# CYBERDREIGINGSBEELD 2020-2021

## ONDERWIJS EN ONDERZOEK

# VOORWOORD **SAMEN WEERBAAR**

Toen het vorige SURF Cyberdreigingsbeeld werd samengesteld, had de ransomware-aanval op de Universiteit Maastricht nog niet plaatsgevonden. De kerstweek van 2019 en de eerste weken van 2020 hebben ons geleerd dat een dreiging van een 'beeld', van een notie, tot een heuse crisis kan uitgroeien. Een crisis die niet alleen van grote betekenis is voor de betrokken instelling, maar die ook impact heeft op een hele sector.

Voor u ligt het SURF Cyberdreigingsbeeld 2020/2021. Daarin valt op dat instellingen de cyberdreiging gemiddeld genomen hoger inschatten dan in 2019. Dat ligt natuurlijk niet alleen aan het incident bij de UM. Ook het thuiswerken vanwege de covid-19-lockdown en de vele incidenten die in 2020 in de media zijn gemeld, dragen daartoe bij. Die incidenten zijn ook een duidelijke indicatie dat externe partijen, criminelen en statelijke actoren in toenemende mate kansen zien om via cyberaanvallen hun doelen te bereiken. 2020 was in vele opzichten een wake-up call.

Ons gezamenlijke cyberdreigingsbeeld is bijgesteld en er zijn bij veel instellingen meer middelen beschikbaar gesteld om de weerbaarheid te versterken. Behalve als individuele instellingen, nemen de partijen ook in samenwerkingsverbanden verantwoordelijkheid.
Zo hebben de instellingen het initiatief genomen om gezamenlijk een 24/7 Security Operations Centre in te richten: SURFsoc is begin januari 2021 van start gegaan. Een ander voorbeeld is de gezamenlijke aanpak waarmee de instellingen invulling hebben gegeven aan de behoefte aan externe toetsing van hun security-volwassenheid (SURFaudit): in het eerste kwartaal van 2021 kunnen we de eerste cijfers van een externe benchmark tegemoetzien.

Kortom, hoewel het fysiek samenkomen sinds voorjaar 2020 nauwelijks meer mogelijk was, zien we in de SURF-community juist een groeiend enthousiasme om samen te werken en informatie uit te wisselen. En door die intensieve samenwerking vergroten we samen over de volle breedte de cyberveiligheid van onderwijs en onderzoek in Nederland.

Cybersecurity is in 2020 overigens ook in politiek opzicht stevig op de agenda gekomen. De samenwerking tussen het NCSC en vier sectorale computercrisisteams, waaronder SURFcert, is begin 2020 in een ministeriële regeling verankerd. 'Samen weerbaar' is daarbij het sector-overstijgend motto. Het kabinet heeft in de brieven aan de Tweede Kamer over 'Kennisveiligheid hoger onderwijs en wetenschap' en 'Samenwerking met China op het gebied van onderwijs en wetenschap' stappen gezet voor het verhogen van kennisveiligheid bij onderwijs- en onderzoeksinstellingen. En de AIVD heeft in december 2020 Russische spionageactiviteiten bij hoger onderwijsinstellingen verstoord.

Ontwikkelingen op het gebied van cyberweerbaarheid zijn met andere woorden als positief te beschouwen. Maar dit cyberdreigingsbeeld geeft tegelijk ook aan dat er nog steeds reden is tot verhoogde dijkbewaking. De OZON2020-oefening, vanwege covid-19 uitgesteld tot maart 2021, kan daarvoor dienstdoen als lakmoesproef. Hopelijk kunnen we in retrospectief over 2021 melden dat het een jaar is geweest van dijkverhoging en crisisoefening in plaats van cyberaanvallen.

**Nick Bos**
*Vice-voorzitter college van bestuur Universiteit Maastricht*

**Jet de Ranitz**
*Voorzitter raad van bestuur SURF*

# BESTUURDERSSAMENVATTING

In dit *Cyberdreigingsbeeld – onderwijs en onderzoek* kijken we terug op 2020 en vooruit naar 2021. We brengen in kaart welke trends er in 2020 in de sector onderwijs en onderzoek waren en welke dreigingen zich hebben gemanifesteerd in de sector. Verder laten we zien welke trends we verwachten in 2021.

**Headlines**

- **Het aantal incidenten is opnieuw toegenomen, met name het aantal phishing-aanvallen. Ook de complexiteit van incidenten is toegenomen.**
- **Grotere afhankelijkheid van een klein aantal grote cloudproviders van buiten de EER maakt onderwijs en onderzoek kwetsbaar.**
- **De toename van dreiging door statelijke actoren vereist meer aandacht voor kennisveiligheid.**
- **Door toegenomen complexiteit en raffinement van dreigingen is investeren in bewustwording en opleiding van gebruikers cruciaal.**
- **Expertise en middelen zijn nog steeds schaars. Samenwerken op het thema cybersecurity zowel binnen onderwijs en onderzoek als daarbuiten is onverminderd belangrijk.**

## Covid-19-pandemie en ransomware-incident Universiteit Maastricht

De covid-19-pandemie en het ransomware-incident eind 2019 bij de Universiteit Maastricht hebben voor een groot deel de agenda van 2020 bepaald. Door covid-19 moesten instellingen van het ene op het andere moment overstappen op online onderwijs en thuiswerken. Om deze stap
snel te kunnen maken heeft het gebruik van clouddiensten een nog grotere vlucht genomen.

Het incident bij de Universiteit Maastricht was voor veel instellingen aanleiding om versneld extra weerbaarheid verhogende beveiligingsmaatregelen in te voeren. Uit de survey blijkt dat veel instellingen meer aandacht hebben besteed aan awareness bij medewerkers en studenten. Op technisch vlak hebben veel instellingen multi-factorauthenticatie en VPN ingevoerd en hebben ze extra aandacht besteed aan patchmanagement en de back-up van hun data. Ondanks de covid-19-pandemie konden deze projecten bij de meeste instellingen gewoon doorgaan.

## Incidenten

Het aantal incidenten is in 2020 opnieuw toegenomen. Vooral het aantal phishing-aanvallen is fors gestegen. Ransomware-aanvallen hebben in Nederland geen sterke stijging laten zien, maar het gevraagde losgeld is wel gestegen.

Een aantal incidenten in 2020 laat zien dat onderwijs en onderzoek in Nederland onverminderd kwetsbaar is. Behalve het ransomware-incident bij de Universiteit Maastricht was er nog een aantal in het oog springende incidenten die de continuïteit van processen bij instellingen hebben verstoord. Zo konden bij de UvA vanwege een storing een kleine 6.000 tentamens niet op het geplande moment doorgaan en konden bij de RUG vanwege een ICT-storing ook enkele honderden online toetsen niet doorgaan.

## Trends

Bij de phishing-incidenten valt op dat cybercriminelen zich steeds beter verdiepen in de organisaties die zij aan willen vallen. Doelgericht worden specifieke functionarissen binnen de organisatie benaderd.

Om onderwijs op afstand en thuiswerken te faciliteren zetten instellingen nieuwe tooling in, waaronder videoconferencingtools en tools voor online proctoring. Hiervoor gebruiken ze meestal clouddiensten. Instellingen zijn hiermee nog

afhankelijker geworden van een beperkt aantal grote cloudproviders, wat in geval van een calamiteit de continuïteit kan verstoren. Ook het ongeldig verklaren van het Privacy Shield door het Europese Hof van Justitie kan uiteindelijk leiden tot continuïteitsproblemen.

De survey laat zien dat veel instellingen extra hebben geïnvesteerd in maatregelen die de weerbaarheid verhogen. Een groot aantal instellingen is geïnteresseerd in de SOC-dienst van SURF die begin 2021 in gebruik is genomen.

Instellingen hebben groeiende aandacht voor kennisveiligheid. Mede door de veranderde internationale verhoudingen beoordelen ze de uitwisseling van kennis in samenwerkingsverbanden of de deelname van sommige buitenlandse studenten op een andere manier. Onder leiding van het ministerie van Onderwijs, Cultuur en Wetenschappen worden instrumenten ontwikkeld die onderwijs- en onderzoeksinstellingen ondersteunen bij het inrichten van kennisveiligheid.

## Actoren

De survey laat zien dat instellingen beroepscriminelen als belangrijkste actoren zien, gevolgd door (h)activisten/cybervandalen. Inmiddels zijn ook binnen onderwijs en onderzoek sterke aanwijzingen dat statelijke actoren vaker bij instellingen in de sector binnendringen. Dit heeft geleid tot een pakket van maatregelen van de overheid om kennisveiligheid beter te borgen.

## Overige resultaten van de survey

De survey laat ten opzichte van 2019 geen grote verschuivingen zien in de typen dreigingen die zijn waargenomen. *Verkrijging en openbaarmaking van data, identiteitsfraude en verstoring van ICT-voorzieningen* zijn nog steeds de meest voorkomende dreigingen. *Overname en misbruik van ICT-middelen* is in 2020 is gestegen.

**Budget en capaciteit**

Bijna de helft van de instellingen besteedt minder dan 5% van het totale IT-budget aan informatiebeveiliging. Opvallend is dat ten opzichte van 2019 het percentage ‘onbekend’ iets is gestegen.
Bijna de helft van de instellingen geeft aan tussen de 2 en 5 fte beschikbaar te hebben voor informatiebeveiliging. Dit is een lichte stijging ten opzichte van 2019.

**Awareness**

De meeste instellingen voeren regelmatig awareness campagnes uit. Ongeveer een kwart van de instellingen geeft aan dat nieuwe medewerkers bij indiensttreding een awareness training ontvangen.

**Security en privacy by design en betrokkenheid van security en privacy officer bij projecten**

Meer dan 80% van de instellingen besteedt aandacht aan security en privacy by design. Tevens is de betrokkenheid van de security officer of privacy officer bij nieuwe projecten verbeterd ten opzichte van 2019.

**Risicoperceptie**

Voor de zeven risicocategorieën worden de risico’s hoger ingeschat dan in 2019 bij het onderwijsproces, het onderzoekproces en de bedrijfsvoering. Alleen bij *Bewust beschadigen van het imago* wordt het risico iets lager ingeschat bij alle drie de processen. Bij het onderwijsproces en bij bedrijfsvoering wordt ook *Spionage* iets lager ingeschat.
Daarnaast hebben we de deelnemers aan de survey gevraagd om een risicoinschatting te geven voor de *Afhankelijkheid van clouddiensten* en die toegevoegd als achtste risico aan tabel 1. Instellingen verplaatsen hun data en applicaties steeds meer naar de cloud. Dat geeft een ander risicoprofiel. Het is bijvoorbeeld veel lastiger de staat van informatiebeveiliging te bepalen bij de clouddiensten zelf en vaak bevinden de data zich buiten de EER, waardoor mogelijk niet wordt voldaan aan de AVG. Ook is er een beperkt aantal leveranciers van clouddiensten, wat hun een monopoliepositie geeft. Daarnaast zijn die leveranciers vooral in de VS gevestigd.

Tabel 1 **Risicoperceptie en dynamiek**

| Categorie | Onderwijs △ | Onderzoek △ | Bedrijfsvoering △ |
|---|---|---|---|
| 1 Verkrijging en openbaarmaking van informatie | Zeer hoog ↑ | Zeer hoog ↑ | Zeer hoog ↑ |
| 2 Identiteitsfraude | Hoog ↑ | Medium ↑ | Hoog ↑ |
| 3 Verstoring ICT | Zeer hoog ↑ | Hoog ↑ | Zeer hoog ↑ |
| 4 Manipulatie van data | Hoog ↑ | Medium ↑ | Medium ↑ |
| 5 Spionage* | Laag — | Medium ↑ | Laag — |
| 6 Overname en misbruik ICT | Hoog ↑ | Hoog ↑ | Zeer hoog ↑ |
| 7 Bewust beschadigen imago | Medium ↓ | Medium ↓ | Medium ↓ |
| 8 Afhankelijkheid van clouddiensten | Zeer hoog ○ | Medium ○ | Hoog ○ |

△ Ontwikkeling 2020 t.o.v. 2019

↑ Forse toename t.o.v. 2019

↑ Toename t.o.v. 2019

— Geen verandering t.o.v. 2019

↓ Afname t.o.v. 2019

↓ Forse afname t.o.v. 2019

○ Geen vergelijking met 2019

** Bij Spionage is de onzekerheid het grootst (36% weet niet of het risico is toe- of afgenomen)*

## Reflectie en conclusies

### Grotere afhankelijkheid van cloudproviders

Voor online onderwijs, online proctoring en thuiswerken wordt in nog steeds toenemende mate gebruik gemaakt van clouddiensten. Hiermee is de afhankelijkheid van een klein aantal grote cloudproviders alleen maar groter geworden. Een aantal verstoringen bij deze grote cloudproviders laat zien dat het Nederlandse onderwijs en onderzoek nog steeds kwetsbaar zijn. Daarnaast leidt ook de ongeldigverklaring van het Privacy Shield door het Europese Hof van Justitie ertoe dat instellingen deze aspecten rondom het gebruik van clouddiensten moeten meewegen bij het opstellen van het risicoprofiel van de instelling.

### Kennisveiligheid

De toename van dreigingen door statelijke actoren vereist dat instellingen nog meer investeren in kennisveiligheid en expertise op het gebied van cybersecurity.

### Bewustwording en opleiding gebruikers steeds crucialer

Het aantal pogingen tot phishing is explosief gestegen en de methoden worden nog steeds geraffineerder. Investeren in opleiding en bewustwording wordt steeds crucialer, zodat de gebruiker ook weerbaarder wordt tegen de nieuwste dreigingen.

**Samenwerken**

Binnen de sector zien we een toenemende samenwerking zowel binnen de sector als daarbuiten. Universitaire security officers zijn het U-CISO-overleg gestart waarin zij kennis bundelen en informatie uitwisselen. In VSNU-verband werken functionarissen gegevensbescherming samen. Op initiatief van de universiteiten is SURF in 2020 gestart met de inrichting van een security operations centre (SURFsoc). SURF doet dit in nauwe samenwerking met de universiteiten en een hbo-instelling. Deze vorm van samenwerking is een goed voorbeeld van het optimaal inzetten van in de sector aanwezige expertise en het efficiënt inzetten van middelen.

Op landelijk niveau wordt sinds begin 2020 samengewerkt op het gebied van incident response in het Landelijk Dekkend Stelsel, een samenwerking van het NCSC met sectorale samenwerkingsverbanden, CERT's en andere publieke en private partijen. SURFcert vertegenwoordigt de sector onderwijs en onderzoek hierin. Doel van deze samenwerking is om informatie en kennis over bijvoorbeeld kwetsbaarheden en dreigingen uit te wisselen.

De komende jaren is er nog grote schaarste aan cybersecurityexpertise. Daarnaast valt te verwachten dat na de covid-19-pandemie financiële middelen ook schaarser worden. Dit versterkt de noodzaak tot verdere samenwerking om het toenemend aantal dreigingen het hoofd te kunnen bieden.

# INHOUD

# 1 INLEIDING

In dit Cyberdreigingsbeeld lees je over security- en privacy-incidenten die zich hebben voorgedaan tussen eind 2019 en november 2020, de gevolgen daarvan voor de sector onderwijs en onderzoek en trends die we signaleren. Daarmee kunnen instellingen hun eigen informatiebeveiliging en privacybescherming verder verbeteren, om zo weerbaarder te zijn tegen dreigingen die op de sector afkomen. Het Cyberdreigingsbeeld richt zich vooral op bestuurders, security officers en privacy officers van Nederlandse onderwijs- en onderzoeksinstellingen.

## Werkwijze

Qua vorm en inhoud bouwt het Cyberdreigingsbeeld voort op de eerdere uitgaven die SURF sinds 2014 jaarlijks publiceert. Net als in voorgaande jaren hebben we gebruik gemaakt van publieke bronnen zoals het jaarlijkse Cybersecuritybeeld Nederland [1] en het ENISA Threat Landscape [2] om diverse trends in kaart te brengen.

In het najaar van 2020 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 2019. De samenstelling van de survey is gevalideerd door een klankbordgroep bestaande uit vertegenwoordigers van onderwijs- en onderzoeksinstellingen.

## Highlights

2020 zal de geschiedenis ingaan als een bijzonder jaar voor onderwijs- en onderzoeksinstellingen. Het afgelopen jaar wordt voor onze sector gekenmerkt door een aantal spraakmakende incidenten, zoals de ransomware-aanval waar de Universiteit Maastricht door is getroffen. En natuurlijk heeft de covid-19-pandemie ons bijna heel 2020 in zijn greep gehouden. Beide gebeurtenissen illustreren hoe afhankelijk onderwijs- en onderzoeksinstellingen zijn (geworden), niet alleen van hun digitale infrastructuur en voorzieningen maar ook van cloud-leveranciers en -diensten voor lesgeven, online colleges en tentamens.

Als reactie op het incident bij de Universiteit Maastricht hebben veel instellingen programma's gestart die de weerbaarheid verhogen. Uit de survey blijkt dat deze programma's ondanks de covid-19-pandemie bij de meeste instellingen niet worden vertraagd.

Helaas neemt het aantal dreigingen nog steeds toe, waarbij criminelen steeds meer samenwerken om hun doel te bereiken en statelijke actoren zich steeds uitgebreider manifesteren.

Hoewel instellingen onderling steeds beter samenwerken en de overheid initiatieven neemt die de weerbaarheid bij instellingen moet verhogen en kennis-veiligheid beter moet borgen, blijft de cyberdreiging onverminderd hoog.

## Leeswijzer

In hoofdstuk 2 vind je een kort overzicht van incidenten en trends die zich in 2020 hebben voorgedaan en de actoren die het meest relevant zijn in de sector onderwijs en onderzoek.
Hoofdstuk 3 gaat in op de resultaten van de survey. Detailinformatie daarover vind je in bijlage 1. In hoofdstuk 4 bespreken we de weerbaarheid van de instellingen om in hoofdstuk 5 af te sluiten met de conclusie.

# 2 INCIDENTEN, TRENDS EN ACTOREN

Dit hoofdstuk gaat uitvoeriger in op relevante incidenten die het nieuws hebben gehaald en geeft een overzicht van de belangrijkste cybersecuritytrends in 2020. Het is samengesteld op basis van de survey en diverse publieke bronnen binnen en buiten de sector onderwijs en onderzoek, waaronder:

- Cybersecuritybeeld Nederland 2020, NCTV (2020) [1]
- Kennis in het vizier – De gevolgen van de digitale wapenwedloop voor de publieke kennisinfrastructuur, Rathenau Instituut (2019) [4]
- Threat Landscape Report 2020, ENISA (2020) [2]
- Turning the Tide, Trend Micro Security Prediction for 2021 (2020) [5]
- Cyber impact – The impact of cyber security incidents on the UK's further and higher education and research sectors, JISC (2020) [6]
- Threat Spotlight: Spear phishing attacks targeting education sector, Barracuda [7]
- 2020 Data Breach Investigations Report (DBIR), Verizon (2020) [8]

## Incidenten

### Ransomware-incident Universiteit Maastricht

Net voor het begin van 2020 werd de Universiteit Maastricht getroffen door een aanval met ransomware die zijn weerslag had op alle universiteiten, hogescholen en mbo-instellingen [3]. In januari maakten een ziekenhuis, een gemeente en enkele ministeries bekend inbraakpogingen als gevolg van een beveiligingslek in Citrix-systemen te hebben gezien. Instellingen moesten direct maatregelen nemen om te voorkomen dat ook zij werden getroffen door die hack [9].

Enkele maanden eerder was de Universiteit Antwerpen ook al getroffen door een vergelijkbare ransomware-aanval, maar had daar weinig ruchtbaarheid aan gegeven en de kenmerken van de aanval niet breed gedeeld [10].
De Universiteit Maastricht daarentegen heeft in februari 2020 een cybersymposium georganiseerd [11] waarbij zij uitgebreid heeft stilgestaan bij de cyberaanval. Zij heeft tijdens het symposium uitgelegd wat er precies is gebeurd, welke stappen inmiddels zijn genomen om herhaling te voorkomen en welke leerpunten het forensisch onderzoek heeft opgeleverd.

> ***"De cyberaanval op Universiteit Maastricht deed alle alarmbellen rinkelen bij instellingen voor hoger onderwijs. Security is daar nu 'top of mind'. Maar het is ook een hele evenwichtskunst voor universiteiten. Aan de ene kant willen ze studenten een open en transparante omgeving bieden, en aan de andere kant moeten ze hen beschermen tegen het voortdurend veranderende bedreigingslandschap."*** Bron: Infosecurity [12]

Een van de vervolgstappen die de universiteiten in VSNU-verband hebben afgesproken, is dat alle universiteiten een audit in 2020 laten uitvoeren door een externe auditor. De audit vindt plaats op basis van het SURFaudit Normenkader Informatiebeveiliging HO en maakt gebruik van een gezamenlijk ontwikkelde auditmethodiek. Een andere vervolgstap is het opzetten van een gezamenlijk security operations centre in samenwerking met SURF.

### Citrix-kwetsbaarheid

In januari maakten een ziekenhuis, een gemeente en enkele ministeries bekend inbraakpogingen te hebben gezien in Citrix-systemen als gevolg van een beveiligingslek. [13]. Instellingen moesten toen direct maatregelen nemen om te voorkomen dat ook zij werden getroffen door een hack in hun Citrix-systemen.

> ***"Het Medisch Centrum Leeuwarden en de gemeente Zutphen zijn de voorbije dagen slachtoffer geworden van een aanval door hackers. Woensdagmiddag waren beide organisaties in de veronderstelling dat er geen belangrijke gegevens zijn buitgemaakt, of bestanden zijn vergrendeld om later losgeld te eisen voor ontsleuteling. Zekerheid daarover konden ze nog niet geven."***

*"Het ziekenhuis en de gemeente waren de voorbije dagen niet de enige organisaties die kwetsbaar waren voor een cyberaanval. Zeker 240 Nederlandse bedrijven hadden woensdagochtend een kwetsbaarheid in software van het Amerikaanse bedrijf Citrix nog onvoldoende gerepareerd, blijkt uit onderzoek van Matthijs Koot. Hij is beveilingsexpert bij cybersecuritybedrijf Secura en gastdocent aan de Universiteit van Amsterdam."* Bron: NRC Handelsblad [14]

**Infectieradar**

Zaterdag 6 juni werd het RIVM opgeschrikt door een datalek van de Infectieradar[1]. Privacygevoelige informatie was vindbaar door een aantal handelingen uit te voeren in het systeem waarmee het RIVM de vragenlijsten afneemt, ondanks de verschillende veiligheidschecks die van tevoren waren uitgevoerd op de software [15].

**Blackbaud en Privacy Shield**

Half juli kregen TU Delft en Universiteit Utrecht bericht van hun Amerikaanse leverancier Blackbaud dat gedurende de eerste helft van het jaar persoonsgegevens uit de crm-applicatie waren gelekt [16]. Bijna gelijktijdig heeft het Europese Hof van Justitie het EU-VS Privacy Shield voor doorgifte van persoonsgegevens naar de VS ongeldig verklaard [17] omdat het Privacy Shield onvoldoende bescherming garandeert. Beide gebeurtenissen geven instellingen stof tot nadenken over het gebruik van cloudleveranciers in het algemeen en Amerikaanse (cloud)leveranciers in het bijzonder.

***"Uitspraak Hof***
*Het Europese Hof van Justitie stelt dat het privacy shield onvoldoende bescherming kan garanderen. Dat komt omdat, op grond van de Amerikaanse wetgeving, de inlichtingen- en veiligheidsdiensten daar het recht hebben om gegevens van EU-burgers in te zien en te gebruiken. Dit is niet beperkt tot strikt noodzakelijk gegevens.*

***Ombudsman***
*Ook stelt het Hof dat het ombudsman-mechanisme niet genoeg bescherming biedt wanneer EU-burgers een klacht hebben over de verwerking van hun persoonsgegevens in de VS. Het mechanisme kan de onafhankelijkheid van de ombudsman en diens bevoegdheid om bindende besluiten te nemen niet verzekeren, aldus het Hof."*
Bron: Autoriteit Persoonsgegevens [17]

**DigiCert-incident**

Op 7 juli kondigde DigiCert, de (voormalig) leverancier van SURFcertificaten, aan dat door een omissie bij de WebTrust-audit een aantal tussenliggende certificaten moesten worden ingetrokken waardoor alle onderliggende certificaten in een keer ongeldig werden [18]. Dit had tot gevolg dat circa 100 bij SURF aangesloten instellingen binnen 4 dagen in totaal zo'n 5.000 certificaten moesten vervangen. Voor enkele instellingen was dit een grote operatie, omdat zij een groot aantal certificaten op korte termijn moesten vervangen.

**Saxion phishing-incident**

Eind oktober werd Hogeschool Saxion overspoeld door duizenden phishing-mails met het verzoek een bestand te downloaden. Ongeveer 350 ontvangers hebben dat naar verluid gedaan, waarvan er waarschijnlijk 3 daadwerkelijk geïnfecteerd zijn geraakt [19]. Dit incident had wellicht voorkomen kunnen worden wanneer er een SOC/SIEM en multi-factorauthenticatie was geweest, omdat ze (achteraf) de inlogpogingen vanuit andere landen hebben gevonden.

*"De phishing mailtjes zijn vorige week maandag 26 oktober en vrijdag 30 oktober verstuurd en bij zeker 2.500 e-mailadressen van Saxion terechtgekomen.*

*Bij phishing zetten cybercriminelen meestal linkjes naar websites of downloadbestanden in de berichten. De inhoud vormt vaak de opmaat naar internetfraude.*

1 https://www.rivm.nl/infectie-radar

*Op Saxion bleek dat niet anders. Wie een bericht binnenkreeg, kon doorklikken en werd vervolgens gevraagd iets te downloaden. Waarschijnlijk was dat het moment, waarop de internetcriminelen zich toegang konden verschaffen om gegevens buit te maken. Uit het onderzoek komt naar voren dat ongeveer 360 mensen op de link hebben geklikt."* Bron: Tubantia [19]

Vergelijkbare incidenten hadden zich in de VS en het VK ook al voorgedaan in oktober 2020. Onderzoekers van INKY hebben in 2020 een groot aantal kwaadaardige campagnes ontdekt, waarbij gecompromitteerde mail accounts van tenminste 13 verschillende universiteiten zijn gebruikt [21].

*"The highest number of phishing emails detected came from compromised Purdue University accounts (2,068), stolen in campaigns from Jan. to Sept.*

*Dave Bagget, CEO and co-founder of INKY, told Threatpost that there is no indication of how the accounts were compromised — but he speculated that the victims fell for a credential-harvesting scheme. Bagget also said that this month researchers continued to see phishing emails from real university accounts, so some accounts appear to still be compromised."*

*"A student may never change an originally assigned password, or may share it with a friend or friends," according to Inky researchers on Thursday. "A professor may give a student the password to an account for a particular project and never change it when the project is done. Hackers tapping around find these carelessly handled accounts, take them over, and change the passwords themselves, locking out the original owner."*
Bron: Threatpost [20]

**Afhankelijk van ICT en clouddiensten**

Op de Universiteit van Amsterdam en de Rijksuniversiteit Groningen was het voor studenten in oktober niet mogelijk tentamens te maken door ICT-storingen. Bij de UvA bleek een inlogstoring de oorzaak te zijn, bij de RUG een overbelaste digitale leeromgeving [22]. De volgende dag had de UvA weer problemen, maar nu met de applicatie Proctorio, waardoor ze weer tentamens moesten uitstellen [23].

*"In totaal konden dinsdagochtend en -middag een kleine 6000 tentamens niet doorgaan aan de UvA. Door een grote inlogstoring lag een groot deel van het netwerk plat.*

*Onder andere Testvision, het programma waarin de digitale tentamens gemaakt moeten worden, was nauwelijks bereikbaar. De storing komt uiterst ongelegen in de eerste tentamenweek van het jaar. Door de coronacrisis vinden vrijwel alle tentamens dit jaar online plaats.* [24]

*Na de eerdere problemen aan de Universiteit van Amsterdam kampt deze week ook de Rijksuniversiteit Groningen met een grote ict-storing tijdens online tentamens. Honderden toetsen zijn geschrapt."* Bron: Digitaal Universiteitsblad DUB [22]

Deze incidenten illustreren dat dreigingen onverminderd doorgaan en dat instellingen voortdurend waakzaam moeten blijven om geen slachtoffer te worden van criminelen en andere actoren.

## Trends

**Belangrijkste trends in onderwijs en onderzoek**

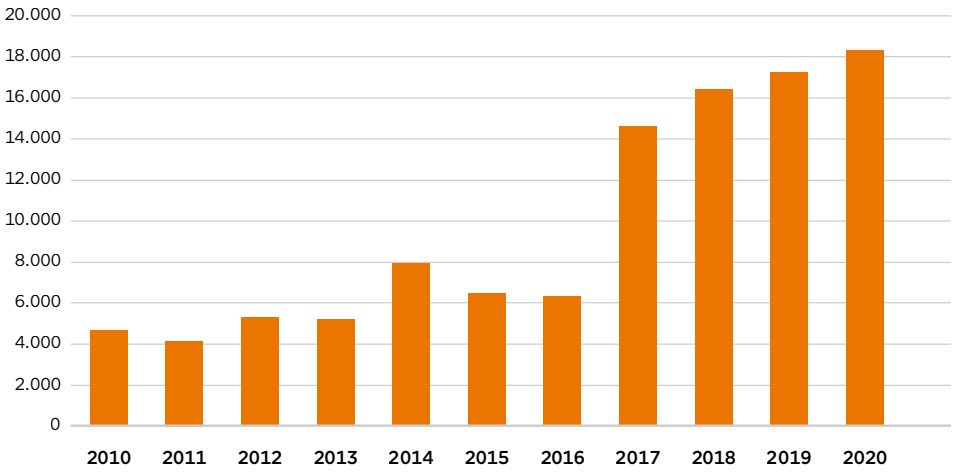
Op 11 maart 2020 was de uitbraak van covid-19 officieel uitgegroeid tot een pandemie [25]. Enkele dagen later werden in Nederland strenge maatregelen afgekondigd, waardoor onder meer fysiek onderwijs niet meer mogelijk was. De pandemie zorgde ervoor dat we onze manier van werken moesten aanpassen. Thuiswerken en onderwijs op afstand kregen de overhand. In allerijl zochten universiteiten, hogescholen en mbo-instellingen naar manieren om onderwijs op een of andere manier te laten doorgaan. Al snel werden online lesgeven en online colleges de norm.

De survey laat ten opzichte van 2019 geen grote verschuivingen zien in de typen dreigingen die zijn waargenomen. *Verkrijging en openbaarmaking van data, identiteitsfraude en verstoring van ICT-voorzieningen* zijn nog steeds de meest voorkomende dreigingen. *Overname en misbruik van ICT-middelen* is een dreiging die in 2020 is gestegen.

De dreigingen zijn wel in aantal weer toegenomen. Dat geldt met name voor phishing, waarbij opvalt dat cybercriminelen zich steeds beter verdiepen in de organisaties die zij aan willen vallen. Doelgericht worden specifieke functionarissen benaderd. Vaak voor financieel gewin, in een aantal gevallen om onderzoeksresultaten te verkrijgen of te beïnvloeden.

Het aantal kwetsbaarheden neemt hand over hand toe. Uit cijfers van de National Vulnerability Database[2] blijkt dat van 2010 tot en met 2016 het aantal kwetsbaarheden met een CVE-nummer jaarlijks ongeveer op hetzelfde niveau bleef. Maar in 2017 is er een opeens sterke stijging die zich daarna voortzet [26]:

Figuur 1 **Aantal CVE-registraties vanaf 2010**




De afhankelijkheid van een beperkt aantal grote cloudproviders is verder toegenomen. Om onderwijs op afstand en thuiswerken te faciliteren zetten instellingen nieuwe tooling in, waaronder videoconferencingtools en tools voor online proctoring. Hiervoor gebruiken ze meestal clouddiensten. Instellingen zijn zo nog afhankelijker geworden van een beperkt aantal grote cloudproviders, wat in geval van een calamiteit de continuïteit kan verstoren. En ook het ongeldig verklaren van het Privacy Shield door het Europese Hof van Justitie kan uiteindelijk leiden tot continuïteitsproblemen.

De survey laat zien dat veel instellingen extra hebben geïnvesteerd in maatregelen die weerbaarheid verhogen, waarschijnlijk mede door het incident bij de Universiteit Maastricht. Sommige instellingen zijn zelf bezig een Security Operations Centre in te richten. Veel andere instellingen zijn geïnteresseerd in SURFsoc [27]. Vanaf januari 2021 kunnen instellingen zich hierbij aansluiten. Daarnaast is met name geïnvesteerd in VPN-oplossingen, multi-factorauthenticatie, patchmanagement, back-ups en awareness.

Behalve voor de hiervoor genoemde trends, hebben instellingen meer aandacht voor kennisveiligheid. Mede door de veranderde internationale verhoudingen beoordelen zij de uitwisseling van kennis in samenwerkingsverbanden of de deelname van sommige buitenlandse studenten op een andere manier. Ook toetsen ze of via deze weg geen ongewenste kennis- en technologieoverdracht naar derde landen kan plaatsvinden. Onder leiding van het ministerie van Onderwijs, Cultuur en Wetenschappen worden instrumenten ontwikkeld die onderwijs- en onderzoeksinstellingen ondersteunen bij het inrichten van kennisveiligheid.

**Belangrijkste trends in andere sectoren**

Ook in andere sectoren is het aantal phishing-incidenten toegenomen. Het aantal ransomware-incidenten lijkt in Nederland niet substantieel te zijn gegroeid, het geëiste losgeldbedrag echter wel. Aanvallers doen vooraf onderzoek naar hun slachtoffers zodat ze hun eisen kunnen afstemmen op de budgettaire mogelijkheden van het slachtoffer.

2 https://nvd.nist.gov/

In een enquête van Forrester Consulting [28] gaf een van de 5.600 respondenten aan in één jaar tijd 45 miljoen euro te hebben uitgegeven aan de gevolgen van gijzelsoftware. Volgens hetzelfde onderzoek kost een dergelijk incident gemiddeld 827.000 euro.

Er wordt verschillend gedacht over het al dan niet betalen van losgeld. Soms is het een simpele rekensom. De gemeente Hof van Twente besloot om het gevraagde losgeld van 50 bitcoins (nu 937.000 euro) niet te betalen [29]. Volgens de gemeente waren de herstelkosten lager dan het gevraagde losgeld.

Het aantal politieaangiftes van cybercrime in 2020 is nog niet bekend. In 2019 is het aantal aangiftes naar bijna 4.500 gegroeid, in 2018 waren dat er 2.700. Omdat veel bedrijven geen aangifte doen, lijkt dit nog maar het topje van de ijsberg [28].

Onder andere vanwege de toename van het aantal dreigingen zal er de komende jaren nog een groot tekort aan cybersecurityexpertise zijn. Een vacaturesite in de Verenigde staten heeft onderzocht dat er in 2021 3,5 miljoen vacatures in het cybersecuritydomein zijn [30].

Ook in de andere sectoren wordt meer geïnvesteerd in maatregelen die de weerbaarheid verhogen. Een nieuwe trend is de belangstelling voor verzekeringen tegen cybercriminaliteit.

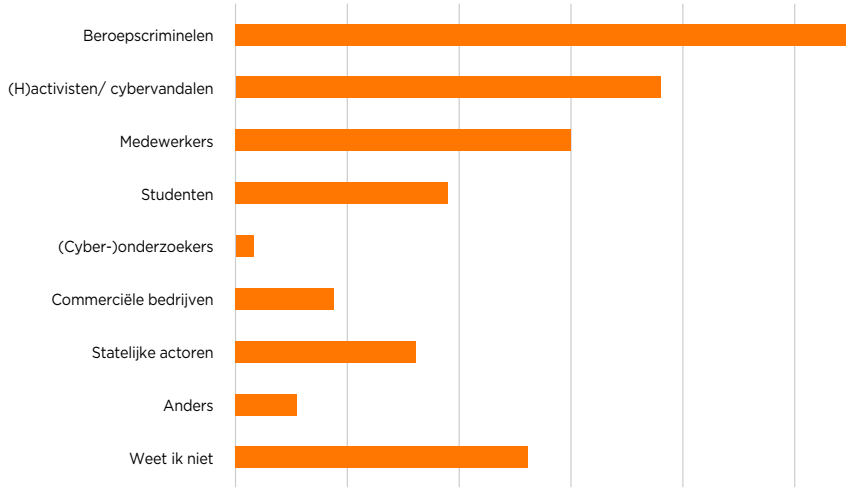
**Werkwijzen die in 2020 manifester zijn gesignaleerd**

Werkwijzen worden nog steeds geraffineerder, waarbij opvalt dat cybercriminelen gaan samenwerken om hun doel te bereiken. Ze delen gegevens van (potentiële) slachtoffers met elkaar en laten hacktools in opdracht ontwikkelen. Bij het gebruik van ransomware wordt vooraf onderzocht hoe het slachtoffer is georganiseerd en wordt ingeschat welk bedrag een slachtoffer kan betalen. In toenemende mate worden bestaande applicaties met malware geïnfecteerd en worden daarmee bij het uitrollen van updates van deze applicaties meerdere bedrijven en instellingen tegelijkertijd geïnfiltreerd [31].

**Actoren**

Als alle dreigingstypen worden samengevoegd, laat de survey zien dat instellingen *beroepscriminelen* als belangrijkste actoren zien, gevolgd door *(h)activisten/cybervandalen*. In het Cyberdreigingsbeeld 2019-2020 merkten we op dat het landelijk beeld, waarbij statelijke actoren en criminelen als voornaamste actoren werden genoemd, afweek van het beeld in de sector onderwijs en onderzoek. Iets wat we zelf niet herkenden. Maar inmiddels zijn er ook bij onderwijs en onderzoek sterke aanwijzingen dat statelijke actoren en criminelen steeds vaker bij instellingen in de sector binnendringen. Dit heeft geleid tot een pakket van overheidsmaatregelen om kennisveiligheid beter te borgen.

Figuur 2 **Meest genoemde actoren**

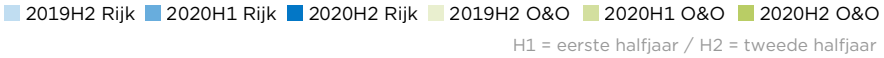


## Bij SURF waargenomen trends

### Internet-veiligheid metingen

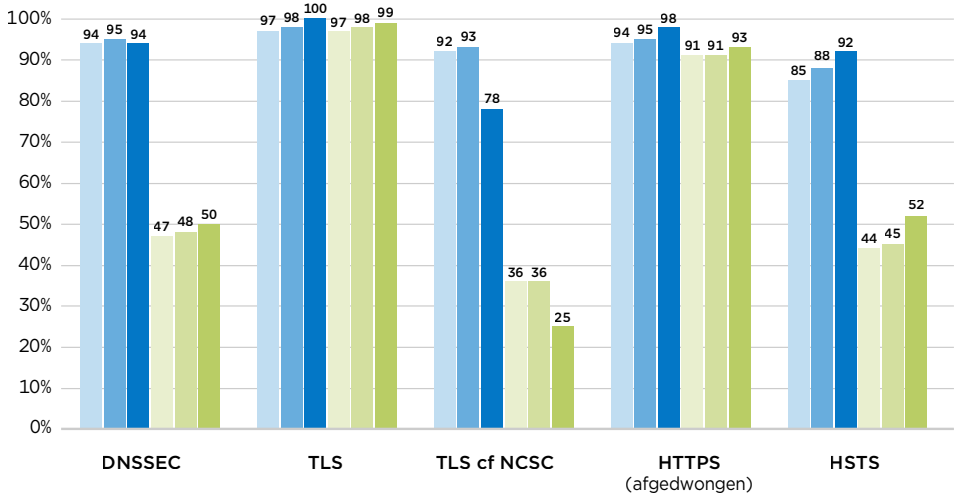
SURF voert al enkele jaren ieder kwartaal internet-veiligheidsmetingen uit, de IV-metingen, om in kaart te brengen in hoeverre onderwijs- en onderzoeksinstellingen voldoen aan de lijst van verplichte standaarden. Rijks- en semi-overheid moeten zich aan de standaarden op deze lijst houden bij de aanschaf en inrichting van ICT-systemen[3]. SURF participeert in het Forum Standaardisatie, dat deze lijst heeft opgesteld. In onderstaande grafieken laten we zien hoe de rijksoverheid (blauw) en de sector onderwijs en onderzoek (groen) ervoor staan. Merk op dat in het algemeen de rijksoverheid het beter doet dan onze sector.

Figuur 3 **IV-metingen 2020 - Rijksoverheid (blauw) en onderwijs & onderzoek (groen)**

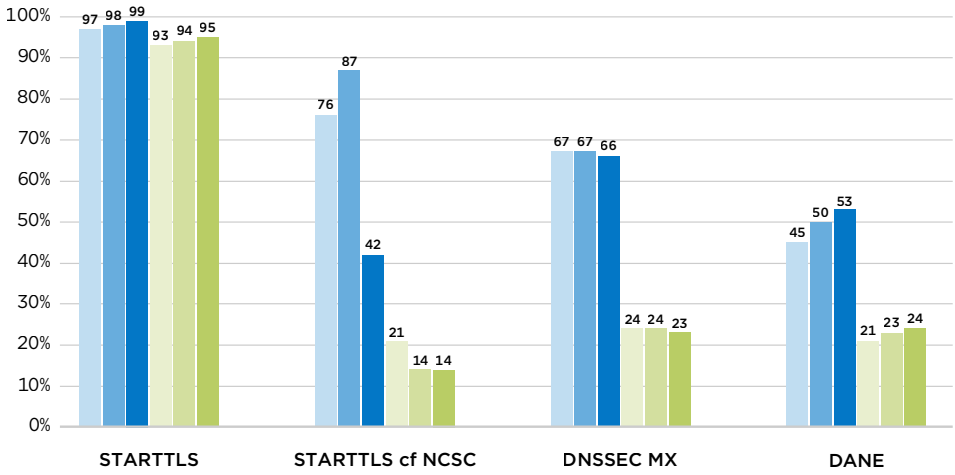



H1 = eerste halfjaar / H2 = tweede halfjaar

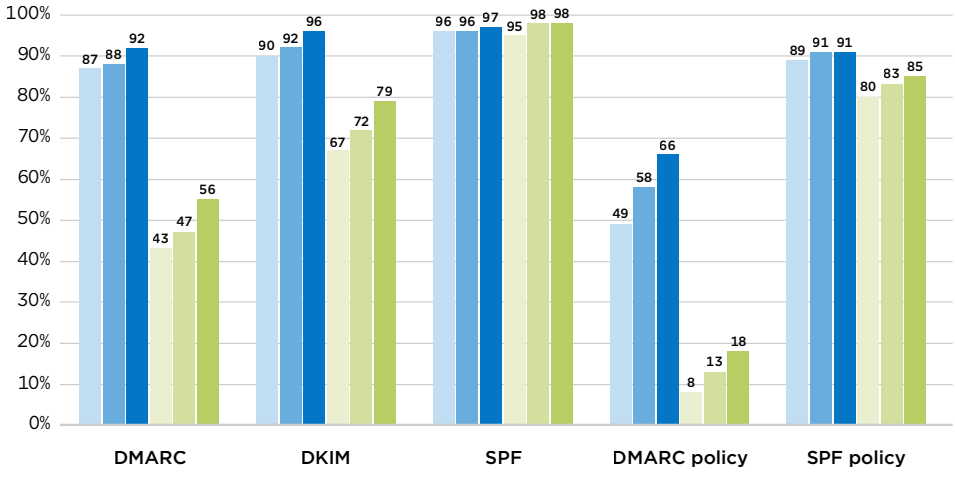
**Webstandaarden**




**Mailstandaarden (vertrouwelijk)**




**Mailstandaarden (anti-phising)**




3 https://www.forumstandaardisatie.nl/open-standaarden

**SURFcert**

SURFcert was na het UM-incident extra waakzaam, net als veel instellingen, maar heeft vervolgens geen grote ransomware aanvallen bij Nederlandse instellingen gezien. Wel werd in oktober 2020 de AP Hogeschool in Antwerpen getroffen door een ransomware-aanval waardoor hun campus tijdelijk gesloten was.

Het aantal Denial-of-Service (DoS)-aanvallen is in 2020 niet veel veranderd ten opzichte van 2019. Wel ziet SURFcert dat aanvallen langer duren en er enkele zeer krachtige aanvallen zijn geweest, wellicht gerelateerd aan de covid-19 pandemie.

SURFcert signaleert in zijn contacten met instellingen dat deze terughoudender zijn geworden met het delen van specifieke informatie over lopende incidenten, ook onderling. Bovendien lijkt de inhoudelijke kennis bij instellingen af te nemen, omdat ze steeds afhankelijker worden van enkele leveranciers. Dit alles bemoeilijkt incidentafhandeling. De invoering van en deelname aan SURFsoc zal dit naar verwachting ondervangen, omdat specifieke informatie dan door SURFsoc wordt verwerkt en daar meer kennis aanwezig is.

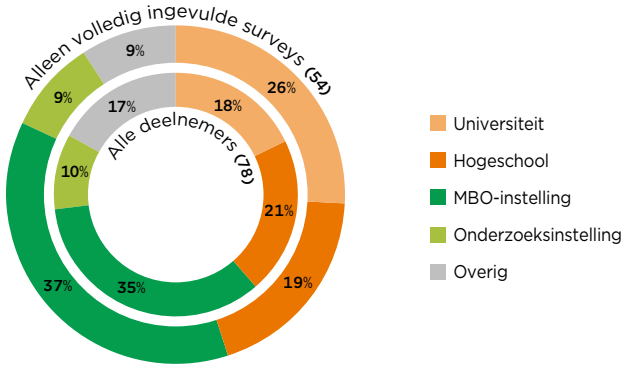
# 3 RESULTATEN VAN DE SURVEY

In dit hoofdstuk vind je een selectie van de resultaten van de survey die we in het najaar van 2020 hebben gehouden onder bij SURF aangesloten organisaties en alle mbo-instellingen. In totaal hebben 78 instellingen de survey ingevuld, 54 daarvan hebben de survey volledig ingevuld. Voor het analyseren van de resultaten hebben we primair de volledig ingevulde surveys gebruikt, maar in enkele gevallen ook extra informatie uit niet-volledig ingevulde surveys.

**Verdeling respondenten**

Van de volledig ingevulde surveys (54) is de verdeling universiteit, hogeschool, mbo-instelling, onderzoeksinstelling en overig als volgt (buitenste ring):

Figuur 4 **Verdeling van instellingen die hebben meegedaan aan de survey**



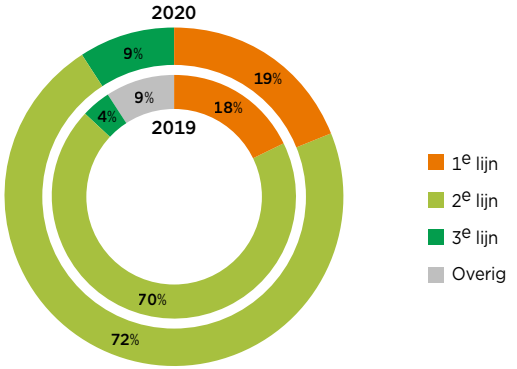

Kijken we naar alle deelnemers aan de survey (78) dan zien we dat de afvallers vooral in de categorie ‘overig’ zitten. In grote lijnen is dit dezelfde verdeling als bij de survey van 2019.

*De resultaten van de survey zijn daarom vooral van toepassing op de onderwijs- en onderzoeksinstellingen en minder op ziekenhuizen en andere niet-onderwijsinstellingen.*

**Rol van de respondenten**

We hebben gevraagd in welke lijn uit het ‘three lines model’ [32] de functie of rol van de respondent zit. Van degenen die de survey volledig hebben ingevuld is de vertegenwoordiging uit de tweede lijn veruit in de meerderheid. Functies in de tweede lijn zorgen voor beheer van risico’s en compliance met regelgeving en interne regels, zoals de security officer en de privacy officer.

Figuur 5 **Functie of rol van de respondenten**

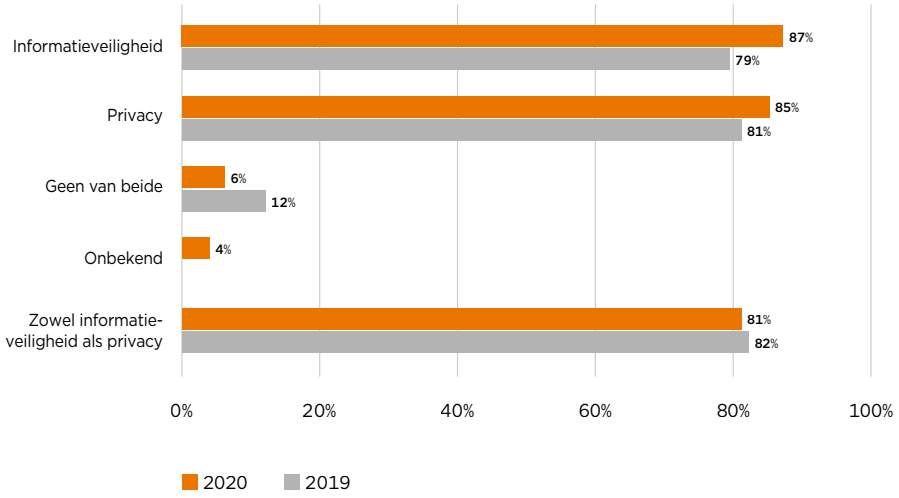



Ook in 2019 hadden de meeste respondenten een functie of rol in de tweede lijn (70%).

## Governance

Het overgrote deel van de instellingen rapporteert periodiek aan het college van bestuur over informatieveiligheid en privacy:

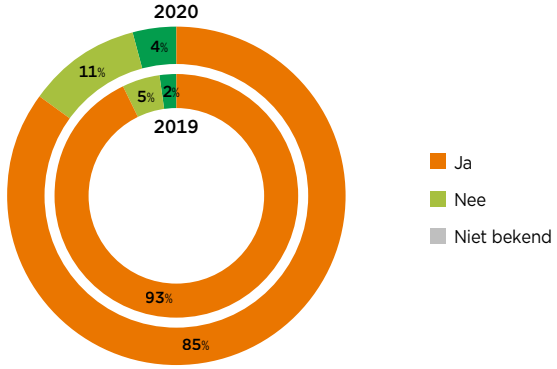
Figuur 6 **Rapportage aan het college van bestuur**




Het percentage instellingen dat over zowel informatieveiligheid als privacy rapporteert is 81%, in 2019 was dat 82%.

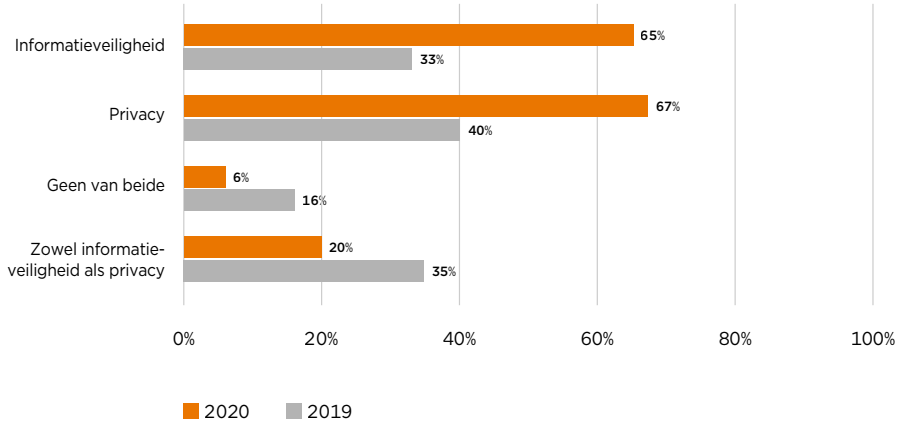
Het aantal instellingen dat bij een ernstig incident direct aan het bestuur rapporteert is iets gedaald ten opzichte van 2019; toen was dat 93%, nu 85%. Het percentage dat niet direct rapporteert bij een ernstig incident is echter gestegen van 5% naar 11%:

Figuur 7 **Rapportage bij een ernstig incident**



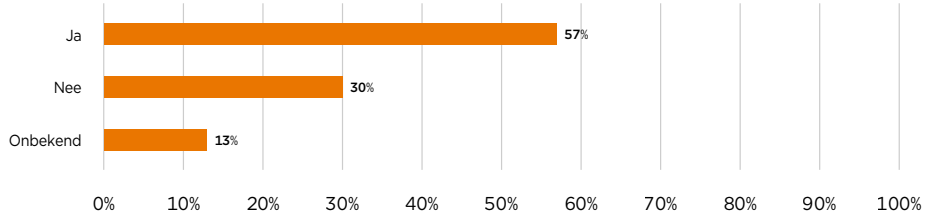

Als het gaat om rapportage aan de raad van toezicht, zien we dat dit bij circa 20% van de instellingen niet bekend is. Dat is een daling ten opzichte van 2019. Toen was dat niet bekend bij 35% van de instellingen. En het aantal instellingen dat aan de raad van toezicht rapporteert over informatieveiligheid en/of privacy is flink toegenomen.

Figuur 8 **Rapportage aan de raad van toezicht**



In 2020 besteedt ruim de helft van de instellingen aandacht aan informatie-veiligheid en privacy in het jaarverslag:

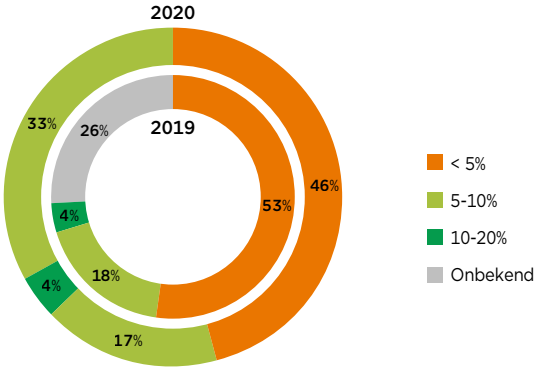
Figuur 9 **Aandacht voor informatieveiligheid en privacy in het jaarverslag**




## Budget en capaciteit

Bijna de helft van de instellingen besteedt minder dan 5% van het totale IT-budget aan informatiebeveiliging. In 2019 was dit percentage iets hoger, terwijl het percentage 'onbekend' iets is gestegen ten opzichte van 2019.

Figuur 10 **Percentage van het IT-budget voor informatiebeveiliging**

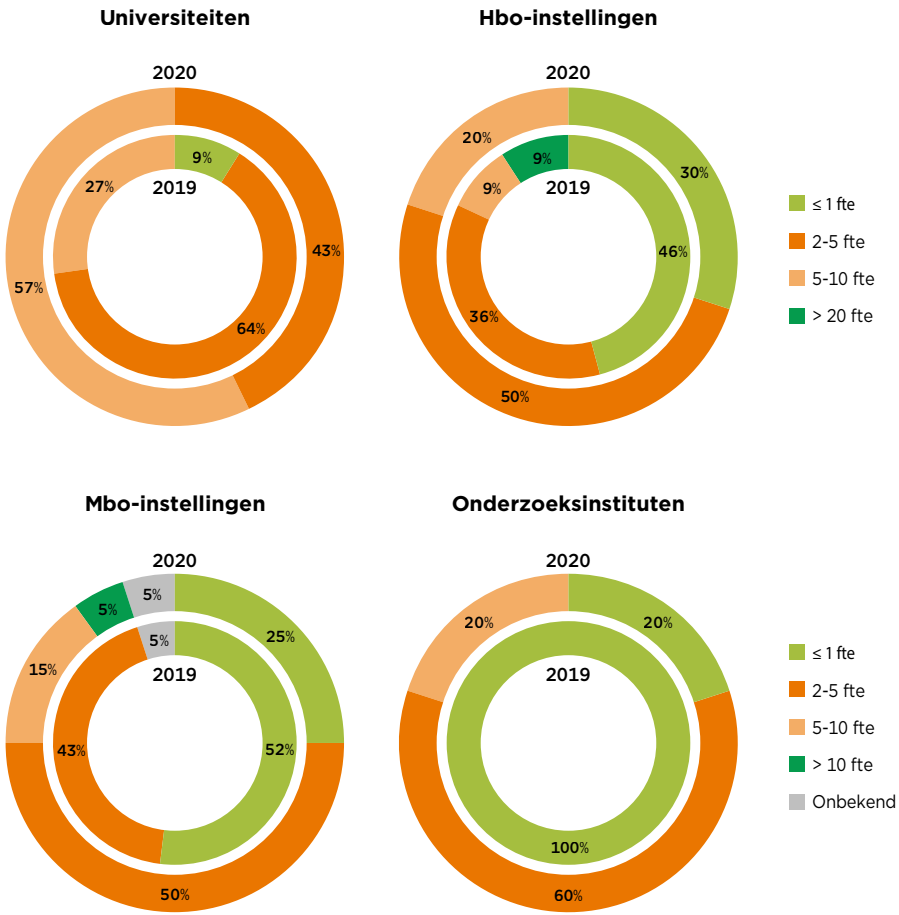



Wanneer we de instellingen naar grootte indelen, blijkt er een relatie te zijn met het aantal fte's dat beschikbaar is voor informatiebeveiliging:

Tabel 2 **Fte's naar grootte van de instelling**

| Fte's | Aantal medewerkers | Aantal studenten |
|---|---|---|
| **meer dan 10 fte** | 2.100 | 20.000 |
| **5 - 10 fte** | 1.150 - 6.100 | 10.000 - 46.000 |
| **2 - 5 fte** | 80 - 7.500 | 5.000 - 40.000 |
| **1 fte of minder** | 400 - 2.600 | 2.600 - 23.000 |

Figuur 11 **Aantallen fte's die beschikbaar zijn voor informatiebeveiliging**

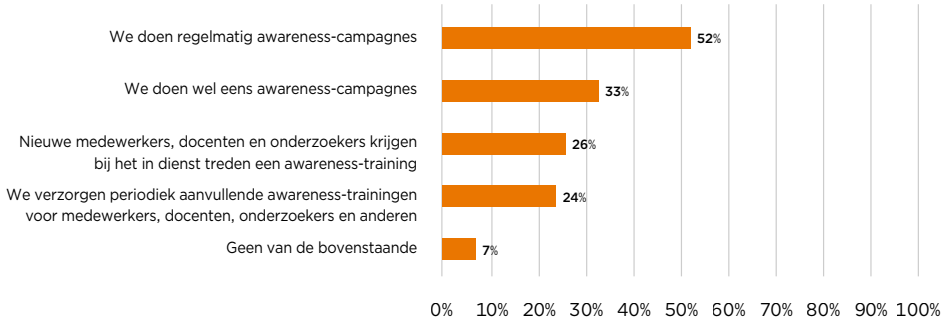



*In vergelijking met 2019 is er meer capaciteit gekomen voor informatie-beveiliging in de sector onderwijs en onderzoek*

## Awareness

Het merendeel van de instellingen voert regelmatig awareness-campagnes uit:

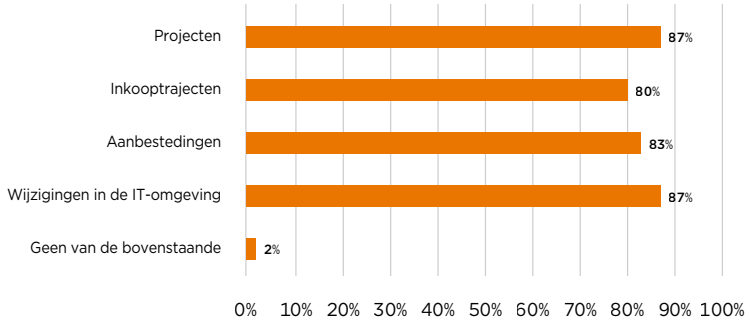
Figuur 12 **Awareness-campagnes**




In de 2019 was de vraag anders geformuleerd, maar het lijkt erop dat er sprake is van een toename in 2020.

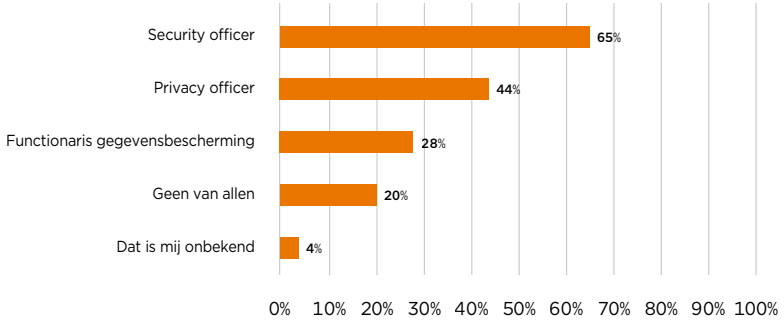
Op de vraag of er aandacht wordt besteed aan security en privacy by design geeft een groot aantal (meer dan 80%) instellingen aan dat dit het geval is:

Figuur 13 **Aandacht voor security en privacy by design**



Het percentage instellingen dat de security of privacy officer betrekt bij projecten is ook hoog (respectievelijk 65% en 44%):

Figuur 14 **Betrokkenheid officers bij projecten**




## Incidenten

In 2020 was er een aantal incidenten die flinke disruptie hebben veroorzaakt. In de eerste plaats zijn dat de ransomware-aanval op de Universiteit Maastricht van eind 2019 en het beveiligingslek in Citrix-apparatuur en -software van begin 2020 dat bij een aantal organisaties misbruikt is.

*In de survey hebben we gevraagd naar de reactie van de instelling op het UM-incident en het Citrix-incident. Specifiek hebben we gevraagd naar de lessons learned die de Universiteit Maastricht heeft genoemd bij de eigen evaluatie van het incident* [33].

*Het merendeel van de instellingen heeft naar aanleiding van deze incidenten bewustwordingscampagnes opgezet om medewerkers beter te informeren over bijvoorbeeld phishing en ransomware. Verder heeft ruim driekwart van de instellingen technische maatregelen ingevoerd of initiatieven voor security operations genomen om hun weerbaarheid te verhogen.*

*Meer dan de helft van de respondenten geeft aan dat er geen up-to-date inventaris van IT-systemen is of weet het niet. En ruim een kwart geeft aan dat de kroonjuwelen niet regelmatig gecontroleerd worden op kwetsbaarheden of aanwezigheid van recente patches.*

*Verder zegt meer dan de helft van de respondenten dat er geen beleid is voor 'true' offline back-ups, back-ups die niet benaderbaar zijn via het interne netwerk of internet nadat ze gemaakt zijn.*

Verder was er de covid-19-pandemie die grote gevolgen heeft gehad voor de instellingen. Er moest snel worden overgeschakeld op online onderwijs, waardoor informatiebeveiliging en gegevensbescherming op het tweede plan dreigden te komen.

*In de survey hebben we ook gevraagd welke invloed de uitbraak van covid-19 op de al genomen initiatieven naar aanleiding van die incidenten heeft gehad en welke extra maatregelen zijn genomen.*

*Meer dan driekwart van de respondenten geeft aan dat eerder opgestarte initiatieven vanwege het UM- of Citrix-incident niet zijn stopgezet. In een aantal gevallen zijn ze vertraagd, in andere gevallen juist versneld.*

*De meest genoemde maatregelen die zijn genomen naar aanleiding van de covid-19-pandemie zijn:*

1. *De uitrol van virtual private networks (VPN);*
2. *Het invoeren van multi-/twee-factorauthenticatie;*
3. *Awareness-campagnes, voorlichting en het geven van instructies over veilig thuiswerken.*

In bijlage 1 vind je meer resultaten van de survey.

**Risicocategorieën**
Voor de sector onderwijs en onderzoek zijn 7 belangrijke risicocategorieën vastgesteld.

In de survey hebben we gevraagd of het aantal incidenten in deze categorieën is toegenomen, afgenomen of gelijk is gebleven ten opzichte van 2019 en in welk proces (onderwijs, onderzoek of bedrijfsvoering) de meeste incidenten zijn voorgekomen.

Tabel 3 **Dynamiek van cyber-incidenten**

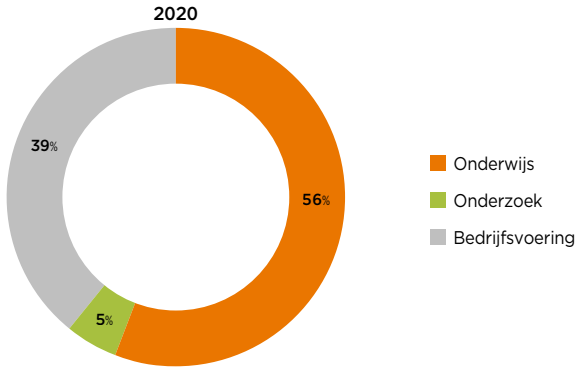
| Categorie | Toe- of afname | Komt meest voor bij |
|---|---|---|
| 1 Verkrijging en openbaarmaking van informatie | Lichte afname | Onderwijs |
| 2 Identiteitsfraude | Geen toe- of afname | Onderwijs |
| 3 Verstoring ICT | Geen toe- of afname | Onderwijs |
| 4 Manipulatie van data | Lichte afname | Onderwijs |
| 5 Spionage | Geen toe- of afname | Onderzoek |
| 6 Overname en misbruik ICT | Lichte afname | Onderwijs |
| 7 Bewust beschadigen imago | Geen toe- of afname | Onderwijs |

We zien dat het totaal aantal incidenten licht is afgenomen ten opzichte van 2019, behalve voor de categorieën *Identiteitsfraude, Spionage** en *Bewust beschadigen van imago** waarbij geen toe- of afname was. We zien ook dat de meeste incidenten zich voordoen bij het onderwijsproces met uitzondering van Spionage.

* Bij de categorieën Spionage en Bewust beschadigen van imago is de onzekerheid waar incidenten het meest voorkomen het hoogst: circa 80% van de respondenten weet het niet.

Uit de antwoorden op de vraag ‘Hoe vaak en bij welk proces hebben zich incidenten voorgedaan met clouddiensten?’ blijkt dat het onderwijsproces de meeste incidenten heeft gehad en het onderzoekproces de minste:

Figuur 15 **Incidenten bij clouddiensten**




## Risicoperceptie

We hebben ook gevraagd naar toe- of afname van het ingeschatte risico ten opzichte van 2019 voor de 7 risicocategorieën met als resultaat dat bij het onderwijsproces, het onderzoekproces en de bedrijfsvoering de risico’s hoger worden ingeschat dan in 2019. Alleen bij *Bewust beschadigen van het imago* wordt het risico iets lager ingeschat bij alle 3 de processen. Bij het onderwijsproces en bij bedrijfsvoering wordt ook voor *Spionage* een iets lagere risico inschatting gedaan.

Daarnaast hebben we gevraagd om een risico-inschatting te geven voor de *Afhankelijkheid van clouddiensten* en die toegevoegd als achtste risico aan tabel 1. Instellingen verplaatsen hun data en applicaties steeds meer naar de cloud. Dat geeft een ander risicoprofiel. Het is bijvoorbeeld veel lastiger de staat van informatiebeveiliging te bepalen bij de clouddiensten zelf, en vaak bevinden de data zich buiten de EER, waardoor mogelijk niet wordt voldaan aan de AVG. Ook is

er een beperkt aantal leveranciers van clouddiensten, wat hen een monopolie-positie geeft, en zijn ze vooral in de VS gevestigd. Naar analogie van Stephen Covey[4] hebben we *Afhankelijkheid van clouddiensten* toegevoegd als achtste risicocategorie aan deze tabel:

Tabel 1 **Risicoperceptie en dynamiek**

| Categorie | Onderwijs △ | Onderzoek △ | Bedrijfsvoering △ |
|---|---|---|---|
| 1 Verkrijging en openbaarmaking van informatie | **Zeer hoog** ↑ | **Zeer hoog** ↑ | **Zeer hoog** ↑ |
| 2 Identiteitsfraude | **Hoog** ↑ | **Medium** ↑ | **Hoog** ↑ |
| 3 Verstoring ICT | **Zeer hoog** ↑ | **Hoog** ↑ | **Zeer hoog** ↑ |
| 4 Manipulatie van data | **Hoog** ↑ | **Medium** ↑ | **Medium** ↑ |
| 5 Spionage* | **Laag** — | **Medium** ↑ | **Laag** — |
| 6 Overname en misbruik ICT | **Hoog** ↑ | **Hoog** ↑ | **Zeer hoog** ↑ |
| 7 Bewust beschadigen imago | **Medium** ↓ | **Medium** ↓ | **Medium** ↓ |
| 8 Afhankelijkheid van clouddiensten | **Zeer hoog** ○ | **Medium** ○ | **Hoog** ○ |

△ Ontwikkeling 2020 t.o.v. 2019

↑ Forse toename t.o.v. 2019

↑ Toename t.o.v. 2019

— Geen verandering t.o.v. 2019

↓ Afname t.o.v. 2019

↓ Forse afname t.o.v. 2019

○ Geen vergelijking met 2019

** Bij Spionage is de onzekerheid het grootst (36% weet niet of het risico is toe- of afgenomen)*

**Toelichting risiconiveaus:**

| **Laag** (groen) | **Medium** (geel) | **Hoog** (oranje) | **Zeer hoog** (rood) |
|---|---|---|---|
| De dreiging is aanwezig, neemt niet toe en voldoende maatregelen zijn beschikbaar, of incidenten doen zich nauwelijks voor. | De dreiging is aanwezig en voldoende maatregelen zijn beschikbaar, of incidenten komen weleens voor. | De dreiging is acuut, neemt toe en maatregelen hebben enig effect gehad, of incidenten komen vaak voor. | De dreiging is acuut, neemt toe en maatregelen hebben nauwelijks effect gehad, of incidenten komen steeds vaker voor. |

4 Stephen R. Covey, The 8th Habit, Simon & Schuster 2005

## Actoren

In de onderstaande tabel zijn de meest genoemde actoren per risicocategorie aangegeven.

Tabel 4 **Belangrijkste actoren voor onderwijs, onderzoek en bedrijfsvoering**

| Categorie | Onderwijs | Onderzoek | Bedrijfsvoering |
|---|---|---|---|
| 1 **Verkrijging en openbaarmaking van informatie** | Medewerkers | Beroeps-criminelen<br>Medewerkers | Medewerkers |
| 2 **Identiteitsfraude** | Beroeps-criminelen<br>Studenten | Beroeps-criminelen | Beroeps-criminelen |
| 3 **Verstoring ICT** | (H)activisten/ cybervandalen | (H)activisten/ cybervandalen | Beroeps-criminelen<br>(H)activisten/ cybervandalen |
| 4 **Manipulatie van data** | Studenten | Beroeps-criminelen | Beroeps-criminelen<br>Medewerkers |
| 5 **Spionage** | Statelijke actoren | Statelijke actoren | Statelijke actoren<br>Onbekend |
| 6 **Overname en misbruik ICT** | Beroeps-criminelen<br>(H)activisten/ cybervandalen | Beroeps-criminelen | Beroeps-criminelen |
| 7 **Bewust beschadigen imago** | (H)activisten/ cybervandalen<br>Onbekend | (H)activisten/ cybervandalen | (H)activisten/ cybervandalen<br>Onbekend |

Opvallende verschillen met 2019 zijn:

1 **Verkrijging en openbaarmaking van informatie:** bij onderzoek worden beroepscriminelen nu het meest genoemd, in 2019 waren dat medewerkers.
2 **Identiteitsfraude:** bij bedrijfsvoering was het aandeel medewerkers in 2019 veel hoger, nu is dat verwaarloosbaar.
3 **Verstoring ICT:** nu worden vooral (h)activisten/cybervandalen genoemd, in 2019 bij onderwijs ook studenten en bij bedrijfsvoering ook medewerkers.
4 **Manipulatie van data:** respondenten noemen beroepscriminelen nu bij onderzoek en bedrijfsvoering als grootste categorie in plaats van respectievelijk medewerkers en (h)activisten/cybervandalen.
5 **Spionage:** geen grote verandering.
6 **Overname en misbruik ICT:** (h)activisten/cybervandalen zijn erbij gekomen voor onderwijs.
7 **Bewust beschadigen imago:** voor onderwijs was dit in 2019 (h)activisten/cybervandalen en studenten.

## Afhankelijkheid van clouddiensten

De categorie *Afhankelijkheid van clouddiensten* hebben we niet in tabel 3 opgenomen, omdat het lastig is hiervoor actoren te noemen; het percentage respondenten dat onbekend antwoordde was heel hoog.

Voor deze categorie ligt de impact vooral op het vlak van continuïteit. Wanneer er een probleem is met een clouddienst, heeft dat direct invloed op de beschikbaarheid. Problemen kunnen technisch van aard zijn (‘internet niet beschikbaar’ kan direct invloed hebben op productiviteit), maar ook anderszins de continuïteit beïnvloeden. De ongeldigverklaring van het EU-VS Privacy Shield bijvoorbeeld betekent dat het gebruik van een dienst bij een bedrijf dat buiten de EER is gevestigd, illegaal [34] kan zijn. Bij een grote afhankelijkheid van een dienst als bijvoorbeeld Microsoft Office 365, is het moeilijk, zo niet onmogelijk, om over te stappen naar een alternatieve leverancier. Instellingen moeten dit risico onderkennen en hiervoor een exit-strategie vaststellen.

In het Cyberdreigingsbeeld 2019-2020 noemden we al de open brief die de rectores magnifici van de Nederlandse universiteiten in de Volkskrant publiceerden [35]. Hierin waarschuwen zij voor de macht 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 schade 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 van geopolitieke conflicten.

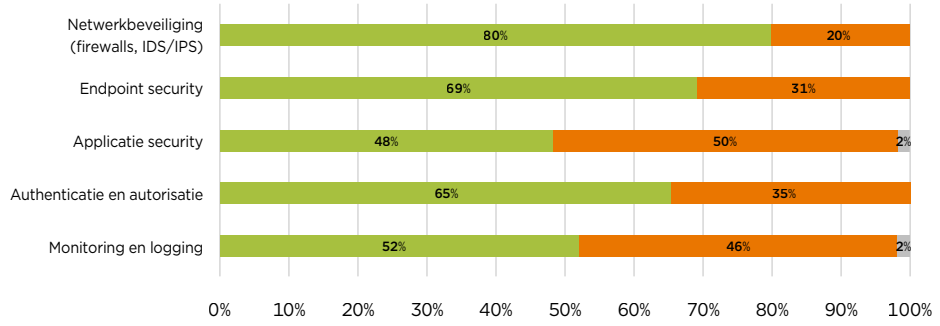
# 4 WEERBAARHEID

Mede ingegeven door het incident bij de Universiteit Maastricht hebben veel onderwijs- en onderzoeksinstellingen extra maatregelen genomen om hun weerbaarheid te verhogen. Uit de survey blijkt dat het niveau desondanks nog niet overal voldoende is.

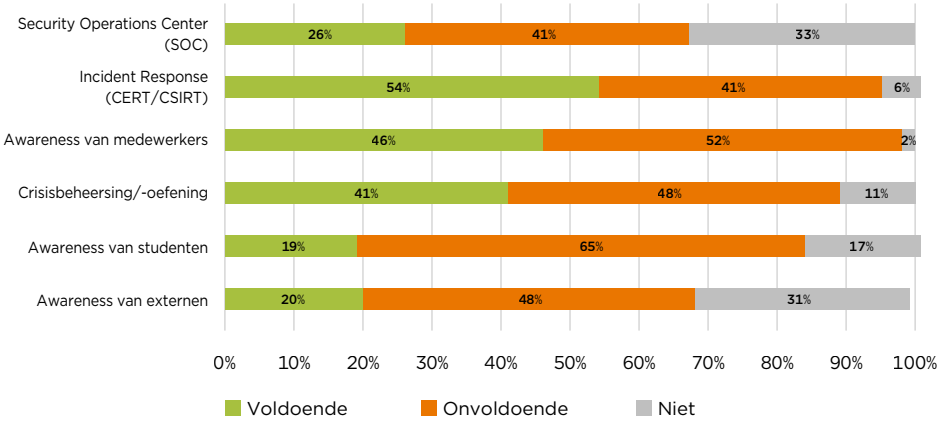
## Investeringen in weerbaarheid

De meeste respondenten vinden dat voldoende wordt geïnvesteerd in operationele security, zoals *Netwerkbeveiliging, Endpoint security, Authenticatie en autorisatie en Incident Response* (zie Figuur 16). Ten opzichte van het Cyberdreigingsbeeld 2019-2020 is opvallend dat de meeste respondenten nu vinden dat er voldoende wordt geïnvesteerd in *Monitoring en logging* en dat *Security Operations Centre* (SOC) daarbij achterblijft. Een mogelijke verklaring is dat veel instellingen wachten tot zij aan kunnen sluiten op SURFsoc. Volgens de survey is in 2020 meer geïnvesteerd in awareness. Desondanks worden investeringen in awareness evenals in 2019 opnieuw als onvoldoende beoordeeld.

Figuur 16 **Mate van investering in beveiligingsmaatregelen (technisch)**



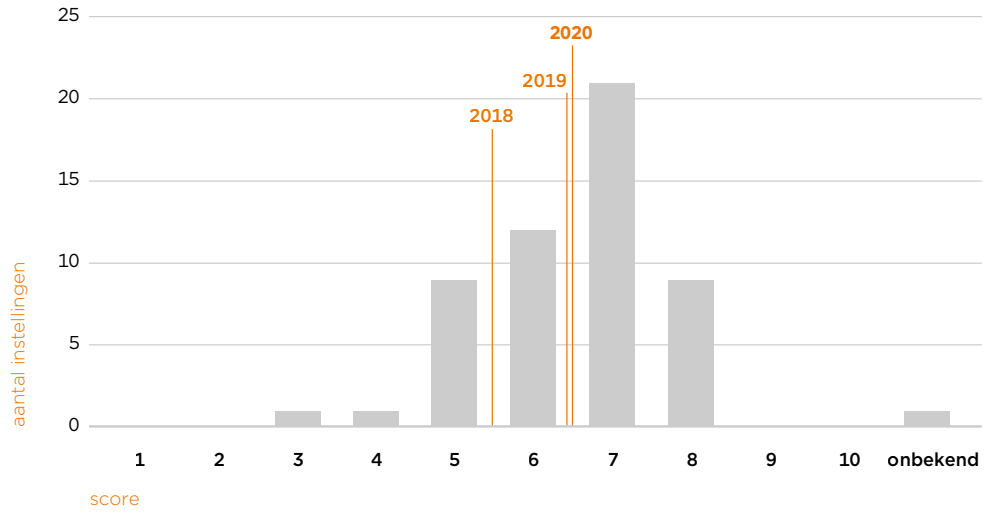

**Mate van investering in beveiligingsmaatregelen (niet technisch)**



**Effectiviteit van maatregelen**
Voor een effectieve weerbaarheid worden *Netwerkbeveiliging (firewalls, IDS/IPS), Awareness van medewerkers* en *Identity en Access Management* als meest effectief beschouwd.

**Beoordeling eigen cyberweerbaarheid sector onderwijs en onderzoek**
Respondenten beoordelen de cyberweerbaarheid van de eigen organisatie gemiddeld met een voldoende (score 6,5 op een schaal van 0 – 10). Dit is een lichte stijging ten opzichte van 2019 toen de score 6,3 bedroeg. Op basis van deze uitkomsten kunnen we stellen dat er, ondanks enige vooruitgang, bij onderwijs- en onderzoeksinstellingen nog genoeg ruimte is voor verdere verhoging van de cyberweerbaarheid.

Figuur 17 **Weerbaarheid 2020 en gemiddelde per jaar**




**Weerbaarheid verhogende maatregelen**
In de survey worden voor 2020 worden *Netwerkbeveiliging (firewalls, IDS/IPS), Awareness van medewerkers en Identity en Access Management* als belangrijkste maatregelen genoemd waarin wordt geïnvesteerd.

**Cyberweerbaarheid overige sectoren**
In de reactie van de minister van Justitie en Veiligheid op het rapport 'Voorbereiden op digitale ontwrichting' van de WRR [36] is een aantal weerbaarheid verhogende maatregelen voor vitale sectoren en voor de overheid zelf aangekondigd of in gang gezet. Belangrijke onderdelen zijn het 'pas toe of leg uit'-principe voor vitale sectoren en overheid waarbij verantwoording moet worden afgelegd bij het niet uitvoeren van beveiligingsadviezen van het NCSC en een verdere samenwerking op zowel nationaal als internationaal niveau. Daarnaast wordt oefening als een belangrijke maatregel gezien om voorbereid te zijn op incidenten. Tot slot wordt voor de vitale sectoren en de overheid meer nadruk gelegd op toezicht en verantwoording. Inzet van het kabinet is om cybersecurity een centraal onderdeel te maken van het brede toezichtsbeleid.

Voor de overige sectoren laat een researchrapport van McKinsey [37] zien dat grote bedrijven (meer dan 5.000 werknemers) het komende jaar voornamelijk investeren in netwerkbeveiliging, identity management en e-mailbeveiliging.

# 5 CONCLUSIE

De covid-19-pandemie heeft ervoor gezorgd dat we op een andere manier zijn gaan werken. Thuiswerken en onderwijs op afstand zijn de norm geworden. Desondanks wijkt het Cyberdreigingsbeeld 2020-2021 onderwijs en onderzoek op het eerste gezicht niet heel veel af van het rapport uit 2019. Het aantal dreigingen is wederom gestegen, maar het type dreigingen is niet wezenlijk veranderd. Phishing, ransomware en identiteitsfraude (als gevolg van phishing) zijn nog steeds de meest voorkomende incidenten. Een nadere analyse van incidenten legt echter wel een paar nieuwe ontwikkelingen bloot.

**Andere actoren en toegenomen complexiteit**

- Hoewel financieel gewin in de meeste gevallen nog het doel is, lijkt er ook een stijgende lijn te zijn in dreigingen afkomstig van statelijke actoren.
- Er lijkt vaker te worden samengewerkt tussen actoren waarbij de ene partij voor een andere softwaretools ontwikkelt (of steelt [38]) om misbruik te plegen.
- De softwaretools zijn steeds geavanceerder waardoor de complexiteit van aanvallen toeneemt.
- De toename van dreigingen door statelijke actoren en de toegenomen complexiteit vereisen dat er nog meer wordt geïnvesteerd kennisveiligheid en expertise op het gebied van cybersecurity.

**Bewustwording en opleiding gebruikers steeds crucialer**

Het aantal pogingen tot phishing is explosief gestegen. Niet alleen via e-mail maar ook via WhatsApp en social media. De methoden worden nog steeds geraffineerder. Investeren in opleiding en bewustwording wordt steeds crucialer zodat de gebruiker ook weerbaarder wordt tegen de nieuwste dreigingen.

**Risicoprofiel cloudgebruik**

In 2020 is de afhankelijkheid van een klein aantal grote cloudproviders verder toegenomen. Het aantal incidenten bij cloudproviders is ook toegenomen. Dit is een risico voor de continuïteit. Ketenafhankelijkheid, back-up, de mogelijkheid om bij een ernstige calamiteit terug te vallen op alternatieven vereisen continue aandacht. Het ongeldig verklaren van het Privacy Shield onderstreept dit en dwingt organisaties na te denken over hun sourcingstrategie.

**Samenwerking**

Vorig jaar deden we al een oproep in het Cyberdreigingsbeeld om meer samen te werken, zodat we dreigingen beter het hoofd kunnen bieden. In 2020 hebben we zowel binnen als buiten de sector onderwijs en onderzoek toenemende samenwerking gezien.

De universiteiten hebben bijvoorbeeld het initiatief genomen om samen met SURF een project voor het inrichten van een Security Operations Centre te starten. Hieruit is de lancering van het SURFsoc in januari 2021 voortgekomen. Deze vorm van samenwerking is een goed voorbeeld van het optimaal inzetten van bij de sector aanwezige expertise en het efficiënt inzetten van middelen.

Op landelijk niveau wordt sinds begin 2020 samengewerkt op het gebied van incident response in het Landelijk Dekkend Stelsel [39], een samenwerking van het NCSC met sectorale samenwerkingsverbanden, CERT's en andere publieke en private partijen om informatie en kennis over bijvoorbeeld kwetsbaarheden en dreigingen uit te wisselen. SURFcert vertegenwoordigt de sector onderwijs en onderzoek hierin.

**Expertise en middelen zijn nog steeds schaars**

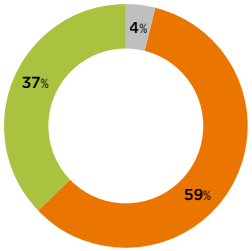
Er zal de komende jaren nog schaarste aan cybersecurityexpertise zijn. Bovendien valt te verwachten dat na de covid-19-pandemie financiële middelen ook schaarser worden. Dit versterkt de noodzaak tot samenwerking. De in deze paragraaf genoemde samenwerkingsverbanden zijn tot nu toe succesvol gebleken en verdienen navolging.

# BIJLAGE 1 **SURVEY RESULTATEN DETAIL**

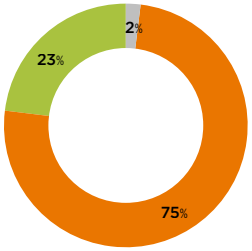
De looptijd van de survey was van 23 september tot 9 november 2020

**Effect van significante gebeurtenissen in 2020**
In de survey hebben we gevraagd naar de reactie van de instelling op het UM-incident en het Citrix-incident. Specifiek hebben we gevraagd naar de lessons learned die de Universiteit Maastricht heeft genoemd bij de eigen evaluatie van het incident [30].

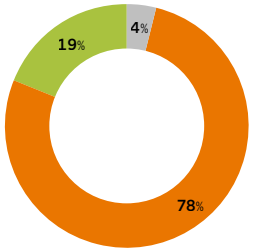
**1** Zijn er bij jouw instelling nieuwe bewustwordings-campagnes opgezet om medewerkers te helpen phishing-mails beter te herkennen?



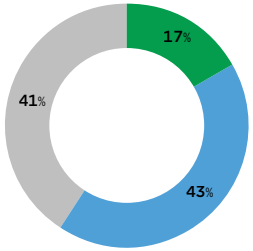

**2** Heeft jouw instelling beleid geïmplementeerd voor het gebruik van ‘privileged accounts’, zoals ‘root’ en ‘administrator’, ook in de Windows-omgeving?



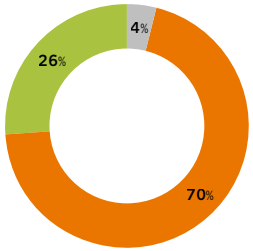

**3** Neemt jouw instelling initiatieven op het vlak van SOC/SIEM, individueel of samen met andere instellingen?



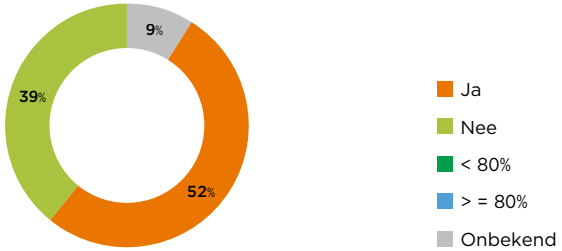

**4** Wat is het percentage systemen waarvan bij jouw instelling een up-to-date inventaris van IT-middelen (CMDB) is, inclusief die in een cloud-omgeving (AWS, Azure et cetera)?




**5** Worden de belangrijke systemen (kroonjuwelen) tenminste enkele keren per jaar gescand op kwets-baarheden en/of patch-niveau?



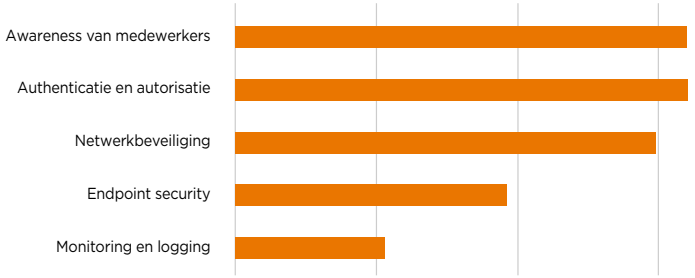

**6** Heeft jouw instelling een backup-restore-beleid waarbij offline back-ups echt niet benaderbaar zijn vanaf het interne of een extern netwerk nadat ze zijn gemaakt (‘true’ offline back-ups)?



## Maatregelen en trends

Welke 5 maatregelen zijn het meest effectief:

Figuur 18 **Top 5 meest effectieve maatregelen voor informatieveiligheid**




Awareness van studenten en van medewerkers worden als meest effectief beschouwd.

Maatregelen die niet zijn uitgevraagd maar ook belangrijk worden gevonden:

- E-mailsecurity-, anti-spam- en anti-phishing-maatregelen
- Het hebben van een ISMS (Information Security Management System zoals bijvoorbeeld is beschreven in de ISO 27001 standaard)
- Business en IT-continuity management
- Segmentering van het netwerk
- Regelmatig pentesten uitvoeren en op kwetsbaarheden scannen

Ook hebben we gevraagd welke aandacht er is voor de trends die in het Cyberdreigingsbeeld van 2019-2020 zijn genoemd en voor ontwikkelingen uit het SURF tweejarenplan die raakvlakken hebben met informatieveiligheid of privacy.

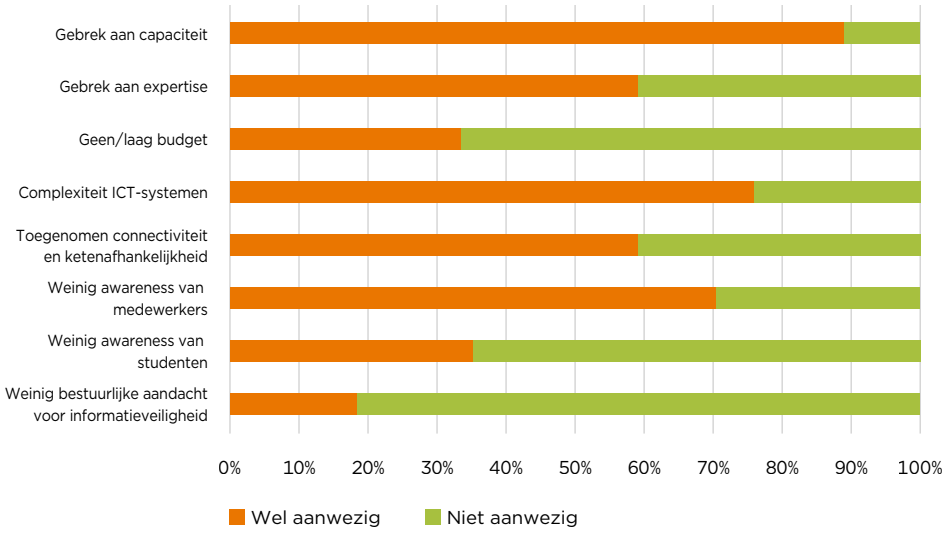
Tabel 5 **Aandacht voor trends en ontwikkelingen**

| Trend of ontwikkeling | Mate van aandacht |
|---|---|
| Internet of things | **Beperkt** |
| Edge computing | **Zeer beperkt** |
| Artificial intelligence | **Beperkt** |
| Trusted data sharing | **Gemiddeld** |
| Public cloud | **Gemiddeld** |
| Afhankelijkheid van beperkt aantal aanbieders | **Gemiddeld** |
| Toename ransomware | **Gemiddeld** |
| Phishing | **Zeer veel** |
| Denial of service | **Gemiddeld** |
| Ketenafhankelijkheid | **Gemiddeld** |

## Kwetsbaarheden in de organisatie

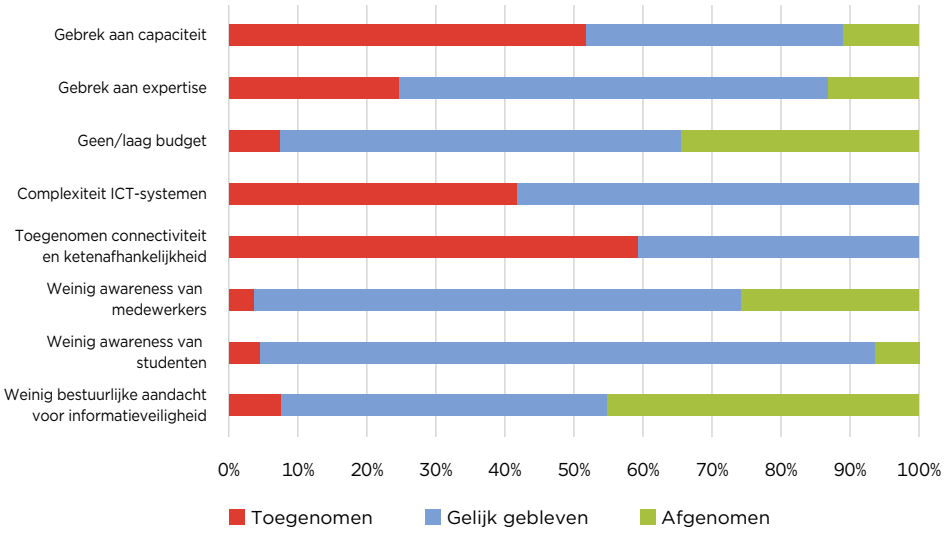
Welke kwetsbaarheden zijn in de organisatie aanwezig:

Figuur 19 **Kwetsbaarheden in de organisatie**



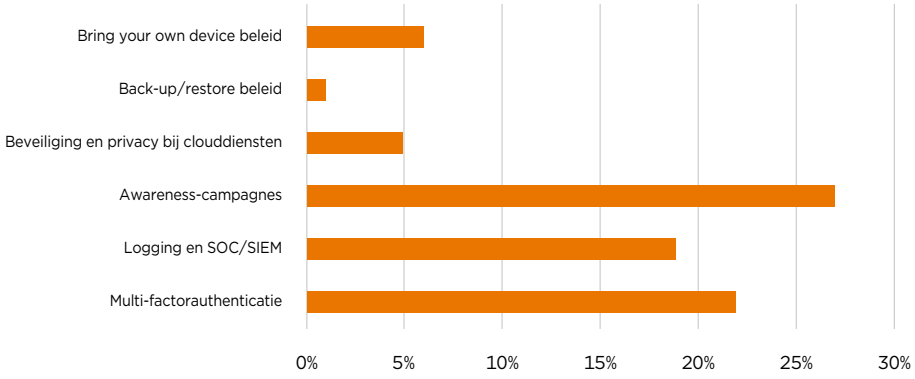

Dynamiek van deze kwetsbaarheden, is er een toe- of afname sinds 2019:

Figuur 20 **Dynamiek van kwetsbaarheden in de organisatie**



Informatieveiligheid wordt beïnvloed door verschillende factoren, bijvoorbeeld het gebruik van clouddiensten, de frequentie van awareness-campagnes, gebruik van multi-factorauthenticatie en de adoptie van BYOD. Welke 3 aspecten van informatieveiligheid hebben bij jouw instelling de hoogste prioriteit voor 2021, dat wil zeggen dat ze benoemd zijn in het jaarplan voor 2021 en/of zijn opgenomen in de begroting 2021:

Figuur 21 **Aspecten die zijn opgenomen in het jaarplan of de begroting**




**Dreigingen**

Wat zijn de top drie dreigingen/risico's voor jouw instelling in 2020?

Bij deze vraag zijn vele dreigingen genoemd, zoals onder andere (in willekeurige volgorde):

- Ransomware
- Informatiebeveiliging en Privacy als onderwerp op agenda bij lijnmanagement
- Datalekken (bijvoorbeeld exportknoppen in systemen met gevoelige data)
- Versnelde digitalisering van onderwijs en onderzoek
- Verstoring van ICT-voorzieningen
- Phishing
- Imagoschade (wetenschappelijke integriteit/ privacy-ongelukken)
- Reputatieschade
- (Business) continuity
- Openbaar maken van data
- Blokkeren of haperen van digitaal/online onderwijs
- Ontbrekende/onvoldoende bestuurlijke inbedding
- Uitval ICT-systemen
- Identiteitsfraude

De 3 meest genoemde dreigingen met hoge impact in 2020 zijn:

1 Phishing
2 Ransomware
3 Datalekken

Dit komt ook overeen met trends in andere sectoren.

# BIJLAGE 2 **AFKORTINGEN EN BEGRIPPEN**

| Begrip / afkorting | Betekenis | Bron[5] |
|---|---|---|
| **Actor** | Ook threat actor of kwaadwillende; iemand die misbruik maakt van kwetsbaarheden om een dreiging ten uitvoer te brengen. | WCN |
| **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 |
| **Awareness** | Bewustzijn. In dit verband wordt bedoeld dat gebruikers zich bewust zijn van cyberdreigingen en daardoor op een verantwoordelijke manier handelen. | 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 |
| **Denial-of-service** | (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 |
| **EER** | Europese Economische Ruimte; landen van de EER hebben toegang tot de interne markt van de EU en zijn ook gebonden aan het vrije verkeer van personen, goederen, diensten en kapitaal. De EER telt 31 lidstaten: de 28 EU-lidstaten plus Noorwegen, IJsland en Liechtenstein. | WP |
| **Endpoint security** | Beveiliging van eindsystemen (PC's, laptops, tablets et cetera) – niet beperkt tot anti-virus, maar ook bijvoorbeeld data-leak protection (DLP). | 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 |
| **Hacktivist** | Iemand die digitale aanvallen uitvoert om een bepaalde ideologie te promoten. | WP |
| **MFA/2FA** | Multi-factorauthenticatie of twee-factorauthenticatie; methode waarbij 2 of meer identificerende factoren worden gebruikt voor authenticatie, bijvoorbeeld een wachtwoord en een vingerafdruk. | WP |

5 WCN: Woordenboek Cyberveilig Nederland (https://cyberveilignederland.nl/woordenboek-cyberveilig-nederland/)
WP: Wikipedia (https://www.wikipedia.org/)

| Begrip / afkorting | Betekenis | Bron[5] |
|---|---|---|
| **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 |
| **Phishing** | Aanval waarbij de aanvaller iemand verleidt om belangrijke informatie te geven, zoals inlog-gegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails, maar 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 versleutelt. 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 |
| **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 phishing-aanval 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 phishing-aanval 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 |
| **Vulnerability scan** | Kwetsbaarhedenscan; en geautomatiseerde controle die zwakke plekken in een systeem opspoort. | WCN |

# BIJLAGE 3 **GERAADPLEEGDE BRONNEN**

| Nr | Auteur(s) | Titel | Uitgever | Datum | URL | Opgehaald |
|---|---|---|---|---|---|---|
| [1] | National Coördinator Terrorisme en Veiligheid | **Cybersecuritybeeld Nederland 2020** | NCTV | 29/06/2020 | https://www.ncsc.nl/documenten/publicaties/2020/juni/29/csbn-2020 | 30/06/2020 |
| [2] | ENISA | **ENISA Threat Landscape - 2020** | ENISA | 20/10/2020 | https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends | 30/06/2020 |
| [3] | security.nl | **Ransomware infecteert systemen Universiteit Maastricht** | security.nl | 24/12/2019 | https://www.security.nl/posting/636630/Ransomware+infecteert+systemen+Universiteit+Maastricht | 10/02/2020 |
| [4] | Diercks Gijs, Deuten Jasper Diederen Paul | **Kennis in het vizier** | Rathenau Instituut | 01/07/2019 | https://www.rathenau.nl/nl/vitale-kennisecosystemen/kennis-het-vizier | 07/12/2020 |
| [5] | Trend Micro Research | **Turning the Tide, Trend Micro Security Prediction for 2021** | Trend Micro | 08/12/2020 | https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021 | 09/12/2020 |
| [6] | JISC | **Cyber Impact** | JISC | 09/11/2020 | https://www.jisc.ac.uk/reports/cyber-impact | 09/12/2020 |
| [7] | Barracuda | **Threat Spotlight: Spear phishing attacks targeting education** | Barracuda | 29/10/2020 | https://blog.barracuda.com/2020/10/29/threat-spotlight-spear-phishing-education/ | 09/12/2020 |
| [8] | Verizon | **2020 Data Breach Investigations Report (DBIR)** | Verizon Business | mei 2020 | https://enterprise.verizon.com/resources/reports/dbir/ | 09/12/2020 |
| [9] | nu.nl | **Beveiligingslek bij Citrix treft Nederlandse ministeries en ziekenhuizen** | nu.nl | 13/01/2020 | https://www.nu.nl/tech/6023545/beveiligingslek-bij-citrix-treft-nederlandse-ministeries-en-ziekenhuizen.html | 27/11/2020 |
| [10] | Monsjou, Daan van | **Universiteit Antwerpen is getroffen door Clop-ransomware** | tweakers.net | 28/10/2019 | https://tweakers.net/nieuws/159138/universiteit-antwerpen-is-getroffen-door-clop-ransomware.html | 27/11/2020 |
| [11] | Camp, Jos van den | **Universiteit Maastricht betaalde 197.000 euro aan Russische hackgroep** | De Limburger | 05/02/2020 | https://www.limburger.nl/cnt/dmf20200205_00146231 | 10/02/2020 |
| [12] | Infosecurity | **De kettingreactie als gevolg van de ransomware-aanval op de Universiteit Maastricht** | Infosecurity | 09/03/2020 | https://www.infosecuritymagazine.nl/blogs/de-kettingreactie-als-gevolg-van-de-ransomware-aanval-op-de-universiteit-maastricht | 09/03/2020 |

## BIJLAGE 3 **GERAADPLEEGDE BRONNEN** (VERVOLG)

| Nr | Auteur(s) | Titel | Uitgever | Datum | URL | Opgehaald |
|---|---|---|---|---|---|---|
| [13] | Nieuwsuur | **Hack(poging) in ziekenhuis en gemeente: 'Urgentie lek leek niet duidelijk'** | NOS | 15/01/2020 | https://nos.nl/nieuwsuur/artikel/2318812-hack-poging-in-ziekenhuis-en-gemeente-urgentie-lek-leek-niet-duidelijk.html | 10/02/2020 |
| [14] | Heck, Wilmer | **Nederlandse bedrijven nog kwetsbaar voor hack** | NRC | 15/01/2020 | https://www.nrc.nl/nieuws/2020/01/15/nederlandse-bedrijven-nog-kwetsbaar-voor-hack-a3987021 | 27/01/2020 |
| [15] | RIVM | **Geen misbruik datalek Infectieradar** | RIVM | 08/06/2020 | https://www.rivm.nl/nieuws/geen-misbruik-datalek-infectieradar | 30/06/2020 |
| [16] | RIVM | **Datalek Blackbaud en aantoonbaar voldoen aan de AVG** | PrivacyWeb | 21/08/2020 | https://www.privacy-web.nl/artikelen/datalek-blackbaud-en-aantoonbaar-voldoen-aan-de-avg | 02/11/2020 |
| [17] | Autoriteit Persoonsgege-vens | **Privacy shield voor doorgifte naar VS ongeldig verklaard** | AP | 20/07/2020 | https://autoriteitpersoonsgegevens.nl/nl/nieuws/privacy-shield-voor-doorgifte-naar-vs-ongeldig-verklaard | 27/11/2020 |
| [18] | DigiCert | **DigiCert ICA Replacement** | DigiCert | 07/07/2020 | https://knowledge.digicert.com/alerts/DigiCert-ICA-Replacement.html | 27/11/2020 |
| [19] | Kleine, Jeroen de | **Internetcriminelen duiken in datalek bij Saxion; duizenden phishing mailtjes gaan rond** | Tubantia | 02/11/2020 | https://www.tubantia.nl/enschede/internetcriminelen-duiken-in-datalek-bij-saxion-duizenden-phishing-mailtjes-gaan-rond-a2cdef150/ | 27/11/2020 |
| [20] | O'Donnel, Lindsey | **University Email Hijacking Attacks Push Phishing, Malware** | Threatpost | 29/10/2020 | https://threatpost.com/university-email-hijacking-phishing-malwarephishing-malware/160735/ | 27/11/2020 |
| [21] | Kay, Roger | **A Lesson in Phishing: University Account Takeover** | Inky | - | https://www.inky.com/blog/a-lesson-in-phishing-university-account-takeover | 27/11/2020 |
| [22] | HOP | **Ook in Groningen geen tentamens door ict-storing** | DUB | 03/11/2020 | https://www.dub.uu.nl/nl/nieuws/ook-groningen-geen-tentamens-door-ict-storing | 03/11/2020 |
| [23] | Strikkers, Henk | **Opnieuw UvA-tentamens afgelast, nu door storing in Proctorio** | Folia | 22/10/2020 | https://www.folia.nl/actueel/141090/opnieuw-uva-tentamens-afgelast-nu-door-storing-in-proctorio | 03/11/2020 |

## BIJLAGE 3 **GERAADPLEEGDE BRONNEN** (VERVOLG)

| Nr | Auteur(s) | Titel | Uitgever | Datum | URL | Opgehaald |
|---|---|---|---|---|---|---|
| [24] | Bijl, Hanna | **Storing UvA opgelost, tentamens gaan woensdag door** | Het Parool | 20/10/2020 | https://www.parool.nl/gs-b52e8cec | 27/11/2020 |
| [25] | JOOP | **WHO: Covid-19-uitbraak is pandemie** | BNNVARA | 11/03/2020 | https://joop.bnnvara.nl/nieuws/who-covid-19-uitbraak-is-pandemie | 13/03/2020 |
| [26] | Security.nl | **Recordaantal kwetsbaarheden aan CVE-database toegevoegd** | Security.nl | 05/01/2020 | https://www.security.nl/posting/684599/Recordaantal+kwetsbaarheden+aan+CVE-database+toegevoegd | 06/01/2021 |
| [27] | SURF | **SURFsoc: samen informatiebeveiliging versterken** | SURF | 2020 | https://www.surf.nl/surfsoc | 22/12/2020 |
| [28] | Gils, Stijn van | **Onderzoek: minder cyberaanvallen, maar zes keer zoveel schade** | FD | 22/06/2020 | https://fd.nl/ondernemen/1348399/onderzoek-minder-cyberaanvallen-maar-zes-keer-zoveel-schade | 24/12/2020 |
| [29] | Security.nl | **Hof van Twente gaat losgeld voor ontsleutelen data niet betalen** | Security.nl | 19/12/2020 | https://www.security.nl/posting/682652/Hof+van+Twente+gaat+losgeld+voor+ontsleutelen+data+niet+betalen | 24/12/2020 |
| [30] | CICS | **Cyber Security Industry Predictions - Looking at the Decade to Come** | CICS | 25/02/2020 | https://www.careersincyber.com/article-details/83/cyber-security-industry-predictions-looking-at-the-decade-to-come/ | 08/01/2021 |
| [31] | Security.nl | **Microsoft: aanvallers SolarWinds waren al in oktober 2019 actief** | Security.nl | 19/12/2020 | https://www.security.nl/posting/682662/Microsoft%3A+aanvallers+SolarWinds+waren+al+in+oktober+2019+actief | 05/01/2021 |
| [32] | The Institute of Internal Auditors | **An update of the Three Lines of Defense** | The IIA | 13/07/2020 | https://global.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Dutch.pdf | 01/09/2020 |
| [33] | Universiteit Maastricht | **Reactie Universiteit Maastricht op rapport FOX-IT** | Rijks-overheid | 05/02/2020 | https://www.rijksoverheid.nl/documenten/rapporten/2020/02/05/reactie-universiteit-maastricht-op-rapport-fox-it | 24/03/2020 |
| [34] | Pelt, Stan van | **Privacyhoogleraar Bart Jacobs: 'Overstap van universiteit naar clouddiensten Microsoft is illegaal'** | VOX | 14/12/2020 | https://www.voxweb.nl/nieuws/privacyhoogleraar-bart-jacobs-overstap-van-universiteit-naar-clouddiensten-microsoft-is-illegaal | 16/12/2020 |
| [35] | Boone, Anouk | **Nederlandse rectoren waarschuwen voor macht van techreuzen** | De Volkskrant | 22/12/2019 | https://www.volkskrant.nl/nieuws-achtergrond/nederlandse-rectoren-waarschuwen-voor-macht-van-techreuzen~b28e509f/ | 12/01/2020 |

BIJLAGE 3 **GERAADPLEEGDE BRONNEN** (VERVOLG)

| Nr | Auteur(s) | Titel | Uitgever | Datum | URL | Opgehaald |
|---|---|---|---|---|---|---|
| [36] | Grapperhaus, F.B.J. (Minister van Justitie en Veiligheid) | **Informatie- en communicatie technologie (ICT); Brief regering; Kabinetsreactie op het rapport 'Voorbereiden op digitale ontwrichting' van de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) en een overzicht van de geleerde lessen van de Citrix-problematiek** | Tweede Kamer | 25/03/2020 | https://zoek.officielebekendmakingen.nl/kst-26643-673.html | 05/01/2021 |
| [37] | Anand, Venky Caso, Jeffrey Schwarz, Andreas | **COVID-19 crisis shifts cybersecurity priorities and budgets** | McKinsey | juli 2020 | https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets | 05/01/2021 |
| [38] | Mandia, Kevin | **FireEye Shares Details of Recent Cyber Attack, Actions to Protect Community** | FireEye | 08/12/2020 | https://www.fireeye.com/blog/products-and-services/2020/12/fireeye-shares-details-of-recent-cyber-attack-actions-to-protect-community.html | 23/12/2020 |
| [39] | Redactie Nationaal Cyber Security Centrum | **Op cybersecurity moet je niet concurreren** | NCSC (NL) | dec. 2019 | https://magazines.ncsc.nl/ncscmagazine/2019/01/lds | 23/12/2020 |

# COLOFON

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

**Redactie**
Jan Michielsen (SURF)

**Coördinatie**
Yvonne Klaassen (SURF)

**Ontwerp**
Studio Koelewijn Brüggenwirth BNO, Den Haag

**Fotografie**
iStock

Februari 2021

**Dit rapport is mede tot stand gekomen dankzij bijdragen van de klankbordgroep bestaande uit:**
Alex Peeters – Helicon Opleidingen
Bart van den Heuvel – Universiteit Maastricht
Bram Bogers – Onderwijsgroep Tilburg
Dietmar Timmerman – Hogeschool Saxion
Donny Toebes – Graafschap College
Eric van den Beld – Hogeschool Saxion
Erwin Elieveld – VU Amsterdam
Gert Douma – Hanzehogeschool Groningen
Jurrian Wijffels – Fontys
Ludo Cuijpers – Vista College
Martijn van Hoorn – CITAVERDE College
Martijn Bijleveld – SaMBO-ICT
Pamela Mercera – VU Amsterdam
Peter Vermeijs – MBO Raad
Raoul Vernède – Universiteit Utrecht
Roeland Reijers – Universiteit van Amsterdam
Sebastiaan Kamp – Erasmus Universiteit Rotterdam

Samen aanjagen van vernieuwing