CYBERDREIGINGSBEELD 2021-2022

ONDERWIJS EN ONDERZOEK

SURF

VOORWOORD
WEERBAARHEID HELE SECTOR MOET NOG VERDER OMHOOG

Het afgelopen jaar kenmerkte zich door een groot aantal cyberincidenten. Ook de onderwijs- en onderzoekssector bleef helaas niet gespaard. In februari kreeg NWO een aanval te verduren die een aantal systemen enkele weken plat legde. In maart lagen de Universiteit van Amsterdam en de Hogeschool van Amsterdam onder vuur. We sloten het jaar af met een datalek bij het Máxima Medisch Centrum Eindhoven.

In september viel ROC Mondriaan ten prooi aan een ernstige ransomware-aanval, waarbij een losgeld van maar liefst 4 miljoen euro werd geëist. Omdat ROC Mondriaan besloot niet in te gaan op de eisen van de hackers, hebben die als drukmiddel een deel van de buitgemaakte gegevens gepubliceerd op het dark web, waarbij gevoelige en persoonsgegevens publiek werden.

Het is dan ook duidelijk dat we de weerbaarheid van de hele sector nog verder moeten verhogen dan we de afgelopen jaren al hebben gedaan. Dat kan alleen maar door met zijn allen een lijn te trekken en gezamenlijk op te trekken. Door bijvoorbeeld als sector losgeld consequent niet te betalen wordt een ransomware-aanval minder aantrekkelijk voor hackers. Maar we moeten moet nog meer doen om het binnendringen van het netwerk, applicaties en systemen zo moeilijk mogelijk te maken.

Monitoring van de ict-infrastructuur van de instelling is een belangrijke stap richting betere weerbaarheid. SURFsoc draait nu meer dan een jaar en veel instellingen hebben zich aangesloten. Andere instellingen hebben ervoor gekozen zelf een security operations centre op te zetten of elders af te nemen. Om meldingen van incidenten af te handelen is ook menskracht bij de instellingen zelf nodig. Die menskracht is schaars of zelfs niet beschikbaar.

Weerbaarheid verhogen vereist ook dat instellingen stappen zetten om operationele security in zijn geheel te verbeteren. Het is daarom belangrijk om de status van informatiebeveiliging in kaart te brengen en verbeterpunten te signaleren. SURF voert daarom al sinds 2011 benchmarks uit. De focus daarvan is procesvolwassenheid. Die is steeds beter geworden, maar capaciteit is beperkt. Om voldoende voortgang te blijven maken is het cruciaal dat we op alle vlakken samenwerken.

Hans Schutte
Bestuursvoorzitter ROC Mondriaan

Jet de Ranitz
Voorzitter raad van bestuur SURF

BESTUURDERSSAMENVATTING

Dit *Cyberdreigingsbeeld – onderwijs en onderzoek* is een terugblik op 2021 en gaat in op incidenten die zich hebben voorgedaan bij organisaties uit de sector onderwijs en onderzoek. Verder worden actuele dreigingen en trends behandeld die relevant zijn voor de sector.

Headlines

- **Ransomware grootste dreiging**
- **Ketenafhankelijkheid steeds manifester**
- **Samenwerking binnen sector onderwijs en onderzoek groeit**
- **Groeiende aandacht voor publieke waarden; nog geen concrete oplossingen**
- **Politieke aandacht voor informatiebeveiliging in sector onderwijs en onderzoek**

Incidenten, trends en actoren

In 2021 is ook in de sector hoger onderwijs en onderzoek het aantal ransomware-aanvallen toegenomen. Het dreigen met publicatie van de gestolen gegevens is daarbij een nieuw pressiemiddel om betaling van losgeld af te dwingen. Bij de hack van NWO, het datalek bij de HAN en de aanval op ROC Mondriaan is hiermee gedreigd, maar deze drie instellingen besloten niet in te gaan op de eisen van de aanvallers. Dit had tot gevolg dat (gevoelige) gegevens gepubliceerd werden.

Ransomware

In het Verizon Data Breach Investigations Report 2021 [4] wordt geconstateerd dat het gebruik van ransomware als middel is verdubbeld ten opzichte van 2020. Bovendien worden de data in veel gevallen eerst weggesluisd en dan pas versleuteld, zodat de aanvaller kan dreigen met publicatie van de gestolen gegevens. Dit zet meer druk op het slachtoffer om het losgeld te betalen.

Professionalisering van aanvallers

Er is een omvangrijke ondergrondse dienstverleningseconomie waarbij vrijwel iedere stap voor het uitvoeren en beschermen van criminele acties als aparte dienst wordt aangeboden. Hierdoor komen geavanceerde aanvalstechnieken en -middelen, bijvoorbeeld *Ransomware as a Service*, beschikbaar voor een grote groep potentiële aanvallers. Omdat deze samenwerkingsverbanden steeds complexer worden, wordt ook het achterhalen van daders en het voorkomen van schade steeds moeilijker.

Ketenafhankelijkheid

ENISA, het EU-agentschap voor Cybersecurity, constateert dat supply chain-aanvallen toenemen in aantal en complexiteit. Instellingen moeten dan ook bij het nemen van voorzorgsmaatregelen om veilig te blijven steeds meer rekening houden met de risico's die hun leveranciers lopen en hierover met hen afspraken maken.

Log4j/Log4shell

Het log4j incident dat zich begin december 2021 voordeed is een voorbeeld van een kwetsbaarheid in de keten. Dit incident kon in potentie zeer grote gevolgen hebben – niet alleen voor onderwijs- en onderzoeksinstellingen, maar voor de hele wereld. Onderzoekers meldden een kritieke kwetsbaarheid in Apache log4 j[1]. Deze software wordt in heel veel applicaties gebruikt om logging af te handelen en wordt zowel gebruikt in applicaties die in eigen beheer zijn als in applicaties die door derden wordt beheerd. Hierdoor was niet altijd meteen helder waar de software werd gebruikt en wie er verantwoordelijk voor het beheer was. Dit incident onderstreept ook het belang van een complete en up-to-date inventarisatie van systemen en applicaties in eigen beheer, maar ook van de applicaties die niet in eigen beheer zijn. Helaas kwam bij dit incident naar voren dat deze inventarisatie nogal eens ontbreekt of niet compleet en/of up-to-date is.

1 https://www.geeksforgeeks.org/what-is-apache-log4j-vulnerability/

Politieke implicaties

Bij verschillende gelegenheden zijn kamervragen gesteld over de staat van informatiebeveiliging bij onderwijsinstellingen of heeft de minister van OCW de kamer geïnformeerd over de stand van zaken in de sector onderwijs en onderzoek.

De Inspectie van het Onderwijs heeft in het rapport 'Binnen zonder kloppen – Digitale weerbaarheid in het hoger onderwijs' [2] in kaart gebracht hoe hogeronderwijsinstellingen hun cyberweerbaarheid kunnen verhogen om de continuïteit van onderwijs en onderzoek te waarborgen.

Actoren

Bij zowel onderwijs, onderzoek als bedrijfsvoering worden beroepscriminelen als de belangrijkste groep actoren gezien.

Risicoperceptie

Voor onderwijs is de risico-inschatting voor *Manipulatie van data, Spionage en Bewust beschadigen van het imago* ten opzichte van 2020 iets lager. Bij bedrijfsvoering geldt dat voor *Spionage en Bewust beschadigen van het imago*. Maar bij onderwijs, onderzoek en bedrijfsvoering worden de risico's op alle andere dreigingstypen voor het derde jaar op rij opnieuw hoger ingeschat dan in 2020.

Tabel 1 **Risicoperceptie en dynamiek**

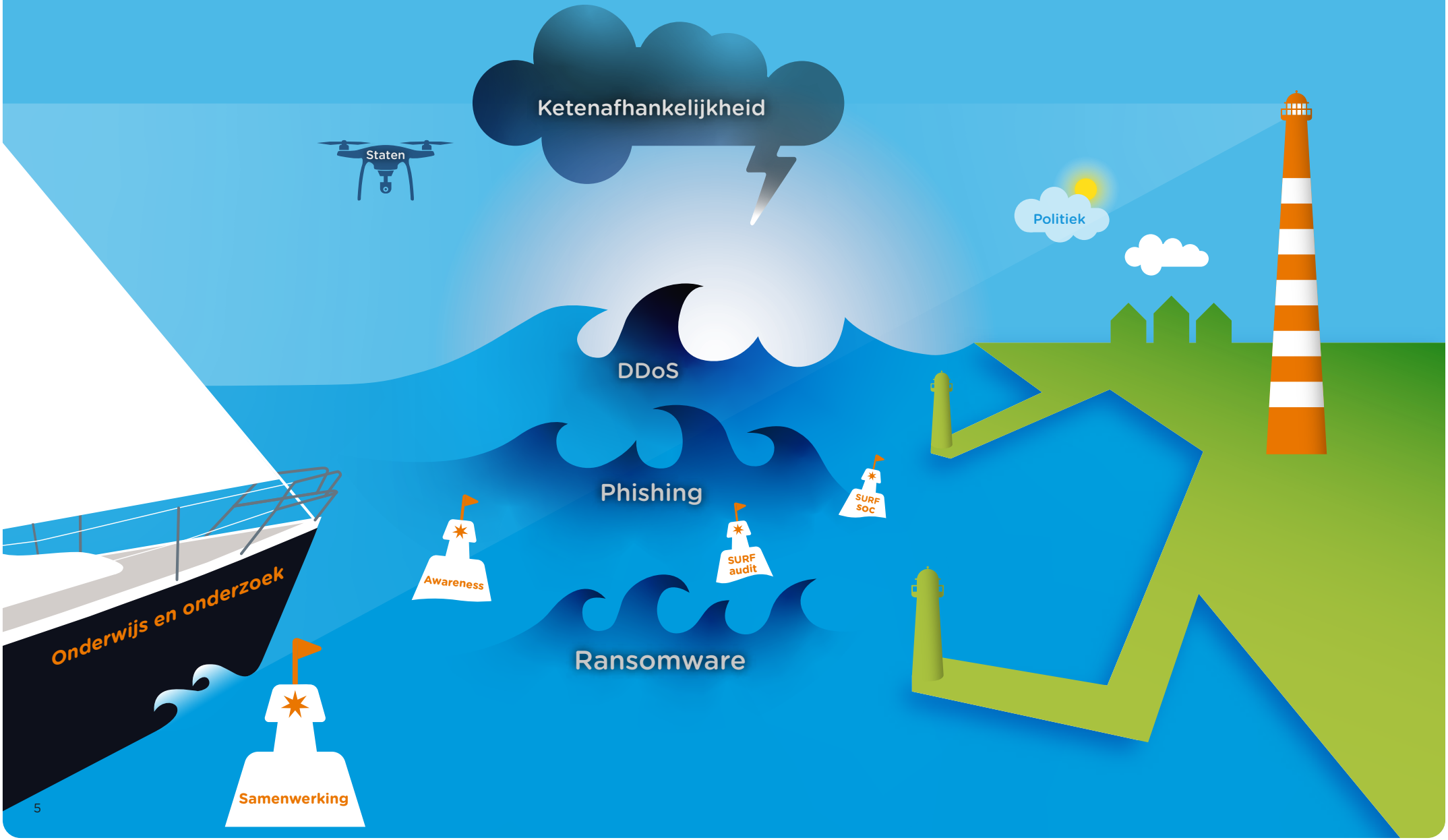
Categorie	Onderwijs	△	Onderzoek	△	Bedrijfsvoering	△
1 Verkrijging en openbaarmaking van informatie	Zeer hoog	↑↑	Zeer hoog	↑↑	Zeer hoog	↑↑
2 Identiteitsfraude	Hoog	↑	Medium	↑	Hoog	↑
3 Verstoring ICT	Zeer hoog	↑	Hoog	↑	Zeer hoog	↑
4 Manipulatie van data	Hoog	—	Medium	—	Medium	↑
5 Spionage*	Laag	—	Medium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

△ Ontwikkeling 2021 t.o.v. 2020
↑↑ Forse toename t.o.v. 2020
↑ Toename t.o.v. 2020
— Geen verandering t.o.v. 2020

** Bij Spionage is de onzekerheid het grootst (46% weet niet of het risico is toe- of afgenomen)*

INFOGRAPHIC CYBERDREIGINGSBEELD ONDERWIJS EN ONDERZOEK 2021-2022

DE SECTOR ONDERWIJS EN ONDERZOEK ZET KOERS NAAR EEN VEILIGE(R) HAVEN



INHOUD

VOORWOORD **2**

BESTUURDERSSAMENVATTING **3**

INFOGRAPHIC **5**

INHOUDSOPGAVE **6**

1 INLEIDING **7**

Nieuwe uitdagingen 7

Politieke implicaties 7

Werkwijze 7

Leeswijzer 8

2 INCIDENTEN, TRENDS EN ACTOREN **9**

Incidenten 9

Trends 15

Actoren 20

3 RISICOPERCEPTIE **22**

4 SAMENVATTING RESULTATEN SURVEY **24**

Governance 24

Technische maatregelen 29

5 WEERBAARHEID **33**

SURF IV-Metingen 33

Andere bronnen 36

Weerbaarheidverhogende maatregelen 38

Inzicht in aanvalsmethoden cybercriminelen 41

6 CONCLUSIE **43**

BIJLAGE 1 **AFKORTINGEN EN BEGRIPPEN** **45**

BIJLAGE 2 **GERAADPLEEGDE BRONNEN** **47**

1 INLEIDING

In dit Cyberdreigingsbeeld lees je over incidenten die zich hebben voorgedaan bij organisaties uit de sector onderwijs en onderzoek, en over actuele dreigingen en trends die relevant zijn voor deze sector. Het rapport is bedoeld om bestuurders, beleidsmakers en professionals daarover te informeren, zodat zij weten welke risico's ze lopen op het gebied van informatiebeveiliging en gegevensbescherming.

In 2021 hebben zich verschillende, soms ontwrichtende, incidenten voorgedaan bij organisaties in de sector onderwijs en onderzoek, die bepalend waren voor het dreigingsbeeld. Daarnaast bleven de beperkende maatregelen vanwege de coronapandemie voor een groot deel van het jaar van kracht. Online oplossingen die eerder waren ingevoerd om onderwijs te kunnen blijven geven en thuiswerken mogelijk te maken, zijn daarom voortgezet en uitgebreid. Wel is de aanvankelijke druk om snel in te voeren verminderd en is de aandacht voor informatiebeveiliging en gegevensbescherming weer toegenomen in vergelijking met 2020.

Nieuw is de discussie over de afhankelijkheid van de techreuzen en de wenselijkheid van het invoeren van allerlei online oplossingen. Die heeft mede geleid tot het uitvoeren van DPIA's[2] op bijvoorbeeld Microsoft Office 365 en Google for Education. Samenwerking tussen onder andere SURF en de Rijksoverheid was daarbij belangrijk om met de techreuzen tot overeenstemming te komen.

Nieuwe uitdagingen

In 2022 zien we nieuwe uitdagingen, onder andere met de Russische inval in Oekraïne. NCSC en de veiligheidsdiensten waarschuwen voor cyberaanvallen met als doel de westerse samenleving te ontwrichten en wellicht ook als antwoord op de sancties die de westerse landen aan Rusland hebben opgelegd na de inval op 24 februari 2022 [1]. Daar krijgen wij als sector ongetwijfeld ook mee te maken. Verder zijn nieuw ontdekte kwetsbaarheden in software een bron van zorg, bijvoorbeeld het probleem met log4j, dat in allerlei producten en diensten wordt gebruikt. Deze problematiek vereist dat er een goede inventarisatie van software en leveranciers nodig is om adequaat te kunnen reageren.

Politieke implicaties

Bij verschillende gelegenheden zijn kamervragen gesteld over de staat van informatiebeveiliging bij onderwijsinstellingen of heeft de minister van OCW de kamer geïnformeerd over de stand van zaken in de sector onderwijs en onderzoek.

Verder heeft de Inspectie van het Onderwijs in het rapport 'Binnen zonder kloppen – Digitale weerbaarheid in het hoger onderwijs' [2] in kaart gebracht hoe hogeronderwijsinstellingen hun cyberweerbaarheid kunnen verhogen om de continuïteit van onderwijs en onderzoek te waarborgen.

Werkwijze

Eind 2021 hebben we twee surveys uitgezet. Iedere survey richtte zich op een andere doelgroep. Enerzijds de security- en privacyprofessionals, zoals CISO's security officers, privacy officers, en FG's, die we in voorgaande jaren ook al hebben bevraagd, en anderzijds de IT-directeuren en CIO's. De tweede survey, een verkorte versie van de eerste, benadrukte de governance-aspecten van informatieveiligheid en privacy. De resultaten van beide surveys komen terug in de volgende hoofdstukken.

2 DPIA: Data Protection Impact Assesment (Gegevensbeschermingseffectbeoordeling)
[1] [2] Zie eindnoten op p.47

Leeswijzer

- In **hoofdstuk 2** gaan we in op een aantal grotere incidenten die zich hebben voorgedaan binnen de sector onderwijs en onderzoek en de politieke implicaties. Vervolgens signaleren we in dit hoofdstuk een aantal trends en laten we zien welke actoren zich het meest manifesteren bij acht verschillende risicocategorieën.
- **Hoofdstuk 3** gaat in op de risicoperceptie van de hiervoor genoemde risicocategorieën voor respectievelijk onderwijs, onderzoek en bedrijfsvoering.
- **Hoofdstuk 4** bevat een samenvatting van de resultaten van de surveys.
- **Hoofdstuk 5** gaat in op de weerbaarheid en geeft handelingsperspectieven in geval van incidenten.
- Tot slot trekken we in **hoofdstuk 6** enkele conclusies.

2 INCIDENTEN, TRENDS EN ACTOREN

Incidenten

In 2021 hebben zich diverse, soms ernstig ontwrichtende incidenten voorgedaan in de onderwijs- en onderzoeksector. Bijna iedere maand was het raak. Een overzicht.

Hack NWO

Het eerste grote incident in 2021 was de aanval op NWO in februari. Na de ontdekking van de hack heeft NWO alle systemen afgesloten, inclusief mail en telefonie. Daardoor was het moeilijk medewerkers van NWO te bereiken. Ook de externe server die in gebruik was voor de subsidieaanvragen is uit veiligheidsoverwegingen afgesloten, waardoor onderzoekers lopende aanvragen niet meer konden inzien en nieuwe aanvragen niet mogelijk waren. Het heeft enkele maanden geduurd voordat NWO weer goed bereikbaar was en de systemen weer volledig up-and-running waren.

Figuur 1 **bron – Tweakers, 15-02-2022**

Nederlandse Organisatie voor Wetenschappelijk Onderzoek is gehackt

De Nederlandse Organisatie voor Wetenschappelijk Onderzoek maakt melding van een hack. Daardoor zijn de applicaties op het netwerk van NWO niet toegankelijk. De organisatie zet subsidieaanvragen tijdelijk stil uit veiligheidsoverwegingen.

Het is niet bekend wie er achter de hack zit en wat de motivatie is. Ook zijn er geen technische details bekendgemaakt. De NWO meldt in een persbericht dat de servers zijn gehackt en dat het netwerk en de interne applicaties van het wetenschapsinstituut daardoor niet toegankelijk zijn. Het is volgens de organisatie niet duidelijk hoe lang het gaat duren voordat het netwerk is hersteld.

Door de hack zijn de mailadressen van NWO, en de regieorganen SIA en NRO niet benaderbaar. Ook kan de organisatie niet bij zijn kantoorsoftware, zoals Outlook. Volgens het instituut is de website niet aangetast. Het is niet duidelijk of er data is buitgemaakt, de organisatie meldt daar niets over. NWO zegt tijdens het onderzoek naar de hack en gedurende de herstelwerkzaamheden geen verdere mededelingen te doen.

Subsidieaanvragen worden via een applicatie op een externe server afgehandeld en die lijkt volgens NWO niet geïnfecteerd te zijn. Uit veiligheidsoverwegingen is de server echter afgesloten voor alle gebruikers. Dat zal zo blijven totdat zeker is dat er geen infectie is, of kan plaatsvinden. Concreet liggen daardoor subsidieaanvragen stil. Het instituut zegt de komende weken te bekijken hoe en wanneer het subsidieproces weer kan worden opgestart.

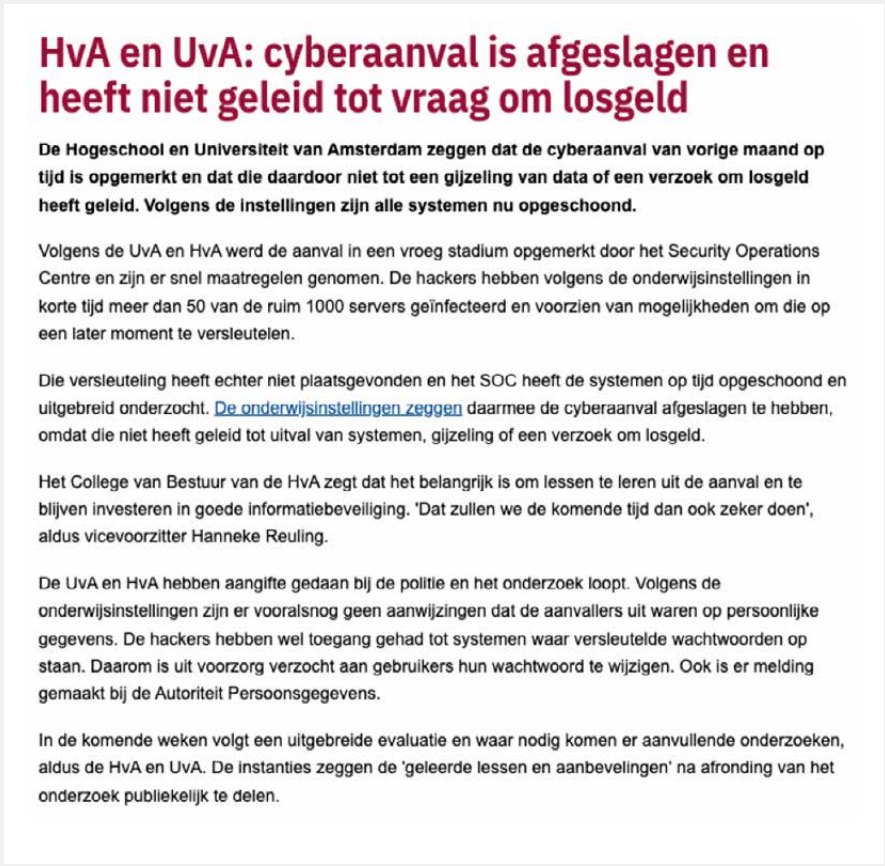
De NWO heeft als doel het bevorderen van kwaliteit en vernieuwing in de wetenschap. De organisatie investeert naar eigen zeggen jaarlijks bijna een miljard euro in onderzoek gericht op maatschappelijke uitdagingen en in onderzoeksinfrastructuur.

UvA/HvA aangevallen

In maart werden de HvA en de UvA belaagd. Hun gezamenlijke security operations centre (SOC) ontdekte de aanval bijtijds en er is, voor zover bekend, geen schade geleden. Wel heeft de opschoonactie de nodige tijd en menskracht gevergd, waarbij op een aantal systemen software is gevonden en verwijderd die tot doel had die systemen te versleutelen. Verder waren er systemen getroffen waarop versleutelde wachtwoorden stonden. Uit voorzorg is alle medewerkers en studenten gevraagd hun wachtwoord direct aan te passen.
In het kader van betere informatie-uitwisseling en kennisdeling hebben de HvA en de UvA in het rapport 'Aanval afgeslagen – Leerevaluatie cyberaanval Hogeschool van Amsterdam en Universiteit van Amsterdam' hun bevindingen en aanpak van het incident gedeeld [3].

Figuur 2 **bron –** https://www.uva.nl/binaries/content/assets/uva/nl/nieuws-en-agenda/leerevaluatie-cyberaanval-hva-uva-definitief-7-juli-2021.pdf

Figuur 3 **bron – Tweakers, 10-03-2021**



HvA en UvA: cyberaanval is afgeslagen en heeft niet geleid tot vraag om losgeld

De Hogeschool en Universiteit van Amsterdam zeggen dat de cyberaanval van vorige maand op tijd is opgemerkt en dat die daardoor niet tot een gijzeling van data of een verzoek om losgeld heeft geleid. Volgens de instellingen zijn alle systemen nu opgeschoond.

Volgens de UvA en HvA werd de aanval in een vroeg stadium opgemerkt door het Security Operations Centre en zijn er snel maatregelen genomen. De hackers hebben volgens de onderwijsinstellingen in korte tijd meer dan 50 van de ruim 1000 servers geïnfecteerd en voorzien van mogelijkheden om die op een later moment te versleutelen.

Die versleuteling heeft echter niet plaatsgevonden en het SOC heeft de systemen op tijd opgeschoond en uitgebreid onderzocht. De onderwijsinstellingen zeggen daarmee de cyberaanval afgeslagen te hebben, omdat die niet heeft geleid tot uitval van systemen, gijzeling of een verzoek om losgeld.

Het College van Bestuur van de HvA zegt dat het belangrijk is om lessen te leren uit de aanval en te blijven investeren in goede informatiebeveiliging. 'Dat zullen we de komende tijd dan ook zeker doen', aldus vicevoorzitter Hanneke Reuling.

De UvA en HvA hebben aangifte gedaan bij de politie en het onderzoek loopt. Volgens de onderwijsinstellingen zijn er vooralsnog geen aanwijzingen dat de aanvallers uit waren op persoonlijke gegevens. De hackers hebben wel toegang gehad tot systemen waar versleutelde wachtwoorden op staan. Daarom is uit voorzorg verzocht aan gebruikers hun wachtwoord te wijzigen. Ook is er melding gemaakt bij de Autoriteit Persoonsgegevens.

In de komende weken volgt een uitgebreide evaluatie en waar nodig komen er aanvullende onderzoeken, aldus de HvA en UvA. De instanties zeggen de 'geleerde lessen en aanbevelingen' na afronding van het onderzoek publiekelijk te delen.

Gegevens bij Universiteit Leiden gelekt

In juli 2021 verscheen een bericht in het AD dat adresgegevens van medewerkers en onderzoeksgegegevens gelekt waren. Dit betrof echter gegevens die eerder in het jaar waren buitgemaakt.

Figuur 4 **bron – medewerkerswebsite Universiteit Leiden, 5-07-2021**

Datalek externe webserver

5 juli 2021

De afgelopen dagen zijn er diverse berichten verschenen in de media over hacks op een externe webserver van de Universiteit Leiden. We kunnen ons voorstellen dat daarover zorgen zijn bij medewerkers en studenten. In dit bericht informeren we je over wat we nu weten.

Bij een hack op een externe webserver van de Sterrewacht van de Universiteit Leiden eerder dit jaar, is een aantal gegevens buitgemaakt. Het gaat om e-mailadressen en adressen van onderzoekers, en onderzoeksomschrijvingen die te koop zijn aangeboden op het dark web. Het incident, een datalek, is gemeld bij de Autoriteit Persoonsgegevens (AP) en bij de betrokken medewerkers en studenten. De externe webserver is afgesloten.

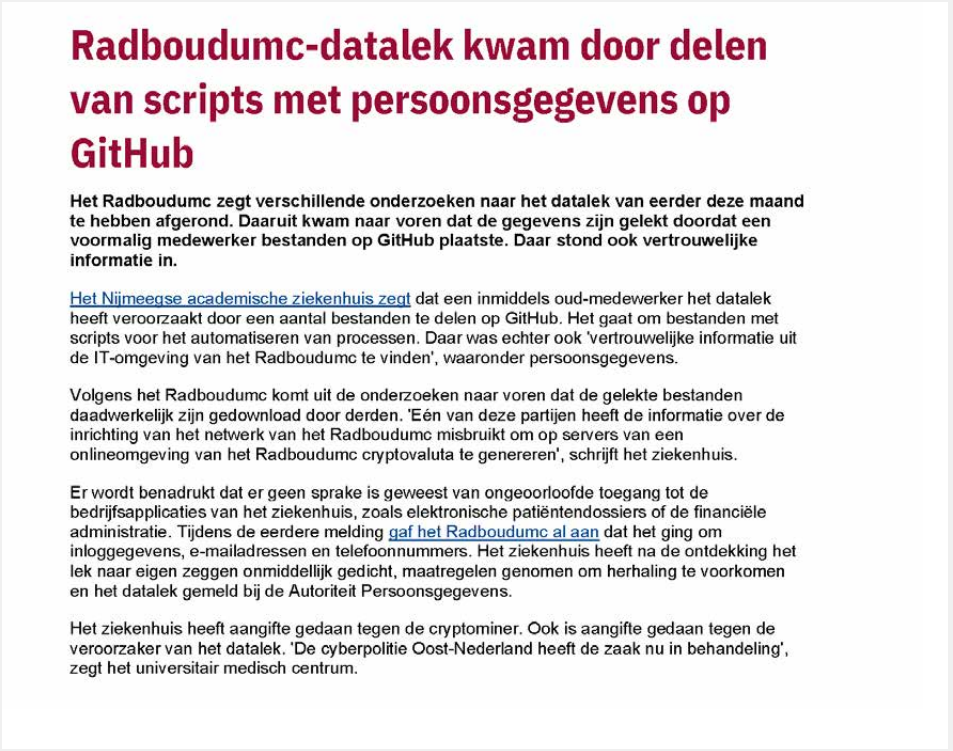
Omdat er opnieuw data gepubliceerd werden op het darkweb op 28 juni, heeft de universiteit extern forensisch onderzoek laten doen naar dit vermoedelijke tweede datalek. Hieruit is gebleken dat de recent op het darkweb gepubliceerde data waarover ook de media de afgelopen dagen berichtten, dezelfde zijn als de data die hierop in januari 2021 verschenen. Het betreft dus een nieuwe upload van eerder gelekte gegevens. In het forensisch onderzoek zijn geen versleutelde data of sporen van hacks aangetroffen.

Indien het externe forensisch onderzoek daartoe aanleiding geeft, komen we bij je terug met aanvullende informatie.

Datalek Radboudumc

In augustus lekten bij Radboudumc gegevens van medewerkers doordat een voormalig medewerker bestanden op GitHub[3] plaatste.

Figuur 5 **bron – Tweakers, 25-08-2021**



Radboudumc-datalek kwam door delen van scripts met persoonsgegevens op GitHub

Het Radboudumc zegt verschillende onderzoeken naar het datalek van eerder deze maand te hebben afgerond. Daaruit kwam naar voren dat de gegevens zijn gelekt doordat een voormalig medewerker bestanden op GitHub plaatste. Daar stond ook vertrouwelijke informatie in.

Het Nijmeegse academische ziekenhuis zegt dat een inmiddels oud-medewerker het datalek heeft veroorzaakt door een aantal bestanden te delen op GitHub. Het gaat om bestanden met scripts voor het automatiseren van processen. Daar was echter ook 'vertrouwelijke informatie uit de IT-omgeving van het Radboudumc te vinden', waaronder persoonsgegevens.

Volgens het Radboudumc komt uit de onderzoeken naar voren dat de gelekte bestanden daadwerkelijk zijn gedownload door derden. 'Eén van deze partijen heeft de informatie over de inrichting van het netwerk van het Radboudumc misbruikt om op servers van een onlineomgeving van het Radboudumc cryptovaluta te genereren', schrijft het ziekenhuis.

Er wordt benadrukt dat er geen sprake is geweest van ongeoorloofde toegang tot de bedrijfsapplicaties van het ziekenhuis, zoals elektronische patiëntendossiers of de financiële administratie. Tijdens de eerdere melding gaf het Radboudumc al aan dat het ging om inloggegevens, e-mailadressen en telefoonnummers. Het ziekenhuis heeft na de ontdekking het lek naar eigen zeggen onmiddellijk gedicht, maatregelen genomen om herhaling te voorkomen en het datalek gemeld bij de Autoriteit Persoonsgegevens.

Het ziekenhuis heeft aangifte gedaan tegen de cryptominer. Ook is aangifte gedaan tegen de veroorzaker van het datalek. 'De cyberpolitie Oost-Nederland heeft de zaak nu in behandeling', zegt het universitair medisch centrum.

3 GitHub is een online platform voor softwareontwikkeling en versiebeheer. https://nl.wikipedia.org/wiki/GitHub

ROC Mondriaan slachtoffer van ransomware-aanval
Eind augustus, vlak voor het begin van het schooljaar, werd ROC Mondriaan gehackt. Een onwaarschijnlijk hoog bedrag aan losgeld werd geëist. ROC Mondriaan weigerde echter te betalen waarop de hackers een set (gevoelige) gegevens op het dark web publiceerden. Dit leidde tot de nodige maatschappelijke commotie. Opmerkelijk daarbij is dat ROC Mondriaan in de publieke opinie deels als dader in plaats van slachtoffer werd gezien, omdat ze volgens velen hun beveiliging niet op orde hadden.

Door de hack was de IT-infrastructuur onbruikbaar geworden en moest deze opnieuw worden opgebouwd. Digitale leermiddelen waren niet beschikbaar en ook e-mailen was niet mogelijk. Het schooljaar startte met pen en papier. Waarschijnlijk is dit tot nog toe de meest ontwrichtende hack waardoor een onderwijsinstelling is getroffen.

Figuur 6 **bron – rocmondriaan.nl, 23-08-2021**

Mondriaan is gehackt

23 augustus 2021

Afgelopen weekend is ROC Mondriaan gehackt.

Er is een melding gedaan bij de Autoriteit Persoonsgegevens. Ook doet ROC Mondriaan aangifte en een forensisch onderzoek is gestart. Dit om de omvang van het probleem in kaart te brengen, helder te krijgen wat de gevolgen zijn en sporen veilig te stellen. Daarnaast bekijken de experts hoe ROC Mondriaan zo veilig en snel als verantwoord is, de systemen weer toegankelijk kan maken.

Harry de Bruijn, lid College van Bestuur ROC Mondriaan: "Het liefste zouden we nu meer vertellen, maar de komende uren en dagen moet eerst het onderzoek opheldering geven. We zetten alles op alles zodat het onderwijs vanaf volgende week kan starten. Dat zal mogelijk wel in aangepaste vorm zijn, want het is op dit moment onzeker of het onderwijs kan rekenen op ondersteuning van de nodige systemen en applicaties. Met dit scenario voor ogen, bereiden we ons nu zo goed mogelijk op de start van het schooljaar".

Hack bij de HAN
In september was de HAN het slachtoffer van een hack, waarbij de aanvaller gegevens van meer dan een half miljoen mensen bemachtigde.

Figuur 7 **bron – NOS 5-10-2021**

Hack bij HAN-hogeschool trof mogelijk ruim half miljoen mensen

De hacker die ruim een maand geleden binnendrong in de systemen van de hogeschool HAN in Arnhem en Nijmegen heeft gegevens van mogelijk 530.000 mensen bemachtigd. Dat zegt de hogeschool na onderzoek.

De inbraak werd op 1 september ontdekt. Uit het onderzoek blijkt dat de hacker via een webformulier op een server heeft ingebroken. Daarop stonden 530.000 mailadressen met bijbehorende persoonsgegevens. Of de hacker die allemaal heeft buitgemaakt, is niet duidelijk. De HAN heeft alle betrokkenen geïnformeerd.

Marcel Kropmans

Onze aanvallers specialiseren zich in onderwijs- en zorginstellingen

Tekst: Marjolein van Trigt

Een week voor de aftrap van studiejaar 2021-2022 wordt het ROC Mondriaan in Den Haag lamgelegd door een aanval met ransomware. Alle systemen zijn uitgeschakeld, tot aan de koffieautomaten aan toe. Toch besluit het ROC om het geëiste losgeld van 100 bitcoins (4 miljoen euro) niet te betalen.

Augustus 2021. Een wakkere netwerkbeheerder merkt om half 3 's nachts dat er wat mis is met het computersysteem van ROC Mondriaan in Den Haag, een mbo-instelling waar 26 scholen onder vallen. Het inderhaast ingeschakelde forensisch it-bedrijf stelt de volgende ochtend vast dat het echt mis is. Voor Hans Schutte, lid van het college van bestuur, is de hack een ruwe onderbreking van de zomervakantie. 'In eerste instantie hoop je dat de omvang meevalt,' zegt hij. 'Maar alles was weg. Dat was een schok. Zelfs de koffieautomaten waren geschakeld aan een systeem.'

Met hagel schieten

In de jaarlijkse mbo benchmark IBP-E scoorde ROC Mondriaan gemiddeld tot bovengemiddeld. Hoewel CIO Marcel Kropmans weet dat zoiets geen garantie is dat je niet wordt gehackt, was hij toch verrast. 'Toen duidelijk werd dat het ging om een grote Russische hackersorganisatie, heb ik me wel afgevraagd waarom juist wij werden lamgelegd.' Experts vermoeden dat de hackers eenvoudigweg op heel veel plekken proberen een ingang te vinden. 'Het is met hagel schieten en kijken wat je raakt,' zegt Kropmans. 'In die zin heeft Mondriaan pech gehad.' Dezelfde organisatie dringt onder meer een Australisch ziekenhuis en een Italiaanse universiteit binnen. 'Waarschijnlijk specialiseren ze zich in onderwijs en zorg vanwege de privacygevoelige data die ze daar buitmaken,' zegt Kropmans. 'Vaak wordt er na onderhandelingen wel iets betaald om te zorgen dat die niet worden gelekt.'

Paspoorten op het Darkweb

Met het Nationaal Cyber Security Centrum (NCSC), het ministerie en SURF komt ROC Mondriaan tot de afweging om in principe niet te betalen, mits het mogelijk is om het ict-landschap weer op te bouwen en de privacygevoeligheid van de buitgemaakte data enigszins meevalt. Een gelukje daarbij is dat de hackers met name zoeken naar financiële gegevens en contracten. Waar dit voor veel bedrijven de meest kwetsbare gegevens zijn, zijn ze in geval van het onderwijs openbaar. Schutte: 'Er zitten altijd vervelende dingen tussen. Zo wisten we dat een aantal kopieën van identiteitsgegevens op het dark web zouden belanden als we niet betaalden. Maar de schade was te overzien. We hebben mensen gevraagd om een nieuwe id-kaart of paspoort aan te vragen, door ons vergoed.'

Systemen opnieuw opbouwen

Terwijl de medewerkers aan het begin van het schooljaar bij de deur staan om schriften en pennen uit te delen aan studenten, wordt achter de schermen gewerkt om de systemen vanaf de grond opnieuw op te bouwen, onder nog hogere beveiligingseisen. 'Dat was een impactvol besluit, waar ik evenwel nog steeds achter sta,' zegt Kropmans. Er is onder meer gekozen om multi-factorauthenticatie voor studenten in te voeren en om de endpoint security op te schroeven. Ook is netwerksegmentatie aangebracht en is versneld een CISO aangesteld.

Inmiddels is een groot gedeelte van de systemen weer beschikbaar. 'Voor de medewerkers en de studenten kan het natuurlijk nooit snel genoeg gaan, maar vanuit it-perspectief denk ik dat we op korte termijn al heel veel hebben kunnen opleveren,' zegt Kropmans. In totaal zal het opnieuw opbouwen ongeveer een jaar in beslag nemen.

Gepakt zijn de Russische hackers nooit. 'Dat is kansloos' zegt Schutte. 'Maar wij hopen dat onze actie om niet te betalen eraan bijdraagt dat voorlopig geen andere Nederlandse onderwijsinstelling slachtoffer wordt.' 'En als het dan toch gebeurt, weet dan wat je meest kritische processen zijn en hoe je zorgt dat je die ontzettend snel weer up and running hebt,' voegt Kropmans eraan toe. 'Je kunt het nooit helemaal voorkomen, maar zorg dat de schade te overzien is.'

Hans Schutte

Log4j/Log4Shell kwetsbaarheid

Begin december 2021 vond een incident plaats met in potentie de grootste gevolgen – niet alleen voor onderwijs- en onderzoeksinstellingen, maar voor de hele wereld. Daarom moest direct actie worden ondernomen. Onderzoekers werkzaam bij Alibaba meldden op 24 november 2021 een kritieke kwetsbaarheid (CVE-2021-44228) in Apache log4j aan de Apache Software Foundation. Log4j[4] is software die veel gebruikt wordt in webapplicaties en allerlei andere systemen.

Het NCSC waarschuwde voor de kwetsbaarheid en kwam met een stappenplan om misbruik van de kwetsbaarheid te minimaliseren[5]. Veel security-specialisten bij onderwijs en onderzoeksinstellingen, en SURFcert, hebben hun kerstdagen besteed aan het inventariseren van systemen om te bepalen in hoeverre ze slachtoffer zouden kunnen zijn van deze kwetsbaarheid. Daarbij kwam naar voren dat een actuele en complete inventarisatie van systemen en applicaties onontbeerlijk is om snel te kunnen reageren. Iets wat iedere ict'er eigenlijk wel weet, maar waar het nogal eens aan ontbreekt.

Datalek Máxima Medisch Centrum

Als afsluiter van het jaar meldde Máxima Medisch Centrum Eindhoven op 31 december 2021 nog een datalek, waarbij patiëntgegevens mogelijk in verkeerde handen zijn gevallen.

Trends

Terwijl er in 2020 slechts enkele ransomware-aanvallen bij onderwijs- en onderzoeksinstellingen hebben plaatsgevonden, zien we flinke een toename in 2021. Bij de aanvallen in 2021 werd bovendien extra druk uitgeoefend om te betalen door te dreigen met publicatie van de gestolen gegevens. Hiervan was in ieder geval sprake bij de hack van NWO, het datalek bij de HAN en de aanval op ROC Mondriaan. Deze instellingen zijn alle drie niet ingegaan op de eisen van de aanvallers, met als gevolg dat (gevoelige) gegevens gelekt zijn.

Figuur 8 **Overzicht van versies en kwetsbaarheden bij Log4j**[5]

Figuur 9 **bron – De Volkskrant, 31-12-2021**

Datalek bij Máxima Medisch Centrum Eindhoven: patiëntengegevens mogelijk in verkeerde handen

Het Máxima Medisch Centrum in Eindhoven meldt dat mogelijk vertrouwelijke gegevens van patiënten in verkeerde handen terecht zijn gekomen. De betrokken patiënten zijn meteen persoonlijk ingelicht, meldt het ziekenhuis op zijn website. Het ziekenhuis beschouwt het voorval als een datalek, dat is gemeld aan de Autoriteit Persoonsgegevens en aan de Inspectie Gezondheidszorg en Jeugd.

4 zie bijvoorbeeld: https://www.geeksforgeeks.org/what-is-apache-log4j-vulnerability/
5 zie https://www.ncsc.nl/onderwerpen/log4j

v.l.n.r.: Remon Klein Tank (Wageningen University & Research), Paul Dekkers (SURF), Florian Draisma (SURF, productmanager SURFcert), Wim Biemolt (SURF), Thijs Kinkhorst (SURF), Jeffeny Hoogervorst (Tilburg University), Luuk Oostenbrink (SURF), Jaap van Ginkel (Universiteit van Amsterdam), Melvin Koelewijn (SURF), Peter Peters (Universiteit Twente). Niet op de foto: Koos van den Hout (Universiteit Utrecht).

Het jaar van SURFcert: heftige ransomware-aanvallen en doorwerken met Kerstmis

Tekst: Marjolein van Trigt

SURFcert, het Computer Security Incident Response Team (CSIRT) van SURF, onderzoekt en coördineert alle ict-beveiligingsinbreuken waarbij op SURF aangesloten instellingen zijn betrokken. Wim Biemolt en Remon Klein Tank van SURFcert vertellen over de hoogte- en dieptepunten van 2021.

2021 was een druk jaar voor SURFcert, met een aantal heftige ransomware-aanvallen, een flinke toename in de intensiteit van DDoS-aanvallen en als kersttoetje de Log4j-kwetsbaarheid. Goed nieuws is er ook: doordat steeds meer instellingen multifactorauthenticatie (MFA) inrichten, neemt de impact van phishingmails af.

Informatie delen en pro-actief waarschuwen

Een voorbeeld van een incident waar SURFcert in 2021 druk mee is geweest, is de ransomware-aanval op NWO in februari 2021. SURFcert was ter plekke om de schade te inventariseren en de omvang te bepalen. In samenwerking met NCSC en een extern forensisch it-bedrijf werd een plan de campagne opgesteld. De aanval leverde onrust op onder de aangesloten onderzoeks-

instellingen. Remon Klein Tank, lid van SURFcert en senior information security officer bij de WUR, vertelt: 'De instellingen maakten zich zorgen over onderzoeksvoorstellen die mogelijk op straat zouden komen te liggen. We probeerden ze handelingsperspectief te bieden door te delen wat we wisten over de aanval.'
Vaak bestaat er terughoudendheid bij slachtoffers om een aanval te melden. Andere instellingen willen juist heel graag dat dingen worden gedeeld. 'Probeer je in beide situaties te verplaatsen,' raadt Wim Biemolt aan. Biemolt is de voorzitter van SURFcert. 'Je hebt gebruikgemaakt van de keren dat er werd gedeeld. Houd dat in gedachte als je onverhoeds zelf het slachtoffer wordt.' Waar nodig anonimiseert SURFcert de informatie. 'Zeker aan het begin van zo'n incident, als je nog geen duidelijk beeld hebt van wat er gaande is, is het wel relevant om informatie te delen, maar niet om te verspreiden wíe er geraakt is,' zegt Klein Tank.

Dreigen met publiceren

Bij de aanval op NWO zag SURFcert voor het eerst een ontwikkeling die inmiddels een trend onder cybercriminelen kan worden genoemd: dreigen met het publiceren van buitgemaakte data. 'Bij NWO hebben de hackers alle registers opengetrokken en zowel de boel versleuteld als gevoelige data gedeeld,' zegt Biemolt. 'Wat we steeds vaker zien, is dat criminelen niet de moeite nemen om te versleutelen, maar alleen dreigen om data te publiceren. Dat is een verdienmodel op zich.'
SURFcert verwacht daarnaast meer incidenten die worden veroorzaakt door statelijke actoren. Biemolt vertelt: 'Een DDoS-aanval op Oekraïne werd onlangs uitgevoerd vanuit een server die in Nederland staat. Dat kan ons ook gebeuren, vanwege onze goede connectiviteit. Maar hoe reëel het is dat we op die manier betrokken raken bij incidenten, vind ik moeilijk te zeggen.'

Actief scannen op kwetsbaarheden

Het jaar werd uitgeluid met de Log4j-kwetsbaarheid. In de veelgebruikte Apache Log4j-software werd een ernstige kwetsbaarheid ontdekt, die zeker tot misbruik zou leiden als organisaties niet op tijd actie ondernemen. Klein Tank: 'Als SURFcert hebben we een buitengewoon goede informatiepositie. We kennen veel andere partijen en we ontvangen dus ook veel. We proberen alle relevante informatie te verzamelen in een open factsheet. Het beeld wordt steeds helderder, totdat we instellingen heel concrete handvaten kunnen geven.'
Biemolt: 'Bij een ontwikkeling zoals Log4j faciliteren we het actief scannen op kwetsbaarheden. We proberen de criminelen een stapje voor te zijn, door kwetsbare instellingen gericht te benaderen: jij hebt daar iets staan waar je nu iets mee moet doen. Zo hoeft niet iedere instelling dat voor zichzelf uit te zoeken.'
Over het feit dat de kwetsbaarheid in Log4j juist rond de kerstdagen aan het licht kwam, doen ze luchtig. 'Het zijn ook de interessantere zaken. Je zit ook bij de brandweer om af en toe een brand te blussen, toch? Niet om alleen maar katten te redden.'

Ransomware

Verizon heeft in het Data Breach Incident Report 2021 [4] onderzocht wat in 2021 de meest voorkomende acties waren bij respectievelijk geslaagde inbraken (Figuur 10 - linker kolom) en bij alle gerapporteerde incidenten (Figuur 10 - rechter kolom). Opvallend is dat phishing bij daadwerkelijk geslaagde inbraken het meest voorkomt als aanvalsmiddel, maar bij alle incidenten een veel kleiner percentage van de aanvalsmiddelen is.

Verizon constateert verder dat het gebruik van ransomware als middel is verdubbeld ten opzichte van 2020. Bovendien worden data in veel gevallen eerst weggesluisd en dan pas versleuteld, zodat de aanvaller kan dreigen met publicatie van de gestolen gegevens om meer druk te zetten op het slachtoffer om het losgeld te betalen.

Als voornaamste drijfveer (*threat actor motive*) wordt geldelijk gewin genoemd (zie figuur 11).

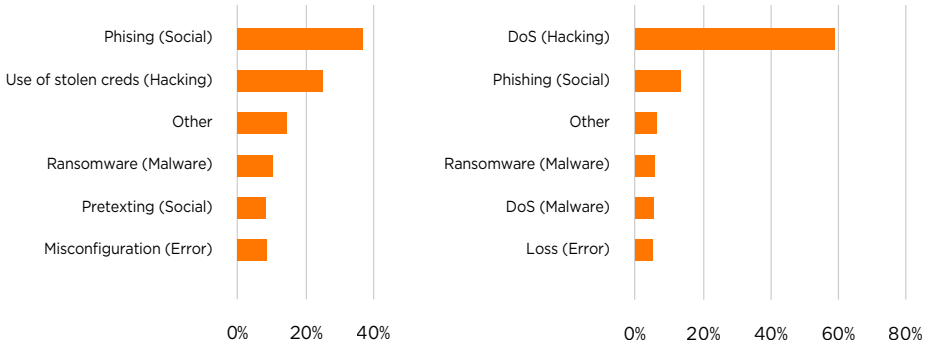
Professionalisering ondergrondse dienstverleningseconomie

Net als het Verizon Data Breach Investigations Report stelt het Cybersecurity-beeld Nederland 2021 [5] dat cybercriminelen in een ecosysteem werken met financieel gewin als de voornaamste drijfveer.

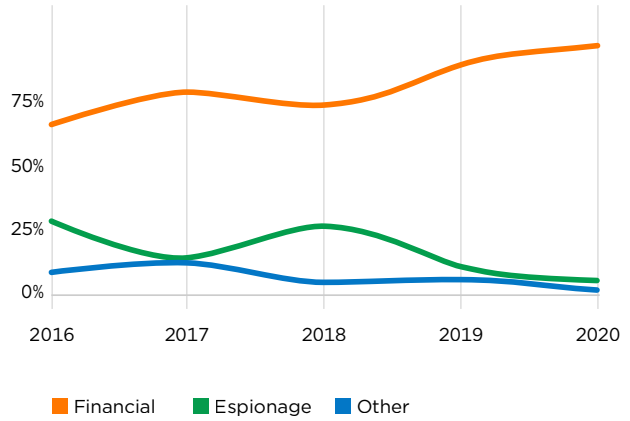
Er is een omvangrijke ondergrondse dienstverleningseconomie waarbij vrijwel iedere stap voor het uitvoeren en beschermen van criminele acties als aparte dienst wordt aangeboden.

Hierdoor komen geavanceerde aanvalstechnieken en -middelen zoals *Ransomware as a Service* beschikbaar voor een grote groep potentiële aanvallers. Bovendien is het voor de aanvallers een voordeel dat deze diensten wereldwijd schalen. Daarmee hebben ze een veel groter bereik. Omdat deze samenwerkingsverbanden steeds complexer worden, wordt ook het achterhalen van daders en het voorkomen van schade steeds moeilijker.

Figuur 10 **bron – Verizon DBIR 2021 p.15 (%)**



Figuur 11 **bron – Verizon DBIR 2021 p.12 (%)**



Ketenafhankelijkheid

ENISA, het EU-agentschap voor Cybersecurity, heeft een apart rapport gewijd aan dreigingen die betrekking hebben op ketenafhankelijkheid [6]. ENISA constateert dat supply chain-aanvallen toenemen in aantal en complexiteit. Als een leverancier eenmaal gecompromitteerd is, kan een aanvaller diens klanten ook treffen. Het blijkt dat de helft van die aanvallen wordt uitgevoerd door Advanced Persistent Threat (APT)-actoren. Dat betekent ook dat organisaties, om veilig te blijven, steeds meer rekening moeten houden met hun leveranciers bij het nemen van voorzorgsmaatregelen.

Kaseya ransomware-aanval [7]

In juli 2021 werd Kaseya getroffen door een ransomware-aanval. Kaseya levert een platform voor systeembeheer, waarmee beheerders systemen op afstand kunnen onderhouden. Het wordt veel gebruikt door beheerpartijen die apparaten van eindgebruikers op afstand beheren. REvil, een Russische hackersgroep, heeft het Kaseya-product VSA gehackt, via een kwetsbaarheid die toegang zonder wachtwoord toeliet. Vervolgens kon REvil alle systemen die met deze software werden beheerd versleutelen. Zo werden onder andere de kassa-systemen van Coop Zweden getroffen, waardoor deze supermarkt-keten bijna alle winkels tijdelijk moest sluiten. Wereldwijd zijn honderden bedrijven getroffen, ook in Nederland. REvil eiste in totaal 70 miljoen dollar losgeld om de decoderingssleutel beschikbaar te maken.

Figuur 12 geeft een overzicht van de methodes en technieken die worden gebruikt om een keten aan te vallen. Figuur 13 laat de technieken zien die worden gebruikt om vervolgens de klanten van een leverancier aan te vallen.

Figuur 12 **bron ENISA Threat Landscape for Supply Chain Attacks**

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN	
Malware Infection	e.g. spyware used to steal credentials from employees.
Social Engineering	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
Brute-Force Attack	e.g. guessing an SSH password, guessing a web login.
Exploiting Software Vulnerability	e.g. SQL injection or buffer overflow exploit in an application.
Exploiting Configuration Vulnerability	e.g. taking advantage of a configuration problem.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Open-Source Intelligence (OSINT)	e.g. search online for credentials, API keys, usernames.
Counterfeiting	e.g. imitation of USB with malicious purposes.

Figuur 13 **bron ENISA Threat Landscape for Supply Chain Attacks**

ATTACK TECHNIQUES USED TO COMPROMISE A CUSTOMER	
Trusted Relationship [T1199]	e.g. trust a certificate, trust an automatic update, trust an automatic backup.
Drive-by Compromise [T1189]	e.g. malicious scripts in a website to infect users with malware.
Phishing [T1566]	e.g. messages impersonating the supplier, fake update notifications.
Malware Infection	e.g. Remote Access Trojan (RAT), backdoor, ransomware.
Physical Attack or Modification	e.g. modify hardware, physical intrusion.
Counterfeiting	e.g. create a fake USB, modify a motherboard, impersonation of supplier's personnel.

Overige trends

Ransomware blijft de grootste dreiging en wordt ook in toenemende mate offensief ingezet door statelijke actoren. Als gevolg van de Russische inval in Oekraïne waarschuwen het NCSC en de veiligheidsdiensten voor cyber-aanvallen met als doel de westerse samenleving te ontwrichten. Hier krijgen wij als sector ongetwijfeld in de nabije toekomst ook mee te maken.

Door nog steeds toenemend cloudgebruik neemt ook het aantal cyberaan-vallen op cloudvoorzieningen toe. Dit onderstreept dat je goed zicht moet hebben op je ketenafhankelijkheden. In 2020 zagen we bijvoorbeeld de eerste grote supply chain attack via de SolarWinds system management tool [8]. In 2021 volgden nog enkele grote incidenten zoals de eerder-genoemde ontdekking van de Log4j-kwetsbaarheid. We verwachten ook in 2022 een toename van het aantal supply chain attacks.

Het aantal IoT-apparaten neemt nog steeds exponentieel toe en daarmee ook de risico's op misbruik via deze apparaten.

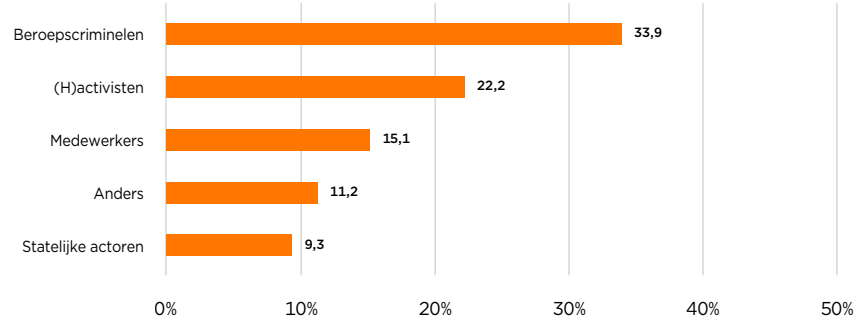
Een geheel andere trend is de toenemende belangstelling van de politiek. In dit Cyberdreigingsbeeld wordt het rapport 'Binnen zonder kloppen' [2] al genoemd. Europa bereidt ook nieuwe wetgeving voor zoals de NIS2-richtlijn [9] waarin aan een brede groep kritische sectoren, waaronder ook onderdelen van onderwijs en onderzoek, eisen op het gebied van cybersecurity worden gesteld.

Actoren

In figuur 14 wordt de top 5 van actoren weergegeven zoals de respondenten van de surveys die hebben aangegeven. De percentages zijn de geaggregeerde totalen van onderwijs, onderzoek en bedrijfsvoering.
Tussen onderwijs, onderzoek en bedrijfsvoering zijn er wel kleine verschillen:

- onderwijs: 1 beroepscriminelen, 2 (h)activisten en 3 studenten
- onderzoek: 1 onbekend, 2 beroepscriminelen en 3 (h)activisten
- bedrijfsvoering: 1 beroepscriminelen, 2 (h)activisten en 3 medewerkers

Figuur 14 **Top 5 actoren, uitgedrukt in percentage van het totaal onderwijs, onderzoek en bedrijfsvoering (exclusief de rubriek 'Onbekend')**



In tabel 2 zijn de meest genoemde actoren per categorie aangegeven voor onderwijs, onderzoek en bedrijfsvoering.

Tabel 2 **Belangrijkste actoren voor onderwijs, onderzoek en bedrijfsvoering**

Categorie	Onderwijs	Onderzoek	Bedrijfsvoering
1 **Verkrijging en openbaarmaking van data**	Beroepscriminelen	Beroepscriminelen	Medewerkers
2 **Identiteitsfraude**	Beroepscriminelen	Beroepscriminelen	Beroepscriminelen
3 **Verstoring van ict-voorzieningen**	Beroepscriminelen	(H)activisten	Beroepscriminelen
4 **Manipulatie van digitaal opgeslagen data**	Beroepscriminelen	Beroepscriminelen	Beroepscriminelen
5 **Spionage**	Statelijke actoren	Statelijke actoren	Statelijke actoren
6 **Overname en misbruik van ICT**	Beroepscriminelen	Beroepscriminelen	Beroepscriminelen
7 **Bewust beschadigen van imago**	(H)activisten	(H)activisten	(H)activisten
8 **Afhankelijkheid van clouddiensten**	Medewerkers	Medewerkers	Medewerkers

In vergelijking met 2020 is het aandeel dat beroepscriminelen in het totaal hebben groter geworden terwijl het aandeel van (h)activisten is gedaald.

3 RISICOPERCEPTIE

In de surveys hebben we gevraagd naar toe- of afname van het ingeschatte risico ten opzichte van 2020 voor de 8 risicocategorieën die we ook in vorige cyberdreigingsbeelden gebruikt hebben:

Verkrijging en openbaarmaking van data – Gevoelige gegevens zoals persoonsgegevens, onderzoeksgegevens en intellectueel eigendom belanden op straat of komen in verkeerde handen.

Identiteitsfraude – 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.

Verstoring van ict – DDoS-aanvallen, malware en virussen zijn aan de orde van de dag, ook voor onderwijs- en onderzoeksinstellingen.

Manipulatie van digitaal opgeslagen data – 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.

Spionage – Buitenlandse overheden proberen gevoelige informatie te verkrijgen. Vooral onderzoeksinstellingen zijn een interessant doelwit door de aanwezige gevoelige onderzoeksgegevens over bijvoorbeeld nieuwe technologie.

Overname en misbruik van ict – 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.

Bewust beschadigen van imago – Verschillende actoren, waaronder activisten, willen de reputatie van instellingen beschadigen. Bijvoorbeeld door het bekladden van de website of het overnemen van social-media-accounts.

Afhankelijkheid van clouddiensten – Instellingen hebben geen inzicht in de staat van informatiebeveiliging bij hun leveranciers of worden mede geraakt door een aanval die een van de leveranciers in de keten ondervindt. Of een leverancier gebruikt een subverwerker waarvan niet duidelijk of die alle gegevens binnen de EER verwerkt.

Net als in 2020 worden bij het onderwijsproces, het onderzoekproces en de bedrijfsvoering in het algemeen de risico's hoger ingeschat dan in het voorgaande jaar. Wel wordt voor *Manipulatie van data* het risico iets lager ingeschat bij het onderwijsproces. Voor *Spionage en Bewust beschadigen van het imago* wordt bij het onderwijsproces en bij bedrijfsvoering een iets lagere risico inschatting gedaan (zie tabel 3).

Tabel 3 **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 van ICT	**Hoog**	↗	**Hoog**	↗	**Zeer hoog**	↑
7 Bewust beschadigen van imago	**Medium**	—	**Medium**	↗	**Medium**	—
8 Afhankelijkheid van clouddiensten	**Zeer hoog**	↑	**Zeer hoog**	↑	**Zeer hoog**	↑

△ Ontwikkeling 2021 t.o.v. 2020

↑ Forse toename t.o.v. 2020

↗ Toename t.o.v. 2020

— Geen verandering t.o.v. 2020

** Bij Spionage is de onzekerheid het grootst (46% weet niet of het risico is toe- of afgenomen)*

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 SAMENVATTING RESULTATEN SURVEY

In het najaar van 2021 hebben we twee surveys gehouden onder bij SURF aangesloten organisaties:

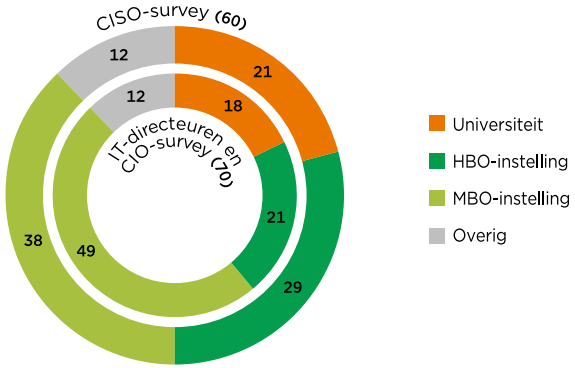
1 onder functionarissen die zich dagelijks bezighouden met informatiebeveiliging en/of privacy en
2 onder IT-directeuren en CIO's. Deze richtte zich meer op governance en risicomanagement.

In dit hoofdstuk vind je een selectie van de resultaten.

Verdeling respondenten

Bij de security-/privacyfunctionarissen zijn 126 surveys uitgezet, bij de IT-directeuren en CIO's 60. De volledig ingevulde surveys (68 door de CISO's en 33 door de IT-directeuren en CIO's) zijn als volgt verdeeld over de sectoren:

Figuur 15 **Verdeling van respondenten over de verschillende sectoren** (in %)



Deze verdeling wijkt niet substantieel af van voorgaande jaren.

Rol van de respondenten

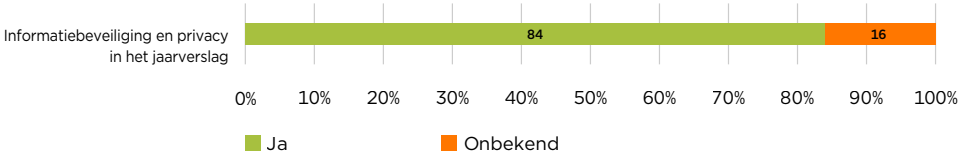
We hebben de respondenten gevraagd naar hun rol binnen de instelling. Bij de eerste groep zijn het voornamelijk CISO's en security officers die de survey hebben ingevuld (60%). 12% zijn privacy officers en FG's. In de relatief grote groep overig (28%) hebben de meeste respondenten een rol binnen IT. In de tweede groep hebben vooral CIO's en IT-/IM-managers de survey ingevuld (70%).

Governance

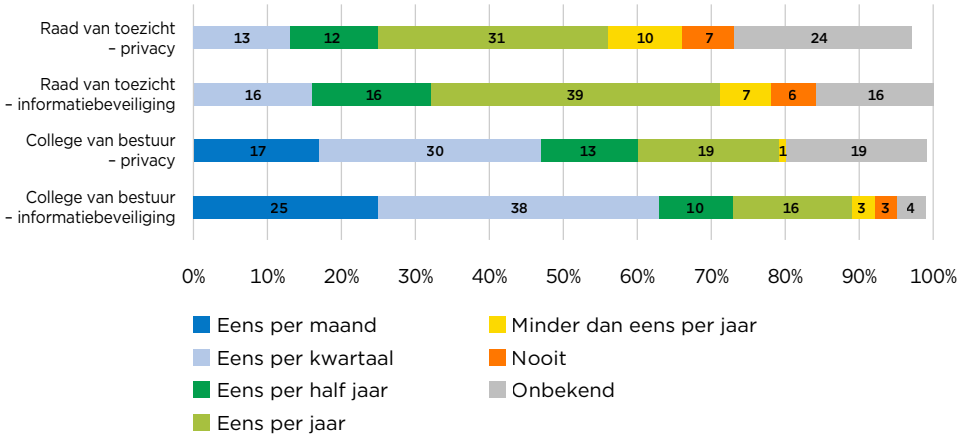
Rapportage

We hebben in de survey gevraagd of, en zo ja hoe vaak, over informatiebeveiliging en privacy wordt gerapporteerd aan het college van bestuur en de raad van toezicht. Daarnaast hebben we gevraagd of in het jaarverslag van de instelling een paragraaf over informatiebeveiliging en privacy is opgenomen.

Figuur 16 **Percentage instellingen dat over informatiebeveiliging en privacy rapporteert in het jaarverslag**



Figuur 17 **Percentage instellingen dat rapporteert over informatiebeveiliging en privacy aan college van bestuur en raad van toezicht**

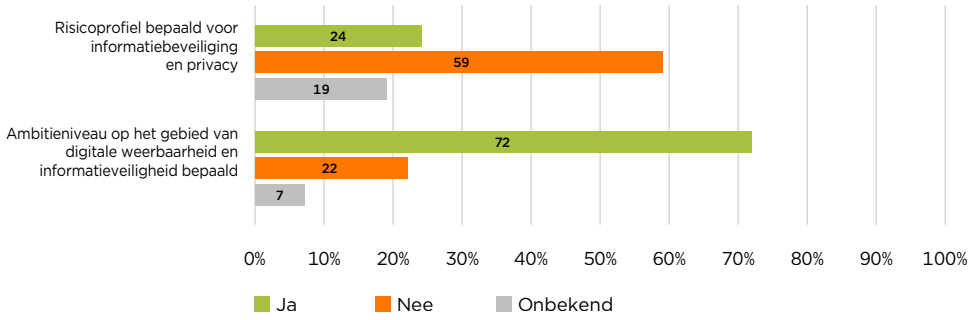


Vrijwel alle instellingen geven aan te rapporteren over informatiebeveiliging en privacy. Ook besteden ze over het algemeen aandacht aan informatiebeveiliging en privacy in hun jaarverslag. De meeste instellingen rapporteren maandelijks aan het college van bestuur en eens per jaar aan de raad van toezicht.

Risicoprofiel en ambitieniveau

Het is van groot belang dat instellingen weten welke risico's zij lopen op het gebied van informatiebeveiliging en privacy en daarom een risicoprofiel opstellen. Daarnaast is het belangrijk om een ambitieniveau vast te stellen om te kunnen bepalen welke maatregelen genomen moeten worden. We hebben dan ook gevraagd of instellingen een risicoprofiel en ambitieniveau hebben opgesteld.

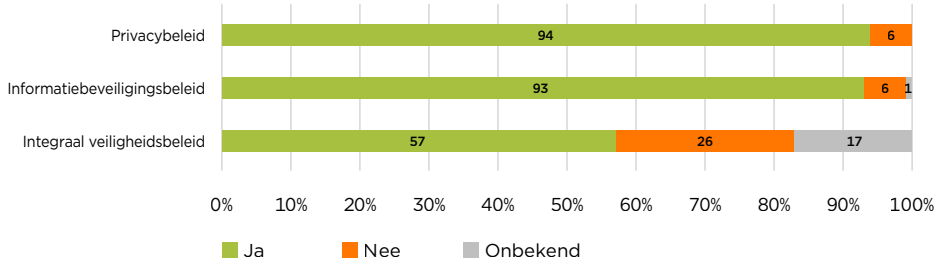
Figuur 18 **Percentage instellingen met risicoprofiel en ambitieniveau op het gebied van informatiebeveiliging en privacy**



Informatiebeveiliging- en privacybeleid

Verreweg de meeste instellingen hebben zowel een informatiebeveiligingsbeleid als een privacybeleid. Iets meer dan de helft van de instellingen heeft inmiddels ook een integraal veiligheidsbeleid. Daarin is behalve voor informatiebeveiliging ook aandacht voor de andere veiligheidsdomeinen, zoals sociale veiligheid, kennisveiligheid, arbo en milieu.

Figuur 19 **Percentage instellingen met een formeel vastgesteld informatiebeveiligingsbeleid, privacybeleid en/of integraal veiligheidsbeleid**

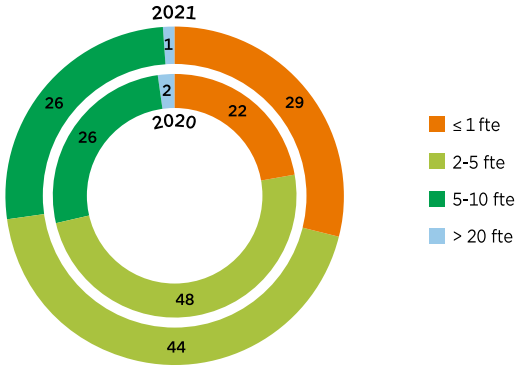


Capaciteit en budget

Ten opzichte van 2020 hebben geen grote verschuivingen plaatsgevonden op het vlak van capaciteit en budget (zie figuur 20). Om weerbaar te zijn tegen cyberdreigingen is voldoende capaciteit, de juiste expertise en voldoende budget voor informatiebeveiliging en privacy van groot belang. Uit de surveys blijkt dat 73% van de CISO's en 50% van de IT-directeuren en CIO's een gebrek aan capaciteit als kwetsbaarheid noemt.

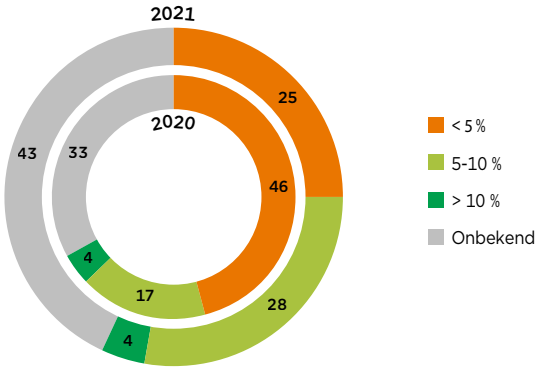
Daarnaast geeft 60% van de CISO's en 34% van de IT-directeuren en CIO's aan dat ze het gebrek aan expertise ook als een belangrijke kwetsbaarheid zien. Dit roept de vraag op of niet meer inspanningen moeten worden gedaan om capaciteit en expertise te vergroten.

Figuur 20 **Percentage instellingen dat x fte beschikbaar heeft voor informatiebeveiliging op strategisch, tactisch en operationeel vlak**



De budgetten voor cybersecuritymaatregelen die het meeste aandacht krijgen en zijn opgenomen in de begroting (zie figuur 21), lijken ten opzichte van 2020 licht gestegen. Wat daarbij opvalt is dat meer respondenten aangeven dat zij de omvang van het beschikbare budget niet te kennen.

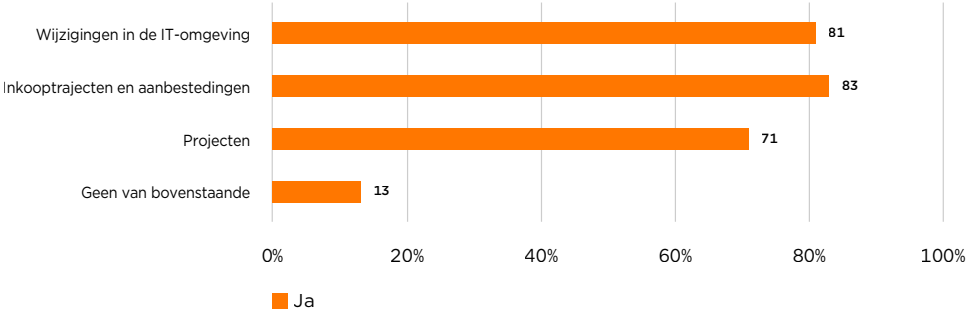
Figuur 21 **Percentage instellingen dat x% van het totale IT-budget beschikbaar heeft voor specifieke cybersecuritymaatregelen**



Aandacht voor informatieveiligheid en privacy

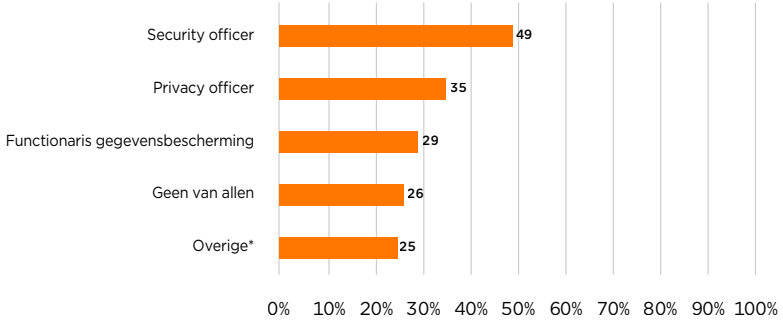
Bij veruit de meeste instellingen wordt structureel aandacht besteed aan informatieveiligheid en privacy bij projecten, bij wijzigingen in de IT-omgeving en bij inkoop en aanbesteding. Dit is ten opzichte van 2020 nauwelijks gewijzigd.

Figuur 22 **Percentage instellingen met aandacht voor informatiebeveiliging bij wijzigingen in de IT-omgeving, bij inkooptrajecten en aanbestedingen en bij projecten**



Ook het percentage instellingen dat vanaf het begin informatie- en/of privacy-deskundigen bij projecten betrekt (zie figuur 23), is niet significant gewijzigd ten opzichte van 2020. Bij de security officers is een daling te zien. Een mogelijke verklaring hiervoor is dat instellingen volwassener zijn geworden op dit gebied en dat de kennis op het gebied van security ook dieper in de organisatie is ingedaald. De categorie 'Overige' bestaat onder andere uit informatiemanagers, securityadviseurs, IT-architecten.

Figuur 23 **Percentage instellingen dat informatiebeveiligings- en/of privacy-functionarissen vanaf het begin bij projecten betrekt**

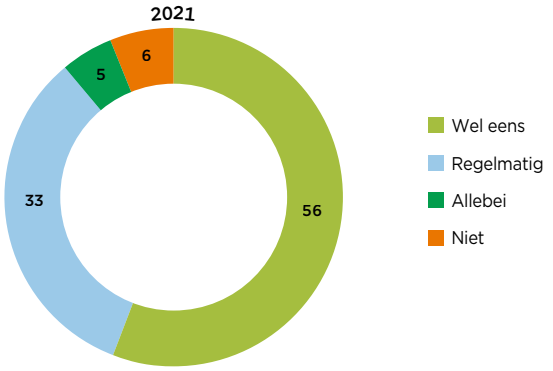


Aandacht voor awareness

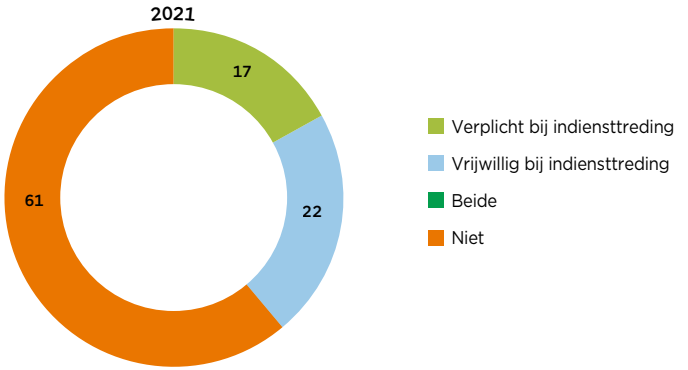
In de survey's hebben we gevraagd in welke mate instellingen aandacht besteden aan awareness, op welke momenten ze dat doen en of aandacht voor awareness al dan niet verplicht is. Onderstaande grafieken (zie figuur 24 – 27) laten zien dat de meeste instellingen aandacht aan awareness besteden. Eenderde van de instellingen doet dit regelmatig.

Bij 39% van de instellingen is aandacht voor awareness bij indiensttreding en bij 31% wordt aanvullend aandacht aan awareness besteed. Bij een minderheid van de instellingen is aandacht voor awareness een verplicht onderdeel.

Figuur 24 **Percentage instellingen dat aandacht aan awareness heeft besteed**

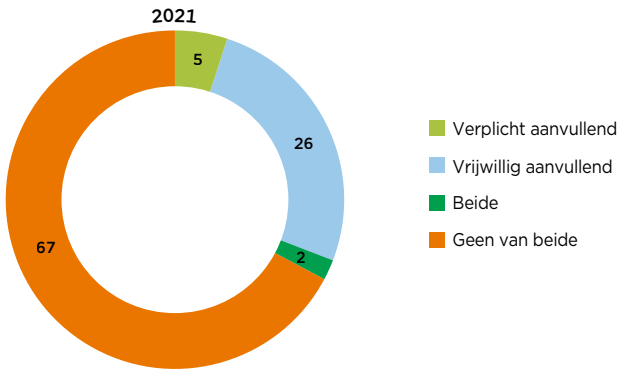


Figuur 25 **Percentage instellingen dat structureel aandacht besteedt aan awareness bij indiensttreding verplicht of vrijwillig**

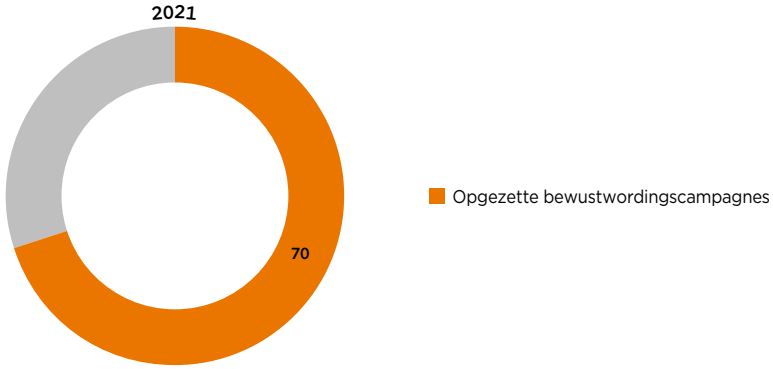


Phishingmails worden nog steeds geraffineerder en het is voor medewerkers vaak lastig om deze als phishing te herkennen. We hebben in de survey gevraagd of in 2021 bewustwordingscampagnes zijn opgezet rond het thema phishing. 70% van de instellingen heeft dat gedaan.

Figuur 26 **Percentage instellingen dat structureel aandacht besteedt aan awareness; aanvullend, verplicht of vrijwillig**



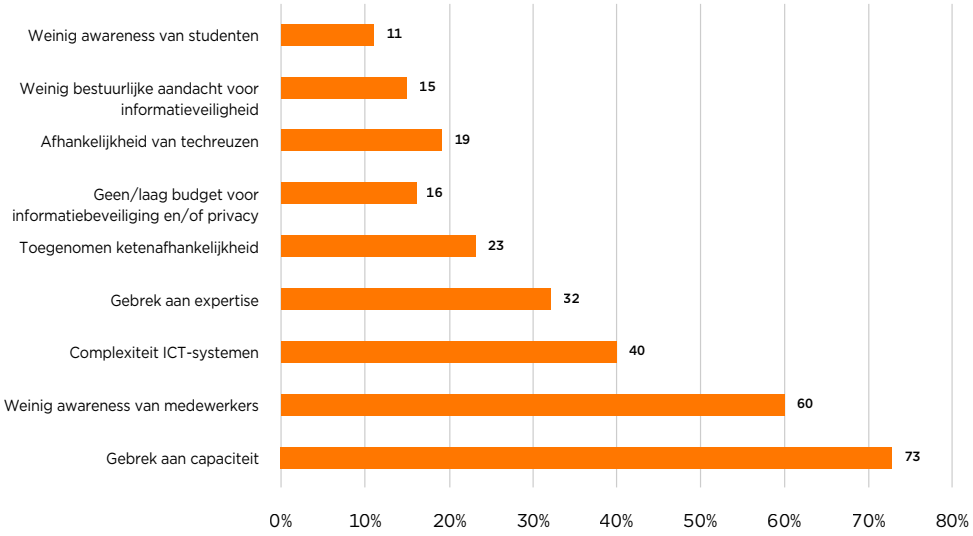
Figuur 27 **70% van de instellingen heeft in 2021 bewustwordingscampagnes opgezet om medewerkers te helpen phishing-mails beter te herkennen**



Kwetsbaarheden

De CISO's zien gebrek aan capaciteit als grootste kwetsbaarheid binnen de eigen organisatie. Weinig awareness van medewerkers en complexiteit van ict-systemen komen op de tweede en derde plaats.
IT-directeuren en CIO's noemen als grootste kwetsbaarheden:
1. weinig awareness van medewerkers; 2. gebrek aan capaciteit;
3. en 4. (ex aequo) toegenomen ketenafhankelijkheid en complexiteit van ict-systemen.

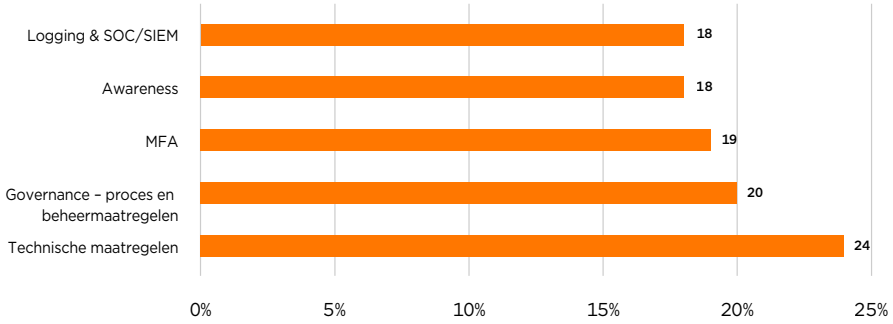
Figuur 28 **Percentage instellingen waar onderstaande kwetsbaarheden van toepassing zijn**



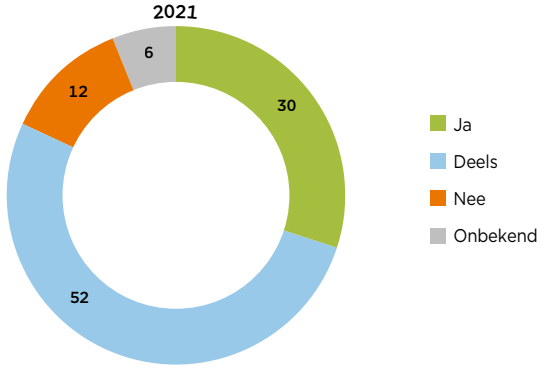
Aspecten met de meeste aandacht

De IT-directeuren en CIO's noemen MFA, awareness en technische maatregelen de drie belangrijkste punten waar aandacht aan besteed wordt.

Figuur 29 **Percentage CISO's dat onderstaande aspecten van informatieveiligheid noemt als aspecten die die de hoogste aandacht hadden in 2021 en zijn opgenomen in de begroting 2022**



Figuur 30 **Percentage instellingen met IAM-beleid**



Beleid identity- en accessmanagement (IAM-beleid)

Het beheersen van identiteiten en toegangsrechten is een belangrijk instrument om ongeoorloofde toegang (manipulatie en diefstal van gegevens) te voorkomen en daarmee vertrouwelijkheid en integriteit van gegevens te waarborgen. Een IAM-beleid waarin dit goed is geregeld draagt in belangrijke mate bij aan de weerbaarheid van een instelling.

De meerderheid van de respondenten geeft aan dat hun instelling een IAM-beleid heeft. 52% geeft aan dat dat ten dele het geval is. Dit houdt in dat het beleid ofwel niet op alle onderdelen van de instelling van toepassing is, ofwel dat er beleid is, maar dat er geen controles plaats-vinden.

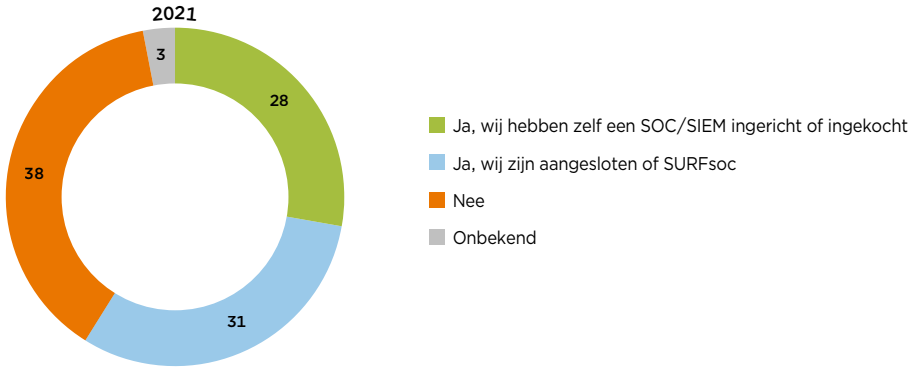
Technische maatregelen

We hebben naar de implementatie van een aantal belangrijke technische maatregelen gevraagd. Deze paragraaf geeft een overzicht van de resultaten.

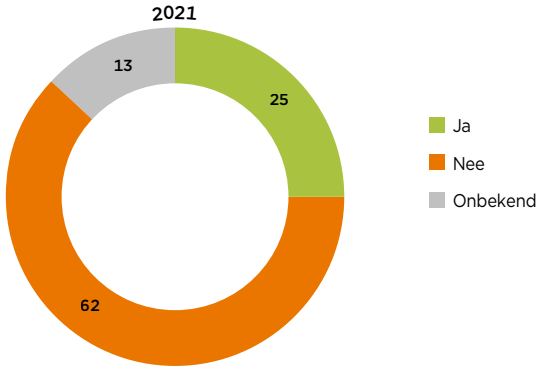
Security operations centre / security information & event management

In totaal maakt bijna 60% van de instellingen gebruik van een Security Operations Centre (SOC) of Security Information & Event Management (SIEM). Ruim de helft daarvan is aangesloten bij SURFsoc, de rest heeft een eigen SOC/SIEM of heeft dat elders ingekocht.

Figuur 31 **Percentage instellingen met initiatieven op het vlak van SOC/SIEM**



Figuur 32 **Percentage instellingen met applicatielogging ingericht voor elk systeem**



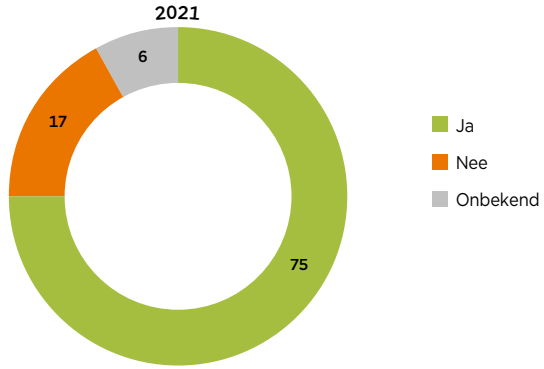
Applicatielogging

De survey laat zien dat bij een meerderheid van de instellingen applicatie-logging niet voor elk systeem is ingericht.

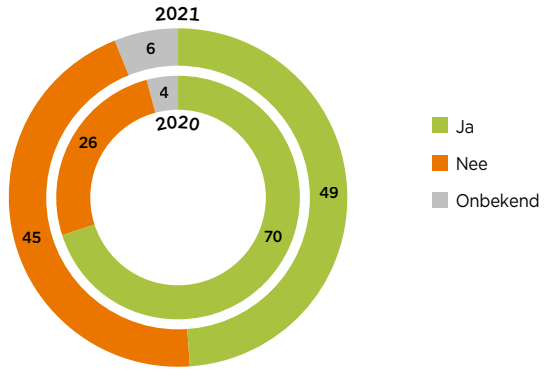
Netwerksegmentatie

Driekwart van de respondenten geeft aan dat bij hun instelling netwerksegmentatie effectief wordt toegepast. Netwerksegmentatie zorgt voor een gelaagde structuur waardoor een netwerk niet in een keer in zijn geheel kan worden gecompromitteerd.

Figuur 33 **Percentage instellingen dat netwerksegmentatie toepast**



Figuur 34 **Percentage instellingen die tenminste enkele keren per jaar belangrijke systemen scannen**



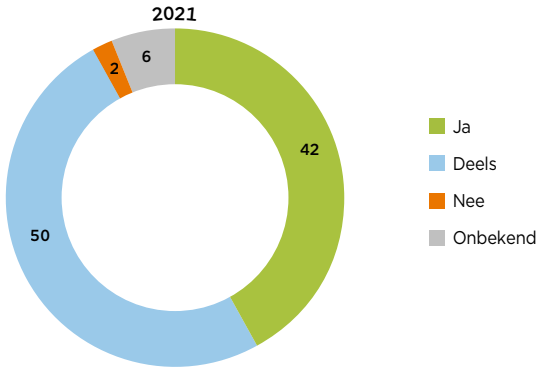
Scannen op kwetsbaarheden

Opvallend is dat de belangrijke systemen in 2021 minder op kwetsbaarheden zijn gescand dan in 2020. Mogelijk is dit verschil te verklaren door een strengere beoordeling in 2021, maar dit is niet helemaal duidelijk.

Patchmanagement

92% van de respondenten geeft aan dat securitypatches op systemen worden uitgevoerd. Echter, 50% van de instellingen doet dat niet structureel of niet op alle systemen.

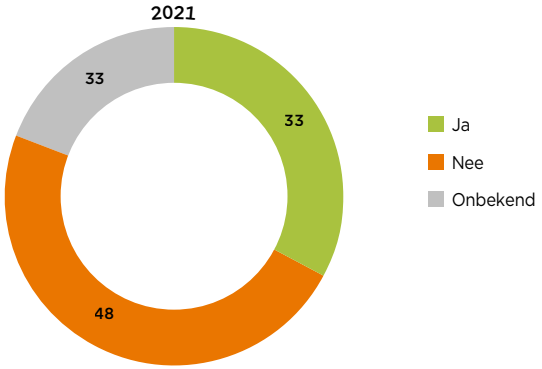
Figuur 35 **Percentage instellingen dat het patchniveau structureel up-to-date houdt**



Versleuteling van gegevens

Gevoelige gegevens worden nog op beperkte schaal versleuteld (zie figuur 36). Een aantal respondenten geeft in de toelichting bij deze vraag aan dat alternatieve maatregelen zijn genomen, zoals generieke versleuteling op systeem- of database-niveau of een striktere toepassing van toegangsbeveiliging.

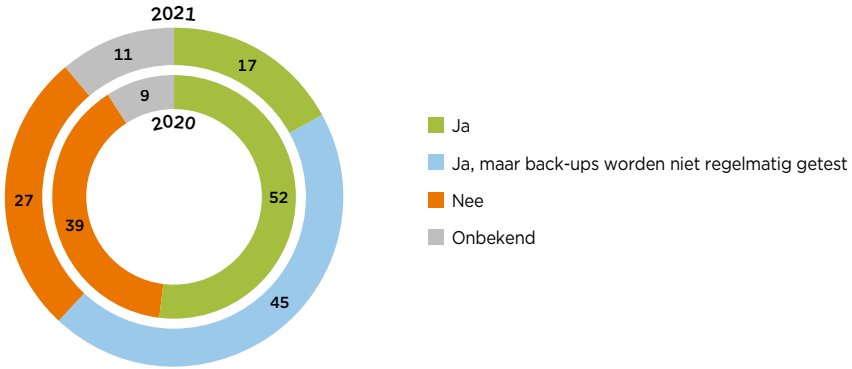
Figuur 36 **Percentage instellingen met versleutelde opslag van gevoelige gegevens, waaronder persoonsgegevens**



Offline back-ups

Het aantal instellingen dat offline back-ups maakt is gestegen sinds 2020. Toen was het percentage instellingen dat offline back-ups maakt 52%. In de survey van 2021 hebben we niet alleen gevraagd of er back-ups worden gemaakt, maar ook of deze regelmatig worden getest. De resultaten van de survey laten zien dat het aantal instellingen dat offline back-ups maakt is gestegen naar 62%, maar dat slechts 17% ze ook regelmatig test.

Figuur 37 **Percentage instellingen dat een backup- en restore-beleid waarin offline backup en regelmatig testen worden geregeld**

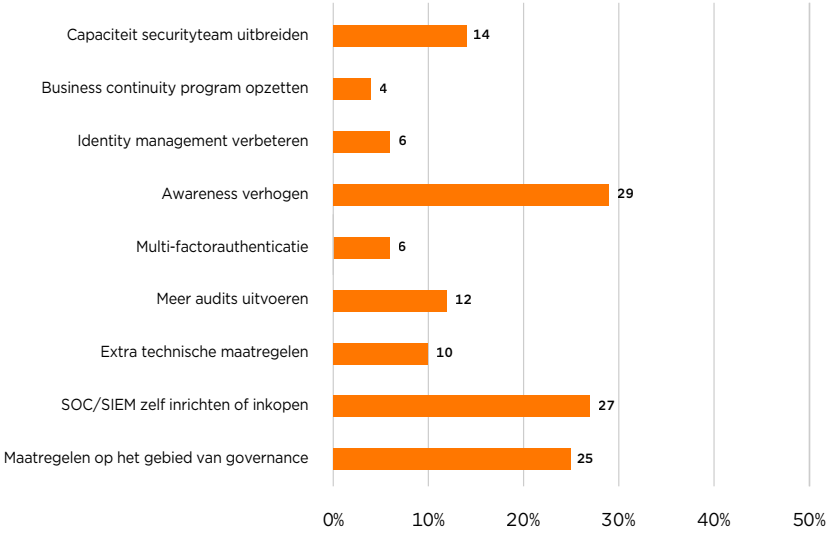


Als budget en capaciteit geen rol spelen

Tot slot hebben we de respondenten gevraagd wat zij het eerst zouden aanpakken als budget en capaciteit geen rol zouden spelen. Hier wordt awareness verhogen het meest genoemd, maar het inrichten van een SOC/SIEM en maatregelen op het gebied van governance scoren nagenoeg even hoog. Bij maatregelen op het gebied van governance wordt een scala aan maatregelen genoemd variërend van het inrichten van een governancestructuur, het inrichten van eigenaarschap tot uitbreiding van het aantal audits. Verder valt op dat het uitbreiden van capaciteit door slechts 14% van de respondenten wordt genoemd terwijl gebrek aan capaciteit door 73% van de CISO's en door 50% van de CIO's en IT-directeuren als kwetsbaarheid voor de instelling wordt gezien.

Figuur 38 **Percentage instellingen dat onderstaande maatregelen noemt als voorgestelde maatregelen als budget**

Als budget en capaciteit geen rol zouden spelen, wat is dan het eerste dat je zou aanpakken in jouw instelling op het gebied van informatieveiligheid en privacy?



5 WEERBAARHEID

Organisaties moeten ervoor zorgen dat hun weerbaarheid op orde is, zeker nu dreigingen zoals ransomware-aanvallen, phishing en DDoS-aanvallen steeds meer toenemen. Weerbaar zijn betekent enerzijds goed beschermd zijn tegen aanvallen en anderzijds in staat zijn bij een incident snel in te grijpen, gevolgen te beperken en door te kunnen gaan met de gewone bedrijfsvoering. Een aantal verschillende bronnen is het eens over welke maatregelen de sector onderwijs en onderzoek als eerste moet nemen om de belangrijkste dreigingen het hoofd te bieden. In dit hoofdstuk noemen we enkele van die weerbaarheidsverhogende maatregelen en zetten deze naast elkaar om de overeenkomsten te laten zien. Daarna volgt een beschrijving van de belangrijkste maatregelen die we als sector moeten nemen of al nemen om weerbaarder te worden.

Onderwijs- en onderzoeksinstellingen doen al sinds 2011 mee met SURFaudit benchmarks informatiebeveiliging[6] om te bepalen hoe hun informatieveiligheid ervoor staat. In de resultaten zien we dat er gestaag vooruitgang wordt geboekt, maar betekent dat ook dat instellingen weerbaarder zijn geworden?

Na het incident bij de Universiteit Maastricht in 2019 hebben we gekeken naar een aantal operationele maatregelen die in de evaluatie van dat incident naar voren zijn gekomen als zwakke punten [10]:

- ontbrekende belangrijke beveiligingsupdates
- beperkte segmentatie binnen het netwerk
- het niet opvolgen van verschillende alarmsignalen
- onveilige netwerk- en systeemconfiguraties

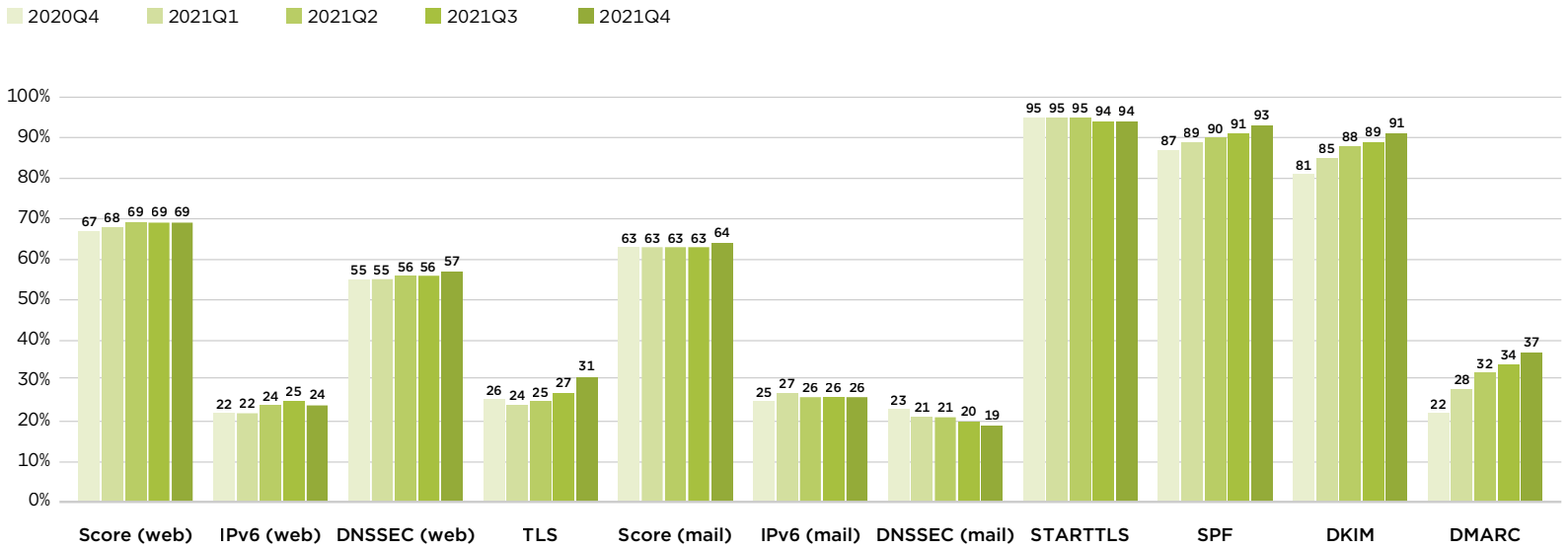
Uit onze survey in 2020 blijkt verder dat een up-to-date inventarisatie van de IT-omgeving (ook wel CMDB - Configuratie Management Database genoemd) in veel gevallen ontbreekt en ook dat vaak niet bekend is welke kwetsbaarheden aanwezig is op kritieke systemen, de kroonjuwelen.
Bij de audit in 2020 bleek dat deze punten niet uniek zijn voor de Universiteit Maastricht, maar ook voorkomen bij andere instellingen. Het blijft daarom belangrijk extra aandacht te besteden aan deze operationele maatregelen.

SURF IV-Metingen

SURF voert al enkele jaren ieder kwartaal internet-veiligheidsmetingen uit, de IV-metingen, om in kaart te brengen in hoeverre onderwijs- en onderzoeks- instellingen voldoen aan de lijst van verplichte standaarden (zie figuur 39 - 41). Rijks- en semi-overheid moeten zich aan de standaarden op deze lijst houden bij de aanschaf en inrichting van ICT-systemen[7].
SURF participeert in het Forum Standaardisatie, dat deze lijst heeft opgesteld. In het algemeen doet de rijksoverheid het consequent beter dan onze sector (zie bijvoorbeeld figuur 41).

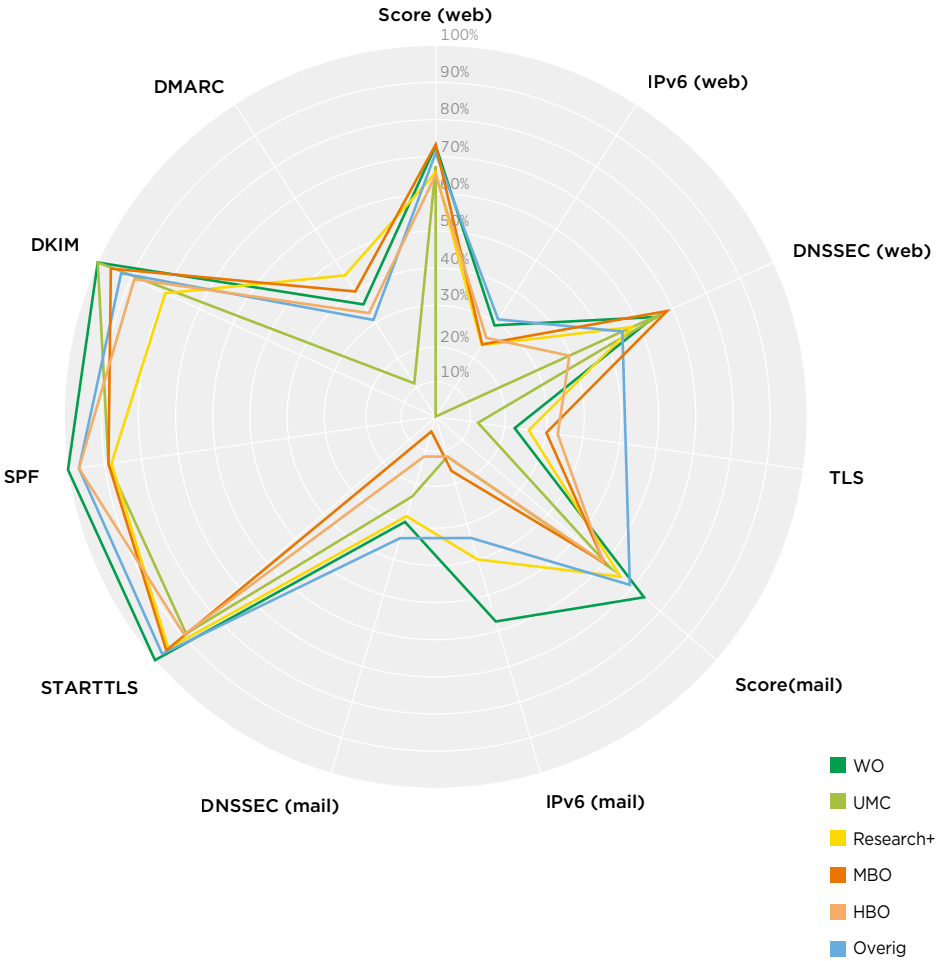
6 zie https://www.surfaudit.nl en https://mbodigitaal.nl/?s=benchmark
7 zie https://www.forumstandaardisatie.nl/open-standaarden

Figuur 39 **IV-metingen 2021**

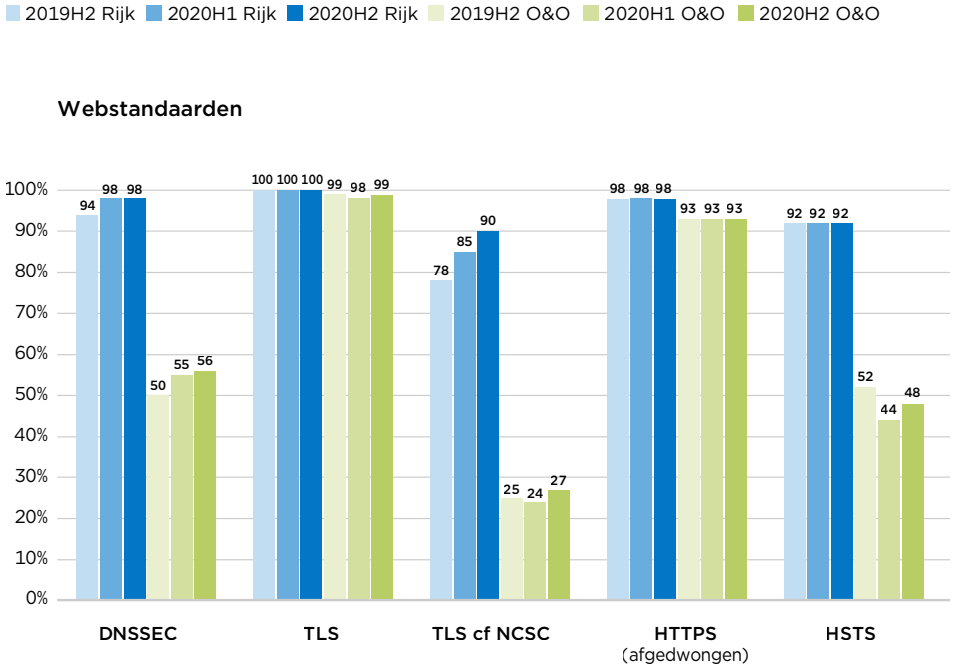


Onderstaande plot (figuur 40) laat duidelijk zien waar bij SURF aangesloten instellingen de sterke en minder sterke punten zitten. Voor de verschillende deelsectoren is het beeld ongeveer hetzelfde.

Figuur 40 **IV-metingen Q4 2021 per sector** (%)



Figuur 41 **Onderwijs en onderzoek vs. overheid - IV-metingen webstandaarden**



Figuur 41

Andere bronnen

Rapport 'Binnen zonder kloppen'

Het ransomware-incident bij de Universiteit Maastricht heeft ervoor gezorgd dat informatieveiligheid in de sector onderwijs en onderzoek ook hoog op de agenda van bestuurders en beleidsmakers is gekomen. De Inspectie van het Onderwijs heeft in september 2021 het rapport 'Binnen zonder kloppen – Digitale weerbaarheid in het hoger onderwijs' [2] gepubliceerd. Dit rapport, gericht op bestuurders in het hoger onderwijs, brengt in kaart hoe hoger-onderwijsinstellingen hun cyberweerbaarheid kunnen verhogen om de continuïteit van onderwijs en onderzoek te waarborgen.

De inspectie van het onderwijs heeft de huidige situatie in het hoger onderwijs uitvoerig onderzocht en geeft aanbevelingen om de kwetsbaarheid van de sector te verminderen. Daarbij benadrukt de inspectie dat besturen de krachten moeten bundelen en digitale veiligheid onderdeel moeten maken van het risico-management. In het Cyberdreigingsbeeld 2018 hebben we al aangegeven dat bestuurlijke aandacht belangrijk is. We hebben toen vijf punten voor reflectie opgesteld die bestuurders kunnen gebruiken voor de dialoog over cyberrisico's en -weerbaarheid in hun eigen instelling.

Tabel 3 **Bestuurlijke reflectie uit Cyberdreigingsbeeld 2018**

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

Het inspectierapport noemt zeven standaarden[8] voor bestuurders die ook aansluiten bij de risicocategorieën die we in de sector onderwijs en onderzoek hanteren:

1 Vergroten bewustzijn
2 Veilige en open cultuur
3 Inrichten risicoteam
4 Borgen risicomanagement
5 Aandacht voor ketensamenwerking
6 Controleren en evalueren
7 Geld investeren in informatiebeveiliging*

* toegevoegd door de Inspectie van het Onderwijs ten behoeve van het rapport 'Binnen zonder kloppen'.

Verder haakt het rapport van de inspectie aan bij de mogelijke cyberincidenten en risico's die door het Nationaal Crisisplan Digitaal zijn geïdentificeerd.

Tabel 4 toont de overeenkomsten met de risicocategorieën het Cyberdreigingsbeeld:

8 zie ook: https://www.bio-overheid.nl/media/1355/bio-leaflet-voor-bestuurders.pdf

Tabel 4 **Risicocategorieën uit het Cyberdreigingsbeeld en risico's uit rapport inspectie van het onderwijs**

Cyberdreigingsbeeld	Binnen zonder kloppen 2021
1 **Verkrijging en openbaarmaking van data**	**Lek** – aantasting van de vertrouwelijkheid als gevolg van natuurlijk, technisch of menselijk falen. **Informatiediefstal** – aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie.
2 **Identiteitsfraude**	
3 **Verstoring van ict**	**Storing/uitval** – aantasting van de integriteit of beschikbaarheid als gevolg van natuurlijk, technisch of menselijk falen. **Verstoring/Sabotage** – het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten
4 **Manipulatie van data**	I**nformatiemanipulatie** – aantasting van de integriteit van informatie door het opzettelijk wijzigen van informatie.
5 **Spionage**	**Spionage** – aantasting van de vertrouwelijkheid van informatie door het kopiëren of wegnemen van informatie door statelijke of staatsgelieerde actoren.
6 **Overname en misbruik van ict**	**Systeemmanipulatie** – aantasting van informatiesystemen of -diensten; gericht op de vertrouwelijkheid of integriteit van systemen of -diensten. Deze worden daarna ingezet om andere aanvallen uit te voeren.
7 **Bewust beschadigen van imago**	**Verstoring/Sabotage** – het opzettelijk aantasten van de beschikbaarheid van informatie, informatiesystemen of -diensten.
8 **Afhankelijkheid van clouddiensten**	

Weerbaarheidverhogende maatregelen

Uit bovengenoemde bronnen kunnen de volgende maatregelen worden gedestilleerd:

- Vergroot het bewustzijn van medewerkers en studenten.
- Zorg voor een veilige en open cultuur.
- Richt een beveiligingsorganisatie in.
- Richt risicomanagement in, ook voor cyberrisico's.
- Evalueer afhankelijkheden in ketenprocessen en -samenwerkingen en pas deze zo nodig aan.
- Voer belangrijke beveiligingsupdates uit op alle op het netwerk aangesloten systemen.
- Segmenteer het netwerk.
- Breid logging en monitoring uit en acteer op de hieruit voortkomende alarmsignalen.
- Richt netwerk- en systeemconfiguraties in volgens het principe security by design.
- Richt een Configuratie Management Database (CMDB) in en houd deze actueel.
- Controleer en evalueer regelmatig.
- Houd investeringen in informatiebeveiliging op niveau.

Er worden in de sector al belangrijke stappen gezet om de weerbaarheid naar een hoger niveau te tillen. De UNL (voorheen VSNU) heeft afgesproken dat alle universiteiten binnen twee jaar gemiddeld volwassenheidsniveau 3 (zie tabel 5) voor het SURFaudit Toetsingskader Informatiebeveiliging [11] behalen en tegelijk operationele maatregelen nemen om de weerbaarheid te verhogen. Bij de VH wordt nu ook een vergelijkbare afspraak gemaakt voor de Nederlandse hogescholen.

Tabel 5 **Volwassenheidsniveaus (VN) in het SURFaudit Toetsingskader Informatiebeveiliging Hoger onderwijs**

VN	Omschrijving	Toelichting
1	**Maatregelen zijn ad hoc**	Beheersmaatregelen zijn niet of slechts gedeeltelijk vastgesteld en/of worden op een inconsistente manier uitgevoerd en zijn **sterk afhankelijk van individuen**.
2	**Maatregelen bestaan en worden op consistente wijze uitgevoerd**	Beheersmaatregelen bestaan en worden op een gestructureerde en consistente, **maar informele manier** uitgevoerd.
3	**Maatregelen zijn gedocumenteerd en de uitvoering is aantoonbaar**	Beheersmaatregelen zijn gedocumenteerd en worden op een gestructureerde en formele manier uitgevoerd. Uitvoering van de maatregelen is **aantoonbaar, getest en effectief**.
4	**Er is een verbeter-cyclus aanwezig en gedocumenteerd**	De effectiviteit van beheersmaatregelen wordt periodiek beoordeeld en indien nodig verbeterd. Deze beoordeling is **gedocumenteerd**.
5	**Er is een bedrijfsbrede aanpak van risico's**	Een bedrijfsbreed risico- en beheersprogramma voorziet in **continue en effectieve beheersing** en aanpak van risico's.

Besturen in de sector onderwijs en onderzoek zelf hebben veel meer aandacht gekregen voor de staat van informatiebeveiliging. Op operationeel niveau werken instellingen steeds vaker en beter samen. Die samenwerkingsverbanden krijgen gestalte bij zowel de koepels (UNL, VH, MBO Raad) als de samenwerkingsorganisaties (SURF, MBO Digitaal, Kennisnet).
Verder doen veel instellingen mee met de crisisoefeningen OZON en NOZON die SURF periodiek organiseert. En het aantal instellingen dat aansluit bij SURFsoc neemt gestaag toe.

‘Als CISO ben ik steeds op zoek naar de balans tussen de belangen van onderwijs en onderzoek, business, innovatie en veiligheid’

Tekst: Marjolein van Trigt

Roeland Reijers is Chief Information Security Officer (CISO) van de Universiteit van Amsterdam en de Hogeschool van Amsterdam. Een hack op deze instellingen werd in februari 2021 net op tijd ontdekt. De rest van het jaar stond in het teken van het herstellen en verbeteren van de cyberveiligheid.

In vacatures wordt snel gesproken van een ‘uitdagende functie’, maar Roeland Reijers heeft er écht een. Hij is CISO van een grote onderzoeks-universiteit en een grote hogeschool, die onder meer de ict met elkaar delen en die zich bevinden in bijna tachtig panden, verspreid over de hoofdstad. Als Reijers veiligheidsadviezen geeft of beleidsmaatregelen oplegt, dan worden die doorgaans opgevolgd. Die bereidwilligheid is alleen maar gegroeid sinds de ontdekking in februari 2021 dat er hackers zaten in de systemen van de UvA en de HvA. Een cyberaanval kon op het nippertje worden afgeslagen. ‘We hebben geluk gehad dat ze de virtuele knop nog niet hadden omgezet,’ zegt Reijers. ‘Misschien waren ze nog druk met een ander slachtoffer, of zochten ze naar meer gevoelige systemen, zodat de aanval meer impact zou hebben. Dat zullen we nooit weten.’

Goede samenwerking na hack

Door de hack werd het belang van asset management voor Reijers nog eens bevestigd. 'Een server blijkt geïnfecteerd, maar je kunt hem niet zomaar uitzetten als dat zou betekenen dat bijvoorbeeld 6.000 studenten hun tentamen niet kunnen afmaken,' zegt hij. 'Als je die informatie niet hebt, omdat je niet weet wie de eigenaar is of welke data erop staan, dan loop je vertraging op, terwijl de hacker daarbinnen bezig is.'
Ook hamert hij sindsdien nog meer op het belang van controleren, testen en audits. 'Het beeld dat mensen hebben, strookt niet altijd met de werkelijkheid. Projecten zijn toch niet opgeleverd zoals het zou moeten, documentatie is niet bijgewerkt, tijdelijke wijzigingen zijn niet teruggedraaid. Dus moet je blijven toetsen of informatie ook echt klopt.'
De hack leverde ook positieve ervaringen op. Zo was er vanuit de hele organisatie een enorm commitment om de crisissituatie op te pakken. 'Uit de evaluatie blijkt dat de samenwerking heel goed ging en dat heb ik zelf ook zo ervaren.'

Behoefte aan generieke dreigingsinformatie

Over SURFcert is Reijers erg te spreken, net als over de samenwerking met andere instellingen. 'Het is echt een publieke kernwaarde om informatie te delen die anderen in staat stelt om zichzelf te beschermen.'
De samenwerking met het NCSC, via SURFcert, moet beter. 'De overheid mocht kennis over aanvallen en andere dreigingsinformatie niet met ons delen. Ik vind dat echt onvoorstelbaar. Er was een wetswijziging voor nodig om het mogelijk te maken.'
Naast het delen van actuele operationele dreigingsinformatie (IoC's), heeft hij behoefte aan meer generieke dreigingsinformatie, bijvoorbeeld voor rapportages aan het bestuur. 'Denk aan informatie over motivatie van de aanvallers, het type aanvallen dat plaatsvindt en over trends.'
Op dit moment levert de markt dit niet. Daarom pleit Reijers ervoor om als sector een breder Cyber Threat Intelligence-netwerk in te richten.

Minder risicotolerantie

De algehele risicotolerantie neemt af sinds de hack op de Universiteit Maastricht, stelt hij vast. De angst voor met name een aanval met gijzelsoftware is groot onder bestuurders. 'Het risico ontstaat dat je doorslaat en je alleen maar richt op dure preventieve maatregelen, terwijl je daarmee misschien de organisatie lamlegt. Een keuze voor optimale veiligheid zou voor de UvA bijvoorbeeld betekenen dat het beter is om de vele bestaande internationale samenwerkingsverbanden te verbreken. De consequentie is alleen dat we dan niet lang meer behoren tot de top vijftig van onderzoeksuniversiteiten waartoe we willen behoren. Het is altijd zoeken naar een balans tussen het belang van onderwijs en onderzoek, business, innovatie en veiligheid.'

Inzicht in aanvalsmethoden cybercriminelen

Om de weerbaarheid te verhogen zou je je moeten verdiepen in de methoden en hulpmiddelen die aanvallers gebruiken om een organisatie aan te vallen. Op die manier kun je effectieve bescherming inrichten, detectie opzetten en bijvoorbeeld aan de hand van scenario's reacties bedenken en oefenen.

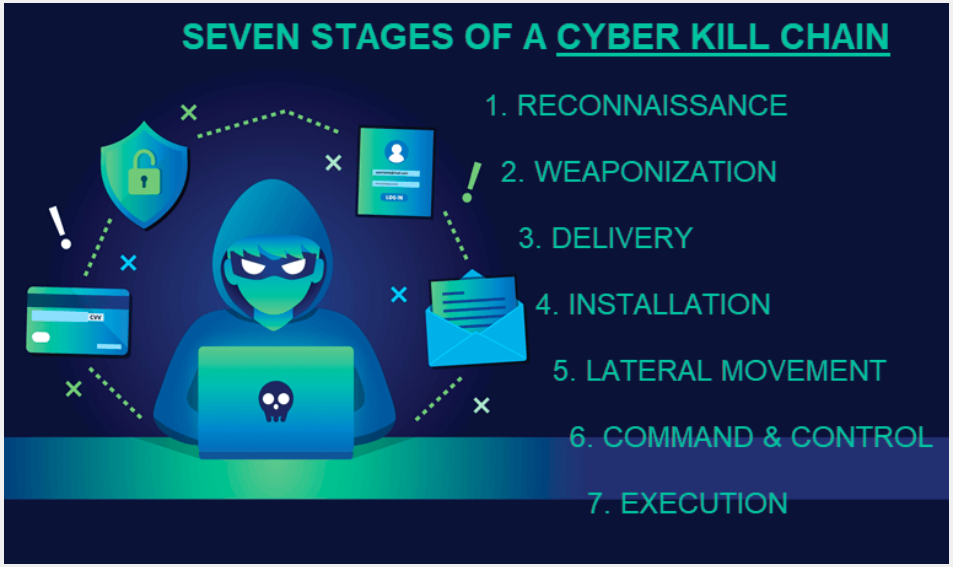
Cyber kill chain

Een van die modellen is de Lockeed Martin *cyber kill chain* [12] (zie figuur 42). Hierop zijn later een aantal varianten zoals het MITRE ATT&CK framework [13] en de Unified Kill Chain [14] ontwikkeld om alle stappen beter af te dekken.

- Deze modellen bevatten allemaal een aantal fasen:
- In de **voorbereidende fase** onderzoekt de aanvaller het doelwit, probeert toegang te krijgen tot het netwerk en/of systemen en bereidt de infrastructuur voor op de aanval.
- In de **consolidatiefase** zorgt de aanvaller ervoor dat hij, als hij binnen is, ook binnen kan blijven, zich de benodigde rechten toeeigent, de nodige tools heeft geïnstalleerd en vooral niet voortijdig gedetecteerd of tegengehouden wordt.
- In de **uitvoerende fase** wordt het 'wapen' ingezet, bijvoorbeeld het wegsluizen en/of versleutelen van data. Daarnaast informeert de aanvaller het slachtoffer over de actie en wat er nodig is om tot een voor de aanvaller bevredigende oplossing te komen.
- In de **afsluitende fase** worden de financiën afgewikkeld, sleutels voor het decoderen van eventueel versleutelde data uitgewisseld en verzekert de aanvaller het slachtoffer dat de kwestie hiermee is afgedaan. Daarna kan de heropbouw van systemen beginnen.

Door zich te richten op de verschillende stappen in de fasen van de Cyber Kill Chain kunnen potentiële slachtoffers op tijd tegenmaatregelen nemen. De AIVD en MIVD hebben in juni 2021 een handreiking gepubliceerd om aan de hand van de Cyber Kill Chain maatregelen te nemen tegen cyberaanvallen door statelijke actoren, die ook nuttig zijn voor niet-statelijke actoren [15]

Figuur 43 **Lockeed Martin Cyber Kill Chain**
bron https://phoenixnap.com/blog/cyber-kill-chain



Hoe bescherm je je organisatie tegen aanvallen? [16]
Mandiant geeft in het rapport 'Proactive Preparation and Hardening to Protect Against Destructive Attacks' algemene tips om een destructieve aanval te voorkomen, inclusief aanbevelingen voor detectie (zie tabel voor een voorbeeld).

Daarbij onderscheidt Mandiant vier aandachtsgebieden:

1 Extern toegankelijke systemen en diensten
2 Kritieke systemen en diensten
3 Laterale verplaatsing (eenmaal binnen)
4 Accounts met verhoogde rechten (privileged accounts)

Aandachtsgebied	Beschrijving	Aanbeveling (hardening)	Detectie
Beveiliging van extern gerichte systemen en diensten	Afdekken van het risico dat aanvallers gebruikmaken van een extern gerichte aanvalsmogelijkheid of gebruikmaken van bestaande technologie voor ongeautoriseerde remote toegang.	**1** Identificeer, inventariseer en beveilig extern gerichte systemen en diensten. **2** Verplicht gebruik van multi-factor authenticatie voor extern gerichte systemen en diensten.	**1** Brute force aanvallen (gebruikers met een excessief aantal mislukte inlogpogingen, meerdere accounts met veel mislukte inlogpogingen vanaf hetzelfde herkomstadres). **2** Mislukte MFA inlogpogingen voor één account vanaf hetzelfde herkomstadres. **3** Mislukte MFA inlogpogingen voor verschillende accounts vanaf een herkomstadres. **4** Toegang tot accounts met veel rechten (privileged accounts) van buitenaf.

Wat doe je tegen ransomware? [17]
Om ransomware te voorkomen geeft het NCSC een aantal tips, die een rol spelen in de verschillende fasen van een aanval:

Tips		
1	Bescherm je organisatie tegen phishing	**voorbereidende fase**
2	Organiseer vulnerabilitymanagement, patchmanagement en netwerksegmentering	**voorbereidende en consolidatie fase**
3	Beperk de mogelijkheden van code execution	**uitvoerende fase**
4	Filter webbrowserverkeer	**voorbereidende fase**
5	Beperk het gebruik van USB-sticks	**uitvoerende fase**

6 CONCLUSIE

Covid-19-pandemie
Onderwijs en onderzoek werden ook in 2021 gedomineerd door de covid-19-pandemie. Dit heeft evenals in 2020 niet geleid tot een afwijkend cyberdreigingsbeeld. Wel zien we dat de intensiteit van incidenten binnen de sector weer toegenomen is. Het incident eind 2019 bij de Universiteit van Maastricht en deze toegenomen intensiteit hebben ook in 2021 tot nog meer politieke aandacht voor de staat van cybersecurity in onze sector geleid. Bovendien is hierdoor de discussie over publieke waarden verder aangejaagd. Instellingen zien ook steeds meer het belang van samenwerking en werken sectorbreed meer samen.

Door de geopolitieke spanningen in de wereld zal het aantal incidenten en de intensiteit daarvan alleen nog maar toenemen. We zien bijvoorbeeld met de Russische inval in Oekraïne wereldwijd een stijging van het aantal digitale aanvallen, die als doel hebben om infrastructuren uit te schakelen of te beschadigen.

Intensiteit van incidenten
Ransomware is ook in 2021 de meestvoorkomende dreiging. Er traden binnen de sector ontwrichtende incidenten op waardoor primaire processen ernstig in gevaar zijn gekomen. Een nieuwe trend daarbij is dat bij het niet betalen van losgeld gegevens openbaar worden gemaakt. In een enkel geval werd een absurd hoog bedrag aan losgeld gevraagd.

Ketenafhankelijkheid in relatie tot incidenten met log4j en Kaseya
De log4j-kwetsbaarheid en de aanval op Kaseya illustreren hoe de afhankelijkheid van softwareleveranciers, serviceproviders en andere derde partijen kan leiden tot problemen. Het is dan ook van groot belang dat we deze afhankelijkheden goed in kaart brengen en goede afspraken maken met leveranciers over wie waarvoor in de keten verantwoordelijk is. Daarnaast moeten we ervoor zorgen dat collega-instellingen snel op de hoogte zijn van problemen, zodat zij actie kunnen ondernemen. Cruciaal hiervoor zijn kennisdeling en informatie-uitwisseling, en dus samenwerking.

Publieke waarden
Onderwijs en onderzoek zijn in steeds grotere mate afhankelijk van de cloud-diensten van een klein aantal grote techbedrijven. In het debat over publieke waarden worden zorgen over dit onderwerp geuit, maar dat heeft nog niet geleid tot concrete stappen om de afhankelijkheid te verminderen.

Politieke aandacht
Het incident eind 2019 bij de Universiteit van Maastricht markeert een keerpunt voor de sector onderwijs en onderzoek. Het heeft bij de meeste instellingen tot extra beveiligingsmaatregelen geleid en er is ook extra bestuurlijke en politieke aandacht voor cybersecurity gekomen. Dit zal alleen maar meer worden, door de grote afhankelijkheid van IT in de primaire processen en de aandacht voor kennisveiligheid. Binnen de koepels[9] zijn afspraken gemaakt om naar een hoger volwassenheidsniveau op het gebied van informatiebeveiliging te groeien. Daarbij is de ambitie om sectorbreed gemiddeld niveau 3 te scoren op de normen uit het SURFaudit Toetsingskader Informatiebeveiliging [11].

Samenwerking
Samenwerking is een terugkerend thema in het Cyberdreigingsbeeld. Instellingen in onderwijs en onderzoek willen nog steeds graag samenwerken op het terrein van informatieveiligheid en privacy. Dat is ook noodzakelijk vanwege het tekort aan expertise op het gebied van informatieveiligheid. Investeringen in meer capaciteit blijven echter achter. Steeds meer instellingen

9 Voor de universiteiten de Universiteiten van Nederland (UNL), voor de hogescholen de Vereniging Hogescholen (VH) en voor het mbo de MBO Raad.

gebruiken SURFsoc, het security operations centre van SURF. Hierdoor worden dreigingen eerder gesignaleerd en met meer instellingen gedeeld.

Ook zien we dat bij grote incidenten zoals het log4j-incident[10] gemakkelijker informatie wordt gedeeld en dat SURF en SURFcert een steeds grotere coördinerende rol op zich nemen. Mede door het al langer bestaande U-CISO-overleg en het onlangs gestarte HBO-CISO-overleg is de drempel om ook vertrouwelijke informatie met elkaar te delen lager geworden. Landelijk is er al sinds 2020 samenwerking op het gebied van incident response in het Landelijk Dekkend Stelsel (LDS) [18]. Dit is 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. Deze uitwisseling vindt steeds meer plaats.

Tot slot is de samenwerking tussen het Rijk en (via SURF) de sector onderwijs en onderzoek op het gebied van inkoop van IT-middelen en IT-diensten gegroeid. Ook worden binnen deze samenwerking risico's voor de verwerking van persoonsgegevens in kaart gebracht, onder andere door gezamenlijk DPIA's uit te voeren. Dit alles draagt uiteindelijk bij aan een grotere weerbaarheid van de sector onderwijs en onderzoek.

10 zie hoofdstuk 3

BIJLAGE 1 **AFKORTINGEN EN BEGRIPPEN**

Begrip / afkorting	Betekenis	Bron[11]
Actor	Ook threat actor of kwaadwillende; iemand die misbruik maakt van kwetsbaarheden om een dreiging ten uitvoer te brengen.	WCN
DDoS	(Distributed) Denial-of-Service, DDoS; 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
DPIA	Data Protection Impact Assessment (Gegevensbeschermingseffectbeoordeling)	AP
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
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
(H)activist	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
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 inloggegevens of creditcardgegevens. Phishing gebeurt vaak via e-mails, maar aanvallers doen het ook via de telefoon, een sms of een app-bericht.	WCN
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

11 WCN: Woordenboek Cyberveilig Nederland (https://www.cybersecurityalliantie.nl/ecp_images/2021/05/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf)
WP: Wikipedia (https://www.wikipedia.org/) AP: Autoriteit persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/)

Begrip / afkorting	Betekenis	Bron[11]
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 centre; afdeling die informatiebeveiligingsvraagstukken afhandelt. Voorziet onder andere in monitoring van netwerken en systemen, in logging van incidenten en het oplossen van problemen.	WP
Vulnerability scan	Kwetsbaarhedenscan; en geautomatiseerde controle die zwakke plekken in een systeem opspoort.	WCN

11 WCN: Woordenboek Cyberveilig Nederland (https://www.cybersecurityalliantie.nl/ecp_images/2021/05/VCNL-Woordenboek-2eDruk-webversie-Final-2.pdf)
WP: Wikipedia (https://www.wikipedia.org/) AP: Autoriteit persoonsgegevens (https://www.autoriteitpersoonsgegevens.nl/)

BIJLAGE 2 **GERAADPLEEGDE BRONNEN**

Nr	Auteur(s)	Titel	Uitgever	Datum	URL	Opgehaald
[1]	National Cyber Security Centrum	**Digitale aanvallen oorlog Oekraïne**	NCSC	maart 2022	https://www.ncsc.nl/onderwerpen/oekraine	03/03/2022
[2]	Inspectie van het onderwwijs	**Binnen zonder kloppen – Digitale weerbaarheid in het hoger onderwijs**	Onderwijsin-spectie	september 2021	https://www.onderwijsinspectie.nl/onderwerpen/themaonderzoeken/documenten/themarapporten/2021/09/15/digitale-weerbaarheid-in-het-hoger-onderwijs	03/03/2021
[3]	AON	**Aanval Afgeslagen - Leerevaluatie cyberaanval HvA UvA**	Universiteit van Amster-dam	juli 2021	https://www.uva.nl/binaries/content/assets/uva/nl/nieuws-en-agenda/leerevaluatie-cyberaanval-hva-uva-definitief-7-juli-2021.pdf	01/02/2022
[4]	Verizon	**2021 Verizon Data Breach Investigations Report**	Verizon Business		https://www.verizon.com/business/resources/reports/dbir/	01/02/2022
[5]	National Cyber Security Centrum	**Cybersecuritybeeld Nederland 2021**	NCSC	juni 2021	https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021	28/06/2022
[6]	ENISA	**Threat Landscape for Supply Chain Attacks**	ENISA	juli 2021	https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks	01/02/2022
[7]	NU.nl	**Vermoedelijke daders megahack vragen 70 miljoen dollar losgeld**	NU.nl	april 2022	https://www.nu.nl/tech/6143561/vermoedelijke-daders-megahack-vragen-70-miljoen-dollar-losgeld.html	02/02/2022
[8]	CIS Center for Internet Security	**The SolarWinds Cyber-Attack: What You Need to Know**	CIS	maart 2021	https://www.cisecurity.org/solarwinds	12/04/2022
[9]	European Commission	**NIS Directive**	European Commission		https://digital-strategy.ec.europa.eu/en/policies/nis-directive	06/04/2020
[10]	Universiteit Maastricht	**Reactie Universiteit Maastricht op rapport FoX-IT**	Universiteit Maastricht	februari 2021	https://www.maastrichtuniversity.nl/file/49715/download?token=L-HUZ5YR	01/02/2020
[11]	SURF	**SURFaudit Toetsingskader 2021**	SURF	mei 2021	https://edu.nl/toetsingskader2021	01/01/2022
[12]	Lockheed Martin	**The Cyber Kill Chain® framework**	Lockheed Martin	2011	https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html	01/02/2022

BIJLAGE 2 **GERAADPLEEGDE BRONNEN** (VERVOLG)

Nr	Auteur(s)	Titel	Uitgever	Datum	URL	Opgehaald
[13]	MITRE	**The MITRE Att&ck Framework**	MITRE	2015	https://attack.mitre.org	01/02/2022
[14]	Paul Pols	**The Unified Kill Chain**	Unified killchain.com	2017	https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf	01/02/2022
[15]	AIVD, MIVD	**Cyberaanvallen door statelijke actoren: zeven momenten om een aanval te stoppen**	AIVD	2021	https://www.aivd.nl/documenten/publicaties/2021/06/28/cyberaanvallen-door-statelijke-actoren---zeven-momenten-om-een-aanval-te-stoppen	29/06/2021
[16]	Mandiant	**Proactive Preparation and Hardening to Protect Against Destructive Attacks**	Mandiant	januari 2022	https://www.mandiant.com/resources/protect-against-destructive-attacks	01/02/2022
[17]	NCSC	**Ransomware**	NCSC		https://www.ncsc.nl/onderwerpen/ransomware	01/02/2022
[18]	NCSC	**Landelijk Dekkend Stelsel**	NCSC		https://www.ncsc.nl/onderwerpen/landelijk-dekkend-stelsel	03/03/2022

COLOFON

Auteurs
Bart Bosma (SURF)
René Ritzen (SURF)

Redactie
Jan Michielsen (SURF)

Interviews
Marjolein van Trigt

Coördinatie
Yvonne Klaassen (SURF)

Ontwerp
Studio Koelewijn Brüggenwirth BNO, Den Haag

Fotografie
Foto omslag: Sicco van Grieken
Foto pagina 12: Dirk Kreijkamp
Foto pagina 16: Paul Dekkers (SURF)

Juni 2022

Dit rapport is mede tot stand gekomen dankzij bijdragen van:
Hans Schutte – Bestuursvoorzitter ROC Mondriaan
Marcel Kropmans - CIO ROC Mondriaan
Roeland Reijers – CISO Universiteit van Amsterdam en Hogeschool van Amsterdam
Wim Biemolt – voorzitter SURFcert
Remon Klein Tank – SURFcert

Samen aanjagen van vernieuwing