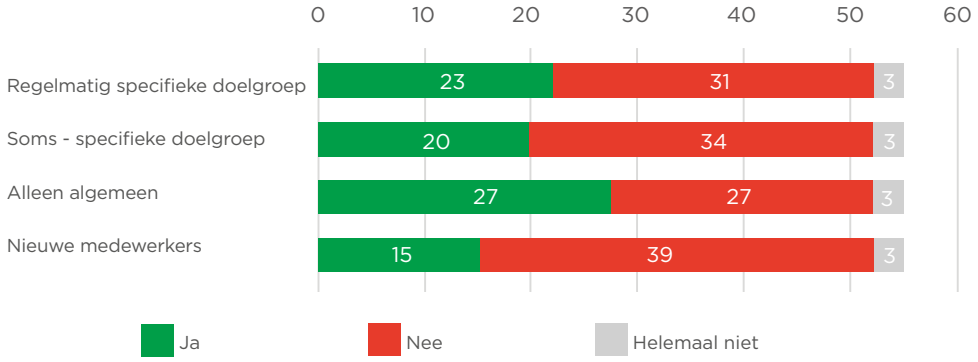


Figuur 12: Aantallen fte's die beschikbaar zijn voor informatiebeveiliging

Awareness

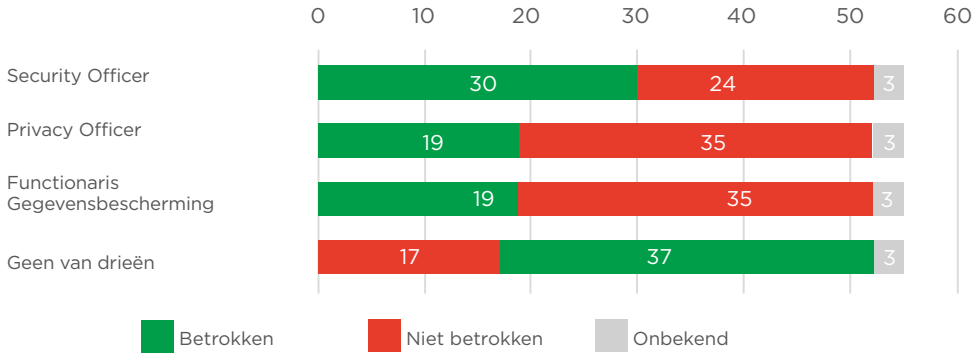
Met de term awareness geven we aan in hoeverre mensen zich bewust zijn van cyberdreigingen en weten wat ze moeten doen om cyberrisico's te verminderen. Dat geldt niet alleen voor 'gewone' gebruikers, zoals medewerkers en studenten (die bijvoorbeeld weten dat ze niet zomaar een link in een e-mail van een onbekende moeten aanklikken). Awareness is ook van toepassing op projecten waarbij bijvoorbeeld security- of privacy-by-design principes worden toegepast, of projecten waar de security officer en de privacy officer vanaf het begin bij betrokken worden.

In veel gevallen krijgen nieuwe medewerkers, docenten en onderzoekers bij het in dienst treden geen awareness-training, terwijl bij minder dan de helft van de instellingen structureel algemene of op specifieke groepen gerichte awareness-trainingen plaats vinden:



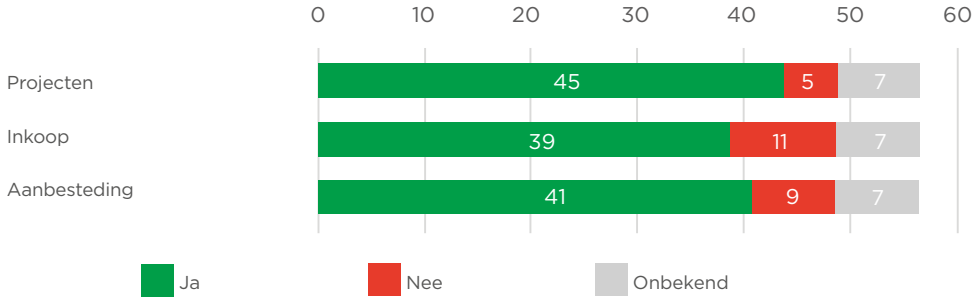
Figuur 13: Awareness-campagnes

De betrokkenheid van functionarissen bij projecten, inkoop en aanbestedingen is als volgt:



Figuur 14: Betrokkenheid functionarissen

Privacy-by-design en security-by-design zijn belangrijke principes om te hanteren in projecten, bij inkoop en bij aanbestedingen voor hardware, software en clouddiensten. Op de vraag of er regelmatig aandacht wordt besteed aan informatieveiligheid en privacy werd als volgt geantwoord:

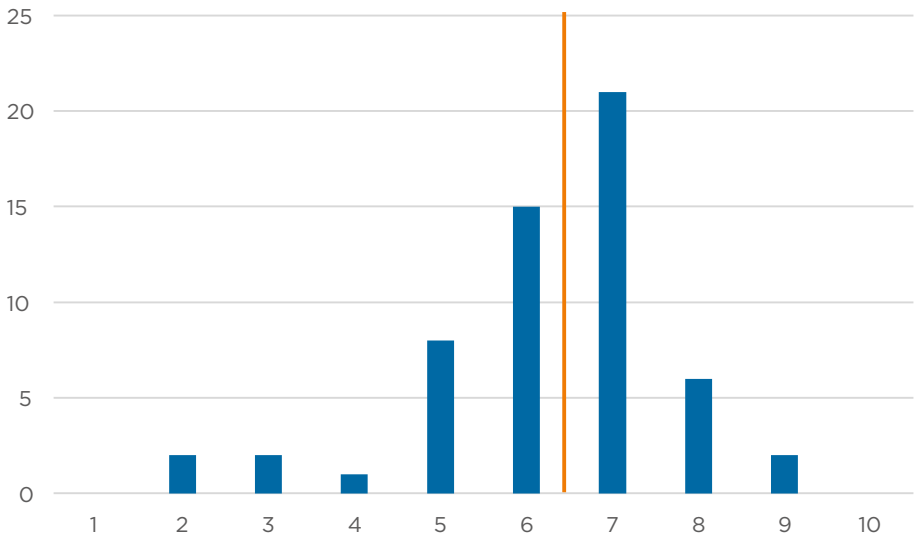


Figuur 15: Aandacht voor informatiebeveiliging en privacy

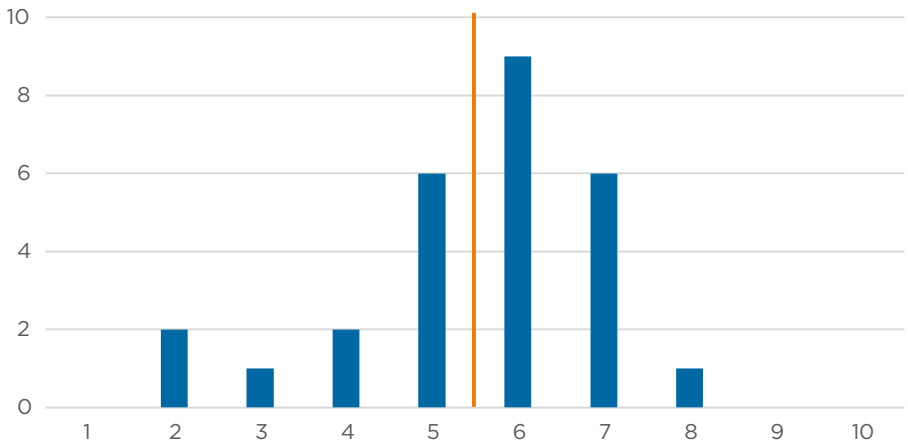
Bij veel instellingen is er dus aandacht voor informatiebeveiliging en bescherming van persoonsgegevens bij projecten, inkoop en aanbestedingen. Bij 7 instellingen (ca. 12%) is dit niet bekend bij de respondent of aangegeven.

Cyberweerbaarheid

Wanneer een instelling in hoge mate cyberweerbaar is, is ze in staat om beveiligingsincidenten te voorkomen en snel te herstellen van incidenten die zich toch voordoen. Instellingen geven zichzelf gemiddeld een 6,3 (op een schaal van 1 – 10), wat duidelijk hoger is dan in 2018 (gemiddeld 5,5).

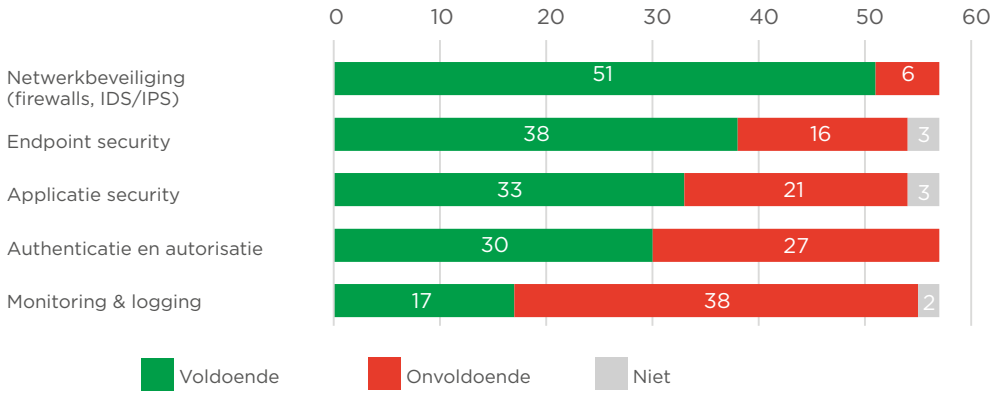


Figuur 16: Cyberweerbaarheid van instellingen 2019, eigen inschatting (schaal van 1 – 10, gemiddelde 6,3)

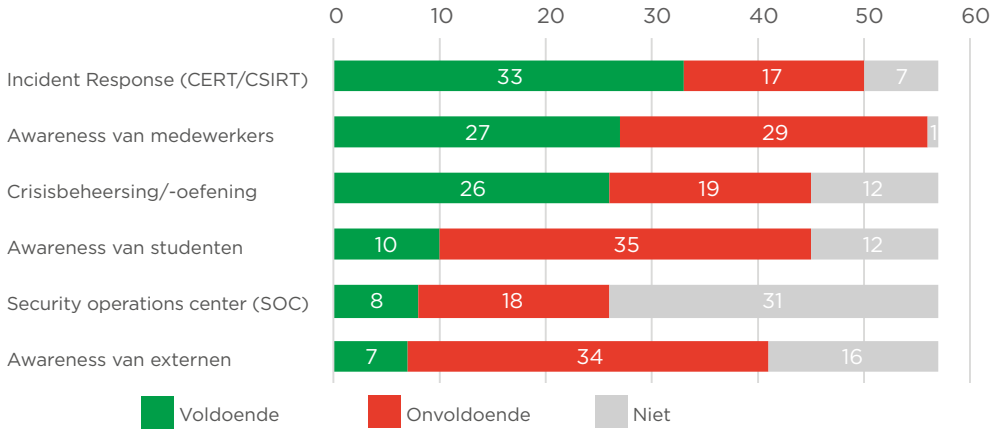


Figuur 17: Cyberweerbaarheid van instellingen 2018, eigen inschatting (schaal van 1 – 10, gemiddelde 5,5)

Om verder in kaart te brengen hoe weerbaar instellingen denken te zijn, hebben we ook een aantal vragen gesteld over investering in diverse maatregelen en de effectiviteit ervan.



Figuur 18: Mate van investering in beveiligingsmaatregelen (technisch)



Figuur 19: Mate van investering in beveiligingsmaatregelen (niet-technisch)

Het diagram in Figuur 18 illustreert dat volgens de meeste respondenten in operationele security zoals *Netwerkbeveiliging* en *Endpoint Security* voldoende wordt geïnvesteerd, met uitzondering van *Monitoring en logging*. In 'zachtere' maatregelen zoals *Awareness van medewerkers*, maar ook een *Security operations center* (SOC), wordt onvoldoende of helemaal niet geïnvesteerd (Figuur 19).

Uit de survey blijkt dat sommige maatregelen als effectiever worden gezien dan andere. Het meest effectief zijn maatregelen in de categorie *Authenticatie en autorisatie* gevolgd door maatregelen in de categorie *Awareness van medewerkers*. Het minst effectief zijn volgens de survey maatregelen in de categorie *Monitoring en logging*, terwijl in die categorie volgens de meeste respondenten ook onvoldoende wordt geïnvesteerd (67%) (Zie Figuur 18).

Over de effectiviteit van maatregelen op het vlak van *Awareness van medewerkers* denken de respondenten verschillend. Ruim 50% denk dat die effectief zijn (meest of redelijk effectief), terwijl bijna 25% van mening is dat die niet effectief zijn (minst of minder effectief dan gemiddeld).

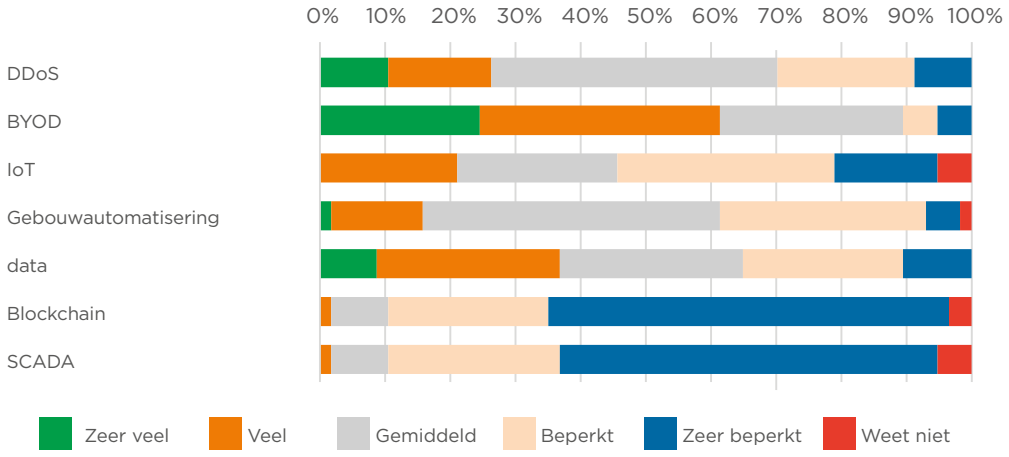
Aandacht voor trends

Om weerbaar te zijn is het belangrijk naar de toekomst te kijken, zodat je tijdig kunt inspelen op trends en ontwikkelingen. Voor de ICT-trends die impact kunnen hebben op informatieveiligheid uit 2018 is wisselende aandacht. In het algemeen is de aandacht voor deze trends in 2019 hetzelfde als in 2018.

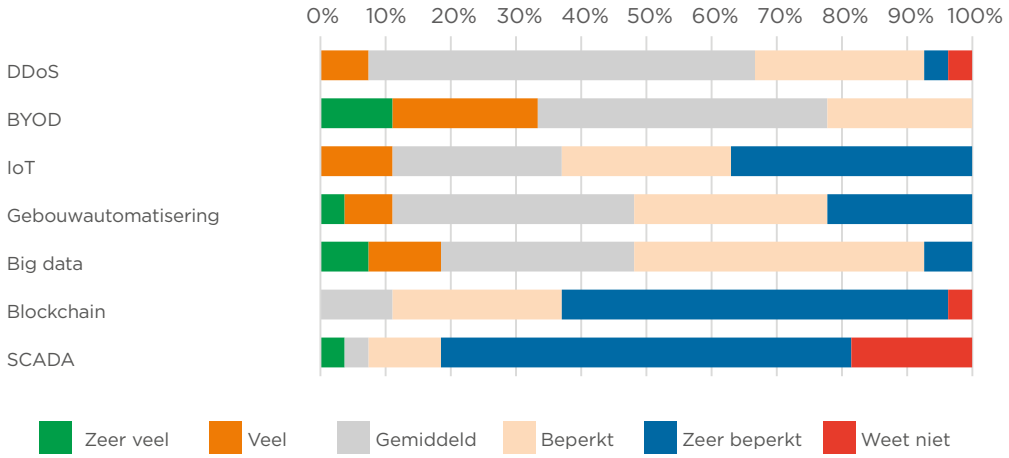
Enkele opvallende verschillen in trends en aandacht voor trends zijn (zie Figuur 20 en 21):

Trend	2018	2019
BYOD	66% zeer veel – gemiddeld	Toegenomen tot bijna 90%
Gebouwautomatisering	48% zeer veel – gemiddeld	Toegenomen tot ruim 60%
Big Data	48% zeer veel – gemiddeld	Toegenomen tot 65%
SCADA	19% weet niet	Afgenomen tot 5%

Tabel 4: Verschillen in aandacht voor ICT-trends 2018/2019



Figuur 20: Aandacht voor ICT-trends (2019)



Figuur 21: Aandacht voor ICT-trends (2018)

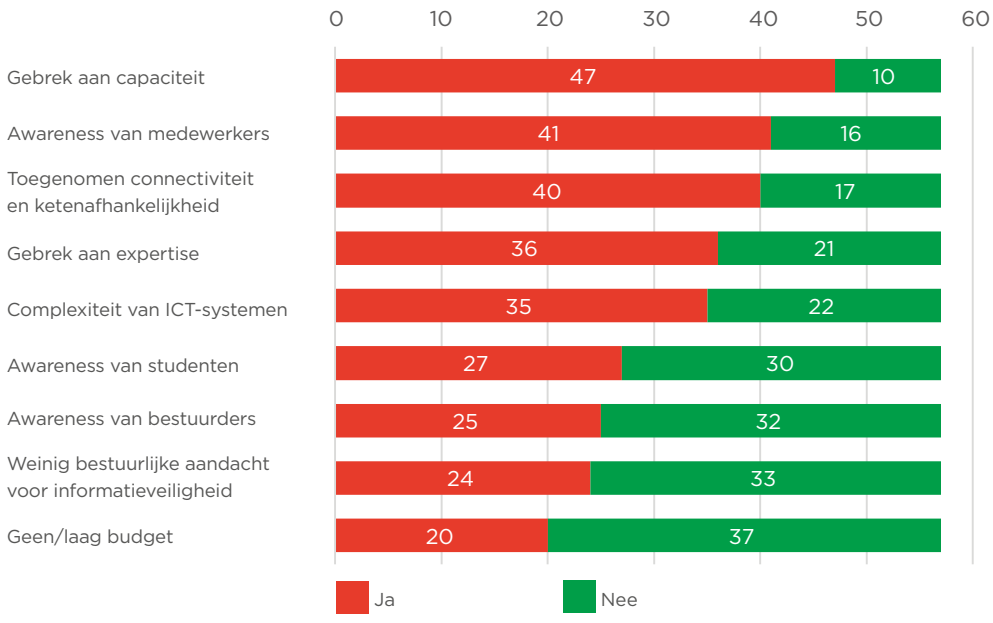
Kwetsbaarheden

Kwetsbaarheden bestaan in twee soorten: technische kwetsbaarheden en niet-technische kwetsbaarheden. Onder technische kwetsbaarheden verstaan we technische problemen die voorkomen in ICT-systemen (hardware en software). Een organisatie kan technische kwetsbaarheden in kaart brengen door kwetsbaarhedenscans (ook vulnerability scans genoemd) of penetratietesten op systemen uit te voeren. Daarnaast zijn er derde partijen die kwetsbaarheden in kaart brengen en daarover rapporteren. Wanneer een kwetsbaarheid bekend is moet de leverancier van het product een update van het product of een zogenaamde patch leveren.

Bij het oplossen van technische kwetsbaarheden spelen twee aspecten: allereerst gaat er tijd overheen voordat een update of patch beschikbaar is én gaat er tijd overheen voordat de update of patch is uitgevoerd. Ten tweede is er sprake van zogenaamde zero-day kwetsbaarheden. Dit zijn kwetsbaarheden die nog niet bekend zijn bij de leverancier. De leverancier kan dan geen update of patch maken en kwaadwillenden kunnen de zero-day kwetsbaarheid misbruiken (zero-day exploit), omdat er nog geen bescherming voor is.

Onder niet-technische kwetsbaarheden verstaan we problemen die zich voordoen doordat de organisatie of een proces in de organisatie, zodanig is opgezet dat misbruik mogelijk is. Niet-technische kwetsbaarheden zijn veel moeilijker op te lossen. Gebrek aan security awareness en te weinig capaciteit voor informatieveiligheid zijn niet-technische kwetsbaarheden in een organisatie. Weinig bestuurlijke aandacht voor informatieveiligheid, inclusief bescherming van persoonsgegevens, is een andere.

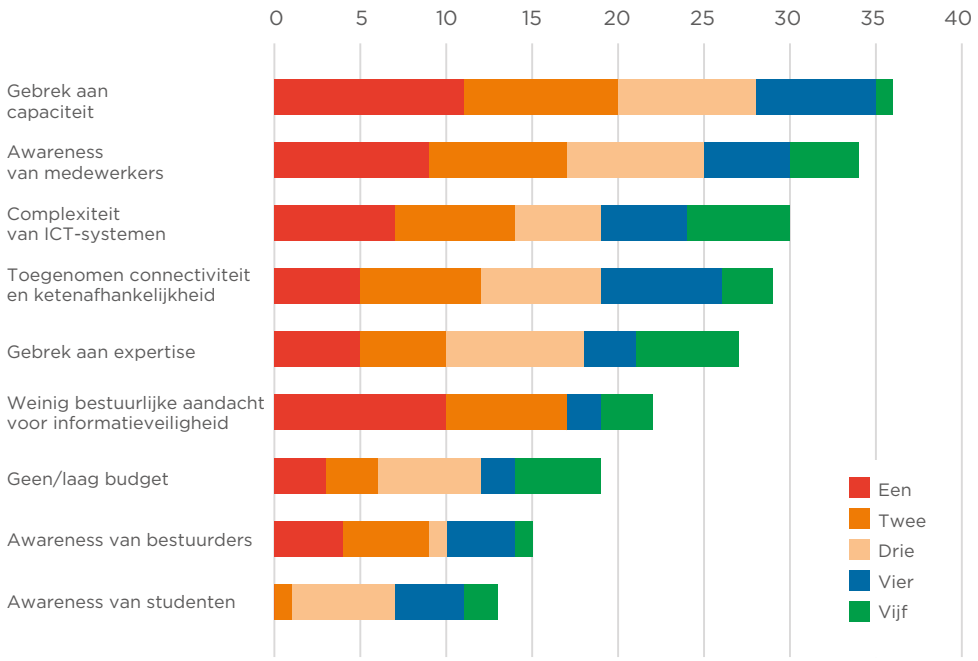
Op de vraag welke kwetsbaarheden voorkwamen in de organisatie scoren *Gebrek aan capaciteit*, *awareness van medewerkers* en *toegenomen connectiviteit en ketenafhankelijkheid* hoog.



Figuur 22: Kwetsbaarheden in de organisatie

In Figuur 23 geven respondenten antwoord op de vraag welke 5 kwetsbaarheden het meest relevant zijn bij instellingen.

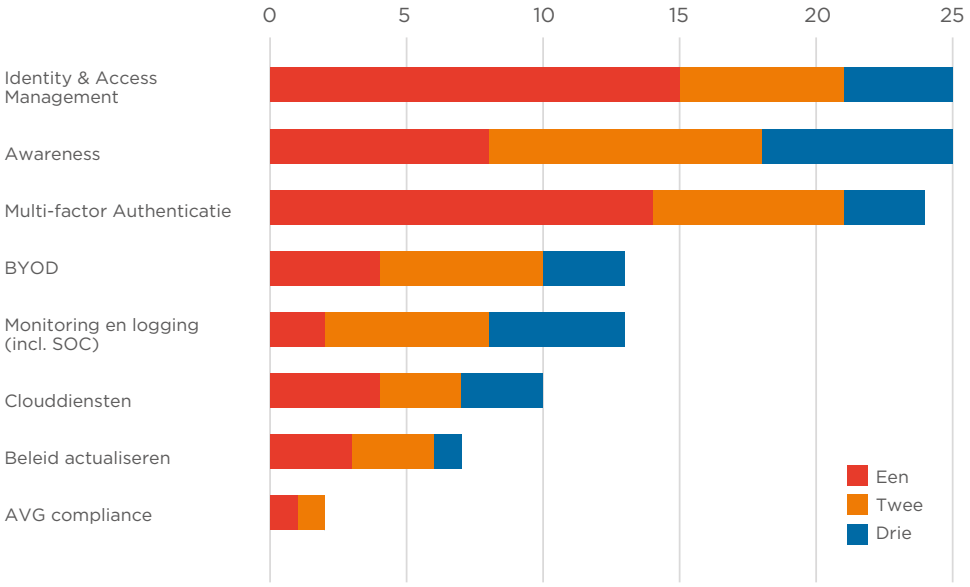
Kijkend naar de totaalscores is duidelijk te zien dat *Gebrek aan capaciteit* en *Awareness van medewerkers* er uit springen, terwijl ook *Complexiteit van ICT-systemen* en *Toegenomen connectiviteit* en *ketenafhankelijkheid* hoog scoren. *Gebrek aan capaciteit* en *Weinig bestuurlijke aandacht voor informatieveiligheid* scoren het meest als nummer 1 kwetsbaarheid. In dat kader is ook opvallend dat *Awareness van bestuurders* hoog scoort.



Figuur 23: Kwetsbaarheden in de organisatie (top 5)

Budget 2020

Vervolgens is dan de vraag wat de verhouding is tussen gesignaleerde kwetsbaarheden en wat er in het budget is opgenomen. Uit de beantwoording[12] blijkt dat *Identity* en *Access Management* (beide), *Awareness* (niet-technisch) en *Multi-factor authenticatie* (technisch) in veel gevallen zijn opgenomen in het budget. Verder valt op dat *AVG-compliance* weinig voorkomt. Er is dus geen sterke link tussen kwetsbaarheden en wat er in het budget is opgenomen. Alleen *Awareness* wordt expliciet genoemd.



Figuur 24: Activiteiten die zijn opgenomen in budget 2020

[12] *Ook hier konden de respondenten zelf invullen wat in het budget was opgenomen en hebben we dat voor het overzicht in categorieën ondergebracht.*

Incidenten, risico's en actoren

In de survey hebben we gevraagd naar aantallen incidenten en naar een inschatting van het risico dat instellingen lopen op de zeven risicocategorieën. Deze zeven risicocategorieën zijn in voorgaande jaren gebruikt om risico's die onderwijs- en onderzoeksinstellingen lopen te groeperen (zie bijlage 1 voor meer detail):

- Verkrijging en openbaarmaking van informatie
- Identiteitsfraude
- Verstoring ICT
- Manipulatie van data
- Spionage
- Overname en misbruik ICT
- Bewust beschadigen imago

	Onderwijs (47)	
	aantal	impact
1. Verkrijging en openbaarmaking van data		1,9
2. Identiteitsfraude		2,3
3. Verstoring van ICT-voorzieningen		2,7
4. Manipulatie van digitaal opgeslagen data		3,0
5. Spionage		2,5
6. Overname en misbruik van ICT-voorzieningen		1,8
7. Bewust beschadigen van imago		1,0

	Onderzoek (26)	
	aantal	impact
1. Verkrijging en openbaarmaking van data		3,0
2. Identiteitsfraude		3,0
3. Verstoring van ICT-voorzieningen		3,2
4. Manipulatie van digitaal opgeslagen data		-
5. Spionage		2,0
6. Overname en misbruik van ICT-voorzieningen		2,0
7. Bewust beschadigen van imago		0

	Bedrijfsvoering (57)	
	aantal	impact
1. Verkrijging en openbaarmaking van data		2,0
2. Identiteitsfraude		2,5
3. Verstoring van ICT-voorzieningen		2,5
4. Manipulatie van digitaal opgeslagen data		2,3
5. Spionage		-
6. Overname en misbruik van ICT-voorzieningen		2,6
7. Bewust beschadigen van imago		3,0

Veel (gewogen aantal * impact > 8) Gemiddeld (gewogen aantal * impact tussen 3 en 8)
Weinig (gewogen aantal * impact < 3) Niet voorgekomen

Tabel 5: Incidenten en hun gemiddelde impact (tussen haakjes aantal respondenten per proces)

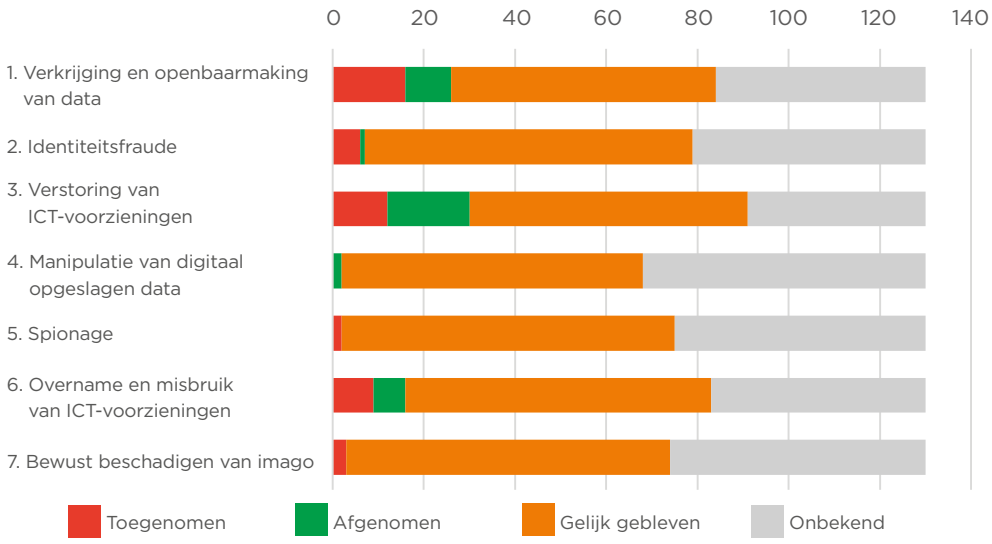
In Tabel 5 staan per dreiging de geschatte[13] hoeveelheid incidenten (veel, gemiddeld of weinig) in de zeven categorieën met hun gemiddelde impact. Voor impact gebruiken we een schaal van 1 – 5 (weinig tot veel), voor aantallen incidenten de kleuren in de legenda. Rood omkaderd zijn de hogere aantallen incidenten in een proces met hun impact. De resultaten zijn uitgesplitst voor onderwijs, onderzoek en bedrijfsvoering.

[13] *Niet alle incidenten worden gemeld en niet alle respondenten zijn even zeker van de betrouwbaarheid van de opgegeven aantallen*

Wat opvalt:

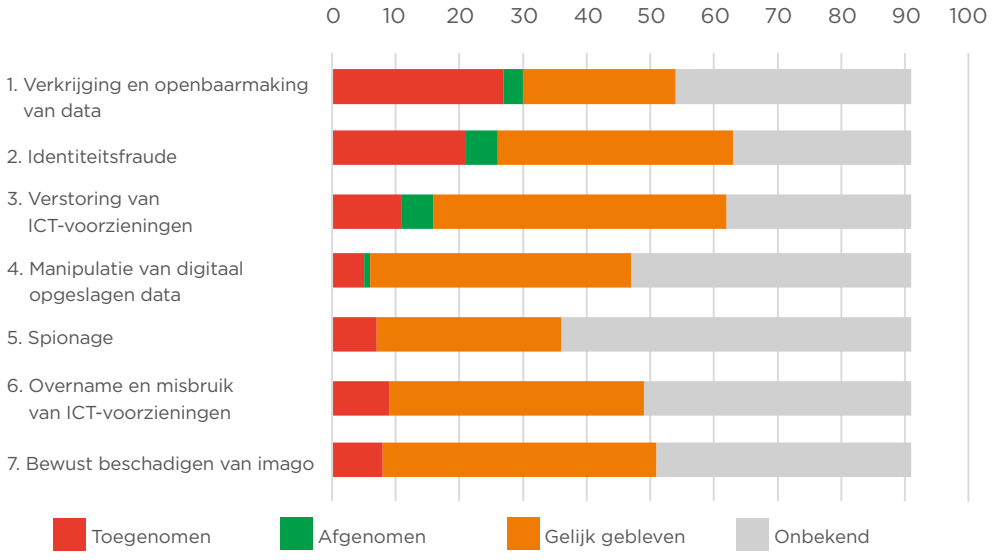
- high-impact incidenten (gemiddelde impact 2,5 of hoger) met betrekking tot *Verstoring van ICT-voorzieningen* komen voor bij onderwijs, onderzoek én bedrijfsvoering.
- relatief veel incidenten op het gebied van *Identiteitsfraude* komen voor bij onderwijs met een iets lagere gemiddelde impact.
- het lage aantal incidenten voor *spionage* bij alle drie de processen.
- het lage aantal incidenten met betrekking tot *bewust beschadigen van imago* bij alle drie de sectoren.
- bij de sector onderzoek komt alleen een significant aantal incidenten op het gebied van *verstoring van ICT-voorzieningen* voor.

Kijken we naar de dynamiek van incidenten dan zien we een beeld dat in grote lijnen overeenkomt met het beeld in 2018 (zie Figuur 25), maar ten opzichte van 2018 is de toename van het aantal incidenten wel iets minder geworden:



Figuur 25: Toename en afname van incidenten (2019 ten opzichte van 2018)

Kennelijk zijn er geen grote veranderingen in aantallen incidenten waargenomen in 2019, of het is niet bekend. Het percentage onbekend blijft vrij hoog.



Figuur 26: Toename en afname incidenten (2018 ten opzichte van 2017)

Risicoperceptie

Voor het bepalen van het risico gebruiken we het product van de kans op schade en de gevolgen van de schade: risico = kans * impact. Kans en impact zijn ingeschat door de respondenten en voor de tabellen gemiddeld.

In Tabel 6 staan de kans, impact en het berekende risico opgesplitst naar onderwijs, onderzoek en bedrijfsvoering. Deze tabel komt slechts ten dele overeen met de incidenten die zijn opgetreden in 2019 (zie Tabel 5). Er waren bij de sector onderwijs bijvoorbeeld slechts 4 incidenten bij risico 7. *Bewust beschadigen van imago* met een lage gemiddelde impact, maar toch wordt het risico daarop vrij hoog ingeschat. Anderzijds komen de aantallen incidenten bij risico 3. *Verstoring van ICT-voorzieningen* en de risico-inschatting daarvoor wel overeen bij onderwijs en bedrijfsvoering, maar weer niet bij onderzoek.

In het algemeen is de gemiddelde impact (schaal 1 – 5) bij de risico-inschatting aanmerkelijk hoger dan de waargenomen impact bij incidenten. Uitzonderingen daarop zijn risico 5. *Spionage* bij de sector onderwijs, en risico 2. *Identiteitsfraude* en risico 3. *Verstoring van ICT-voorzieningen* bij de sector onderzoek, waarvan de risico-inschatting hoger is dan de waargenomen impact bij de incidenten.

De kans-inschatting (schaal 1 – 5) komt grotendeels overeen met de aantallen incidenten per risico.

- Risico 1. *Verkrijging en openbaarmaking* van data en risico 3. *Verstoring van ICT- systemen* scoren hoog en hadden ook veel incidenten.
- Risico 2. *Identiteitsfraude* en risico 4. *Overname en misbruik van ICT-voorzieningen* scoren redelijk hoog en incidenten komen ook vrij veel voor.
- Risico 5. *Spionage* en risico 7. *Bewust beschadigen van imago* scoren laag en kwamen ook vrij weinig voor.

	Onderwijs (47)		
	kans (1-5)	impact (1-5)	risico
1. Verkrijging en openbaarmaking van data	2,7	3,3	8,8
2. Identiteitsfraude	2,5	3,0	7,4
3. Verstoring van ICT-voorzieningen	2,6	3,5	9,2
4. Manipulatie van digitaal opgeslagen data	2,1	3,6	7,3
5. Spionage	1,3	1,9	2,4
6. Overname en misbruik van ICT-voorzieningen	2,3	3,1	7,2
7. Bewust beschadigen van imago	2,0	3,8	7,5

	Onderzoek (26)		
	kans (1-5)	impact (1-5)	risico
1. Verkrijging en openbaarmaking van data	2,7	3,3	8,8
2. Identiteitsfraude	2,4	2,7	6,6
3. Verstoring van ICT-voorzieningen	2,7	2,8	7,3
4. Manipulatie van digitaal opgeslagen data	1,8	3,8	7,1
5. Spionage	2,4	3,0	7,3
6. Overname en misbruik van ICT-voorzieningen	2,7	2,8	7,3
7. Bewust beschadigen van imago	2,0	3,6	7,3

	Bedrijfsvoering (57)		
	kans (1-5)	impact (1-5)	risico
1. Verkrijging en openbaarmaking van data	2,4	3,4	8,2
2. Identiteitsfraude	2,3	3,2	7,3
3. Verstoring van ICT-voorzieningen	2,7	3,4	9,0
4. Manipulatie van digitaal opgeslagen data	1,9	3,5	6,7
5. Spionage	1,3	2,2	2,8
6. Overname en misbruik van ICT-voorzieningen	2,4	3,5	8,2
7. Bewust beschadigen van imago	1,7	3,6	6,1

Hoog risico Laag risico

Tabel 6: Risico-inschatting 2019

Actoren

In de sector onderwijs en onderzoek zijn verschillende actoren actief die gebruik maken van diverse technieken en middelen om misbruik te maken van kwetsbaarheden bij de instellingen. En actoren hebben een verscheidenheid aan motieven om actie te ondernemen. Studenten zijn bijvoorbeeld vooral geïnteresseerd in het manipuleren van resultaten, terwijl statelijke actoren meer geïnteresseerd zijn in het vergaren van innovaties die uit wetenschappelijk onderzoek kunnen voortkomen.

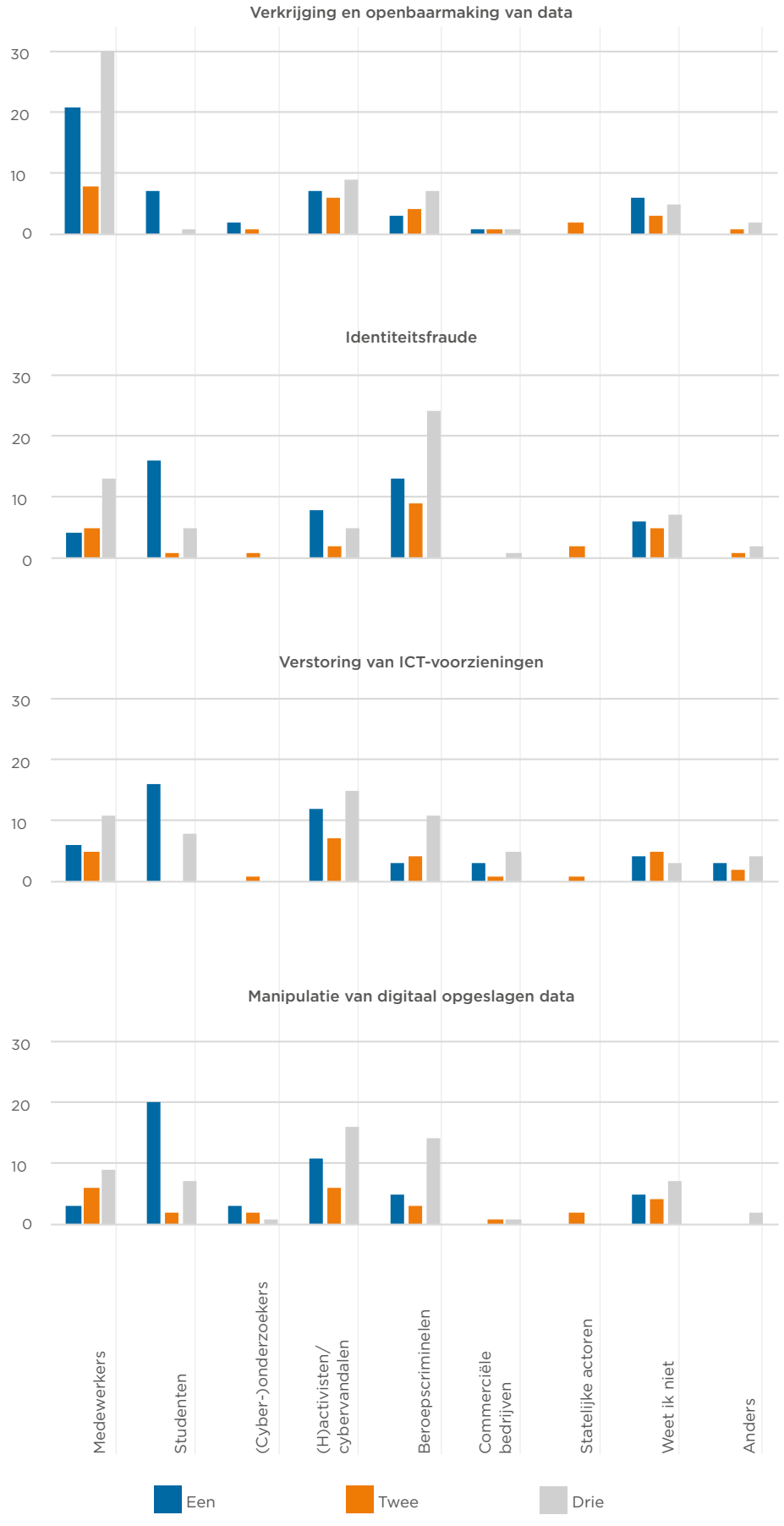
Actoren die geïdentificeerd zijn voor de sector onderwijs en onderzoek zijn (zie bijlage 2 voor meer detail):

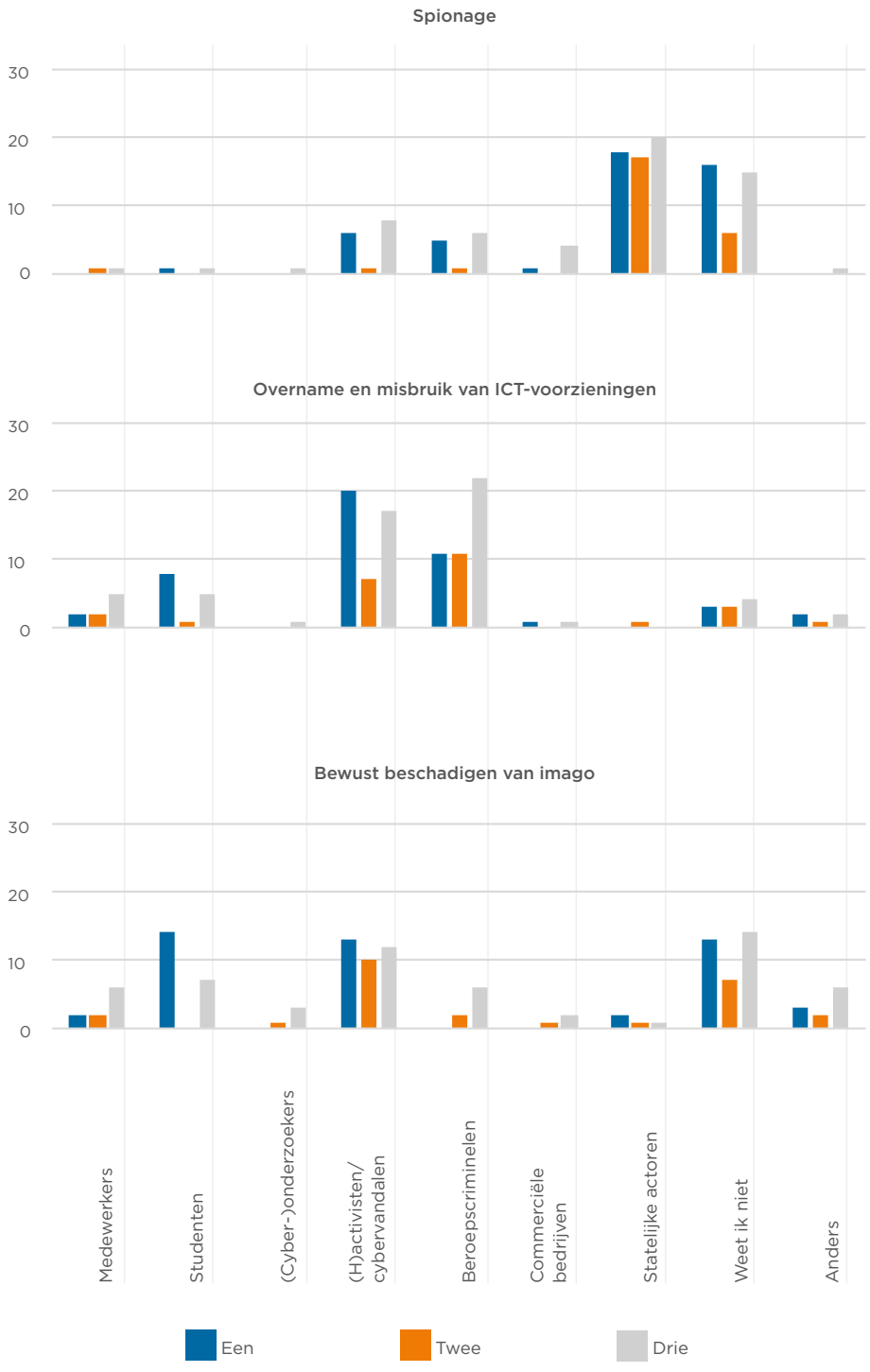
- Studenten
- Medewerkers
- Cybercriminelen
- Cyberonderzoekers
- Staten
- Commerciële bedrijven en partnerinstellingen
- Activisten
- Cybervandalen

In Tabel 7 staan de meest genoemde actoren per risico-categorie. In veel gevallen zijn de meest voorkomende actoren hetzelfde per proces (onderwijs, onderzoek en bedrijfsvoering). Bijvoorbeeld voor risico *Verkrijging en openbaarmaking van data* wordt medewerkers het meest genoemd als actor die, al dan niet opzettelijk, datalekken veroorzaken.

	Onderwijs	Onderzoek	Bedrijfsvoering
1. Verkrijging en openbaarmaking van data	Medewerkers	Medewerkers	Medewerkers
2. Identiteitsfraude	Studenten Beroepscriminelen	Beroepscriminelen	Medewerkers Beroepscriminelen
3. Verstoring van ICT-voorzieningen	Studenten Hactivisten/vandalen	Hactivisten/vandalen	Hactivisten/vandalen Beroepscriminelen Medewerkers
4. Manipulatie van digitaal opgeslagen data	Studenten	Medewerkers	Hactivisten/vandalen Beroepscriminelen
5. Spionage	Statelijke actoren Onbekend	Statelijke actoren	Statelijke actoren Onbekend
6. Overname en misbruik van ICT-voorzieningen	Hactivisten/vandalen	Beroepscriminelen	Beroepscriminelen
7. Bewust beschadigen van imago	Studenten Hactivisten/vandalen	Hactivisten/vandalen	Onbekend

Tabel 7: Top-actoren per dreiging/risico


Verkrijging en openbaarmaking van data
Identiteitsfraude
Verstoring van ICT-voorzieningen
Manipulatie van digitaal opgeslagen data
30
20
10
0
Medewerkers
Studenten
(Cyber-)onderzoekers
(H)activisten/ cybervandalen
Beroepscriminelen
Commerciële bedrijven
Statelijke actoren
Weet ik niet
Anders
Een
Twee
Drie



Figuur 27: Top actoren per dreiging/risicocategorie

3. TRENDS

Dit hoofdstuk geeft een overzicht van de belangrijkste cybersecurity-trends. Het is samengesteld op basis van de in het vorige hoofdstuk opgenomen survey én van trends uit genoemde publieke bronnen.

3.1 Belangrijkste 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.

3.2 Belangrijkste trends in andere sectoren

Cybercriminelen hebben onverminderd succes met beproefde en bewezen aanvals-technieken. Aanvalsmiddelen zijn eenvoudig te verkrijgen en laagdrempelig om in te zetten [2]. Daarnaast blijft het aantal geregistreerde kwetsbaarheden ook groeien. In 2019 werden 17.300 kwetsbaarheden aan de internationaal erkende CVE-database toegevoegd, ten opzichte van 16.300 in 2018. Deze sterke toename wordt met name toegeschreven aan de slechte beveiliging van IoT-apparaten [22].

Afhankelijkheid van een beperkt aantal aanbieders en landen [2]

Organisaties in zowel de publieke als de private sector maken in steeds toenemende mate gebruik van een kleine groep aanbieders van hard- en software, digitale diensten en platformen uit een beperkt aantal landen. Hoewel het vanwege technische mogelijkheden of de prijsprestatieverhouding aantrekkelijk kan zijn om van deze aanbieders gebruik te maken, kunnen onderbrekingen in de dienstverlening of compromittering leiden tot dataverlies of grote continuïteitsproblemen voor de afnemende organisaties. Daarnaast zijn de aanbieders gehouden aan andere wet- en regelgeving waardoor zij gedwongen kunnen worden om niet in het belang van hun afnemers te handelen. Dit kan ook het gevolg zijn geopolitieke conflicten.

De zorg over de hiervoor genoemde afhankelijkheden is ook uitgesproken door de rectores magnifici van de Nederlandse universiteiten [20].

Werkwijzen van cybercriminelen

De meest voorkomende werkwijzen van cybercriminelen zijn [2] [5]:

- **Gijzelingssoftware (ransomware)**
  Gijzelingssoftware is nog steeds de meest voorkomende vorm van kwaadaardige software; cybercriminelen lijken zich meer op grote organisaties te richten waar ze meer schade aanrichten en grotere bedragen vragen.
- **Website spoofing**
  Spoofing en defacing van legitieme websites blijven zich voordoen, hoewel de impact van dergelijke aanvallen minimaal is.
- **Phishing**
  Cybercriminelen maken veelvuldig gebruik van e-mail als een instrument voor het verspreiden van kwaadaardige software of voor phishing doeleinden waarbij er een toename is van spearphishing. Bij spearphishing bouwen criminelen zo veel mogelijk kennis op van één specifieke organisatie om deze vervolgens doelgericht aan te kunnen vallen.

- **Gestolen credentials**
  Veel inbreuken vinden plaats met gestolen login-informatie verkregen via phishing of brute-force aanvallen.
- **DDoS-aanvallen**
  Denial-of-service aanvallen zijn nog steeds een veelgebruikte methode om bedrijven mee aan te vallen. Hun aantal is toegenomen. In sommige gevallen is een DDoS-aanval ingezet als afleidingsmanoeuvre voor andere inbreuken.

Deze werkwijzen van cybercriminelen bestaan al langer, soms al een aantal jaren. Ze ontwikkelen zich echter in hoog tempo.

Werkwijzen die in 2019 manifester zijn gesignaleerd [2] [5]:
- Misbruik van leverancierskетens:
  Bedrijven en instellingen zijn door het gebruik van SaaS-/cloud-oplossingen en uitbesteding van (ondersteunende) processen in toenemende mate afhankelijk van andere partijen. Het ontbreekt dan vaak aan voldoende controle op en/of inzicht in de hele keten. Cybercriminelen maken hier gebruik van door te infiltreren in de zwakke schakels om door te dringen tot het eigenlijke doel.
  Er bestaan verschillende varianten van deze werkwijze:
  - Veel bedrijven en instellingen hebben onderdelen van hun ondersteunende processen uitbesteed. Denk bijvoorbeeld aan het beheer en onderhoud van gebouwautomatisering. Het monitoren en het beheer van deze installaties wordt door de onderhoudspartij veelal vanaf een externe locatie uitgevoerd. Minder goede beveiliging bij deze externe onderhoudsbedrijven en slechte of soms geen compartimentering hebben ertoe geleid dat cybercriminelen via deze weg toegang tot gegevens van bedrijven en instellingen hebben gekregen.
  - Veel bedrijven en instellingen maken voor een deel van hun geautomatiseerde processen gebruik van externe SaaS-/cloudapplicaties. Onvoldoende beveiliging van deze externe applicaties kan tot schade leiden. Een voorbeeld hiervan is het gebruik van een externe mailer die namens een bedrijf via de eigen mailsystemen mail kon versturen. Criminelen konden met behulp van deze externe mailer grote hoeveelheden phishingmail versturen die afkomstig leek van het bedrijf dat hiervan gebruik maakte.

- Aanvallen via sociale media, chat, sms [2] [12] [13]
  - Sociale media als Twitter en Facebook worden behalve voor het verspreiden van nepnieuws ook in toenemende mate misbruikt om malware te verspreiden.
  - Sociale media zijn voor cybercriminelen een vruchtbare bron voor social engineering.
  - Sms-phishing (SMiShing) en Voice-phishing (Vishing) zijn een uitbreiding op de al langer bestaande phishingtechnieken en worden succesvol toegepast.

- Misbruik van mobiele devices [14]
  Bij mobiele devices lopen zakelijk gebruik en privégebruik vaak door elkaar heen. Veelal prevaleert gebruiksgemak bij de inrichting van deze devices boven informatieveiligheid en hebben de organisaties onvoldoende zicht op de bedrijfsgegevens die zich op het device bevinden. Hierdoor kunnen deze bedrijfsgegevens makkelijk weglekken.

3.3 Actoren

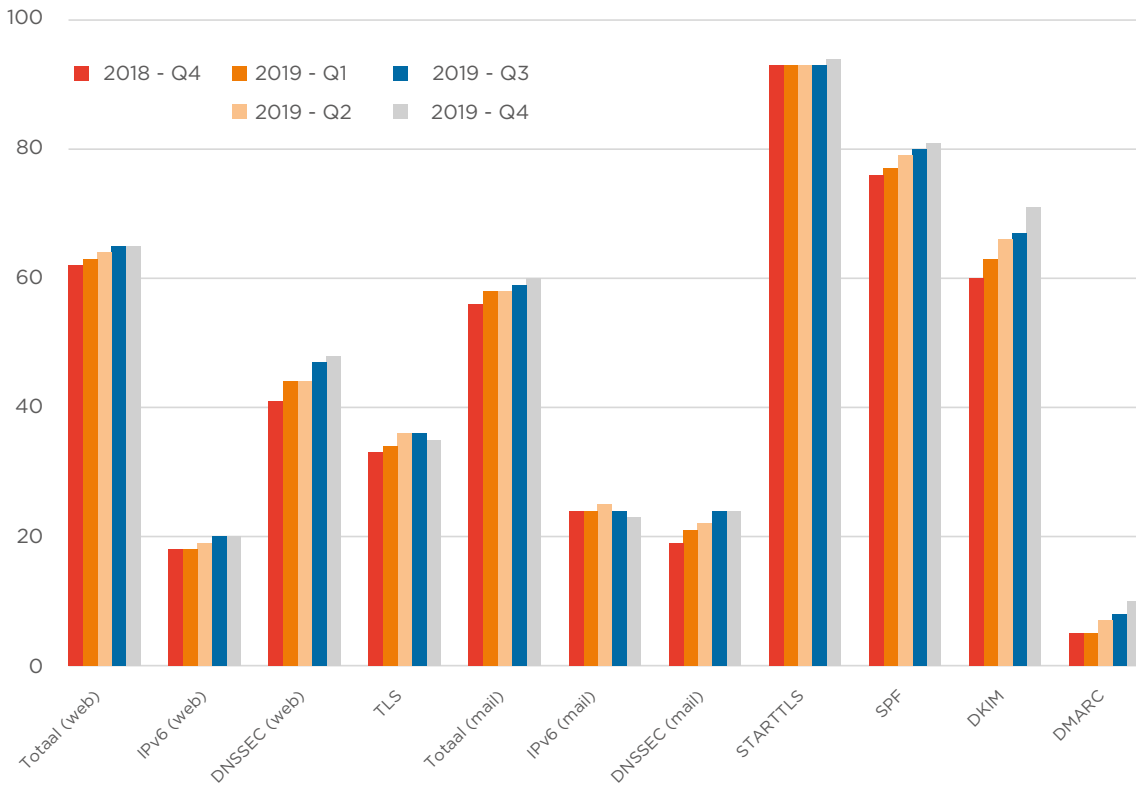
Als alle dreigingstypen worden samengevoegd dan laat onze survey zien (zie Figuur 27 op pagina 27 en 28) dat instellingen de eigen medewerkers als belangrijkste actoren zien, gevolgd door (h)activist/cybervandalen en beroepscriminelen. Dit beeld wijkt iets af van het landelijke beeld in het Cybersecuritybeeld Nederland 2019 [2] waarin vooral statelijke actoren en beroepscriminelen als voornaamste actoren worden genoemd.

Deze actoren worden door het Britse NCSC ook als belangrijkste actoren voor universiteiten genoemd [7]. Waarom deze situatie afwijkt van de cijfers uit de survey, vereist nader onderzoek.

3.4 Bij SURF waargenomen trends

Internet veiligheid-metingen

SURF doet al enkele jaren ieder kwartaal metingen om in kaart te brengen in hoeverre onderwijs- en onderzoeksinstellingen standaarden van Informatie Veiligheid hebben geïmplementeerd, de zogenaamde IV-metingen. De standaarden zijn opgesteld door het Forum voor Standaardisatie [19] en staan op de Pas Toe Of Leg Uit (PTOLU)-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). Onderstaande grafiek (Figuur 28) laat zien dat er in 2019 weer veel vooruitgang is geboekt.

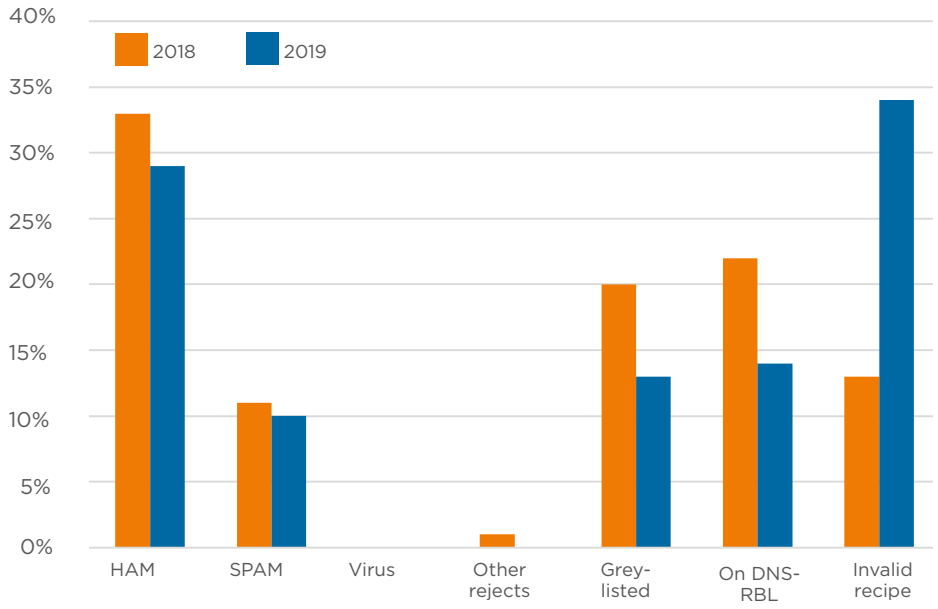


Figuur 28: IV-metingen

Figuur 28 laat zien dat in 2019 de resultaten van de IV-metingen een licht stijgende lijn vertonen, met uitzondering van IPv6-adoptie voor mailservers. De totaal scores zijn de gemiddelde scores van alle gemeten domeinen en mailservers bij Internet.nl. Verder zijn aparte metingen gedaan voor de adoptie van IPv6, het gebruik van DNSSEC, ondersteuning van TLS (voor webservers) en STARTTLS (voor mailservers) en gebruik van de mailstandaarden SPF, DKIM en DMARC (zie bijlage 3).

SURFmailfilter

SURFmailfilter is de anti-spam dienst die SURF aan de aangesloten instellingen aanbiedt. Circa 75% van de mbo-instellingen maken geen gebruik van SURFmailfilter, maar van Office 365, bij hbo-instellingen is dat bijna 60%. Onderzoeksinstellingen, universiteiten en de categorie 'overig' gebruiken SURFmailfilter of een eigen oplossing.

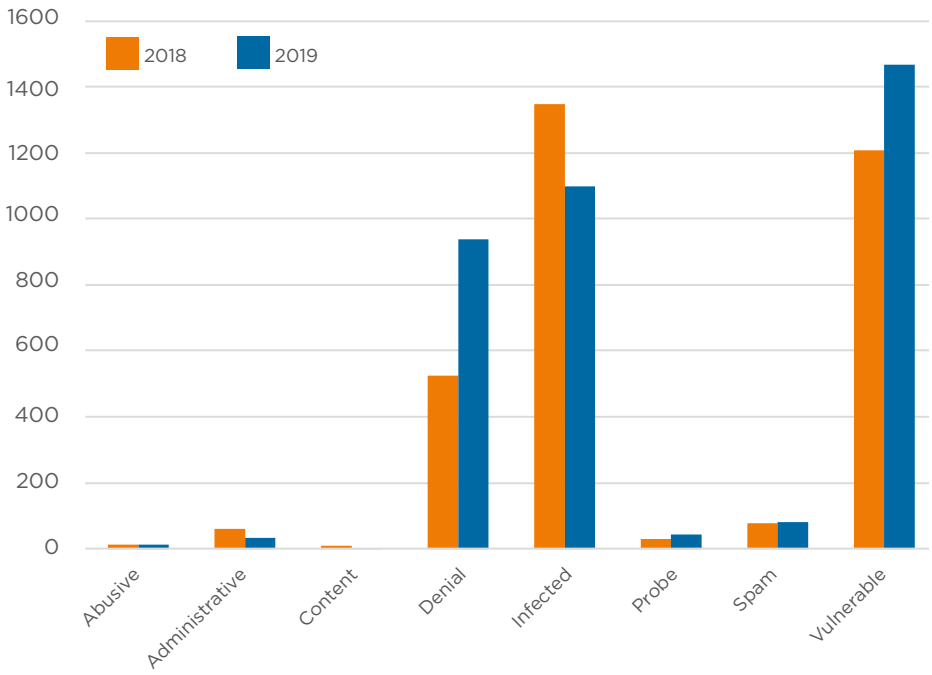


Figuur 29: SURFmailfilter statistieken 2018 en 2019.

Opvallend is de stijging van 'invalid recipients' (zie Bijlage 3) die ongeveer halverwege 2019 is begonnen. Hiervoor is geen verklaring anders dan de aanname dat spammers nu lijken te werken met namenlijsten en die combineren met domeinen en dan versturen om te zien wat er wordt geaccepteerd.

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. De verdeling van incidenten was in 2019 en 2018 als volgt (zie bijlage 4 voor de categorieën):



Figuur 30: SURFcert incidenten 2018 en 2019

Van de meest voorkomende incidenten is er een daling in 2019 ten opzichte van 2018 bij de categorie *Infected* (systemen die contact zoeken met IP-adressen waarvan bekend is dat geassocieerd zijn met malware – zie bijlage 4), terwijl de categorieën *Denial* (meldingen over systemen die betrokken zijn bij een DDoS-aanval) en *Vulnerable* (meldingen over systemen bij instellingen waarop bij SURFcert bekende kwetsbaarheden zijn gevonden) significant zijn toegenomen.

4. WEERBAARHEID

De digitale weerbaarheid van onderwijs- en onderzoekinstellingen is nog niet overal op voldoende niveau. Daarin staat de sector niet alleen. Uit de trends (hoofdstuk 3) blijkt dat andere sectoren ook nog stappen kunnen maken om hun weerbaarheid te vergroten. De toenemende complexiteit en connectiviteit van het ICT-landschap zet de weerbaarheid verder onder druk.

Investeringen in weerbaarheid

Uit de survey (zie Figuur 18 en Figuur 19) blijkt dat volgens de meeste respondenten in operationele security zoals *Netwerkbeveiliging* en *Incident response* voldoende wordt geïnvesteerd, met uitzondering van een *Security operations center* (SOC). Investeringen in *awareness* en *monitoring en logging* worden als onvoldoende beoordeeld.

Effectiviteit van maatregelen

Voor een effectieve weerbaarheid worden *Awareness van medewerkers* en maatregelen op het gebied van *Authenticatie en autorisatie* als meest effectief beschouwd. Opmerkelijk hierbij is dat *Monitoring en logging* als minder effectief wordt gezien, terwijl veel instellingen vinden dat er onvoldoende in wordt geïnvesteerd.

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.

Weerbaarheid verhogende maatregelen

In de survey worden voor 2020 *Identity en Access Management*, *Awareness en Multi-factor authenticatie* als belangrijkste maatregelen genoemd waarin wordt geïnvesteerd.

Cyberweerbaarheid overige sectoren

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. Ook de Algemene Rekenkamer rapporteert in haar verantwoordingsonderzoek over 2018 [15] dat de rijksoverheid de informatiebeveiliging niet op orde heeft.

Conclusie

Om risico's te verminderen is het absoluut noodzakelijk om de weerbaarheid te vergroten. Connectiviteit en complexiteit bij organisaties nemen nog steeds toe terwijl basale 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 belangrijkste instrument om deze dreigingen te bestrijden.

5. CONCLUSIES

Globaal gezien wijkt het Cyberdreigingsbeeld 2019/2020 onderwijs en onderzoek niet veel af van het rapport 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.

Bewustwording een 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

Door het nog steeds toenemend gebruik van cloudtoepassingen die door een klein aantal grote, niet-Europese 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. In verband met deze nieuwe werkelijkheid is het noodzakelijk om weerbaarheid van de organisatie op deze aspecten (opnieuw) te bezien:

- is de back-up van bedrijfskritische data ingericht en getest?
- is in geval van een ernstige calamiteit terugval mogelijk, eventueel naar analoge processen?
- zijn in het geval van multi-cloud alle ketenafhankelijkheden goed in beeld en zijn met alle partijen goede afspraken vastgelegd?
- is de sourcingstrategie nog up-to-date of moet deze worden bijgesteld?

Tot slot blijft ook de detectietijd achter bij de snelheid van aanvallen [2]. Volgens een rapport van FireEye [16] bedroeg in 2018 de tijd tussen het moment van inbraak op een systeem en het moment van ontdekking wereldwijd gemiddeld 78 dagen. Een rapport van Crowdstrike [17] signaleert dat aanvallers binnen enkele uren na initiële toegang al toegang tot andere delen van het bedrijfsnetwerk weten te verkrijgen. Het is dan ook noodzakelijk om weerbaarheidsmaatregelen te nemen waarmee dreigingen eerder kunnen worden gesignaleerd.

Hoge investeringen, hooggekwalificeerde expertise noodzakelijk

De hiervoor genoemde weerstand verhogende maatregelen vergen hoge investeringen. Budgetten voor informatiebeveiliging staan echter altijd onder druk. Dit gaat 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. Cijfers over de Nederlandse situatie zijn niet voorhanden, maar volgens een rapport van ISC2 uit 2017 [18] zullen er wereldwijd in 2022 1,8 miljoen openstaande vacatures op het gebied van cybersecurity zijn.

Nog meer samenwerken

Om de toenemende dreigingen het hoofd te bieden, is samenwerking cruciaal. In SURF-verband wordt er al veel samengewerkt en kennis gedeeld, bijvoorbeeld in community's als SCIPR en SCIRT[14], via de dienst SURFcert[15] en bij het Platform Integrale Veiligheid Hoger Onderwijs[16].

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.

[14] *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)*
[15] *Zie: https://www.surf.nl/en/surfcert-247-support-in-case-of-security-incidents*
[16] *Zie: https://www.integraalveilig-ho.nl/*

BIJLAGE 1
CYBERDREIGINGEN

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

#	Categorie	Manifestatie van dreiging	Beschrijving
1	Verkrijging en openbaarmaking van data	→ Onderzoeksgegevens worden gestolen	Gevoelige gegevens zoals persoonsgegevens, onderzoeksgegevens en intellectueel eigendom belanden op straat of komen in verkeerde handen.
		→ 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	Studenten kunnen zich voordoen als een andere student of medewerker om hun eigen studieresultaten te verbeteren of om ongeautoriseerd toegang te krijgen tot geheime informatie, bijvoorbeeld over toetsen.
		→ 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	DDoS aanvallen, malware en virussen zijn aan de orde van de dag, ook voor onderwijs- en onderzoeksinstellingen.
		→ 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 data, zoals het wijzigen van studieresultaten door studenten, kan de naam van de gehele instelling in het geding brengen, met ernstige reputatieschade tot (mogelijk) gevolg.
		→ Manipulatie van onderzoeksgegevens	
		→ Aanpassing van bedrijfsvoering data	
5	Spionage	→ Onderzoeksgegevens worden afgetapt	Buitenlandse overheden proberen gevoelige informatie te verkrijgen. Vooral onderzoeksinstellingen zijn een interessant doelwit door de aanwezige gevoelige onderzoeksgegevens over bijvoorbeeld nieuwe technologie.
		→ Via een derde partij wordt intellectueel eigendom gestolen	
		→ Controleren van buitenlandse studenten door staten	
6	Overname en misbruik ICT	→ Opstelling van onderzoeksinstellingen worden overgenomen	Onderwijs- en onderzoeksinstellingen hebben vaak toegankelijke ICT-systemen met veel rekenkracht. Deze systemen zijn een interessant doelwit voor overname en misbruik, bijvoorbeeld voor cryptomining of het uitvoeren van een DDoS-aanval.
		→ Systemen of accounts worden misbruikt voor andere doeleinden (botnet, mining, spam)	
7	Bewust beschadigen imago	→ Website wordt beklad	Verschillende actoren, waaronder activisten, willen de reputatie van instellingen beschadigen. Bijvoorbeeld door het bekladden van de website of het overnemen van social media-accounts.
		→ Socialmedia-account wordt gehackt	

Tabel 8: Risicocategorieën voor onderwijs en onderzoek.[17]

[17] *Bron: SURF Cyberdreigingsbeeld 2014 t/m 2018*

BIJLAGE 2
ACTOREN

#	Actor	Beschrijving
1	Studenten	Studenten hebben belang bij goede studievoortgang. Een manier om dat voor elkaar te krijgen is het aanpassen van studieresultaten. Ook hacking om status te verwerven kan een motivatie van studenten zijn. In potentie zijn studenten vaardige hackers, zeker als ze een technische opleiding volgen, en hebben ze al toegang tot applicaties en netwerken van de instelling.
2	Medewerkers	Medewerkers zijn gedreven door prestatiedrang. Die blijkt bijvoorbeeld uit vak-evaluaties die ze daarom positief willen beïnvloeden. Dreigend ontslag of een reorganisatie kan een medewerker ertoe brengen schade te veroorzaken. Net als studenten hebben medewerkers al toegang tot applicaties en netwerken van de instelling.
3	Cybercriminelen	Criminelen zijn vooral uit op financieel gewin. Ze stelen data om die te kunnen verkopen of ontoegankelijk te maken om vervolgens aan de instelling losgeld te vragen om weer toegang te krijgen.
4	Cyber-onderzoekers	Cyberonderzoekers zijn een groep hackers die als doel hebben om kwetsbaarheden te identificeren, vaak met goede bedoelingen (responsible disclosure).
5	Staten	Staten, vaak landen als China, Iran, Rusland en de Verenigde Staten, zijn geïnteresseerd in informatie die hun economische of politiek strategische positie ten opzichte van andere landen kan verbeteren. In onderzoeksinstellingen wordt ook onderzoek gedaan naar gevoelige en innovatieve technologieën die voordeel kunnen opleveren in zowel de fysieke als de digitale wereld. Staten beschikken over veel kennis en middelen om digitale aanvallen met succes uit te voeren.
6	Commerciële bedrijven en partner-instellingen	Commerciële bedrijven kunnen belang hebben bij informatie uit onderzoek, bijvoorbeeld om een voorsprong te krijgen op concurrenten. Ook al worden de resultaten van onderzoek vaak gepubliceerd, kan het eerder beschikken over de informatie voordeel opleveren. Hetzelfde geldt voor onderzoekers van 'collega'-instellingen.
7	Activisten	Activisten zijn gedreven door politieke of ideële motieven en kunnen om die reden proberen 'ongewenste' onderzoeken te dwarsbomen of wraak te nemen vanwege 'ongewenste' uitspraken.
8	Cybervandalen	Cybervandalen zijn veelal gemotiveerd door de uitdaging van hacking. Websites van onderwijsinstellingen kunnen aantrekkelijk zijn om te bekladden vanwege hun grote zichtbaarheid.

Tabel 9: Actoren[18]

[18] Bron: SURF Cyberdreigingsbeeld 2014 t/m 2018

BIJLAGE 3
IV-METINGEN

#	Actor	Beschrijving
1	IPv6	Internet Protocol versie 6 – opvolger van versie 4. Omdat de adressen van IPv4 bijna op zijn, is het noodzakelijk IPv6 te gaan gebruiken.
2	DNSSEC	Security extensie voor het Domain Name System (DNS) waarbij responses ondertekend en gevalideerd worden.
3	TLS	Transport Layer Security (voorheen SSL) – voorziet in versleuteling van verkeer op het netwerk. Webservers ondersteunen TLS, zodat het verkeer tussen de server en de webbrowser versleuteld is.
4	STARTTLS	Mechanisme voor mailservers om TLS te gebruiken voor communicatie onderling.
5	SPF	Sender Policy Framework – Protocol om SPAM tegen te gaan door vast te stellen of de verzender van een e-mail bericht gerechtigd is de betreffende mailserver te gebruiken.
6	DKIM	DomainKeys Identified Mail – wordt gebruikt om de validiteit van de afzender van e-mails te kunnen controleren. Bij het verzenden van e-mails wordt een digitale handtekening meegestuurd. Deze wordt gecontroleerd door middel van de sleutel (of key) die in het DKIM-record is opgenomen.
7	DMARC	Domain-based Message Authentication, Reporting and Conformance – maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkom stig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

Tabel 10: IV-metingen

BIJLAGE 4
SURFMAILFILTER – CATEGORIEËN

#	Categorieën	Toelichting
1	HAM	Mail die wordt doorgelaten.
2	SPAM	Mail die wordt geblokkeerd vanwege hoge spam-score.
3	Virus	Mail die wordt geblokkeerd vanwege de aanwezigheid van een (of meer) virus(sen).
4	Greylisted	Mail die in eerste instantie wordt geweigerd, maar bij opnieuw aanbieden alsnog wordt geaccepteerd.
5	On DNS-RBL	Mail die wordt geweigerd omdat de afzender voorkomt op de DNS-based real-time block list, waarop adressen van afzenders die spam versturen worden bijgehouden.
6	Invalid Recpt	Mail die wordt geblokkeerd omdat het afzender-adres niet klopt.
7	Other rejects	Mail die om andere redenen wordt geblokkeerd.

Tabel 11: SURFmailfilter

BIJLAGE 5
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.
5	spam	spamverkeer.
6	denial	meldingen over systemen die betrokken zijn bij een DDoS-aanval.
7	vulnerable	meldingen over systemen bij instellingen waarop bij SURFcert bekende kwetsbaarheden zijn gevonden.
8	infected	systemen die contact zoeken met IP adressen waarvan bekend is dat ze geassocieerd zijn met malware.

Tabel 12: SURFcert, type incidenten

AFKORTINGEN EN BEGRIPPEN

Begrip / afkorting	Betekenis	Bron
Actor	Ook threat actor of kwaadwillende – iemand die misbruik maakt van kwetsbaarheden om een dreiging ten uitvoer te brengen.	WCN [19]
AVG	Algemene Verordening Gegevensbescherming – Wet die sinds 1 mei 2018 van kracht is en de verwerking van persoonsgegevens behandelt. Het is de Nederlandse implementatie van de Europese GDPR (General Data Protection Regulation).	WP [20]
Awareness	Bewustzijn. In dit verband wordt bedoeld dat men zich bewust is van cyberdreigingen en gebruikers daardoor op een verantwoordelijke manier handelen.	WP
Big data	Grote sets van ongestructureerde data die niet in een gewone database onderhouden kunnen worden. Steeds meer data worden verzameld en opgeslagen om te analyseren met als gevaar dat dit gebeurt voor doeleinden die niet altijd overeenkomen met het doel waarvoor die data oorspronkelijk verzameld zijn.	WP
Blockchain	Gedistribueerd system om gegevens vast te leggen; er is geen centrale autoriteit waardoor het vervalsen van de vastgelegde gegevens nagenoeg onmogelijk is.	WCN
Botnet	Een netwerk van computer-systemen die zelfstandig kwaadaardige taken uitvoeren, zoals het versturen van spam of het uitvoeren van een DDoS-aanval. Een command-and-controlserver stuurt dit netwerk aan.	WCN
Brute-force	Het achterhalen van geheime informatie, bijvoorbeeld een wachtwoord, door alle mogelijke combinaties geautomatiseerd uit te proberen tot succes bereikt is.	WP
BYOD	Bring Your Own Device; trend waarbij gebruikers hun zelfgekozen of eigen hard- en software meenemen en koppelen aan het instellingsnetwerk. In veel gevallen zijn dit onbeheerde apparaten waarvan niet bekend is of ze voldoen aan de beveiligingseisen die de instelling stelt aan haar eigen apparaten.	WCN
Compliance	Het voldoen aan gestelde wet- en regelgeving of algemeen geaccepteerde standaarden	WP
Credential	Verificatiegegeven, veelal gebruikersnaam en wachtwoord	WP
CVE	Cybersecurity Vulnerabilities and Exposures - lijst van publieke kwetsbaarheden (https://cve.mitre.org/cve/).	
Dark web	Een besloten deel van het internet dat men niet vindt met normale browsers en zoekmachines. Het staat vooral bekend als een plek waar criminelen hun zaken doen.	WCN
DDoS	Distributed Denial-of-Service; aanvallen waarbij diensten onbereikbaar worden gemaakt voor gebruikers. DDoS services kunnen makkelijk en goedkoop worden afgesloten via het internet (dark web) en maken veelal gebruik van zogenaamde botnets bestaande uit IoT apparaten.	WCN
Defacing	Het bekladden van een web site om een eigen bericht te plaatsen. Wordt veelal gebruikt door hactivisten.	WP
Endpoint security	Beveiliging van eindsystemen (PCs, laptops, tablets et cetera) – niet beperkt tot anti-virus, maar ook bijvoorbeeld data-leak protection (DLP).	WP
Exploit	Methode (programma) die hackers gebruiken om een kwetsbaarheid te misbruiken.	WCN
Gebouw-automatisering	Een veelvoorkomende vorm van SCADA, bijvoorbeeld software voor klimaatbeheer, brandmelders, fysieke toegangscontrole en camerasystemen. Omvat in het algemeen regelsystemen en sensoren die veel data verzamelen en uitwisselen.	WP
Governance	De manier waarop het bestuur van een organisatie is ingericht.	WP
Hacker	Iemand die systemen wil proberen te doorgronden puur en alleen om zijn of haar nieuwsgierigheid te bevredigen. Tegenwoordig worden kwade bedoelingen verondersteld.	WCN
Hactivist	Iemand die digitale aanvallen uitvoert om een bepaalde ideologie te promoten.	WP
IoT	Internet of Things; ontwikkeling waarbij apparaten zijn gekoppeld aan het internet en informatie uitwisselen met elkaar en met centrale systemen. Deze apparaten hebben vaak ingebouwde software die ontsloten is. De beveiliging hiervan laat in veel gevallen te wensen over.	WCN

[19] *WCN: Woordenboek Cyberveilig Nederland (https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/)*
[20] *WP: Wikipedia (https://www.wikipedia.org/)*

Begrip / afkorting	Betekenis	Bron
MFA/2FA	Multi-factor authenticatie of Twee-factor authenticatie – methode waarbij 2 of meer identificerende factoren worden gebruikt voor authenticatie, bijvoorbeeld een wachtwoord en een vingerafdruk.	WP [20]
NCSC	Nationaal Cyber Security Centrum – instituut van het ministerie van Justitie en Veiligheid met als wettelijke taak onder andere Vitale aanbieders en onderdelen van het Rijk bij te staan bij het treffen van maatregelen om de continuïteit van hun diensten te waarborgen.	WP
Patch	Nieuwe versie van software of firmware door de producent. Repareert bekende kwetsbaarheden, zorgt eventueel voor nieuwe beveiliging en extra functies.	WCN [19]
Penetratietest	Handmatige controle waarbij men zo diep mogelijk wil binnendringen in een systeem om zwakke plekken te vinden en de gevolgen hiervan te kennen.	WCN
Phishing	Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals bijvoorbeeld inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails. Maar aanvallers doen het ook via de telefoon, een sms (Smishing), een videobijlage (Vishing) of een app-bericht.	WCN
Privacy-by-design	Het afdwingen, zowel technisch als organisatorisch, van een zorgvuldige omgang met persoonsgegevens vanaf de ontwerpfase van een systeem. Volgens de AVG zijn verwerkers verplicht rekening te houden met privacy-by-design en privacy-by-default principes.	WP
Ransomware	Gijzelsoftware – malware die bestanden versleuteld. De sleutel wordt pas na betaling van losgeld vrijgegeven. Een nieuwere variant dreigt tevens de data openbaar te maken als het losgeld niet wordt betaald.	WP
Responsible disclosure	Actie waarbij men gevonden beveiligingslekken op een verantwoorde manier bekend maakt. Meestal meldt men het lek eerst bij de eigenaar van het systeem waar het is gevonden.	WCN
SaaS	Software-as-a-service – een applicatie die in de cloud of gehost wordt aangeboden en via internet benaderd wordt. Het beheer van het hele systeem wordt door de leverancier uitgevoerd; de gebruiker is alleen verantwoordelijk voor de data.	WP
SCADA	Supervisory Control and Data Acquisition. In de regel is dit software die gegevens kan lezen en schrijven naar besturingseenheden van machines.	WCN
SCIPR	SURF Community voor Informatiebeveiliging en Privacy – community of practice om leden te helpen informatiebeveiliging verder te professionaliseren.	
SCIRT	SURFnet Community van Incident Response Teams – doel is om het algehele kennis- en ervaringsniveau van operationele security experts naar een hoger niveau te tillen binnen de sector onderwijs en onderzoek.	
Security-by-design	Het afdwingen, zowel technisch als organisatorisch, van een zorgvuldige omgang met gegevens vanaf de ontwerpfase van een systeem.	WP
SIEM	Security Incident & Event Management – systeem dat informatie over systemen, netwerken en incidenten verzamelt en analyseert met als doel verdacht gedrag te vinden. Wordt vaak in een SOC gebruikt als hulpmiddel.	WP
SOC	Security Operations Center – afdeling die informatiebeveiligingsvraagstukken afhandelt. Voorziet onder andere in monitoring van netwerken en systemen, in logging van incidenten en het oplossen van problemen.	WP
Spear phishing	Een phishingaanval die gericht is op een bepaald persoon. Soms is de aanval ook speciaal aangepast voor deze persoon. Daardoor is het heel moeilijk om te herkennen dat het een phishingaanval is. Wordt ook wel CxO-fraude genoemd, omdat spear-phishing wordt gebruikt om namens de CEO of CFO een medewerker van de financiële afdeling te verleiden om geld over te maken.	WCN
Spoofing	Zich voordoen als iemand anders of als een ander systeem. De afzender van een e-mail kan bijvoorbeeld gespoofd worden.	WP
Statelijke actor	Een land dat digitale aanvalsmiddelen inzet voor spionage en sabotage, en voor het verspreiden van desinformatie. (https://www.nctv.nl/themas/statelijke-dreigingen)	
Vulnerability scan	Kwetsbaarheden scan - Een geautomatiseerde controle die zwakke plekken in een systeem opspoort.	WCN
Zero-day aanval	Aanval of methode die misbruikt maakt van een kwetsbaarheid (de zero-day vulnerability) die nog niet bekend is bij anderen (leverancier, gebruiker), waardoor er nog geen patch beschikbaar is.	WCN

BIBLIOGRAFIE

#	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	16-10-19
[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	20-09-19
[3]	Nationaal Cybersecurity Centrum Nederland	**Cyberkompas 2019**	NCSC (NL)	2019	https://www.ncsc.nl/aan-de-slag/cyberkompas	16-12-19
[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	10-09-19
[5]	Verizon Business	**Verizon Data Breach Investigations Report 2019**	Verizon	2019	https://enterprise.verizon.com/resources/reports/dbir/	13-08-19
[6]	ENISA	**ENISA Threat Landscape Report**	ENISA	2019	https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018	05-09-19
[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	16-12-19
[8]	Cyberveilig Nederland	**Cybersecurity Woordenboek**	Cyberveilig Nederland	2019	https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/	17-12-19
[9]	Palo Alto Unit42	**Cloudy with a Chance of Entropy**	Palo Alto	2019	https://www.paloaltonetworks.com/resources/research/unit42-cloud-with-a-chance-of-entropy	18-12-19
[10]	Tubantia	**Hackers rommelen in systeem Aventus Apeldoorn**	Tubantia	2019	https://www.tubantia.nl/apeldoorn/hackers-rommelen-in-systeem-aventus-apeldoorn-ze-hebben-schoolcijfers-gewijzigd-aa75df55/	02-01-20
[11]	1limburg	**Groot cyberhack bij UM: 'Criminele aanval niet uitgesloten'**	1limburg	2019	https://www.1limburg.nl/groot-cyberhack-bij-um-criminele-aanval-niet-uitgesloten?context=topstory	24-12-19
[12]	Cyberint	**Social Media: A Holiday Haven for Threat Actors**	Cyberint	2019	https://blog.cyberint.com/social-media-a-heaven-for-cyber-criminals	10-01-20
[13]	Butler, Laura	**Cybercriminals raking in over $3bn a year from social media crime**	University of Surrey	2019	https://www.surrey.ac.uk/news/cybercriminals-raking-over-3bn-year-social-media-crime	10-01-20
[14]	Crowdstrike	**2019 Mobile Threat Landscape Report**	Crowdstrike	2019	https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/?ctm_source=Digital&ctm_medium=blog&ctm_campaign=WC_2019_Threat_Landscape_Mobile_Malware	10-01-20

#	Auteur(s)	Titel	Uitgever	Jaar	URL	opgehaald
[15]	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	10-01-20
[16]	Mandiant	**M-Trends 2019**	FireEye	2019	https://content.fireeye.com/m-trends/rpt-m-trends-2019	10-01-20
[17]	Crowdstrike	**2019 Global Threat Report**	Crowdstrike	2019	https://www.crowdstrike.com/resources/reports/2019-crowdstrike-global-threat-report/	10-01-20
[18]	ISC2	**Global Cybersecurity Workforce Shortage to Reach 1.8 Million as Threats Loom Larger and Stakes Rise Higher**		2017	https://www.isc2.org/News-and-Events/Press-Room/Posts/2017/06/07/2017-06-07-Workforce-Shortage	12-01-20
[19]	Forum Standaardisatie		Rijksoverheid	2020	https://www.forumstandaardisatie.nl/	12-01-20
[20]	Boone, Anouk	**Nederlandse rectoren waarschuwen voor macht van techreuzen**	Volkskrant	2019	https://www.volkskrant.nl/nieuws-achtergrond/nederlandse-rectoren-waarschuwen-voor-macht-van-techreuzen-b28e509f/?utm_source=link&utm_medium=app&utm_campaign=shared%20content&utm_content=free	12-01-20
[21]	COT	**Dreigingsbeeld HO**	IV-HO	2018	https://www.integraalveilig-ho.nl/instrument/dreigingsbeeld-ho/	12-01-20
[22]	Mitre	**CVE List Home**	Mitre	2020	https://cve.mitre.org/cve/	12-01-20

COLOFON

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

Redactie
Jan Michielsen (*SURF*)

Coördinatie
Nanda Bazuin (*SURF*)

Vormgeving
Vrije Stijl, Utrecht

Fotografie
Istock

Februari 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