CYBERDREIGINGSBEELD 2014-2024

ONDERWIJS EN ONDERZOEK

SPECIALE EDITIE

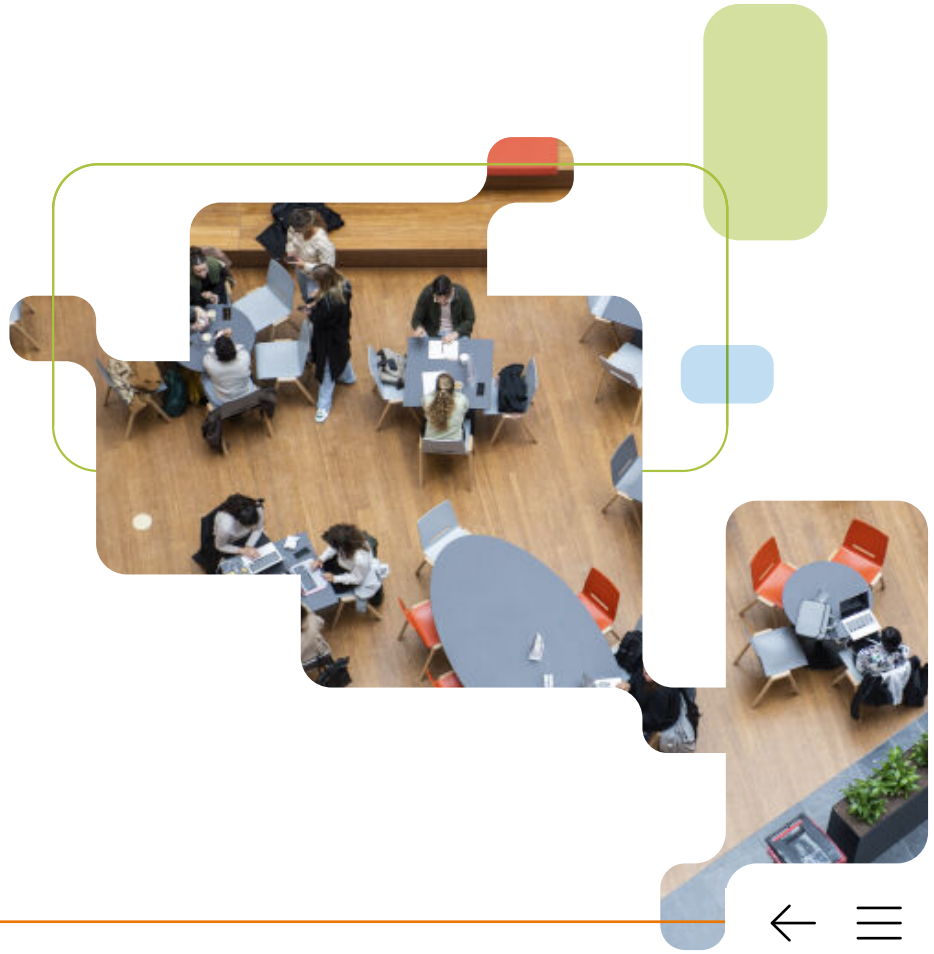
INHOUD

INLEIDING

In 2014 bracht SURF de eerste editie van het Cyberdreigingsbeeld uit. Inmiddels is cybersecurity niet meer weg te denken in onderwijs en onderzoek en speelt het onderwerp een grote rol op uiteenlopende podia. In deze speciale editie van het Cyberdreigingsbeeld nodigt SURF je uit om terug te blikken op het afgelopen decennium. Wat hebben we geleerd? Hoe hebben dreigingen zich ontwikkeld? Hoe reageerde de sector daarop? Uiteraard kijken we ook vooruit: wat kunnen we verwachten in de (nabije) toekomst?

Voor onderwijs- en onderzoeksinstellingen, in het bijzonder voor ict-professionals, beleidsmakers en bestuurders die verantwoordelijk zijn voor de digitale veiligheid binnen hun organisatie, is het Cyberdreigingsbeeld een waardevol rapport. Het biedt relevante kennis om de digitale weerbaarheid binnen instellingen te vergroten. Ook bevat het persoonlijke inzichten van specialisten binnen en buiten de sector die deze kennis in een bredere context plaatsen.

Met dit Cyberdreigingsbeeld hopen we bij te dragen aan een veiligere en weerbare digitale omgeving voor alle onderwijs- en onderzoeksinstellingen in de toekomst.



TERUGBLIK 10 JAAR CYBERDREIGINGSBEELD

In dit hoofdstuk vind je alle dreigingen die we de afgelopen jaren hebben geïdentificeerd. Je leest hoe de perceptie van die dreigingen in de loop der tijd is veranderd, welke actoren (daders), motieven en methodes de dreigingen vormden en wat de verwachte relevantie en impact is voor de toekomst. Bart Bosma, voormalig productmanager van SURFaudit, is sinds de eerste editie als auteur betrokken bij het Cyberdreigingsbeeld. Hij reflecteert op enkele van de meest impactvolle gebeurtenissen van de afgelopen tien jaar.

MAASTRICHT, COVID EN GEVOLGEN VOOR DE COÖPERATIE

Als ik terugdenk aan belangrijke gebeurtenissen in de afgelopen tien jaar, komt als eerste het ransomware-incident op de Universiteit Maastricht in december 2019 in me op. Dat was een belangrijk kantelpunt in de beleving van dreigingen binnen de onderwijs- en onderzoeksector. Het was niet alleen een markant moment vanwege de aanval op zich, maar ook omdat die periode het begin was van de Covid-pandemie. Naast alle maatregelen die instellingen moesten treffen om zich tegen een vergelijkbare ransomware-aanval te beschermen, moesten ze opeens zo snel mogelijk allerlei thuiswerkfaciliteiten inrichten die ook nog eens veilig en privacyvriendelijk moesten zijn. Deze periode had veel impact op de sector.

Niks te halen

Voor 2020 waren er natuurlijk wel cyberincidenten, maar die werden in het algemeen netjes afgehandeld door de securityspecialisten of de ict-afdelingen van de instellingen, eventueel met hulp van SURFcert. Zo waren er veel denial-of-service-aanvallen op instellingen, hoewel die in vakantieperiodes veel minder voorkwamen. Ransomware was in opkomst en phishing-incidenten werden geavanceerder en namen toe. Hele ernstige incidenten kwamen vooral voor in andere sectoren. Bij onderwijs- en onderzoeksinstellingen, zo dachten we, was tenslotte niks te halen, toch?

Gouden strategie: openheid geven

Het incident in Maastricht maakte voor het eerst pijnlijk duidelijk dat onderwijs- en onderzoekinstellingen wel degelijk het doelwit kunnen zijn van cybercriminelen en dat de impact gigantisch is. Hoewel de overheid adviseerde om nooit losgeld te betalen, koos de Universiteit Maastricht ervoor om dat wel te doen, zodat ze zo snel mogelijk weer up-and-running waren. Dat verhevigde de discussie bij de instellingen: was dat de juiste keuze en wat waren de gevolgen? Na het incident gaf de Universiteit Maastricht openheid over wat er was gebeurd en waarom ze bepaalde keuzes hadden gemaakt. In mijn ogen was dat een gouden strategie; die openheid heeft ertoe geleid dat de sector in relatief korte tijd grote stappen zette in het verhogen van de weerbaarheid tegen cyberdreigingen.

Cyberveiligheid op de agenda

Bestuurders van universiteiten, hogescholen, mbo-scholen en onderzoeksinstellingen werden met hun neus op de feiten gedrukt. Ineens was er het besef: er valt wel degelijk iets te halen bij onderwijs- en onderzoeksinstellingen, het incident in Maastricht kan ons ook overkomen. Sindsdien staat cyberveiligheid op de agenda bij besturen, is de samenwerking tussen instellingen, ook via SURF, geïntensiveerd en hebben Universiteiten van Nederland, de Vereniging Hogescholen en de MBO Raad doelen geformuleerd om als sector weerbaarder te worden.

Ook de politiek begon zich te roeren. Het mbo kreeg subsidie van het ministerie voor een meerjarenprogramma en in Den Haag hield men zich bezig met vragen als: hoe kan het dat dit is gebeurd, hoe weerbaar is het Nederlandse onderwijs eigenlijk, hoe kunnen ze dit in de toekomst voorkomen en wanneer zijn de instellingen nu eindelijk eens 100 procent veilig …

'Topjaar' 2021

Na Maastricht volgde er nog een aantal incidenten, sommige ook met grote impact. Het 'topjaar' was toch wel 2021. Denk bijvoorbeeld aan het grote datalek bij de HAN en de ransomware-aanval op ROC Mondriaan. Mondriaan koos ervoor om geen losgeld te betalen en alles opnieuw op te bouwen, waardoor ze het enige tijd zonder ict-systemen moesten doen.

In dat jaar werd ook een aantal belangrijke leveranciers getroffen. Cybercriminelen hackten Kaseya, een ict- en securitymanagementbedrijf dat softwarepakketten levert aan bedrijven die op hun beurt de computersystemen van hun klanten op afstand onderhouden en beheren. De hack zorgde ervoor dat de bestanden en systemen van die klanten werden versleuteld, waardoor honderden bedrijven werden getroffen, die de software van Kaseya gebruikten.

In hetzelfde jaar bleek ook Log4j, een veelgebruikte opensourcelibrary, een zogenaamd zero-day-beveiligingslek te bevatten. Log4j wordt in duizenden applicaties gebruikt om log-informatie te verzamelen en door te geven aan andere systeemservices. De enige oplossing was om publiek toegankelijke systemen zoals websites en webapplicaties offline te halen, totdat er nieuwe patches beschikbaar kwamen voor de getroffen systemen. De impact was gigantisch.

Al die incidenten hebben ertoe geleid dat crisisbeheersing een veel belangrijker thema is geworden. Eén van de resultaten daarvan was dat in 2022 maar liefst 72 instellingen en circa 2.000 medewerkers in de onderwijs- en onderzoek-sector deelnamen aan de tweejaarlijkse OZON-cybercrisisoefening van SURF.

Cloud- en ketenafhankelijkheid

De incidenten bij Kaseya en Log4j laten zien hoe afhankelijk we zijn geworden van anderen. Dit geldt voor bijna alle instellingen en organisaties, zowel binnen als buiten de onderwijs- en onderzoeksector. Allemaal maken we gebruik van clouddiensten, waarmee we ons in hoge mate afhankelijk hebben gemaakt van big tech. Daardoor gaat het niet meer alleen om onze eigen weerbaarheid, maar moeten we ons ook afvragen hoe weerbaar leveranciers zijn, hoe snel zij maat-regelen treffen en hoe ze daarover communiceren.

Een foutieve update bij Microsoft kan miljoenen Windows-systemen laten crashen, met als gevolg dat talloze overheidsdiensten niet meer werken en vliegtuigen niet meer kunnen vliegen. De impact is wereldwijd enorm.

Samen kom je verder

Enerzijds laten de afgelopen tien jaar zien dat veel hetzelfde blijft: denial-of-service-aanvallen, ransomware-hacks en phishing komen nog steeds voor, en criminelen maken misbruik van de zwakste schakel, vaak de mens. Anderzijds vinden er steeds verschuivingen plaats en worden aanvallen geraffineerder en moeilijker te detecteren. Ook komen er nieuwe dreigingen bij, zoals bijvoorbeeld de invloed van AI.

Het incident in Maastricht heeft laten zien dat samenwerking tussen instellingen en binnen de sector als geheel van groot belang is. Dat kost in eerste instantie misschien meer inspanning, vooral tijdens een incident, maar op de lange termijn is iedereen erbij gebaat. Om dat bewustzijn te benadrukken gebruikte René Ritzen, jarenlang mijn mede-auteur bij het Cyberdreigingsbeeld en een ervaren informatiebeveiligingsexpert, het Afrikaanse spreekwoord: alleen ga je sneller, samen kom je verder.

In het Cyberdreigingsbeeld hebben we de afgelopen tien jaar dreigingsinformatie verzameld, grote en kleine incidenten geanalyseerd en dit overzichtelijk samengevat. Ik hoop dat we daarmee aanzienlijk hebben bijgedragen aan de weerbaarheid van de sector.

OVERZICHT VAN DREIGINGEN

In zijn reflectie noemt Bart Bosma een aantal dreigingen die de media haalden. In het volgende overzicht lees je welke soorten dreigingen de afgelopen tien jaar nog meer voorkwamen, wat de meest voorkomende actoren, motieven en methodes waren, en wat de verwachting voor de toekomst is.

HACKTIVISME

Bij hacktivisme, samenvoeging van de woorden ‘hacken’ en ‘activisme’, worden computerkennis en het internet ingezet als daad van protest. Tien jaar geleden was het doel hiervan voornamelijk om het imago van een persoon of instelling bewust te beschadigen. Vandaag de dag voeren hacktivisten hun aanvallen ook uit om hun mening over bepaalde (politieke of maatschappelijke) ontwikkelingen, zoals bijvoorbeeld klimaat of mensenrechten, kracht bij te zetten. De meest gebruikte hacktivistische methodes zijn *defacement* (bekladding: het ongeoorloofd veranderen van een website), DDoS-aanvallen of hack- en lekaanvallen.

Meest voorkomende actoren, motieven, methodes

Actoren	Cybervandalen Activisten binnen de organisatie (bijvoorbeeld studenten/medewerkers) Activisten van buiten de organisatie
Motieven	Activistische boodschap verspreiden, aandacht vragen Protest Voor de kick Imago van persoon of instelling beschadigen Een beslissing of uitspraak afdwingen
Methodes	Defacement Overname socialmedia-account Hack-en-lek Phishing DDoS-aanval Misbruik kwetsbaarheden website of Content Management Systeem Misbruik kwetsbaarheden via hosting partij Misbruik zwakke authenticatiemethodes

Perceptie en impact

In de vroege edities van cyberdreigingsbeelden zien we een lage risicoperceptie ten aanzien van de bewuste imagobeschadiging van personen of instellingen. Ook bleef de aanvalsmethode voornamelijk beperkt tot defacement.

Invoering AVG

In 2018 schoot de risicoperceptie binnen het onderwijs ineens naar ‘hoog’. Het Cyberdreigingsbeeld van dat jaar verklaarde deze piek door de invoering van de AVG, waardoor het bewustzijn rondom imagoschade omhoog ging. De jaren na de invoering van de AVG zakte de risicoperceptie iets, naar middelhoog (‘midden’), en bleef daarna stabiel.

Hacktivisme (voorheen Bewust beschadigen imago)										
	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	L	L	L	L	H	M	M	M	M	M
onderzoek	L	L	L	L	M	M	M	M	M	M
bedrijfsvoering	L	L	L	L	M	M	M	M	M	M

L = laag / M = midden / H = hoog / ZH = zeer hoog

* In het Cyberdreigingsbeeld 2019-2020 is eenmalig een afwijkend scoringsmechanisme gebruikt. In die uitgave werd alleen de classificatie 'hoog' en 'laag' gebruikt. In de overzichten in dit document hebben we die twee classificaties overgenomen, en de overige getallen uit de oorspronkelijke bron als 'midden' geclassificeerd.

Actor cyberonderzoeker

Een belangrijke verandering die we sinds de allereerste editie van het Cyberdreigingsbeeld in 2014 waarnemen, is dat we 'cyberonderzoekers' (oftewel: ethisch hackers) destijds als actoren identificeerden. Tien jaar later zien we ethisch hackers niet meer als bedreiging voor ons imago, maar juist als nuttige partners in onze strijd tegen cybercriminaliteit. De meeste cyber-onderzoekers houden zich aan gedragscodes en bij veel instellingen is het nu mogelijk om beveiligingslekken op een verantwoorde manier te melden/bekend te maken via responsible disclosure.

Geopolitieke DDoS-aanvallen

Geopolitieke gebeurtenissen zorgen de laatste jaren voor een verhoging van de kans dat hacktivisme leidt tot verstoringen. Volgens het Nationaal Cyber Security Centrum (NCSC) waren veel Nederlandse organisaties in 2023 vooral het doelwit van symbolische DDoS-aanvallen[1], ook een aantal ziekenhuizen[2] en bleven de gevolgen daardoor beperkt. Er zijn ook hacktivistische aanvallen waargenomen op universiteiten in het VK[3] en Israël[4]. Dat zich nog geen zware incidenten hebben voorgedaan biedt echter geen garantie voor de toekomst en ook onze sector kan een interessant doelwit zijn.

Verwachting

In het Cyberdreigingsbeeld 2023 werd extra aandacht besteed aan hacktivisme, omdat meerdere instanties waarschuwden voor de mogelijke opleving van ervan door het veranderende geopolitieke en maatschappelijke klimaat. Instellingen die banden hebben met bepaalde bedrijven, landen of sectoren die een gevoelige positie innemen in het maatschappelijk debat, kunnen te maken krijgen met pogingen tot digitale verstoring door hacktivisten vanwege de invloed van geopolitieke gebeurtenissen.

De verwachting is dat die dreiging de komende jaren actueel blijft, maar dat de impact beperkt zal blijven. Dat laatste heeft te maken met het feit dat de groeperingen achter DDoS-aanvallen hun sterke retoriek voornamelijk gebruiken om aandacht te vragen voor politieke doelstellingen. Ze verschaffen zichzelf geen toegang tot vertrouwelijke informatie en zijn niet uit op financieel gewin. Dat betekent niet dat de effecten van DDoS-aanvallen minder voelbaar zijn. DDoS-aanvallen kunnen in uitzonderlijke gevallen dagen duren, waardoor websites of andere online diensten van getroffen organisaties gedurende die periode niet of verminderd bereikbaar zijn.

MANIPULATIE VAN DATA

Bij manipulatie van data gaat het om het bewust invoeren of veranderen van (valse) data om uitkomsten te manipuleren. Binnen onderwijs en onderzoek gaat het dan bijvoorbeeld om het wijzigen van studieresultaten door studenten, of wetenschapsfraude door de manipulatie van onderzoeksresultaten. Binnen bedrijfsvoering kan het gaan om het manipuleren van persoonsgegevens of financiële gegevens.

Meest voorkomende actoren, motieven, methodes

Actoren	Medewerkers (docenten, onderzoekers) Studenten Cybercriminelen
Motieven	Vervalsing studieresultaten om betere cijfers te registreren. Aanpassing onderzoeksdata om bijvoorbeeld de concurrentiepositie te verbeteren. Veranderen van gegevens in personeelsdossier, zoals beoordelingsformulieren.
Methodes	Wijziging van data door middel van toegekende rechten. Intimidatie en dwang om toegangsrechten te verkrijgen of te verhogen.

Perceptie en impact

Binnen de onderwijsprocessen gaat deze dreiging vooral over studenten die studieresultaten of tentamens willen veranderen.

Manipulatie van data	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	H	H	H	H	M	M	M	H	M	M
onderzoek	L	L	L	L	M	M	M	M	M	M
bedrijfsvoering	L	L	L	L	M	M	M	M	M	M

L = laag / M = midden / H = hoog / ZH = zeer hoog

Vanaf 2018 is de risicoperceptie binnen onderzoek en bedrijfsvoering iets hoger geworden. Voor onderwijsprocessen schommelt de perceptie gedurende de afgelopen jaren tussen hoog en midden.

Over de processen onderzoek en bedrijfsvoering schreven we in 2021 dat er een verandering in perceptie plaatsvond. Vanaf toen werden beroepscriminelen als een grotere dreigingsactor gezien dan medewerkers of studenten. De kans dat studenten of medewerkers data manipuleren voor persoonlijk voordeel wordt laag ingeschat doordat over het algemeen goede preventieve maatregelen zijn getroffen. Het is waarschijnlijker dat als data wordt gemanipuleerd, dat het door cybercriminelen wordt geïnitieerd.

Verwachting

Handmatige manipulatie van data is een informatiebeveiligingsincident dat nauw samenhangt met (wetenschaps)fraude en sociale veiligheid, bijvoorbeeld wanneer mensen worden geïntimideerd om data te manipuleren. Incidenten worden daardoor niet altijd bij de afdeling informatiebeveiliging geregistreerd, maar eerder bij integrale veiligheidsmanagers of de juridische afdeling. Aangezien we geen integraal overzicht hebben van gebeurtenissen binnen deze categorie, is de toekomstige impact lastig in te schatten.

IDENTITEITSFRAUDE

Bij identiteitsfraude doen aanvallers zich online of fysiek als iemand anders voor. Het doel is om vertrouwen te winnen en het doelwit er vervolgens toe te brengen om vertrouwelijke informatie vrij te geven of specifieke acties uit te voeren. Dit is een vorm van social engineering; misbruik van persoonlijke en digitale identiteiten. Identiteitsfraude richt zich vaak op financieel gewin, maar wordt ook ingezet om bepaalde data te verkrijgen of te manipuleren.

Studie- en onderzoeksresultaten

Identiteitsfraude binnen het onderwijs komt vaak tot stand door middel van phishing. Het komt ook voor dat studenten zich voordoen als iemand anders, bijvoorbeeld om hun studieresultaten te verhogen of gratis gebruik te kunnen maken van software. Het valt ook onder identiteitsfraude als iemand zich met diens daadwerkelijke identiteit voordoet als student of onderzoeker om op die manier data of kennis te verzamelen (vaak in opdracht van een statelijke actor).

Meest voorkomende actoren, motieven, methodes

Actoren	Opportunisten Medewerkers (docenten, onderzoekers) Studenten Cybercriminelen Statelijke actor
Motieven	Financieel gewin Verandering van data Toegang tot onderzoeksdata Toegang tot faciliteiten Toegang tot kennis en informatie
Methodes	Student laat iemand anders examen maken. Iemand doet zich voor als medewerker om toegang te krijgen tot gegevens. Activist/spion doet zich voor als onderzoeker. Iemand doet zich (tijdelijk) voor als student om toegang te krijgen tot leeromgeving/software. Verhoging van privileges/rechten om handelingen in systemen uit te voeren.

Digitalisering

Vooral in jaren van de Covid19-pandemie steeg de risicoperceptie van identiteitsfraude. Dit had te maken met de overgang naar thuiswerken en de digitalisering van lesmethodes en tentaminering. Door de groeiende aandacht voor kennisveiligheid[5] in de afgelopen jaren is er een stijging in de risicoperceptie binnen het onderzoek te zien.

Identiteitsfraude	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	H	H	H	H	M	M	M	H	M	M
onderzoek	M	M	M	M	M	M	M	M	H	H
bedrijfsvoering	L	L	L	L	M	M	M	H	M	M

L = laag / M = midden / H = hoog / ZH = zeer hoog

Perceptie en impact

Hoewel er schade kan ontstaan bij de inzet van digitale identiteiten voor grootschalig gebruik van cloudfaciliteiten, blijft de impact van identiteitsfraude voor instellingen over het algemeen beperkt. Op het moment dat medewerkers of studenten onder echte of valse identiteiten data verzamelen of beïnvloeden, of derden inzetten om betere studieresultaten te behalen, heeft dit pas direct impact op de instelling zelf wanneer de kwaliteit van diploma's op het spel staat. Toch worden deze actoren door de Nederlandse Inlichtingendiensten gezien als schadelijk voor de nationale veiligheid.

Financiële gevolgen

Op het moment dat identiteitsfraude wordt ingezet om licenties te overschrijven of ertoe leidt dat dienstverleners extra facturen gaan sturen, kan dit grote financiële gevolgen hebben voor instellingen. Dit geldt in mindere mate voor instellingen die te maken krijgen met valse inschrijvingen. Hoewel het enige financiële gevolgen heeft als (nep)studenten geen collegegeld betalen of een tijd lang gebruikmaken van softwarelicenties, is de impact bij deze vorm van identiteitsfraude minder groot.

Verwachting

Misbruik van digitale of persoonlijke identiteiten komt voor in de vorm van phishing: e-mails die van een bekende afzender (lijken te) komen om toegang te krijgen tot faciliteiten of om toegangsrechten te verhogen. Dit soort incidenten wordt vaak gemeld bij de integrale veiligheidsmanager of coördinator kennisveiligheid en komen daardoor niet altijd terecht in de registers van incidenten en risico's voor informatiebeveiliging. De verwachting is dat er altijd mensen zullen zijn die deze vorm van misbruik zullen toepassen, zowel via digitale middelen als via persoonlijke contacten. Het blijft dus belangrijk om alert te zijn en samen te werken om veiligheid te waarborgen.

VERKRIJGEN EN OPENBAAR MAKEN VAN DATA

Aanvallers die gegevens in handen proberen te krijgen om deze openbaar te publiceren of verkopen zijn vaak duidelijk geïdentificeerd. Zo lekken activisten vaak gegevens om aandacht te vragen voor een zaak die zij belangrijk vinden en zijn statelijke actoren vaak verantwoordelijk voor diefstal van onderzoeksdata of intellectueel eigendom om hun nationale belangen te dienen. Cybercriminelen worden gemotiveerd door financieel gewin en gaan strategisch te werk om aan gevoelige informatie te komen.

Onrechtmatig verkregen tentamenopgaven worden vaak verspreid of doorverkocht door studenten en medewerkers. Hun belangrijkste beweegredenen hiervoor zijn persoonlijke gewin of de druk om te presteren.

Meest voorkomende actoren, motieven en methodes

Actoren	Klokkenluiders en statelijke actoren Studenten Medewerkers (docenten, onderzoekers) Cybercriminelen
Motieven	Financieel gewin Persoonlijk gewin Nationale belangen Aandacht vestigen op een situatie Geen motief: vergissing of onbewuste handelingen
Methodes	Systeem binnendringen, data kopiëren, slachtoffer afpersen en de data verrijken met andere datasets om te verkopen. Rechtmatig verkregen informatie onrechtmatig openbaar publiceren. E-mails of bestanden met persoonsgegevens naar mensen versturen die de gegevens niet zouden moeten krijgen.

Perceptie en impact

Tot en met 2018 zagen we het verkrijgen en openbaar maken van data voornamelijk als een risico voor onderzoeksgegevens. De focus lag hierbij op intellectueel eigendom, onderzoeksopzetten, data van onderzoekspartners en informatie over gevoelige onderzoeksactiviteiten die openbaar gemaakt konden worden.

Sinds 2019 is de risicoperceptie voor de drie primaire processen binnen academische instellingen – onderwijs, onderzoek en maatschappelijke dienstverlening – significant verschoven naar 'hoog'/'zeer hoog'. Dit wijst op een verbreding van de scope van potentiële cyberdreigingen die nu een breed scala aan gevoelige informatie omvat, variërend van persoonsgegevens tot intellectueel eigendom. Deze verandering maakt duidelijk dat instellingen steeds meer beseffen hoe noodzakelijk het is om robuuste cybersecuritymaatregelen en -beleid te implementeren. Niet alleen ter bescherming van onderzoeksgegevens, maar voor alle vormen van gevoelige informatie die instellingen beheren.

Verkrijging en openbaarmaking van informatie

	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	M	M	M	M	M	H	H	ZH	ZH	H
onderzoek	H	H	H	H	H	H	H	ZH	ZH	H
bedrijfsvoering	M	M	M	H	M	H	H	ZH	ZH	H

L = laag / M = midden / H = hoog / ZH = zeer hoog

Verwachting

De methoden waarmee actoren onrechtmatig data verkrijgen en openbaar maken, zijn vaak net zo divers als de potentiële impact. De technieken variëren van geavanceerde cyberaanvallen, zoals het benutten van kwetsbaarheden in slecht beveiligde systemen, tot meer directe methoden die minder technische kennis vereisen.

De politie schrijft in het Cybercrimebeeld Nederland[6] dat cybercriminelen het versleutelen van data als afpersingstactiek niet langer toepassen. In plaats daarvan kopiëren ze de data en gaan ze meteen over tot afpersing. Vervolgens verrijken ze de data, bijvoorbeeld door datasets met elkaar te combineren om de waarde, nauwkeurigheid of bruikbaarheid te vergroten, en verkopen deze door aan andere criminelen. Dit soort methoden kunnen een grote impact hebben voor onderwijsinstellingen. Tentamenfraude, het onrechtmatig verkrijgen en doorverkopen van toetsingsmaterialen, kan de academische integriteit bijvoorbeeld ernstig ondermijnen. Dat soort acties kunnen leiden tot imagoschade voor de instelling, met als extra risico de manipulatie van cijfers en de aansprakelijkheidsclaims die volgen op het lekken van persoonsgegevens. Wanneer gevoelige onderzoeksdata worden gelekt, kunnen subsidies worden ingetrokken en in de nabije toekomst kunnen boetes worden gegeven voor datalekken. Dat zorgt voor een groter risico op financieel verlies.

‘Elke dreiging wordt een keer werkelijkheid. Als het nog niet is gebeurd, dan komt het nog.’

Eind 2019 werd de Universiteit Maastricht slachtoffer van een grote ransomware-aanval die de hele sector wakker schudde. Michiel Borgers, nu Directeur IT bij het ministerie van Defensie, was destijds CIO bij Universiteit Maastricht en herinnert zich de aanval nog goed. ‘Er waren al uiteenlopende voorbereidende stappen gezet door de universiteit. Maar we hebben onszelf nooit afgevraagd hoeveel tijd we nog hadden.’

Een jaar voordat de universiteit werd aangevallen stonden maatregelen en discussies rondom cybersecurity al op de agenda. Dat Borgers alsnog werd overvallen door het incident ziet hij als een waardevolle les. ‘Opeens is de tijd op,’ vertelt hij, ‘en niemand is zich daar voldoende van bewust.’

Blinde vlek

Die naïviteit ziet hij tot op zekere hoogte nog steeds binnen de sector. ‘In onze dagelijkse werkzaamheden is cyberveiligheid nog steeds geen topprioriteit. Vraag jezelf als bestuurder maar eens af: hoe vaak staat dit onderwerp hoog op de agenda? Hoe vaak word ik er echt over geïnformeerd?’ Volgens Borgers ligt dit aan het feit dat we ons vooral focussen op dreigingen die we al kennen. ‘We hebben een blinde vlek voor de dreigingen waar we nog geen weet van hebben. Daarom is het belangrijk om altijd 360 graden om je heen te blijven kijken.’

Gevaar voor iedereen

Die alertheid voor het onbekende is essentieel, vindt Borgers. ‘Andere landen benaderen dingen op een compleet andere manier,’ licht hij toe. ‘Cyberaanvallen volgen geen hiërarchie, kijken niet naar hoe je als instelling of land bent georganiseerd. In een land als China is er bijvoorbeeld geen scheiding tussen publiek en privaat, dus voor aanvallen vanuit die hoek maakt het niet uit of het om een bank, een provincie of een universiteit gaat. Zeker niet als het doel is om informatie te stelen of systemen te ontwrichten. We moeten ons ervan bewust zijn dat we niet alleen vanuit ons eigen wereldbeeld naar cyberdreigingen kunnen kijken.’

Ratrace

Van bestuurders hoort Borgers regelmatig dat er te weinig capaciteit is om cybersecurity topprioriteit te geven, maar dat vindt hij een 'slap excuus'. 'Tijdens een oorlog zeggen we ook niet dat we Nederland onvoldoende kunnen verdedigen door gebrek aan mensen. Dan moet je het op een andere manier oplossen. De vraag is dus eerder: heb je echt te weinig cybersecurity-experts of maak je er als manager te weinig tijd voor vrij en zie je alternatieve oplossingen, zoals de inzet van technologie, over het hoofd?'

Borgers benadrukt ook dat cyberdreigingen niet kleiner zullen worden. 'Het is een ratrace en die gaat hard. Elke dreiging wordt een keer werkelijkheid. Als het nog niet is gebeurd, dan komt het nog. De enige manier om je daarop goed voor te bereiden is een zerotolerancebeleid.'

Insider threats

Borgers is ervan overtuigd dat er meer intellectueel eigendom wordt gestolen van instellingen dan we waarnemen. Dat komt volgens hem doordat de menselijke kant van cyberdreiging nog steeds wordt onderschat. Als voorbeeld noemt hij Stuxnet, het schadelijke computerprogramma dat werd ontwikkeld om het nucleaire programma van Iran te saboteren.

'Zoiets kan ook gebeuren binnen de onderzoekswereld,' licht hij toe. 'De concurrentie onder wetenschappers is enorm groot. Dit kan aanleiding geven tot het saboteren van onderzoeken en onderzoeksdata van anderen, om vertraging bij de concurrentie te veroorzaken.' Borgers vraagt zich af of onderwijsinstellingen er genoeg bij stilstaan dat dit soort 'insider threats' misschien al lang binnen hun eigen organisatie rondlopen.

Showcase voor samenwerking

Ondanks de urgente boodschap in Borgers' verhaal is hij wel positief over de ontwikkelingen binnen de onderwijswereld na de aanval op Universiteit Maastricht. Het opzetten van een sectorbreed Security Operations Centre (SOC) bij SURF noemt hij een 'showcase van samenwerking' tussen de aangesloten instellingen. Zijn ultieme droom is dat verschillende partijen elkaar versterken zonder te kijken naar het eigen belang. Een voorbeeld hiervan is een recente cybersecurity-oefening waaraan niet alleen overheids-instanties, maar ook hogescholen en banken meededen. 'Er moet nog veel meer publiek-private samenwerking komen,' besluit Borgers. 'Hierin zullen we elkaar op inhoud moeten vinden. Samen staan we sterk!'

'Vraag jezelf als bestuurder maar eens af: hoe vaak staat cyberveiligheid hoog op de agenda?'

ICT-VERSTORING

Ict-verstoringen hebben als doel om de ict-voorzieningen van organisaties plat te leggen via methoden als DDoS-aanvallen en malware (ransomware en virussen). De kern van ict-verstoringen is het uitschakelen van essentiële systemen en operationele netwerken. De aanvallen kunnen zich richten op specifieke portalen en omgevingen, maar ook op gehele netwerken. Ook infrastructuur die cruciaal is voor onderzoekers, zoals rekenservers, valt hieronder.

Meest voorkomende actoren, motieven en methodes
Ict-verstoringen worden veroorzaakt door verschillende actoren met uiteenlopende motieven. Het kunnen studenten zijn die ict-systemen proberen te manipuleren voor hogere cijfers of toegang tot examenmateriaal. Ook acties van cyberonderzoekers die betrokken zijn bij het ontdekken en melden van kwetsbaarheden kunnen tot onbedoelde verstoringen leiden. Activisten kunnen ict-verstoringen veroorzaken als vorm van protest en insiders met kwade bedoelingen kunnen de toegang tot systemen misbruiken om schade te veroorzaken.

Actoren	Cybercriminelen Activisten Statelijke actoren
Motieven	Processen verstoren voor financieel gewin Processen verstoren om aandacht te krijgen voor een boodschap Processen verstoren om de samenleving te destabiliseren
Methodes	Malware DDoS-aanvallen

Beroepscriminelen en statelijke actoren vormen een significant risico binnen dit domein; zij gebruiken geavanceerde technieken om systemen te verstoren, vaak gedreven door motieven als financieel gewin of geopolitieke conflicten. Deze actoren zien de open en verbonden systemen van onderwijs- en onderzoeksinstellingen als aantrekkelijke doelwitten vanwege de waardevolle data en de essentiële dienstverlening.

Perceptie en impact
Tot en met 2018 bleef de risicoperceptie van ict-verstoringen over het algemeen gelijk, ongeacht de context. Vanaf 2019 is echter een verandering te zien: de algemene risicoperceptie ten aanzien van alle primaire processen is toegenomen, en deze trend zette zich voort in 2021.

Verstoring ict	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	M	M	M	M	H	H	H	ZH	ZH	H
onderzoek	M	M	M	M	M	M	M	H	H	H
bedrijfsvoering	M	M	M	M	M	H	H	ZH	ZH	H

L = laag / M = midden / H = hoog / ZH = zeer hoog

Wat opvalt is dat er in 2024, na twee opeenvolgende jaren waarin deze risicocategorie voor zowel onderwijs als bedrijfsvoering als 'zeer hoog' werd ingeschat, weer een daling te zien is. Binnen het onderzoeksdomein is de risicoperceptie sinds 2021 echter 'hoog' tot 'zeer hoog' gebleven. In 2019 waren er een aantal high-profile incidenten, zoals de hack op een leerlingvolgsysteem bij Aventus en de ransomware-aanval op de Universiteit Maastricht. In 2020 konden tentamens bij de UvA en RUG niet doorgaan vanwege een aantal verstoringen. Ook waren er dat jaar een aantal datalekken in het nieuws, zoals het incident rondom de Citrix-files. In 2021 steeg de perceptie naar zeer hoog door een ernstige verstoring bij ROC Mondriaan en een datalek bij HAN. NWO kampte dat jaar met een hack en in de kerstvakantie van 2021 had het hele land last van de Log4j-kwetsbaarheid.

Dit soort grote verstoringen die de media halen zorgen ervoor dat cybersecurity het gesprek van de dag is, waardoor het bewustzijn stijgt. Dit gebeurde bijvoorbeeld ook na een succesvol afgewende aanval op UvA/HvA. De open informatiedeling daarover droeg bij aan een hoger risicobewustzijn bij andere instellingen. In relatief rustige jaren daalt de perceptie vervolgens weer.

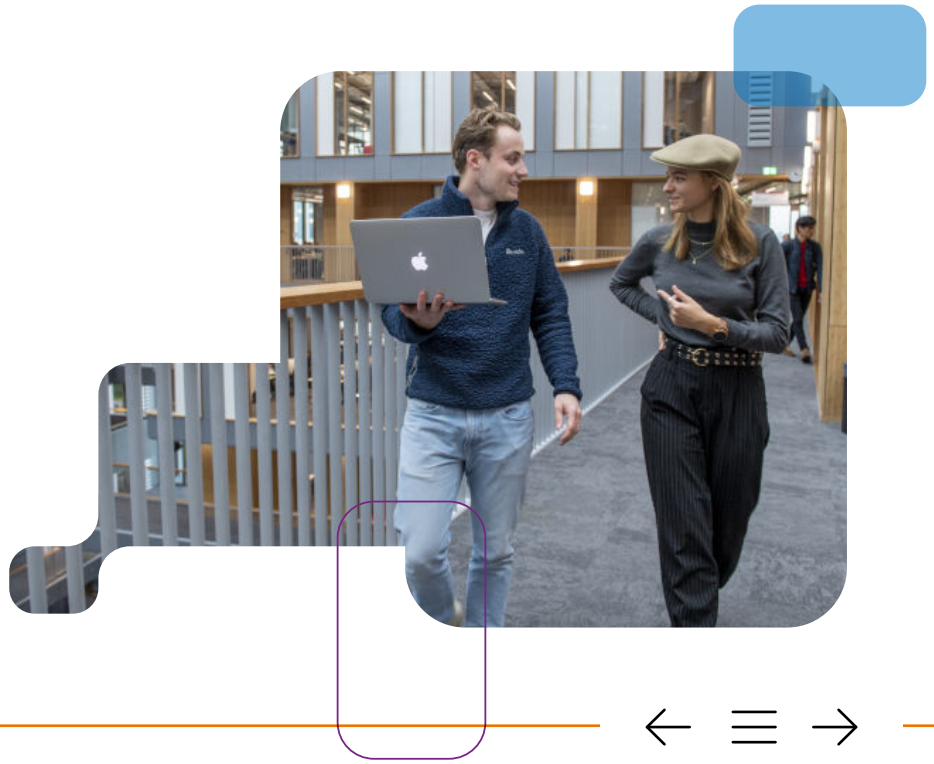
Risico's binnen het onderwijs
De impact van bovengenoemde aanvallen is groot. Ict-voorzieningen worden onbereikbaar en leggen essentiële diensten stil. Onderwijsmiddelen raken geïnfecteerd met malware, waardoor ze onbruikbaar worden voor docenten en studenten. Langdurige aanvallen hebben niet alleen operationele, maar ook financiële schade tot gevolg. Zonder adequate back-up en centrale opslag van gegevens, kunnen cruciale examengegevens van instellingen verloren gaan. Dit vormt een directe bedreiging voor de academische integriteit en continuïteit.

Verwachting
Onderwijs- en onderzoeksinstellingen die ict-verstoringen willen aanpakken, moeten zich weren tegen DDoS-aanvallen. Deze veelgebruikte methode is betrekkelijk makkelijk te organiseren met de hulp van botnet-netwerken. Daarnaast zetten actoren malware in, zoals virussen, spyware en ransomware, om systemen te infiltreren en beschadigen.

Deze dreigingen zijn bijzonder uitdagend voor de onderwijssector, omdat onderwijsinstellingen van nature open en toegankelijk zijn. Veel leeromgevingen zijn bijvoorbeeld direct via het internet toegankelijk zonder de bescherming van een VPN. Sinds 2014 is het aantal DDoS-aanvallen opmerkelijk toegenomen, maar tegelijkertijd zijn instellingen beter geworden in het afweren ervan. Dit komt deels door de bescherming die instellingen hebben als ze zijn aangesloten op het SURF-netwerk.

Digitale sabotage
In het AIVD-jaarverslag 2023[7] noemt de inlichtingendienst digitale sabotage de potentieel meest gevaarlijke cyberdreiging, vanwege het grote risico op economische schade en maatschappelijke ontwrichting. In 2023 nam de AIVD verschillende buitenlandse cyberoperaties waar die dit soort sabotage hoogstwaarschijnlijk als einddoel hadden. De operaties werden uitgevoerd door of in opdracht van statelijke actoren en waren specifiek gericht op de vitale infrastructuur in andere landen. Hun vermeende doel was het inbouwen van een mogelijkheid om op een later moment, bijvoorbeeld bij een conflict, de communicatie te verstoren of het energienetwerk plat te leggen.

De AIVD schrijft verder dat de vraag om actuele informatie en praktisch advies de laatste jaren is gestegen. Dat heeft alles te maken met het groeiende aantal cyber- en spionage-incidenten waarmee Nederlandse hightechbedrijven, kennisinstellingen en de Rijksoverheid te maken krijgen. In 2023 investeerde de AIVD daarom in kennisveiligheid, economische veiligheid en de bescherming van vitale belangen.



SPIONAGE

Spionage is een geavanceerde en aanhoudende dreiging voor de onderwijs- en onderzoeksector en richt zich met name op het onrechtmatig vergaren van hoogwaardige intellectuele en gevoelige informatie. Detectie van spionage is moeilijk, omdat de dreiging op subtiele wijze en gedurende langere periodes plaatsvindt. Cybercriminelen gebruiken spionagetactieken om op onrechtmatige wijze informatie te verkrijgen die ze doorverkopen aan derden. Onderzoeksinstellingen zijn een primair doelwit vanwege hun waardevolle kennis en data. Die kunnen van groot belang zijn voor concurrerende instellingen of buitenlandse wereldmachten.

Meest voorkomende actoren, motieven en methodes

Actoren	Cybercriminelen Onderzoekers Statelijke actoren
Motieven	Informatie/kennis vergaren Financieel gewin Concurrentiepositie
Methodes	Voordoen als student, onderzoeker of medewerker. Medewerkers, studenten, onderzoekers onder druk zetten om informatie te verzamelen.

Perceptie en impact

Door de jaren heen komt duidelijk naar voren dat spionage bijna alleen een bedreiging is voor de onderzoeksector. In elk Cyberdreigingsbeeld van de afgelopen tien jaar is de risicoperceptie van spionage binnen het onderwijs of de bedrijfsvoering laag.

Spionage	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	L	L	L	L	L	L	L	L	L	L
onderzoek	H	H	H	H	M	M	M	M	M	H
bedrijfsvoering	L	L	L	L	L	L	L	L	L	L

L = laag / M = midden / H = hoog / ZH = zeer hoog

Binnen het onderzoeksdomein is het beeld heel anders. Tussen 2014 en 2017 is de risicoperceptie hoog, terwijl dit in 2018, 2019, 2021 en 2022 naar 'midden' zakt (voor 2020 was er geen eenduidig beeld). In 2023 staat het perceptieniveau weer op hoog. Deze schommeling is lastig te verklaren. Verschillende dreigingsbeelden nemen aan dat de moeilijke detecteerbaarheid van spionage ervoor zorgt dat instellingen niet goed kunnen inschatten hoe vaak het in hun sector voorkomt. In het Cyberdreigingsbeeld van 2018 werd spionage ook genoemd als een van de dreigingen die instellingen het minst onder controle hebben. Inzichten van inlichtingendiensten vormen daarom de primaire bron van informatie over hoe spionage zich ontwikkelt.

Verwachting

Sinds het eerste dreigingsbeeld in 2014 wordt spionage als een serieuze dreiging beschouwd die vooral een risico vormt voor het onderzoeksdomein. Dit ligt aan de gevoelige informatie over technologische ontwikkelingen binnen dat domein en de waarde van die informatie voor verschillende actoren, in het bijzonder statelijke actoren.

Vanwege de transitie naar het bredere thema van kennisveiligheid, staat spionage sinds 2023 nog meer op de kaart. Hierdoor krijgt het onderwerp meer aandacht en wordt de dreiging holistisch benaderd om kennis te beschermen tegen kwaadwillende invloeden. Spionage wordt vooral uitgevoerd door statelijke actoren om nieuwe kennis over technologische ontwikkelingen te gebruiken voor verschillende doeleinden. Dit zal de komende jaren actueel blijven.

OVERNAME EN MISBRUIK ICT

Een ander risico is overname en misbruik van toegankelijke ict-systemen in onderwijs- en onderzoeksinstellingen, bijvoorbeeld voor cryptomining of als onderdeel van DDoS-aanvallen.

Meest voorkomende actoren, motieven en methodes

Actoren	Cybercriminelen
Motieven	Cryptomining voor financieel gewin Eerste stap om later andere aanvallen uit te voeren DDoS faciliteren
Methodes	Gebruikmaken van instellingsacounts van cloudvoorzieningen met via phishing verkregen data. Via phishing verkregen toegang tot netwerken.

Perceptie en impact

De risicoperceptie van ict-overname en -misbruik geeft een wisselend beeld over de afgelopen tien jaar. Van 2014 tot 2018 is het beeld stabiel: de risico-perceptie voor de onderzoeksector is middelhoog en voor het onderwijs laag, met uitzondering van 2018. In 2021 en 2022, jaren die in één editie van het Cyberdreigingsbeeld zijn samengevoegd, is het niveau hoog en zeer hoog. Op basis van de context lijkt hier geen directe aanleiding voor te zijn. In 2023 werd het risico weer middelhoog ingeschat op alle onderdelen.

Misbruik en overname van ICT

	2014	2015	2016	2017	2018	2019	2020*	2021	2022	2023
onderwijs	L	L	L	L	M	M	M	H	H	M
onderzoek	M	M	M	M	M	M	M	H	H	M
bedrijfsvoering	M	M	M	M	M	H	H	ZH	ZH	M

L = laag / M = midden / H = hoog / ZH = zeer hoog

Ict-overname en -misbruik lijkt door de jaren heen geen serieuze dreiging te zijn. In 2016 werd de kans op deze dreiging als ‘klein’ ingeschat en in 2018 gaven respondenten aan dat de dreiging zich niet had gemanifesteerd. De conclusie was dat de risico’s goed afgedekt waren en dat we deze dreiging, samen met verstoring en manipulatie, het beste onder controle hebben.

Verwachting

Ict-overname en -misbruik is een dreiging die instellingen binnen hun eigen ict-infrastructuur vaak goed onder controle hebben. Toch zal het een actueel thema blijven waar we aandacht aan moeten besteden, omdat misbruik van ict-leveranciersketens en cloudoplossingen afhankelijk is van de samenwerking met die leveranciers en van de kwaliteit van hun beveiligingsmaatregelen.

‘Tien jaar is vrij kort om een cultuuromslag voor elkaar te krijgen’

Cybersecurity is een grensoverschrijdend thema, en dan hebben we het niet alleen over landsgrenzen. Om goed voorbereid te zijn op cyberdreigingen moeten ministeries en organisaties ook over hun eigen grenzen heen denken. Dat begrijpt Mirjam Bult-Spiering, staatsraad in de Afdeling advisering van de Raad van State en lid van de Raad van Toezicht bij de Universiteit Utrecht, als geen ander. Door haar jarenlange ervaring, zowel binnen als buiten de sector, weet ze: ‘We zijn nog lang niet klaar.’

De afgelopen tien jaar is de focus in het cybersecuritylandschap verschoven van geheimhouding en controle naar transparantie en samenwerking. Doordat de onderwijs- en onderzoekwereld traditioneel eerder terughoudend is in het delen van kwetsbaarheden, vreesde Bult-Spiering in het begin dat instellingen zouden terugschrikken voor het delen van incidenten. Terugkijkend is ze echter positief verrast over de ontwikkeling die de sector hierin heeft gemaakt. ‘Tien jaar is vrij kort voor de cultuuromslag die nodig was om dit voor elkaar te krijgen.’

Strijd tegen waarden

De huidige cyberdreigingen hebben een ander karakter dan tien jaar geleden. ‘Digitale weerbaarheid maakt nu deel uit van de geopolitieke discussie,’ legt Bult-Spiering uit. ‘Daardoor is het een vorm van oorlogvoering geworden, een strijd tegen andere maatschappelijke en democratische waarden. Dat maakt de noodzaak om weerstand te bieden niet alleen groter, maar ook moeilijker, omdat we ons in die onbekende andere waarden moeten kunnen verplaatsen.’

Volgens Bult-Spiering is de verspreiding van nepinformatie een directe bedreiging voor onze democratie, maar ook vragen over soevereiniteit zijn urgenter geworden, bijvoorbeeld met betrekking tot data-opslag. ‘Weerbaarheid is verweven met andere gebieden zoals kennisveiligheid, maar dreigingen ontwikkelen zich sneller dan we menselijk gedrag en processen kunnen veranderen. Daar moeten we oplossingen voor vinden.’

Digitale ontwrichting

Inmiddels is er uitgebreide wet- en regelgeving rondom cyberincidenten, maar volgens Bult-Spiering is er nog te weinig aandacht voor digitale ontwrichting. In 2019 al riep de Wetenschappelijke Raad voor het Regeringsbeleid (WRR) Nederland en Europa op om zich beter voor te bereiden op digitale rampscenario's[8]. 'Er is veel aandacht voor preventie en detectie, maar weinig voor de herstelperiode na een cyberincident,' zegt Bult-Spiering. 'In het geval van cybercrises is het nog complexer, omdat dit beleidsterrein-overstijgende impact heeft. Daarom is het belangrijk om verschillende scenario's vanuit een crisismodus te doordenken en dit vast te leggen in nood- en crisisrecht. Hierin moeten vangnetvoorzieningen voor onvoorziene omstandigheden worden opgenomen, zodat je de wetgeving niet pas gaat maken of aanpassen op het moment dat een crisis al in volle gang is.'

Publieke waarden

De WRR is hierin een waardevolle bron van informatie, vindt Bult-Spiering. 'Ze hebben een overkoepelende visie en systeembenadering, maar bieden tegelijk ook handelingsperspectieven.' Ook voor adviezen met betrekking tot technologische ontwikkelingen kijkt Bult-Spiering naar de WRR. 'In 2021 publiceerde de WRR een rapport over AI[9] met de hoofdboodschap: "AI is niet zomaar een technologie, maar een systeemtechnologie die de samenleving fundamenteel zal veranderen." Hierdoor is meer dan ooit de behoefte aanwezig om zeker te stellen dat onze publieke waarden worden geborgd.'

Cruciale responsfase

Daarnaast is geen enkel verhaal over cybersecurity compleet zonder te spreken over samenwerken. 'Samenwerking tussen instellingen is op alle niveaus essentieel,' zegt Bult-Spiering. Ze ziet niet alleen behoefte aan samenwerking binnen gespecialiseerde security-afdelingen, maar ook tussen wetenschappers, Colleges van Bestuur en Raden van Toezicht. OZON[10], de tweejaarlijkse, sectorbrede cybercrisisoefening voor onderwijs en onderzoek, is voor haar het ultieme voorbeeld van hoe je die samenwerking kunt testen en verbeteren. 'Aan een OZON-oefening doen alle niveaus binnen de organisatie mee. Dat is heel waardevol, omdat je dan die cruciale responsfase echt goed in kaart kunt brengen.'

Sectorale ambities

Concreet raadt Bult-Spiering bestuurders in onze sector aan om te blijven werken aan cyberveiligheid en de aandacht niet te laten verslappen. 'Monitor niet alleen de inspanningen die je doet om cyberdreigingen te voorkomen, maar ook de effecten ervan. Leg vast welke norm je stelt en rapporteer daarover. Risicomanagement werd lange tijd alleen geassocieerd met commerciële bedrijven, maar is vandaag de dag minstens zo belangrijk binnen onze sector. Het zou een vast onderdeel moeten zijn van onze sectorale ambities. Want we zijn nog lang niet klaar.'

'Samenwerking tussen instellingen op het gebied van cybersecurity is op alle niveaus essentieel'

FACTOREN DIE WEERBAARHEID VERMINDEREN

In vorige edities van het Cyberdreigingsbeeld zijn drie factoren geïdentificeerd die de weerbaarheid verminderen, en die ook de komende jaren actueel zullen blijven:

Capaciteitstekort
Het tekort aan specialisten in informatiebeveiligingsteams heeft impact op de werkdruk en de mogelijkheden om preventieve maatregelen in te voeren. Daarnaast werkt capaciteitstekort door op het collectief: het is soms lastig voor individuele instellingen om tijd te steken in werkgroepen van het Security Expertise Centrum, de beveiligingscommunity SURF Community voor Informatiebeveiliging en PRivacy (SCIPR) of Integraal Veilig. Toch is investeren in deze capaciteit voor de gezamenlijke weerbaarheid van de onderwijs- en onderzoeksector essentieel. De resultaten die uit die werkgroepen komen zijn kennisproducten of diensten in SURF-verband waar de hele sector van profiteert.

Ketenafhankelijkheid
De tweede factor is de afhankelijkheid van leveranciers en clouddiensten die bij verstoring of misbruik tot grote schade leiden. Deze ketenafhankelijkheid is ook aanwezig in het ecosysteem waarbinnen onderwijs- en onderzoeksinstellingen samenwerken. Een incident bij de ene instelling kan negatieve gevolgen hebben voor de andere instellingen in een samenwerkingsverband. Deze afhankelijkheid is complexer dan de klant-leverancierrelatie en is niet altijd in SLA's of contracten vast te leggen.

Menselijk gedrag
De derde categorie is de menselijke factor. Veel incidenten ontstaan door onbedoelde fouten van medewerkers, bijvoorbeeld als die in phishingtrucs trappen. Het is belangrijk dat iedereen die met digitale voorzieningen werkt weet hoe je die zo veilig mogelijk gebruikt en wat je moet doen als je toch een keer een vergissing maakt. De mens is de sterkste schakel in de cyberweerbaarheid.

SAMENVATTING

Alle dreigingen die in de eerste editie van het Cyberdreigingsbeeld in 2014 werden genoemd, zijn nog steeds relevant. Soms stijgt het bewustzijn rondom een specifieke dreiging, doordat een getroffen instelling ermee in het nieuws komt of open communiceert over een incident, zodat andere instellingen daarvan kunnen leren. Het bewustzijn voor spionage door statelijke actoren en de opkomst van hacktivisme stijgt, doordat de overheid steeds vaker voor deze dreigingen waarschuwt. Onder invloed van geopolitieke ontwikkelingen verschuift de aandacht de laatste jaren meer naar dreigingen zoals spionage en kennisveiligheid. Daarnaast is er meer bewustzijn gekomen voor het verhogen van de weerbaarheid, doordat instellingen investeren in bewustwordingscampagnes en gedragsverandering, het opbouwen van securitycapaciteit en ketenbeheer.

Wanneer binnen de onderwijs- en onderzoeksector een groot incident plaatsvindt, bieden andere instellingen direct hulp aan en ontwikkelt men samen oplossingen en nieuwe preventieve maatregelen. Instellingen zijn afhankelijk van elkaar en werken veel samen. Dat creëert aan de ene kant een sterk ecosysteem, maar aan de andere kant vormt dit ook een wederzijds risico. Dit besef komt duidelijk naar voren in de vele community's van experts die zich in de afgelopen tien jaar hebben gevormd en waarin kennisdeling en informatie-uitwisseling een belangrijke rol spelen. Dit is tegelijk de kracht van de SURF-coöperatie. Het is belangrijk dat we die het komende decennium blijven stimuleren en er capaciteit voor vrij blijven maken.

NIEUWE TECHNOLOGIEËN: AI DRINKT GEEN KOFFIE

De opkomst van AI brengt nieuwe uitdagingen met zich mee, zoals zorgen over kennisveiligheid en de impact op data-integriteit. Binnen de onderwijs- en onderzoeksector wordt veel gesproken over ethiek, leveranciersmanagement en privacy. De vraag is echter ook welke invloed AI gaat hebben op het werk van informatiebeveiligingsteams en op de ontwikkeling van huidige en nieuwe cyberdreigingen.

In sessies met de CISO-beraden van universiteiten en hogescholen hebben we hun visies op dit thema opgehaald. Dit hoofdstuk vat samen wat de CISO's verwachten voor de komende twee tot drie jaar.

Volgens CISO's zal AI de meeste invloed hebben op de volgende dreigingen:

- verkrijgen en openbaar maken van data
- identiteitsfraude
- overname en misbruik ict

De twee gezichten van AI

CISO's verwachten dat AI de grootste invloed zal hebben op de dreiging 'verkrijgen en openbaar maken van informatie'. Die invloed kan zowel positief als negatief uitpakken.

Aan de ene kant kan AI het eenvoudiger maken om informatie te verkrijgen over systeembeveiliging, bijvoorbeeld met tools zoals Microsoft Copilot. Dit kan security officers helpen in hun werk. Aan de andere kant kan dit beginnende cybercriminelen de tools geven om hun eerste stappen te zetten. Daarnaast kunnen aanvallen professioneler worden, met een toename van hack-as-a-service. Deepfakes die steeds moeilijker te detecteren zijn, zullen het eenvoudiger maken om fraude te plegen. Tegelijkertijd kan AI ook de verdediging versterken, waardoor we aanvallen sneller detecteren en automatisch kunnen tegenhouden.

De dreiging van phishing door middel van spraakberichten en identiteitsfraude onder CEO's zal naar verwachting toenemen door het gebruik van AI-technologieën. AI kan worden ingezet om informatie te verzamelen en te combineren, zodat OSINT (Open Source Intelligence) kan worden geautomatiseerd.

Kennisveiligheid en data-integriteit

Kennisveiligheid is een groeiende zorg. AI-systemen bevatten grote hoeveelheden documenten, wat kan leiden tot ketenafhankelijkheid en risico's op datalekken bij AI-systeemaanbieders. Bovendien vergroot het gebruik van AI door leveranciers de afhankelijkheid en het risico, zonder dat klanten hiervan op de hoogte zijn.

AI kan ook invloed hebben op toetsresultaten en de integriteit binnen het onderwijs. Bewustwording bij gebruikers over de risico's, zoals de waarde van diploma's, is essentieel. Daarnaast zullen algoritmes steeds vaker bepalen wat als betrouwbare data wordt gezien, wat de betrouwbaarheid van data onder druk zet.

Samenwerking cruciaal

CISO's benadrukken het belang van een kritische benadering bij de inzet van AI. Samenwerking met vakgenoten is cruciaal, evenals het ontwikkelen van een brede visie op AI en het vergroten van bewustwording. Binnen verschillende instellingen zijn hubs opgericht voor samenwerking en kennisdeling. Een centraal loket voor AI-gerelateerde vragen kan bijdragen aan leren, kennisdeling en acceptatie. Met de opkomst van nieuwe technologieën wordt het steeds belangrijker om de authenticiteit van data te waarborgen.

Mens blijft onmisbaar

Hoewel AI nieuwe methodes mogelijk maakt, verwachten de CISO's geen fundamentele verandering in de actoren en hun motieven. Er kunnen nieuwe dreigingen ontstaan, maar die zullen in wezen variaties zijn op bestaande dreigingen. Als malware geavanceerder wordt, blijft het in essentie hetzelfde probleem als waar we nu al mee te maken hebben.

Momenteel bestaat er nog geen echte AI-verdediging. Ook niet in SOC/SIEM-tooling, ondanks dat commerciële partijen dit vaak als marketingterm gebruiken. De denkkracht van mensen blijft voorlopig onmisbaar. De beste aanpak nu is het op orde brengen van basismaatregelen en het verbeteren van end-point detectie.

Er zijn echter mogelijkheden voor AI om in de toekomst bij te dragen aan de weerbaarheid, bijvoorbeeld door het verbeteren van detectiesystemen en het automatiseren van bepaalde beveiligingsprocessen. Toch blijft de consensus dat menselijke expertise en controle essentieel zullen blijven in cybersecurity.

De grootste uitdaging voor organisaties blijft hierbij de uitvoering van cyber-securitybeleid en -procedures. Het is één ding om beleid en processen op papier te zetten, maar zorgen dat mensen zich eraan houden is een ander verhaal. Of, zoals een CISO treffend opmerkte: 'Effectieve cybersecurity draait uiteindelijk om het opbouwen van relaties en het creëren van een cultuur van veiligheidsbewustzijn. Dat zijn processen die tijd, geduld en veel persoonlijk contact vereisen. Cybersecurity blijft dus een kwestie van koffiedrinken.' Daar biedt AI geen vervanging voor.

Het waterbed-effect

Het tekort aan cybersecurity-specialisten zal niet worden opgelost door AI-ontwikkelingen. We hoeven ook niet bang te zijn dat mensen overbodig zullen worden. Menselijke expertise blijft nodig om dreigingen te duiden en beleid te ontwikkelen.

We moeten ons echter bewust zijn van het zogenaamde 'waterbed-effect': zodra we maatregelen nemen om bepaalde dreigingen of kwetsbaarheden aan te pakken, zal dit ertoe leiden dat de dreiging zich naar een andere plek verplaatst of een andere vorm aanneemt. Hierdoor verschuift de vraag naar kennis en capaciteit. In de toekomst hebben we niet alleen cybersecurity-specialisten nodig, maar ook AI-experts; een 'schaap met zes poten' in plaats van vijf.

Samengevat biedt de toekomst, met AI als belangrijkste nieuwe factor, zowel kansen als uitdagingen. De wapenwedloop tussen cybercriminelen en verdedigingsmaatregelen zal naar verwachting versnellen, maar in essentie niet veranderen. Cybersecurity blijft grotendeels mensenwerk, waarbij we risico's en gedrag moeten blijven afwegen. AI gaat de mens niet vervangen, maar biedt wel waardevolle hulpmiddelen. Om die zo goed mogelijk te benutten, is het noodzakelijk om cybersecurityteams aan te vullen met experts die nieuwe en andere competenties hebben. Op die manier kunnen we AI inzetten voor cybersecurity en beter adviseren over de risico's van AI-systemen in bedrijfs-voeringsprocessen, onderwijs en onderzoek.

‘Wie het onzichtbare wil zien moet gewoon beter kijken’

Na jaren in het werkveld is er maar weinig wat Martijn de Hamer nog verbaast. Als voormalig FG bij de Hogeschool van Amsterdam en huidige CISO bij het ministerie van Onderwijs, Cultuur en Wetenschap, kijkt hij bijna nostalgisch terug op een tijd waarin de Waarschuwingsdienst nog over individuele virussen schreef. Inmiddels gaat het om miljoenen virussen per dag en is de schaal van de problematiek veel groter dan we ooit hadden voorzien.

De Hamer was één van de mensen die in 2011 getuige was van de DigiNotar-hack, waarbij een beveiligingslek leidde tot de uitgave van valse SSL-certificaten. Ook Nederlandse overheidswebsites waren getroffen. ‘De DigiNotar-hack was een gevaar voor de nationale veiligheid,’ vertelt De Hamer. ‘Ineens was duidelijk: dit overstijgt het niveau van individuele hackers die voor de roem en zichtbaarheid een vlag op iemands scherm willen laten wapperen.’

Niet ‘of’, maar ‘wanneer’

Het DigiNotar-incident fungeert tot op de dag van vandaag als belangrijke les binnen cybersecurity. ‘Doordat we steeds meer geld gingen verdienen via het internet, werden de belangen steeds groter,’ licht De Hamer toe. ‘We beseften: als het internet platligt, ligt de complete economie plat.’ Destijds werd op DG- en ministerniveau gesproken over de vraag aan Microsoft om de uitrol van een nieuwe patch in Nederland tegen te houden. ‘Die uitrol had allerlei kernprocessen kunnen verstoren, zoals bijvoorbeeld het inklaren van goederen in de Rotterdamse haven. Door toenemende belangen en afhankelijkheden worden de gevolgen van een hack steeds ingrijpender.’

Destijds was voor De Hamer al duidelijk dat niemand veilig is. ‘Aanvallers,’ zo licht hij toe, ‘hebben immers aan één zwakke plek genoeg, terwijl organisaties zich op alle fronten moeten verdedigen. Zelfs de CIA werd op een gegeven moment gehackt. De vraag is dus niet of, maar wanneer je als organisatie wordt aangevallen.’

Leren van anderen

Onzichtbare dreigingen vormen volgens De Hamer het grootste risico. Denk aan aanvallen met nooit eerder gebruikte technieken, of moedwillige verstoringen van binnenuit. Hoewel het paradoxaal lijkt om energie te stoppen in het opsporen van onzichtbare dreigingen, is De Hamer heel stellig: 'Wie het onzichtbare wil zien moet beter of anders kijken.' Enerzijds betekent dat: slimmer kijken naar je logs, zodat je dingen gaat herkennen die je voorheen niet zag. Maar ook: leren van aanvallen op andere organisaties.

'Leren van anderen kan op verschillende manieren,' zegt De Hamer. 'Eén ervan, binnen de Rijksoverheid, is bijvoorbeeld de database van het project Versterken SOC Stelsel Rijk (VSSR), waarin de use cases van andere organisaties beschikbaar worden gemaakt. Die kun je op het technische systeem van je eigen organisatie toepassen, zodat je een melding krijgt als er iets verdachts op je netwerk gebeurt.'

Samenwerking en vertrouwen

Een andere manier om je cyberweerbaarheid te vergroten is door nog meer sectoraal samen te werken. Een goed voorbeeld daarvan vindt De Hamer de samenwerking bij bijvoorbeeld de financiële dienstverlening en bij de telecomsector. 'Binnen die sectoren is al jaren sprake van onderlinge informatie-uitwisseling, zonder zich druk te maken over concurrentieposities. Daar is algemeen bekend dat een aanval op één organisatie een les is voor de hele sector. Informatie-uitwisseling is dus cruciaal. Daar is boven alles vertrouwen voor nodig.'

In die context prijst hij de transparantie van het ministerie van Defensie en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). De dienst openbaarde in februari dit jaar dat het geavanceerde Chinese malware had gevonden. Volgens de MIVD was een Chinese staatsactor hiervoor verantwoordelijk, op basis van hun eigen inlichtingen. De MIVD koos voor het eerst om een technisch rapport over de werkwijze van Chinese hackers openbaar te maken. De Hamer was positief verrast. 'Die twee organisaties laten normaal gesproken weinig los over hun werkwijze. In dit geval deden ze dat wel, met als doel om de samenleving te helpen. Dat vond ik heel krachtig.'

Groeiplekken voor jonge professionals

Toch vreest de Hamer ook een potentieel terugkerende kwetsbaarheid in de vorm van verwaterende expertise. Dit gebeurde al eerder, tijdens de invoering van de AVG. 'Er was destijds een enorme vraag naar experts en organisaties namen daardoor vrij gemakkelijk minder gekwalificeerde privacy experts in dienst,' licht De Hamer toe. 'Zodra de Cyberbeveiligingswet – de Nederlandse implementatie van NIS 2, ter verbetering van de cyberbeveiliging binnen de EU – in 2025 in werking treedt, kan dit opnieuw gebeuren. Zeker nu er zo'n krapte is op de arbeidsmarkt. Het gevaar bestaat dat organisaties sneller denken: "Dan hebben we tenminste iemand".'

Als mogelijke oplossing voor deze expertiseverwatering ziet De Hamer kansen in het werven van en investeren in jonge professionals. 'Wanneer we net afgestudeerde informatiebeveiligers direct groeiplekken binnen onze organisaties aanbieden, vullen we de poule met experts aan de onderkant aan. Daar kunnen we in de toekomst dan allemaal op teruggrijpen.'

Optimistisch

Vooruitkijkend verwacht De Hamer zelf geen grote verrassingen meer, – 'Je wordt een beetje blasé als je langer in het veld zit,' lacht hij – maar hij denkt wel dat de maatschappij steeds opnieuw zal worden verrast. 'Elke technologie kan gehackt worden en wie inhoudelijk niet goed op de hoogte is, zal daar nooit goed genoeg op voorbereid zijn.'

De grootste uitdaging ziet hij dan ook in het overbrengen van de urgentie van cybersecurity op de mensen die ermee te maken krijgen. 'Bestuurders zijn vooral bezig met hun kerntaken,' legt hij uit. 'Voor hen is cybersecurity een middel om ervoor te zorgen dat al die kerntaken niet worden verstoord. Ze hebben te weinig tijd om zich voldoende in het onderwerp te verdiepen.' Toch is De Hamer optimistisch. 'Ik zie daarin wel langzaam verandering komen. En hoe traag het ook gaat, het gebeurt gelukkig wel.'

CONCLUSIES EN AANBEVELINGEN

Als sector zijn we qua volwassenheidsniveau op het gebied van cybersecurity in tien jaar flink gegroeid. We slaan de handen ineen als een instelling hulp nodig heeft en we weten elkaar te vinden voor het delen van kennis en informatie. Hieronder lees je de belangrijkste algemene conclusies van tien jaar samenwerking tegen cyberdreigingen.

Bewustzijn: stijging en daling

Het afgelopen decennium is de awareness voor cyberdreigingen langzaam gestegen, met een piek na de invoering van de AVG in 2018. Het bewustzijn bereikte een hoogtepunt na een aantal incidenten in de periode 2019–2021. Ook het gebruik van digitale middelen en online systemen tijdens de coronapandemie kan het risicobewustzijn hebben verhoogd.

Vanaf 2022 lijkt het alsof de inschatting van de ernst van dreigingen weer iets is gezakt. De meeste instellingen werken al jarenlang hard om hun weerbaarheid te verhogen, waardoor wellicht het gevoel is ontstaan dat ze door alle preventieve maatregelen inmiddels voldoende grip hebben op cyberveiligheid. Steeds meer instellingen binnen de sector doen regelmatig mee aan oefeningen ter voorbereiding op een cybercrisis, waardoor ze goed weten hoe ze moeten reageren in een crisis en hoe ze de schade kunnen beperken. Het feit dat er minder impactvolle incidenten lijken te zijn, betekent echter niet dat de dreigingen afnemen en dat de sector veilig is. De strijd tussen cybercriminelen en beschermende maatregelen dendert op volle snelheid door.

Blijvend relevante adviezen

De adviezen over cyberveiligheid zijn in de afgelopen tien jaar niet veel anders of minder relevant geworden. De belangrijkste aanbevelingen blijven:

- Breng de basishygiëne van je instelling op orde.
- Werk samen en deel kennis.
- Schaam je niet als het een keer misgaat.
- Deel fouten en tips om anderen te helpen.
- Oefen regelmatig.

Als we vooruitkijken, kunnen we hier de volgende verwachtingen aan toevoegen:

- Dreigingen zijn permanent, alleen verschuift de focus soms van de ene naar de andere dreiging onder invloed van de actualiteit.
- Ernstige en impactvolle incidenten leiden vaak tot iets positiefs, zoals versterkte samenwerking, nieuwe diensten en meer kennisdeling.
- De collectiviteit is sterker dan ooit: de laatste jaren zien we zelfs nieuwe impulsen door de oprichting van CISO-raden en, na afloop van het subsidieprogramma IV-HO, de permanente status van het bestuurlijk overleg over integrale veiligheid in onderwijs en onderzoek.
- We moeten blijven opletten dat capaciteitstekort niet als excuus wordt gezien voor verminderde weerbaarheid of ontbrekende samenwerking.

Nieuwe technologieën

Daarnaast verwachten we dat de opkomst van nieuwe technologieën niet direct invloed zal hebben op het soort cybersecuritymaatregelen of de aard van de dreigingen. De wedloop tussen dreigingen en beveiligingsmaatregelen blijft in essentie dus hetzelfde, maar doordat de snelheid waarmee veranderingen zich voltrekken exponentieel toeneemt, is een nog alertere en flexibelere aanpak van cybersecurity noodzakelijk.

Niet ‘wat’, maar ‘hoe’

De grootste uitdaging binnen cybersecurity zit niet, zoals vaak wordt gedacht, in de techniek waarmee we onze instellingen beveiligen, maar juist in het organiseren van processen en verantwoordelijkheden in onze instellingen, samenwerkingsverbanden en toeleveringsketens. Oftewel: cybersecurity is veel meer een organisatorisch vraagstuk dan een puur technisch probleem. De nadruk ligt te vaak op geavanceerde technische oplossingen, terwijl vrijwel alle inbreuken veroorzaakt worden door bekende en eenvoudig op te lossen zwakheden, zoals:

- niet-gepatchte software
- gebrek aan adequate back-ups
- afwezigheid van tweefactorauthenticatie (2FA)
- overmatige en onnodige gebruikersrechten
- zwakke wachtwoorden

Bovengenoemde ‘usual suspects’ zijn verantwoordelijk voor ongeveer 98%[11] van de cyberveiligheidsproblemen. Ondanks het feit dat deze zwakheden al jaren bekend zijn, blijven ze een terugkerend probleem. Hoewel de industrie zich vaak richt op nieuwe dreigingen en geavanceerde technische oplossingen, is het cruciaal dat organisaties prioriteit geven aan het verstevigen van de basis: het implementeren en handhaven van fundamentele beveiligingsmaatregelen. Door deze shift in focus kunnen organisaties hun cyberveiligheid aanzienlijk verbeteren, risico's verminderen en een solide fundament leggen voor meer geavanceerde beveiligingsstrategieën in de toekomst. Uiteindelijk is het de combinatie van een sterke basis en innovatieve oplossingen die zal leiden tot een robuustere en effectievere cyberveiligheidsaanpak.

Toekomstperspectief

De toekomst biedt zowel uitdagingen als kansen. Hoewel ontwikkelingen in AI, quantum computing en de uitbreiding van het IoT onze digitale weerbaarheid op de proef zullen stellen[12], bieden deze technologieën tegelijkertijd nieuwe mogelijkheden[13]. Het is aan ons allen – bestuurders, CISO's, ict-professionals en eindgebruikers – om samen deze uitdagingen aan te gaan en de kansen te benutten. ‘Verwacht het onverwachte’ schrijft de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)[14]. Door kennis van diverse disciplines te bundelen kunnen we onszelf zo goed als mogelijk op die toekomst voorbereiden[15]. Intensieve samenwerking en kennisdeling zorgen voor een veilige digitale toekomst voor onderwijs en onderzoek.

Cybersecurity-dashboard: actuele status dreigingen, overzicht risico’s en handelingspersectieven

Op het cybersecurity-dashboard vind je op ieder willekeurig moment van het jaar de meest actuele status van dreigingen, kwetsbaarheden en bijbehorende handelingsperspectieven. Ook vind je hier een actueel van overzicht van:

- relevante en actuele trends
- cybersecuritynieuws uit de sector
- incidenten en meldingen bij SURFcert
- benchmarkresultaten
- awarenessniveau
- adoptie van web- en e-mailstandaarden

Ga naar https://edu.nl/cyberbeeld
Of scan de QR-code

Inloggen met SURFconext

BRONDOCUMENTEN

1 https://www.ncsc.nl/actueel/nieuws/2023/augustus/8/nederlandse-organisaties-doelwit-van-ddos-aanvallen
2 https://z-cert.nl/actueel/nieuws/ddos-aanvallen-treffen-aantal-ziekenhuizen
3 https://www.insidehighered.com/news/global/2024/02/22/uk-universities-targeted-cyberattack-supporting-israel
4 https://security.geant.org/ghosts-of-palestine-launches-cyberattack-on-israeli-universities-in-protest/
5 https://www.loketkennisveiligheid.nl
6 https://fts.politie.nl/cybercrimebeeld/
7 https://www.rijksoverheid.nl/documenten/rapporten/2024/04/15/openbaar-jaarverslag-aivd-2023
8 https://www.wrr.nl/publicaties/rapporten/2019/09/09/voorbereiden-op-digitale-ontwrichting
9 https://www.wrr.nl/publicaties/rapporten/2021/11/11/opgave-ai-de-nieuwe-systeemtechnologie
10 https://www.surf.nl/diensten/ozon-en-nozon
11 https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022
12 Platform Integrale Veiligheid Hoger Onderwijs & Instituut Clingendael. Risico- en dreigingsbeeld Hoger Onderwijs 2024. Een verkenning van actuele en toekomstige uitdagingen.
13 https://www.surf.nl/en/tech-trends
14 https://www.nctv.nl/onderwerpen/cybersecuritybeeld-nederland
15 https://sec.surf.nl/cybersecurity-risicoanalyse-met-methodes-van-futurologen/

COLOFON

Auteurs
Nicole van Deursen (SURF)
Abdul Altawekji (SURF)
Nicole van der Meulen (SURF)
Bart Bosma (SURF)

Interviews
Nicole van der Meulen (SURF)
Evelyne Hermans (SURF)

Eindredactie
Evelyne Hermans (SURF)

Ontwerp
Studio Koelewijn Brüggenwirth BNO, Den Haag

AI-illustratie
De afbeelding op pagina 1 is door SURF gegenereerd met Midjourney 6.1. De prompt voor deze afbeelding was: cybersecurity students working together, minimalism, colorful --s 50 --v 6.1 --style raw --aspect 7:4. Over deze illustratie zijn vlakken geplaatst uit de SURFhuisstijl. De foto's in de vlakken op de cover en in het binnenwerk komen uit de beeldbank van SURF en zijn rechtenvrij.

Oktober 2024

Samen aanjagen van vernieuwing