# CYBERDREIGINGSBEELD 2023

## ONDERWIJS EN ONDERZOEK

# INHOUD

# VOORWOORD
# BLIJVEN SAMENWERKEN, INFORMATIE DELEN EN RISICOGEBASEERD WERKEN

2022 leek een rustig jaar als het gaat om cybersecurity, omdat relatief weinig incidenten in onze sector de media haalden. Dit betekent niet dat het ook rustiger ís. We zien nog altijd veel phishing-, ransomware- en DDoS-aanvallen, datalekken, leveranciersrisico's en kennisdiefstal. We moeten alert blijven, want de dreiging is permanent. Cybercriminelen ontwikkelen op een hoger tempo nieuwe en schaalbare aanvalsmethoden dan wij onze weerbaarheid verbeteren. Kunstmatige intelligentie of extended reality doen hun intrede in onderwijs en onderzoek, en brengen nieuwe risico's en dilemma's met zich mee voor informatiebeveiliging en privacy. We moeten daarom nog beter leren om nieuwe technologie veilig te ontwerpen en in te zetten.

Voor het tweede jaar op rij blijkt uit de survey voor dit cyberdreigingsbeeld onder instellingen dat het gebrek aan menskracht en awareness urgente belemmeringen zijn om informatiebeveiliging en privacy op het gewenste niveau te brengen. Dit is niet uniek voor onze sector, want wereldwijd is er een capaciteitstekort: ook als er wel formatieruimte is, maakt de krappe arbeidsmarkt het moeilijk mensen te vinden.

Om met deze informatiebeveiligings- en privacy-uitdagingen om te gaan moeten we intensief samenwerken, zowel ter preventie van incidenten als tijdens en na incidenten. Door informatie zo snel mogelijk te delen, kunnen andere instellingen cyber-ellende beter voorkomen. We zien echter dat dit in de praktijk niet altijd gebeurt. Niet voor niets werd het woord cyberschaamte verkozen tot het cybersecuritywoord van 2022. Cyberschaamte hebben mensen die zich generen voor een fout of bang zijn voor imagoschade. Een incident kan echter ook de meest volwassen organisaties overkomen. De wedloop met cybercriminelen kun je als individuele instelling niet winnen. We maken het meest kans als we het samen doen.

Weerbare organisaties werken risicogebaseerd. Hierin kunnen we ons verder ontwikkelen. Risico's voor informatiebeveiliging en privacy zijn sterk verbonden met andere veiligheidsrisico's in organisaties én met de risico's van ketenpartners. We zagen dat in 2022 toen een leverancier van campuspassen was gehackt. Daarmee ontstond niet alleen een groot datalek, maar er waren ook zorgen over de fysieke veiligheid van mensen en gebouwen. Door ons te richten op multidisciplinaire samenwerking valt de komende jaren nog veel winst te behalen. Binnen het programma Integraal Veilig Hoger Onderwijs hebben we hier al ervaring mee opgedaan. Dit gaan we verder uitbouwen de komende jaren.

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

# 2 SAMENVATTING

## 2.1 Dreigingen en kwetsbaarheden permanent aanwezig

De laatste jaren verandert het beeld over dreigingen en kwetsbaarheden weinig. Ze worden vooral veroorzaakt door statelijke actoren, cybercriminelen, (h)acktivisten en mensen binnen organisaties die onbedoeld incidenten veroorzaken. Het aantal incidenten blijft nog steeds stijgen. Ook worden er steeds meer kwetsbaarheden gevonden in systemen en applicaties en blijven DDoS-aanvallen, phishing-mails en ransomware-aanvallen aan de orde van de dag.

## 2.2 Weerbaarheid blijft aandachtspunt

De professionaliteit van kwaadwillenden ontwikkelt zich vaak sneller dan de snelheid waarmee instellingen hun weerbaarheid kunnen verbeteren. De snelheid waarmee nieuwe aanvalstechnieken worden ontwikkeld is aanzienlijk en zorgt voor permanente uitdaging om bij te blijven. De metingen die SURF uitvoert op procesvolwassenheid, internetveiligheid en awareness, laten zien dat weerbaarheid een aandachtspunt blijft. Het besef groeit dat niet alleen de interne processen en systemen op orde moeten zijn, maar dat ook het menselijk handelen en processen voor samenwerkingsverbanden, ketenpartners en leveranciers aan passende richtlijnen moeten voldoen.

## 2.3 Incidenten beter gedetecteerd maar nog niet altijd gedeeld

Instellingen worden beter in het detecteren van incidenten, zeker nu steeds meer instellingen monitoring en detectie inrichten of uitbesteden. Toch nemen instellingen tijdens een incident niet altijd contact op met SURFcert. Niet alleen kan SURFcert ondersteuning bieden, maar kunnen zij ook de (technische) informatie over het incident delen om andere instellingen voor eenzelfde lot te behoeden.

## 2.4 Risicobeheer nog in de kinderschoenen

Er zijn nog maar weinig instellingen die risicogebaseerd werken. Risico-eigenaarschap is nog beperkt ingebed bij het hogere management. Functionarissen die risico-eigenaren moeten ondersteunen zijn vaak nog niet goed in positie gebracht en worden gehinderd door capaciteitsproblemen. Toch zien we dat bestuurders steeds meer betrokken zijn en in de hele sector worden verbeterprogramma's uitgevoerd.

## 2.5 Dashboard sectoraal beeld 2022

### Risicobeeld 2022

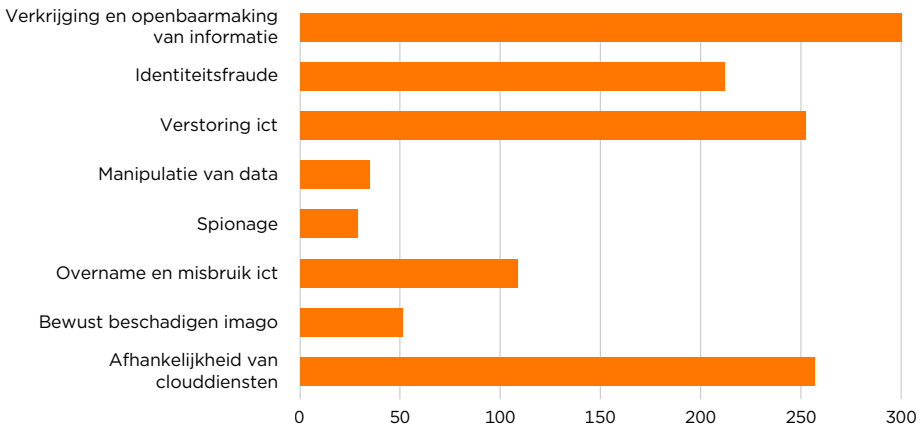
Ten opzichte van het vorige dreigingsbeeld valt op dat dit jaar geen van de risicocategorieën als ‘zeer hoog’ wordt ingeschat. Daarnaast zijn er twee nieuwe categorieën toegevoegd: Onveilig gedrag en gebrek aan awareness en Capaciteitstekort.

| | Onderwijs | Onderzoek | Bedrijfsvoering |
|---|---|---|---|
| **Onveilig gedrag en gebrek aan awareness** | Hoog | Hoog | Hoog |
| **Capaciteitstekort** | Hoog | Hoog | Hoog |
| **Verkrijging en openbaarmaking van informatie** | Hoog | Hoog | Hoog |
| **Ketenafhankelijkheid** | Hoog | Hoog | Hoog |
| **Verstoring ict** | Hoog | Hoog | Hoog |
| **Identiteitsfraude** | Midden | Hoog | Midden |
| **Spionage** | Laag | Hoog | Laag |
| **Manipulatie van data** | Midden | Midden | Midden |
| **Overname en misbruik ict** | Midden | Midden | Midden |
| **Bewust beschadigen imago** | Midden | Midden | Midden |

### Incidentbeeld in 2022

In 2022 hebben er incidenten plaatsgevonden in alle risicocategorieën uit het Cyberdreigingsbeeld van 2021-2022.

**Aantal incidenten per risicocategorie uit 2022**




### Weerbaarheidsbeeld 2022

*Eigen inschatting weerbaarheid*

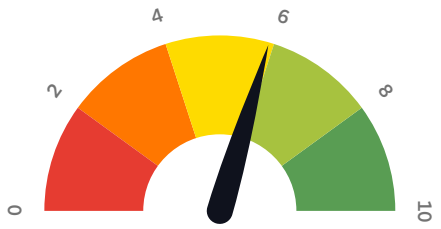
Instellingen geven hun eigen weerbaarheid een krappe voldoende, maar hebben nog niet alle waardevolle assets adequaat beschermd.

| | Eigen inschatting* |
|---|---|
| **De algemene indruk over de weerbaarheid van de instelling** | 6 |
| **De mate waarin er een actueel overzicht is van de kroonjuwelen** | 5 |
| **De mate waarin de beschikbaarheid, integriteit en vertrouwelijkheid van de kroonjuwelen op een passend niveau zijn beschermd** | 5 |
| **De mate waarin de kroonjuwelen worden gemonitord op mogelijke inbreuken** | 5 |

* op een schaal van 0 tot 10

*Awarenessmeting*

De gemiddelde score op de security- en privacy-awarenessmeting was 5,9 (schaal van 1-10)




5,9

## Weerbaarheidsbeeld 2022 (vervolg)

*Benchmark SURFaudit toetsingskader informatiebeveiliging*

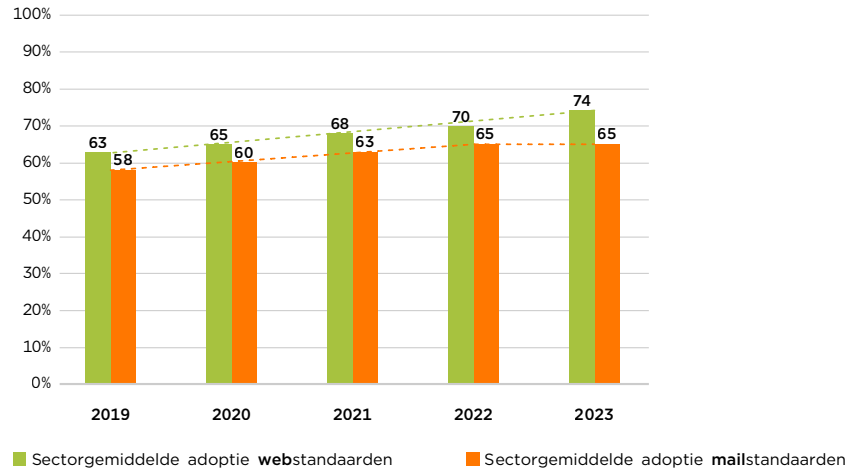
De benchmarkscore van het SURFaudit toetsingskader 2021 (schaal van 0-5) was licht gedaald ten opzichte van 2019.

| Domein | Sectorgemiddelde 2019 (35 deelnemers) | Sectorgemiddelde 2021 (51 deelnemers) | |
|---|---|---|---|
| Governance | 2,4 | 2,3 | ↓ |
| Organisatie | 2,3 | 2,3 | ↔ |
| Risicobeheer | 1,8 | 1,8 | ↔ |
| Personeelsbeheer | 2,3 | 2,3 | ↔ |
| Configuratiebeheer | 2,3 | 2,2 | ↓ |
| Incident-/probleembeheer | 2,6 | 2,4 | ↓ |
| Wijzigingsbeheer | 2,2 | 2,1 | ↓ |
| Systeemontwikkeling | 2,0 | 1,9 | ↓ |
| Gegevensbeheer | 2,2 | 2,0 | ↓ |
| Identiteits- en toegangsbeheer | 2,1 | 1,9 | ↓ |
| Beveiligingsbeheer | 2,2 | 2,2 | ↔ |
| Fysieke beveiliging | 2,5 | 2,4 | ↓ |
| IT-operatie | 2,7 | 2,3 | ↓ |
| Bedrijfscontinuïteitsbeheer | 2,4 | 2,2 | ↓ |
| Ketenbeheer | 2,3 | 2,2 | ↓ |
| Gemiddelde van alle statements | 2,3 | 2,2 | |

*Internetveiligheid*

De adoptie van internetveiligheidsstandaarden voor mail en web is in de loop der jaren verbeterd.

**Adoptie e-mail- en webstandaarden voor de hoofddomeinen van de sector onderwijs en onderzoek**




*Actuele thema's*

De thema's waar veel over werd gesproken in 2022:

- Toekomst
- Governance
- Incidenten

**AI** **Extended reality**
**Cyberschaamte** **Kennisveiligheid**
**Ketenafhankelijkheid** **Weerbaarheid**
**NIS2-richtlijn** **Risicobeheer** **DDoS**
**Datalekken** **Capaciteitstekort** **Informatiedelen**
**Leveranciers** **Awareness** **Ransomware**
**(H)Acktivisme** **Phishing**

# 3 INLEIDING

## 3.1 Doel en doelgroep van dit document

Sinds 2014 publiceert SURF in het jaarlijkse Cyberdreigingsbeeld onderwijs en onderzoek over dreigingen en trends die relevant zijn voor de sector. Het doel van dit cyberdreigingsbeeld is om een indruk te geven van de ontwikkelingen en trends die relevant zijn voor informatiebeveiliging voor onderwijs-, onderzoeks- en bedrijfsvoeringsprocessen. De voornaamste doelgroep van dit document bevindt zich op het strategische niveau in een instelling, die het document als inspiratiebron en conversatiestarter kan gebruiken. We stimuleren instellingen om de informatie in dit document als basis te gebruiken om een eigen beeld te vormen van relevante risico's voor hun instelling.

## 3.2 Totstandkoming

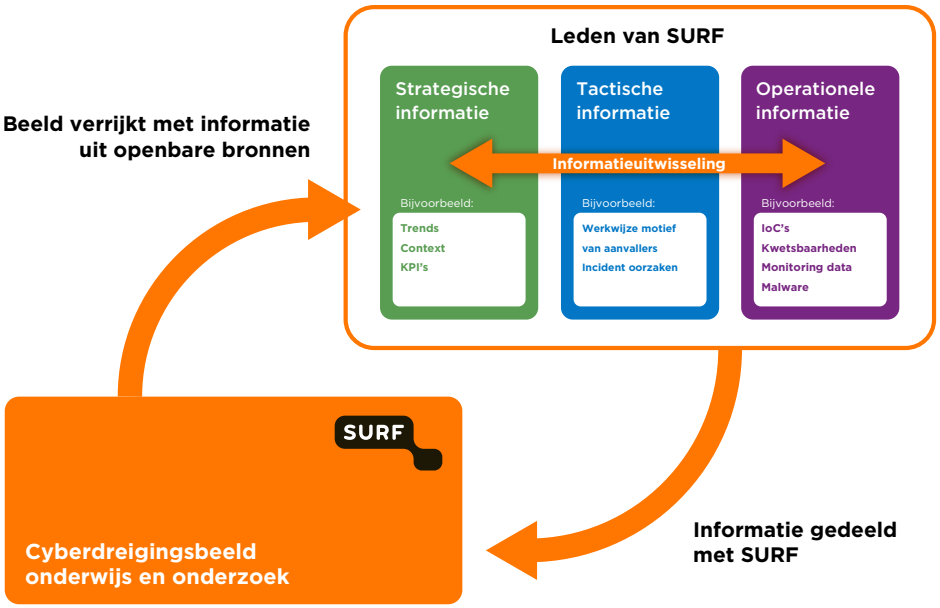
Gedurende het hele jaar verzamelt SURF relevante informatie uit openbare bronnen en voeren we gesprekken met experts uit de sector. Daarnaast hebben we een survey uitgezet onder de leden met vragen over de domeinen onderwijs, onderzoek en bedrijfsvoering. De werkwijze en totstandkoming worden in meer detail toegelicht in bijlage 1.

## 3.3 Leeswijzer

Het document bevat twee inhoudelijke hoofdstukken, hoofdstuk 2 en 3. Hoofdstuk 4 schetst het beeld van 2022 waarin we de stand van zaken over risico's, incidenten en weerbaarheid beschrijven. Hoofdstuk 5 kijkt vooruit en gaat in op wat we moeten doen: zowel nu als op langere termijn.

Wij hopen dat het Cyberdreigingsbeeld wordt gebruikt om gesprekken te starten. Als hulpmiddel daarbij hebben we op diverse plekken in de hoofdstukken vragenkaartjes opgenomen die samenhangen met het onderwerp van dat hoofdstuk.

Figuur 1 **Positie van het Cyberdreigingsbeeld ten opzichte van dreigingsinformatie binnen instellingen**




**Uitleg bij figuur 1** Het Cyberdreigingsbeeld is geen vervanging voor interne informatie-uitwisseling over risico's en is ook geen risicobeoordeling die een-op-een van toepassing is op individuele instellingen. Samenwerking en informatie-uitwisseling tussen de operationele, tactische en strategische niveaus binnen organisaties is essentieel om een volledig beeld te vormen. Door het Cyberdreigingsbeeld onderwijs en onderzoek naast het instellingsbeeld te leggen verbetert de informatiepositie op strategisch niveau. Figuur 1 illustreert hoe dit document zich verhoudt tot de risico- en dreigingsinformatie binnen een instelling.

# 4 HET BEELD VAN 2022

In dit hoofdstuk beschrijven we de risico's, incidenten en weerbaarheid in 2022.

## 4.1 Risico's

De digitalisering van onze sector brengt continu nieuwe kansen. We moeten echter ook weerbaar zijn tegen de permanente dreigingen die deze kansen met zich meebrengen. Veel mensen denken dat weerbaarheid een ict-vraagstuk is, de kwestie is breder. Weerbare organisaties hebben niet alleen basismaatregelen voor cyberveiligheid genomen, maar werken ook risicogebaseerd[1]. In de sector onderwijs en onderzoek is op dit terrein nog veel winst te behalen.

**Dialoogvragen Risico's**

- **Hebben we de risicobeheercyclus goed ingericht?**
- **Evalueren we regelmatig de risicobeheercyclus?**
- **Zijn lijnmanagers voldoende getraind in risicobeheer?**
- **Welke algemeen bekende dreigingen zijn ook relevant voor onze instelling?**
- **Zien we daarnaast nog andere relevante risico's?**
- **Is ons risicoregister volledig en actueel?**
- **Vallen de risico's nog binnen de risicobereidheid?**

### Algemeen beeld governance en risicobeheer

*'Risicomanagement nog in kinderschoenen'*

Het algemene beeld voor heel Nederland is helder in de Nederlandse Cybersecurity Strategie: 'Risicomanagement staat nog in de kinderschoenen'[2]. Risicobeheer blijkt vaak organisatorisch complex te zijn, ook in onze sector. We zien dit terug in de SURFaudit benchmark[3], het instrument waarmee de compliance wordt gemeten tegen het SURFaudit toetsingskader informatiebeveiliging. De benchmark scores in tabel 1 laten zien dat het volwassenheidsniveau van risicobeheer en governance bij de deelnemende leden nog niet op het geambieerde volwassenheidsniveau 3 is. Het volwassenheidsniveau van het domein risicobeheer is al twee metingen op rij de laagste van alle vijftien deelgebieden van het toetsingskader. Instellingen die bij risicobeheer op niveau 2 zijn, hebben wel beleid en processen voor (informatiebeveiliging)risicobeheer, maar gebruiken die voornamelijk bij grote projecten of als reactie op problemen. Informatie- en privacy risicobeoordeling op basis van organisatiedoelstellingen gebeurt op beperkte schaal. Daarbij is het eigenaarschap van risico's slechts gedeeltelijk toegewezen aan senior managers.

Tabel 1 **Benchmark-scores relevante deelgebieden SURFaudit toetsingskader informatiebeveiliging**

| | Sectorgemiddelde 2019 (35 deelnemers) | Sectorgemiddelde 2021 (51 deelnemers) | |
|---|---|---|---|
| **Governance** | 2,4 | 2,3 | ↓ |
| **Risicobeheer** | 1,8 | 1,8 | ↔ |

Uit de survey blijkt dat bestuurders van de meeste instellingen met regelmaat rapportages over informatiebeveiliging en privacy ontvangen. Bij bijna de helft van de instellingen vindt daarbij elk kwartaal een dialoog plaats tussen het college van bestuur en de rapporterende functionaris. Er is weinig uniformiteit in de rapportagevormen: de respondenten van de survey rapporteren elk op hun eigen wijze aan verschillende gremia. Het is nog uiterst zeldzaam dat directies een rapportage over informatiebeveiliging en privacyrisico's opnemen als onderdeel van de plannings- en controlcyclus. Tenslotte geeft ruim de helft (55%) van de respondenten aan dat ze nog beter kunnen functioneren als:

- Risico-eigenaarschap van directeuren en decanen en bijbehorende verantwoordelijkheden duidelijker vastliggen en als hier beter op wordt gestuurd.
- De CISO buiten de IT-afdeling/CIO-office en dichter bij het bestuur is gepositioneerd.
- Bestaan en werking van processen verbetert.

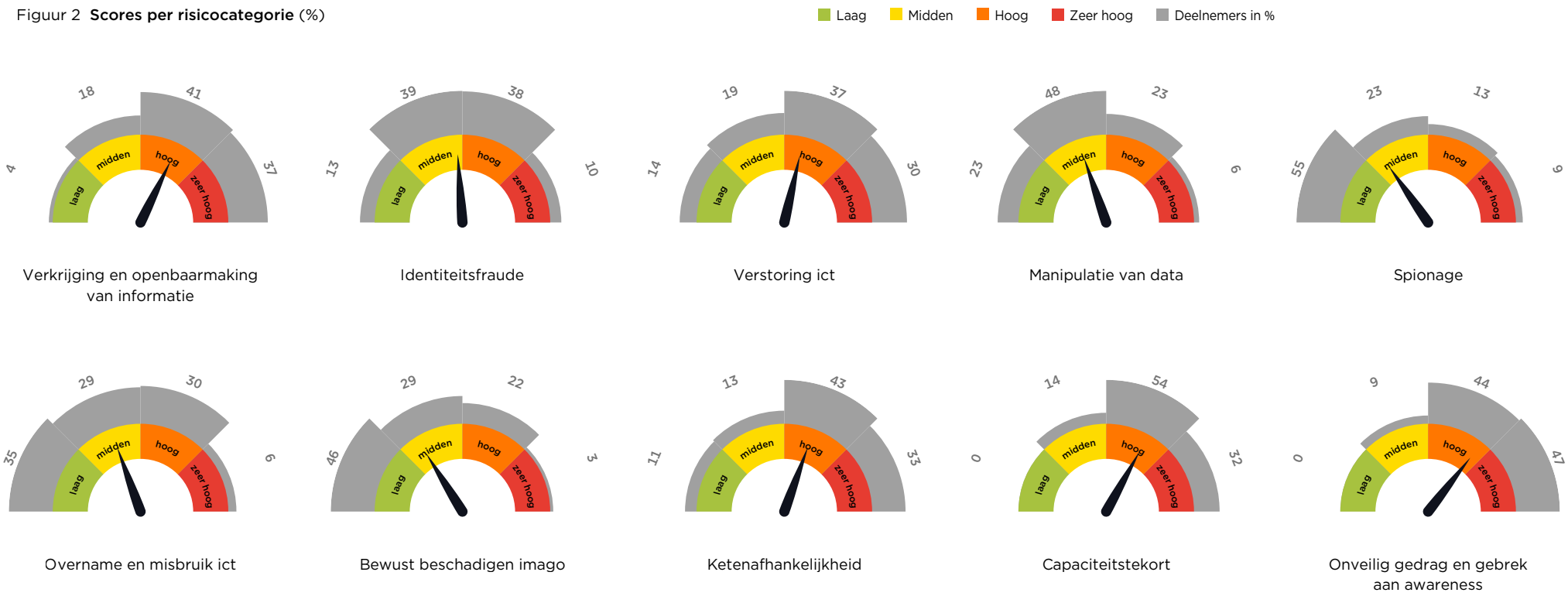
*Betrokkenheid van bestuurders groeit*

We zien ook optimistische resultaten uit de survey. Bij 77% van de deelnemers is tenminste één lid van het college van bestuur (CvB) actief betrokken bij informatiebeveiliging en privacy, en vinden er regelmatig dialogen tussen CvB en de CISO of privacyfunctionaris plaats.

## Risico's en dreigingen

Sinds vele jaren zien we dezelfde risicocategorieën in het Cyberdreigingsbeeld onderwijs en onderzoek. Dat bevestigt dat dreigingen permanent zijn en dat alertheid geboden blijft. We vroegen de respondenten om de categorieën uit het vorige cyberdreigingsbeeld opnieuw een score te geven van laag, midden, hoog tot zeer hoog. Uit het gemiddelde van de antwoorden blijkt dat geen enkele risicocategorie dit jaar als zeer hoog wordt beoordeeld. De risico-inschattingen voor de processen onderzoek, onderwijs en bedrijfsvoering wijken onderling niet veel af van elkaar. De scores zijn weergegeven in figuur 2. Voor de resultaten per apart proces verwijzen we naar bijlage 2. Naar aanleiding van suggesties van respondenten hebben we dit jaar twee nieuwe categorieën toegevoegd: Capaciteitstekort en Onveilig gedrag en gebrek aan awareness.

Figuur 2 **Scores per risicocategorie** (%)




**Uitleg bij de figuur 2** De respondenten schatten een categorie in op laag, midden, hoog of zeer hoog, waarbij laag een waarde heeft van 1 punt en zeer hoog 4 punten. Deze categorieën zijn te zien in de halve ring met vier kleuren. De gemiddelde score komt tot uitdrukking in uitslag van de zwarte meter binnen de ring. Buiten de ring staan taartpunten die gebaseerd zijn op absolute aantallen per categorie. Deze taartpunten geven een beeld van de verdeling van de antwoorden. Instellingen die deze categorieën willen vergelijken met terminologie die zij intern hanteren, kunnen gebruik maken van bijlage 3 waarin we een cross reference hebben opgenomen van onze categorieën en de definities in internationale classificaties.

**De volgende categorieën vallen op in 2022:**

*Bewust beschadigen imago*

De categorie Bewust beschadigen imago wordt al meerdere jaren door respondenten op medium geschat. Toch blijft waakzaamheid geboden. De eerste reden is de evolutie van de werkwijze van cybercriminelen: ransomware-aanvallen worden soms gecombineerd met bekendmaking van de aanval en dreiging met openbaarmaking van de informatie. De tweede reden is dat hacktivisme in het veranderende geopolitieke en maatschappelijke klimaat mogelijk een comeback kan maken[4]. Instellingen met banden met bepaalde bedrijven, landen of sectoren die in het maatschappelijk debat gevoelig liggen, kunnen te maken krijgen met pogingen tot verstoring door activisten.

*Ketenafhankelijkheid*

De categorie Ketenafhankelijkheid heette vorige jaar Afhankelijkheid van clouddiensten. We hebben de naam aangepast om een bredere lading te dekken. Respondenten gaven aan dat zij niet alleen met cloud-leveranciers, maar ook met andere leveranciers uitdagingen ervaren. Bovendien is het van belang om ook de risico's bij samenwerkingen met partnerorganisaties te beheersen. Organisaties zijn digitaal verbonden en verweven, ook met samenwerkingspartners, leveranciers en overheden. Wanneer een van de partijen wordt getroffen door een incident, kan dat gevolgen hebben voor meerdere organisaties. En die gevolgen kunnen zich uitstrekken buiten informatiebeveiliging: toen in 2022 een leverancier van toegangspassen was getroffen door een incident, was dat niet alleen een datalek, maar was er ook een mogelijke impact op de fysieke beveiliging.

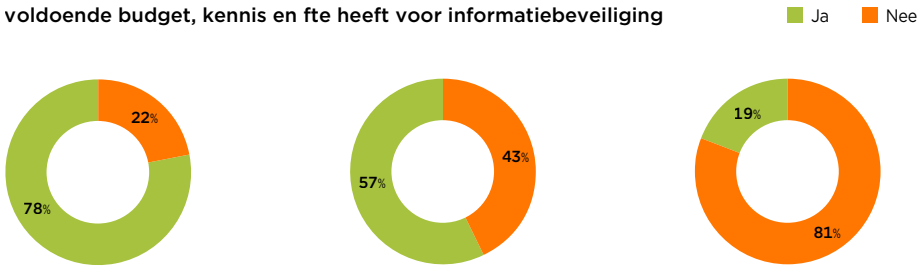
*Spionage*

Voor onderzoek zien we wel dat de risicoperceptie voor spionage hoger ligt dan voor onderwijs en bedrijfsvoering. Hier ligt ook een verband met kennisveiligheid.

*Capaciteitstekort*

We hebben deze categorie dit jaar toegevoegd omdat het tekort aan mensen en kennis in de survey veelvuldig werd genoemd als een hoog tot zeer hoog urgent risico, dat ook andere risicocategorieën beïnvloedt: maar liefst 81% van de respondenten in de survey gaf aan dat hun instelling onvoldoende mensen heeft om informatiebeveiligings- en privacytaken uit te voeren, zie figuur 3. Tijdelijke inhuur van professionals lijkt dit probleem niet op te lossen omdat ook ict-dienstverleners kampen met personeelstekorten. Vacatures voor informatiebeveiliging en privacy zijn lastig te vervullen. Het probleem is niet beperkt tot informatieveiligheid, maar betreft de hele ict-sector[5]. Door gebrek aan goed geschoolde en ervaren medewerkers kunnen instellingen niet groeien in weerbaarheid en cybervolwassenheid.

Figuur 3 **Percentages respondenten (n=86) dat vindt dat hun instelling voldoende budget, kennis en fte heeft voor informatiebeveiliging**




**Dialoogvragen Capaciteit**

- **Kunnen de privacy en security officers met voldoende capaciteit en kennis functioneren?**
- **Kunnen we capaciteit voor het uitvoeren van risicoanalyses efficiënt inzetten?**
- **Hebben we genoeg (technische) kennis in huis of beschikbaar om maatregelen op systeem/applicatie/infrastructuur-niveau te implementeren?**
- **Hoe kunnen we het voor informatiebeveiliging- en privacy professionals aantrekkelijk maken om bij ons te komen werken?**

*Onveilig gedrag en gebrek aan awareness*

De meerderheid van cyberincidenten vindt plaats als gevolg van onbedoeld onveilig handelen door mensen[6,7]. Dit beeld is niet uniek voor onze sector. Voor veel mensen is het nog geen routine om basale cybersecuritymaatregelen toe te passen, of om daarbij hulp te vragen. Van medewerkers en studenten wordt verwacht dat zij weten hoe zij met ict moeten omgaan, terwijl niet iedereen daarin een basisniveau heeft. Bovendien kan hoge werkdruk leiden tot vergissingen. Uit de reacties van de respondenten bleek dat bepaalde soorten vergissingen binnen hun organisatie herhaaldelijk de oorzaak waren van incidenten:

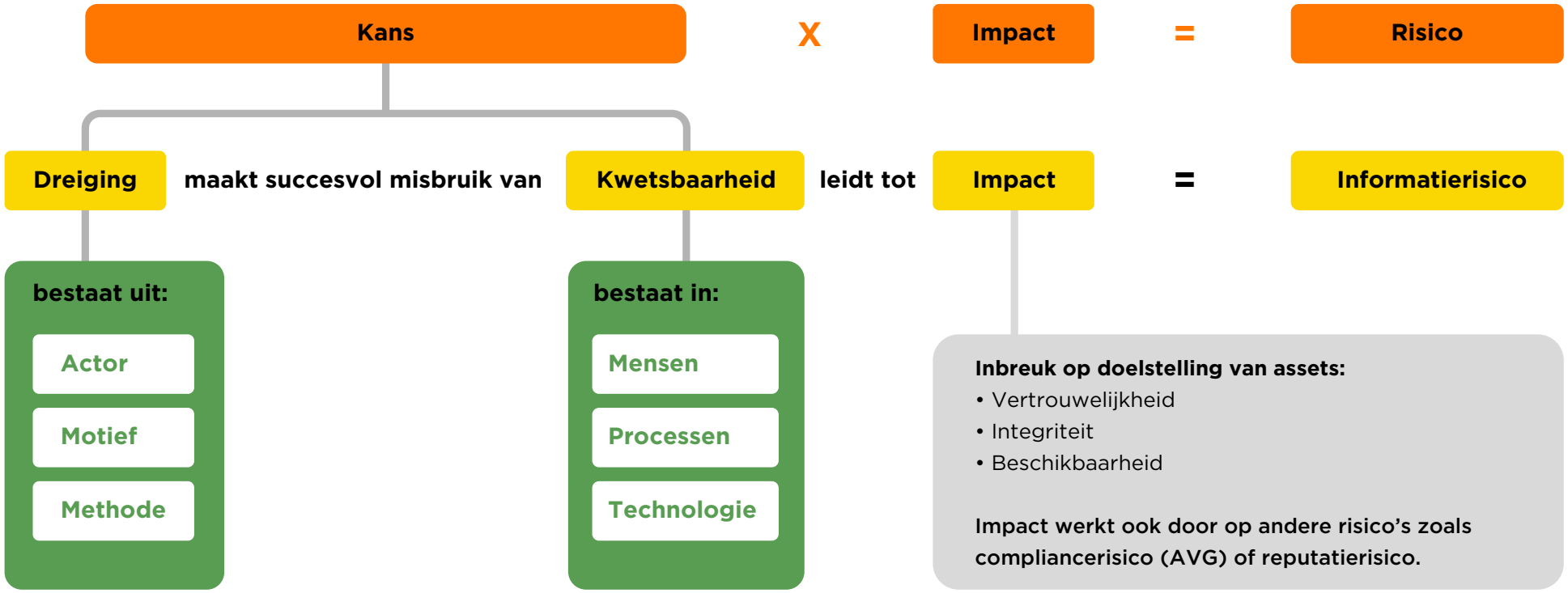
- Fouten met het versturen van e-mails, waarbij persoonsgegevens bij de verkeerde ontvanger terecht komen.
- Klikken op linkjes in phishingmails en vervolgens accountgegevens invoeren op een malafide website.
- Een drive met documenten delen met personen die daartoe geen toegang nodig hebben.
- Het delen van inloggegevens.
- Onvoldoende kennis van autorisaties in een samenwerkingsomgeving.
- Vergissingen van ict-beheerders bij wijzigingen in systemen waardoor de autorisaties veranderen.
- Buiten de procedures om ict inkopen, waardoor de basismaatregelen voor privacy en informatiebeveiliging niet zijn geborgd.

De respondenten van de survey zijn het ermee eens dat structurele aandacht voor security en privacy onontbeerlijk is om een weerbare organisatie te zijn, en dat medewerkers hier een belangrijke rol in spelen. Een aantal respondenten geeft aan dat security en privacy nu te vrijblijvende thema's zijn. Zij pleiten daarom voor het invoeren van bijvoorbeeld verplichte awarenesstrainingen en phishingtesten. De respondenten zien dit als een stok achter de deur; zij zijn zich ervan bewust dat collega's mogelijk minder gemotiveerd zijn door werkdruk, onduidelijke regels en gebrek aan interesse. Door awareness-activiteiten verplicht te maken, wordt voor de instelling ook duidelijk welke investering er van medewerkers verwacht wordt.

**Dialoogvragen Awareness**

- **Doen we genoeg om onze medewerkers en studenten te steunen om risico's te begrijpen en daarnaar te handelen?**
- **Zijn onze medewerkers en studenten digitaal geletterd genoeg om met de ict-systemen te werken?**
- **Kunnen medewerkers en studenten op een veilige plek terecht om iets verdachts of een incident te melden?**

Figuur 4 **De opbouw van een risico**




**Uitleg bij figuur 4**
De termen risico's en dreigingen worden in de praktijk vaak door elkaar gebruikt. In dit document nemen we het concept risico als basis. Een risico wordt gevormd door een aantal componenten, die we risicocategorieën noemen.

We beschouwen de volgende risicocategorieën:

- Een **dreiging** gaat om alles dat de organisatie schade zouden kunnen berokkenen. Het identificeren van de belangrijkste actoren, hun motieven en hun methoden is belangrijk voor het prioriteren van onze risicobeperkende maatregelen. Wij kunnen huidige dreigingen observeren en proberen toekomstige dreigingen te voorspellen.
- **Kwetsbaarheden** zijn de zwakke plekken in de technologie, processen of in gedrag. We kunnen daarop invloed uitoefenen door het ontwerpen en uitvoeren van risicobeperkende maatregelen.
- Bij **impact** gaat het om de in inbreuk op de informatiebeveiligingsdoelstellingen.

Gezamenlijk vormen de drie categorieën een risicio-scenario.

## *Fontys-bestuurder over informatieveiligheid:*

# *‘Geen zaak van de dienst IT alleen, integendeel’*

**Al voor de hack bij de Universiteit Maastricht stond het thema informatieveiligheid en privacybescherming bij Fontys hoog op de agenda. ‘De complexiteit van onze organisatie speelde hierin een belangrijke rol’, blikt bestuurder Hans Nederlof terug. Hij heeft onder meer ict in zijn portefeuille.**

*‘Vier à vijf jaar geleden hadden we als grote hogeschool nog te maken met een heel versnipperd IT-landschap. Met veel autonomie voor de verschillende opleidingen. We gebruikten bijvoorbeeld meerdere digitale leeromgevingen en ook verschillende systemen voor toetsen. Dat we door deze versnippering wel eens extra kwetsbaar konden zijn op het onderwerp cyberveiligheid, hadden we als bestuur al vrij snel door.’*

### *Planmatige aanpak*

*Reden voor Fontys om rond informatiebeveiliging en privacy in 2017-2018 al een specialistische club op te richten, het Information Security & Privacy (ISP)-Office. ‘Het moet binnen je organisatie ergens samenkomen om te voorkomen dat je afhankelijk wordt van een groepje goedbedoelende eenlingen’, legt de bestuurder uit.*

*‘Centrale facilitering dus, om zo te komen tot een planmatige benadering van cybersecurity. Een roadmap waarin je aangeeft waar je op welk moment wilt staan qua cybervolwassenheid en welke stappen je neemt om dit bereiken’, gaat hij verder.*

### *Volwassenheidsniveau bepalen*

*De basis voor deze roadmap vormde voor Fontys de SURFaudit-benchmark die de hogeschool destijds al deed. 'Waardoor we wisten op welk volwassenheidsniveau we zaten qua informatiebeveiliging en privacybescherming. En niet onbelangrijk: op welke vlakken er voor ons nog serieus werk te doen was', stelt Nederlof. Zaken die het bestuur volgens hem, ook toen al, in alle openheid besprak met de raad van toezicht.*
*'Toen de hack in Maastricht naar buiten kwam, konden wij de raad van toezicht dan ook vrij snel enigszins geruststellen. Zo konden we bijvoorbeeld aangeven dat we met behulp van die roadmap een planmatige verbeteraanpak volgden en in het geval van zo'n ernstig incident konden terugvallen op een expertpartner die binnen vier uur met een heel team op de stoep zou staan.'*

### *Verankering*

*Om aan te geven hoe serieus Fontys het thema neemt, legt Nederlof uit dat de onderwerpen informatiebeveiliging en privacybescherming prominent zijn verankerd in de managementrapportagecyclus van de hogeschool. Zo rapporteren alle (meer dan dertig) instituten en diensten drie keer per jaar over deze thema's aan het bestuur.*

*Terwijl daarbovenop het ISP-Office in een aparte managementrapportage drie keer per jaar direct aan Nederlof rapporteert over de voortgang van de roadmap. En als derde lijn rapporteert dan ook nog de wettelijk verplichte functionaris gegevensbescherming aan het college van bestuur op het vlak van privacy. Fontys heeft in dezen dus gekozen voor het three lines-model van risicomanagement*[8]*.*

*'Informatieveiligheid en privacy begint bij jezelf', benadrukt Nederlof. 'Het is niet iets van een ander of van de dienst IT, zoals vaak wordt gezegd. Nee, de meeste datalekken ontstaan door menselijk falen. Door één individu die onbedoeld iets doms doet. Precies de reden voor ons om álle directeuren te vragen hierop te rapporteren en dit niet een zaak te laten zijn van IT alleen', legt hij die keuze uit.*

### *Advies voor collega's*

*Fontys heeft ook een multidisciplinair team opgericht dat vooral focust op de gedragskant en op dat vlak awareness vergroot, workshops geeft en handreikingen doet. Een belangrijk advies dat Nederlof ook andere bestuurders wil meegeven in hun strijd voor informatieveiligheid.*
*Tot slot benadrukt Nederlof dat het anno nu voor collega-instellingen eenvoudiger is geworden om met het thema aan de slag te gaan. 'Wij moesten destijds nog veel zelf uitvogelen', herinnert hij zich. 'Maar wanneer je nu als organisatie het gevoel hebt dat je achterloopt, is er heel veel kennis en kunde om uit te putten.'*
*'Je kunt dus relatief eenvoudig stappen zetten', stelt de bestuurder. 'Neem het voorbeeld van SURFsoc, waar in principe iedere instelling uit de onderwijs- en onderzoekssector bij kan aansluiten. Een beslissing die je als instelling vandaag nog kunt nemen.'*

*'Wanneer je nu als organisatie het gevoel hebt dat je achterloopt, is er heel veel kennis en kunde om uit te putten'*

## 4.2 Incidenten

In de volgende paragrafen gaan we in op de incidenten van 2022. Eerst beschrijven we het landelijk beeld zoals dat wordt gecommuniceerd door diverse overheidsorganisaties. Daarna gaan we in op het beeld van de sector. Daarbij baseren we ons op drie bronnen: de media, SURFcert en de survey voor dit Cyberdreigingsbeeld.

**Dialoogvragen Incidenten**

- **Welke incidenten zien wij zelf bij onze instelling?**
- **Kan onze instelling tijdig identificeren of er een aanval aan de gang is?**
- **Weten we wat we moeten doen als het toch misgaat?**
- **Kunnen we snel genoeg en voldoende herstellen?**
- **Leren we voldoende van incidenten?**
- **Hebben we genoeg samenwerking en contact met experts wanneer er een incident optreedt?**

### Landelijk beeld

*Volgens de politie*

In 2022 registreerde de politie in Nederland bijna 14.000 meldingen van cybercriminaliteit, een lichte daling van het aantal ten opzichte van een jaar eerder[9]. In een verklaring geeft de politie aan dat de cijfers nog steeds zorgwekkend hoog zijn en dat niet altijd aangifte wordt gedaan omdat organisaties bang zijn voor imagoschade. De impact van cybercriminaliteit blijkt nog steeds enorm en er is toenemende mate sprake van zware, internationaal georganiseerde criminaliteit op dit gebied.

*Volgens de inlichtingendiensten*

In het AIVD-jaarverslag 2022[10] staat dat Nederland voortdurend werd geconfronteerd met digitale aanvallen. De risico's hiervan zijn enorm voor overheid, bedrijven en kennisinstellingen. Spearphishing en supply-chainaanvallen bleven in 2022 vaak voorkomen. Zowel de MIVD als AIVD onderstreept dat statelijke actoren (China, Iran, Noord-Korea en Rusland) actief betrokken zijn bij kennisdiefstal en cyberaanvallen. Deze actoren zijn uit op kennis over hoogwaardige technologie en militaire technologie waarbij via kennisinstellingen, wetenschappers en promovendi kennis wordt vergaard, maar ook via professionele cyberspionagecampagnes[11]. Tenslotte constateert de AIVD een toename van 'living-off-the-land'-aanvallen, waarbij aanvallers legitieme software benutten voor kwaadaardige doeleinden. De AVID ziet ook dat aanvallers steeds vaker misbruik maken van bekende kwetsbaarheden, waardoor tijdige beveiligingsupdates nog belangrijker worden bij het beperken en voorkomen van schade.

*Volgens de NCTV en NCSC*

De Nationaal Coördinator Terrorisme en Veiligheid (NCTV) waarschuwt in zijn Cybersecuritybeeld Nederland van 2022[12] voor de scheefgroei tussen de schaalbaarheid van cyberaanvallen en de weerbaarheid van organisaties. De belangrijkste incidenten betreffen ransomware, zero-day kwetsbaarheden en verstoring van clouddiensten. Aanvallen met gijzelsoftware worden steeds vaker ingezet met dubbele of zelfs drievoudige afpersing. Hierdoor wordt niet alleen de primair getroffen organisatie afgeperst maar ook de klanten, partners of leveranciers daarvan.

Het Nationaal Cyber Security Centrum (NCSC) ziet verder een toename van het aantal zero-day kwetsbaarheden. Misbruik daarvan kan grootschalige impact hebben als de kwetsbaarheid in veelgebruikte software of hardware zit. Ook misbruik van de cloud neemt toe. Clouddiensten zijn de afgelopen jaren cruciaal onderdeel geworden van bedrijfsprocessen. Uitval of verstoring kan grootschalige gevolgen hebben voor Nederlandse organisaties en sectoren.

*Volgens de toezichthouders*

In 2022 hebben verschillende toezichthouders een gezamenlijk beeld opgesteld van hun bevindingen uit cybersecurity-inspecties[13]. Over incidenten schrijven ze dat er geen cybersecurity-incidenten bij toezichthouders zijn gemeld die onder de meldplicht van de Wet beveiliging netwerk- en informatiesystemen (Wbni)[14] vielen. De Autoriteit Persoonsgegevens heeft wel veel meldingen ontvangen, waarover zij rapporteert in de Datalekkenrapportage.

De Autoriteit Persoonsgegevens schrijft hierin onder andere dat ze in 2021 28 cyberaanvallen bij ict-leveranciers heeft gesignaleerd. Deze incidenten hebben impact op tenminste 1.800 klanten van deze ict-leveranciers.

## Sectoraal beeld

*Incidenten in de media*

In 2022 publiceerden de lokale of landelijke media over veertien incidenten bij onderwijs- en onderzoekinstellingen, zie tabel 2. Een hack bij een leverancier van toegangspassen[15] had de grootste impact. Deze hack leidde tot impact bij drie instellingen. Hierbij werden persoonsgegevens van duizenden medewerkers en studenten van meerdere instellingen buitgemaakt en openbaar gemaakt. Niet alleen onze sector maar bijvoorbeeld ook de rijkoverheid werd door deze leveranciershack geraakt. De aanvallers maakten gebruik van gecombineerde technieken.

Tabel 2 **Openbaar gepubliceerde incidenten onderwijs 2022**

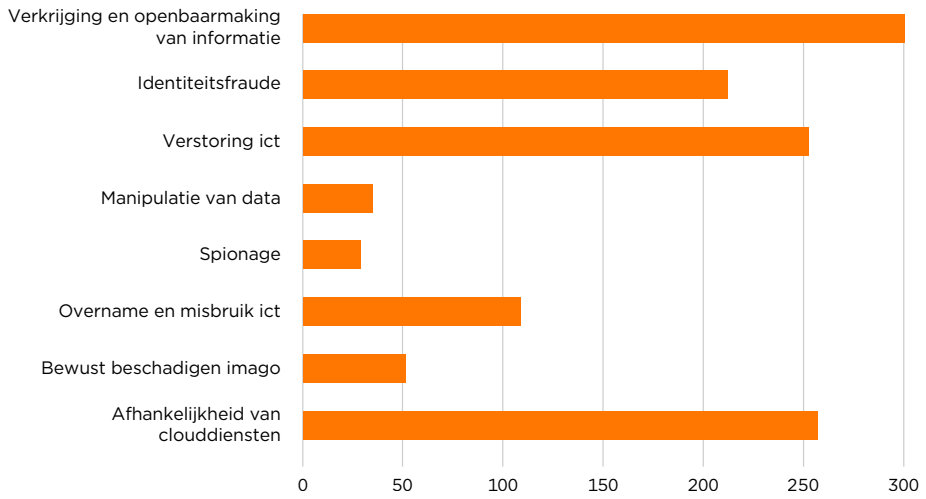
| Datum | Incident | Aantal records/ betrokkenen |
|---|---|---|
| 30-12-2022 | Business Email Compromise (BEC) | onbekend |
| 23-12-2022 | Gijzelsoftware (ransomware) | onbekend |
| 20-12-2022 | Datalek, inbraak of kwetsbaarheid (externe oorzaak) | onbekend |
| 08-12-2022 | (D)DoS-aanval | onbekend |
| 20-10-2022 | Datalek, inbraak of kwetsbaarheid (externe oorzaak) | 5.000 |
| 20-10-2022 | Datalek, inbraak of kwetsbaarheid (externe oorzaak) | 21.000 |
| 15-10-2022 | Datalek, inbraak of kwetsbaarheid (externe oorzaak) | 2.000 |
| 22-09-2022 | AVG compliance issue | onbekend |
| 16-09-2022 | Datalek, verlies of misbruik (interne oorzaak) | onbekend |
| 05-05-2022 | Datalek, verlies of misbruik (interne oorzaak) | 3.500 |
| 29-04-2022 | Datalek, verlies of misbruik (interne oorzaak) | 600 |
| 02-02-2022 | Datalek, inbraak of kwetsbaarheid (externe oorzaak) | 8 |
| 24-01-2022 | Datalek, verlies of misbruik (interne oorzaak) | 1.150 |
| 18-01-2022 | Datalek, verlies of misbruik (interne oorzaak) | 75 |

bron: datalekt.nl

*Inzicht incidenten uit de survey*

Uit onze survey blijkt dat lang niet alle incidenten de media halen. Wij vroegen de respondenten om in grote lijnen en per risicocategorie het aantal mogelijke incidenten in te schatten. De antwoorden van bijna 70 instellingen zijn weergegeven in figuur 5. Uit de antwoorden blijkt dat de meeste incidenten zich hebben voorgedaan binnen de categorieën Verkrijging en openbaarmaking van informatie, Identiteitsfraude, Verstoring ict en Afhankelijkheid van clouddiensten (Ketenafhankelijkheid). Dit sluit aan bij de hoge risicoperceptie van die categorieën. Voor de categorieën Capaciteitstekort en Awareness zijn geen gegevens beschikbaar over 2022 omdat deze categorieën pas naar aanleiding van de survey van dit jaar zijn toegevoegd.

Figuur 5 **Aantal incidenten per risicocategorie uit 2022**




In onze survey hebben we de deelnemers gevraagd naar het incident met de grootste impact op hun instelling in 2022. We waren geïnteresseerd in de oorzaak, gevolgen, impact, geleerde lessen en eventuele informatiedeling met andere instellingen. We ontvingen 36 verhalen over incidenten van 32 instellingen. Daarin zagen we enkele gemeenschappelijke thema's. Zo waren incidenten bij leveranciers, phishing en menselijke fouten de oorzaak van ongeveer 60% van de gerapporteerde incidenten. Leveranciersincidenten vormden de grootste groep, wat overeenkomst met het eerder beschreven beeld door de Autoriteit Persoonsgegevens. Datalekken en ransomware waren de meest voorkomende gevolgen, waarbij de omvang van de datalekken varieerde en ransomware-aanvallen in wisselende mate succesvol waren.

De belangrijkste leereffecten van incidenten zijn volgens de respondenten: procesverbetering, nieuwe afspraken met leveranciers, implementatie van (technische) maatregelen zoals multifactorauthenticatie en netwerksegmentatie, en het opzetten van voorlichtingscampagnes. In de meeste gevallen bleef de communicatie over het incident beperkt tot interne kanalen.

*SURFcert-meldingen*

SURFcert ontvangt meldingen uit verschillende bronnen over (mogelijke) kwetsbaarheden en incidenten. Niet elke melding is altijd een incident met grote schade. Soms gaat het om een melding over een verouderd certificaat of een poort die open staat. Andere keren gaat het wel daadwerkelijk om een incident met impact, zoals bijvoorbeeld een besmetting met malware. SURFcert geeft relevante incidentmeldingen snel door aan de betreffende instelling, zodat zij maatregelen kunnen treffen. Tabel 3 geeft het aantal meldingen per incidentcategorie in 2022. Het aantal meldingen is gestegen ten opzichte van vorig jaar. De stijging zit vooral in het aantal meldingen over kwetsbare systemen. Dat heeft impact op de benodigde capaciteit bij instellingen om tijdig maatregelen te kunnen treffen.

Tabel 3 **SURFcert-meldingen 2021-2022**

| Categorie (op basis van ENISA incident taxonomie[17]) | 2021 | 2022 | |
|---|---|---|---|
| **Malicious code** (software die opzettelijk in een systeem wordt ingevoegd om schade aan te richten) | 474 | 380 | ↓ |
| **Intrusion attemps** (poging om een systeem te compromitteren of een dienst te verstoren door kwetsbaarheden te misbruiken) | 48 | 33 | ↓ |
| **Spam** (ongewenste bulk-e-mail) | 14 | 22 | ↑ |
| **Fraud** (middelen gebruiken voor ongeautoriseerde doeleinden) | 9 | 1 | ↓ |
| **Abusive content** (bedreiging of discriminatie van personen, geweld) | 13 | 4 | ↓ |
| **Availability** (systeemcrashes of vertragingen) | 407 | 183 | ↓ |
| **Vulnerable** (systemen die openstaan voor misbruik) | 891 | 1741 | ↑ |
| **Information gathering** (pogingen om zwakke punten te ontdekken, netwerkverkeer af te luisteren en vast te leggen, of social engineering) | 0 | 3 | ↑ |
| **Intrusions** (geslaagde compromittering van een systeem of applicatie) | 0 | 20 | ↑ |
| **Information content security** (ongeautoriseerde toegang of wijziging) | 0 | 1 | ↑ |
| **Totaal** | **1862** | **2402** | |

*DDoS-aanvallen*

DDoS-aanvallen blijven een probleem, vanwege veranderende methoden en aanvalspatronen. In 2022 nam SURFcert minder volumetrische DDoS-aanvallen waar; dit zijn aanvallen waarbij een doel overspoeld wordt met een grote hoeveelheid verkeer. De daling kan worden toegeschreven aan twee factoren. Ten eerste was er in voorgaande jaren een buitengewoon grote piek in dergelijke aanvallen, grotendeels veroorzaakt door activisme in de context van de Covid-19 situatie. Dit hoge niveau was dus niet de norm en de daling kan deels worden gezien als een terugkeer naar normale niveaus. Ten tweede heeft de verschuiving naar het gebruik van clouddiensten ook bijgedragen aan de daling, aangezien incidenten die gericht zijn tegen een doel buiten het netwerk van SURF niet meer worden waargenomen door SURFcert. Zowel sectoraal als nationaal werden minder DDoS-aanvallen waargenomen[16], maar het aantal bleef aanzienlijk, vooral tijdens tentamenweken. Waakzaamheid blijft geboden, doordat aanvallers steeds andere technieken gebruiken. Momenteel zien we bijvoorbeeld een stijging van het aantal aanvallen die gericht zijn op DNS-servers.

*IPv6*

Tenslotte richten criminelen zich tegenwoordig niet alleen op IPv4 maar ook op IPv6. Veel organisaties die IPv6 gebruiken, zijn zich er niet van bewust dat ze hiervoor ook adequate beveiliging moeten inrichten. Hierdoor heeft SURFcert veel incidentmeldingen moeten uitsturen. Het is essentieel dat IT-medewerkers goed worden getraind in nieuwe versies van systemen of protocollen om beveiligingsproblemen te voorkomen.

# *OZON laat je een cybercrisis ‘met elkaar doorleven’*

**Zo’n zeventig onderwijs- en onderzoeksinstellingen werden afgelopen maart overvallen door een reeks van cyberaanvallen. Niet in de echte wereld, maar wel heel realistisch tijdens OZON, de tweejaarlijkse grote cybercrisisoefening voor de onderwijs- en onderzoekssector.**

*Deelnemers kregen bijvoorbeeld te maken met een aanval op het inschrijfsysteem of het inlogsysteem, bij andere instellingen viel het netwerk uit. Problemen die werden veroorzaakt door een eigen medewerker die ook voor een criminele organisatie bleek te werken, een insider threat.*

*Daarnaast openbaarde een groep activisten op dezelfde dag elke twintig minuten een zero day vulnerability: een nieuwe kwetsbaarheid die nog niet gepatcht kan worden. ‘Een ongeluk komt immers nooit alleen’, stelt Charlie van Genuchten, projectleider OZON bij SURF.*

### *Belang: je zeker voelen*

*Dit keer namen er zo’n zeventig onderwijs- en onderzoeksinstellingen, ketenpartners en koepelorganisaties deel aan de oefening. Het hoogste aantal sinds de eerste oefening in 2016. ‘Het gaat me echter niet om het aantal deelnemers’, benadrukt Van Genuchten. ‘Ik vind het belangrijk dat iedere organisatie de basis voor crisismanagement, inclusief cybercrisismanagement, heeft staan. En dat een instelling zich zeker voelt over de eigen crisisprocedures.’*

*Voorwaarden die je volgens haar creëert door te oefenen én te evalueren. Om te weten wat er op je afkomt tijdens een cybercrisis, moet je zo’n crisis in haar woorden ‘met elkaar doorleven’. ‘Zodat iedereen weet wat er van hem of haar wordt verwacht op het moment dat het misgaat. Goed voor de bewustwording en het versterkt de weerbaarheid.’*

*Wie doen er mee?*

*Gemiddeld nemen organisaties met zo'n dertig mensen deel aan de oefening, maar dat aantal kan oplopen tot wel honderd. Het belangrijkste is volgens Van Genuchten dat je met de hele keten ervaring opdoet. Op operationeel, strategisch en tactisch niveau.*

*'Dat betekent dat organisaties niet alleen IT'ers en leden van het centraal Crisis Management Team mee laten doen, maar juist ook mensen van de afdeling communicatie en in het geval van onderwijsinstellingen de studentenadministratie bijvoorbeeld. Collega's die bepaalde crisisprocedures waarschijnlijk niet zo vaak met elkaar bespreken', legt ze uit.*

*Gezamenlijke afstemming steeds beter*

*Wat Van Genuchten tijdens de afgelopen OZON is opgevallen, is dat het delen van informatie tussen organisaties steeds beter gaat. Zo was er bijvoorbeeld een deelnemer die nog voor het einde van de oefening precies op een rijtje had gezet wat zij als organisatie allemaal hadden gedaan. Informatie die ze met alle deelnemers hebben gedeeld. 'Superwaardevol, omdat er zo voor alle deelnemers een checklist ontstaat.'*

## *'Deelnemers worden steeds fanatieker, ze willen de oefening te slim af zijn'*

*'Ook was er op operationeel en op strategisch niveau meer dan voorheen contact met bijvoorbeeld ketenpartners en koepelorganisaties', geeft ze aan. 'Met als concreet resultaat dat er een aantal gezamenlijke persberichten naar buiten is gebracht.'*

*'Het besef dat we bij een crisis móeten samenwerken, is voor iedereen duidelijk', concludeert ze. 'Dit hebben we niet alleen via OZON geleerd, maar het is recent ook gebleken in de echte wereld. Denk aan de uitbraak van de coronapandemie. Toen hebben we ook sámen bepaalde structuren moeten opbouwen.'*

*De crisiskoffer!?*

*Tot slot vond Van Genuchten het heel leuk dat OZON-deelnemers steeds fanatieker worden. 'Ze willen de oefening te slim af zijn', lacht ze. 'Zo ontstaan er al in de aanloop naar OZON allerlei appgroepjes. Mensen bedenken dus van tevoren wie er in hun netwerk zit en wie ze denken nodig te hebben.'*

*'Dat is mooi, want het feit dat deelnemers hierover nadenken helpt hen ook in het geval van een echte crisis. Zoals dat ook geldt voor de naarstige zoektocht naar de crisiskoffer, waar in verschillende appgroepen over werd gesproken. Of de vraag of het crisishandboek ook ergens offline te vinden is ...'*

## 4.3 Weerbaarheid

SURF en de leden hebben nog niet voldoende meetinstrumenten om cyberweerbaarheid goed te meten, dus we kunnen nog geen volledige uitspraak doen over de weerbaarheid van de sector. Daarom richt dit deel van het hoofdstuk zich op de metingen die we wel hebben en op een zelfevaluatie door de respondenten van de survey. Voor de categorie mensen hebben we de awarenessmetingen, voor processen hebben we de benchmark, en voor technologie hebben we internetveiligheidmetingen.

**Over weerbaarheid**
Weerbaarheid is het vermogen om incidenten te voorkomen. Daarbij draait het om risicogebaseerd werken en om het treffen van passende maatregelen in drie hoofdcomponenten: mensen, processen en technologie.

**Mensen** zoals medewerkers, studenten en inhuurkrachten spelen een cruciale rol, aangezien zij vaak het doelwit zijn van cyberaanvallen. Daarom is training en bewustwording essentieel.

**Processen** omvatten de formele en informele procedures, richtlijnen en werkwijzen die binnen een organisatie worden gevolgd om informatie te beheren, te beschermen en te onderhouden.

**Technologie** bestaat uit de hardware, software en (netwerk)infrastructuur die worden gebruikt om informatie te creëren, op te slaan, te verwerken en te communiceren.

*Zelfevaluatie weerbaarheid*
De respondenten hebben een matig vertrouwen in de weerbaarheid van hun instelling. Wij vroegen de respondenten om rapportcijfers te geven (waarbij het cijfer 10 het hoogst haalbare is) over de weerbaarheid van de kroonjuwelen: de te beschermen systemen, data, processen en mensen.

Tabel 4 **Perceptie van respondenten over weerbaarheid van hun instelling**

| Onderdeel | Eigen inschatting |
|---|---|
| De algemene indruk over de weerbaarheid van de instelling | 6 |
| De mate waarin er een actueel overzicht is van de kroonjuwelen | 5 |
| De mate waarin de beschikbaarheid, integriteit en vertrouwelijkheid van de kroonjuwelen op een passend niveau zijn beschermd | 5 |
| De mate waarin de kroonjuwelen worden gemonitord op mogelijke inbreuken | 5 |

*Volwassenheid op het SURFaudit toetsingskader informatiebeveiliging*
Periodiek nemen diverse instellingen deel aan de SURFaudit-benchmark op het SURFaudit Toetsingskader Informatiebeveiliging. Hiermee kunnen zij vergelijken waar zij staan ten opzichte van andere instellingen binnen de sector. Het gemiddelde van de sector lag in 2021 (de meest recente uitvoering van de benchmark) nog niet op het geambieerde gemiddelde niveau 3, zie tabel 5. Er is ten opzichte van 2019 een lichte teruggang te zien van de gemiddelden per domein. Een van de oorzaken daarvan is dat een deel van de audits in 2021 werden uitgevoerd door externe auditors, wat tot lagere scores leidt dan de zelf uitgevoerde assessments in 2019. Een andere oorzaak is dat relatief veel instellingen voor het eerst meededen in 2021.

Tabel 5 **Volwassenheidsscores SURFaudit-benchmark in 2019 en 2021**

| Domein | Sectorgemiddelde 2019 (35 deelnemers) | Sectorgemiddelde 2021 (51 deelnemers) | |
|---|---|---|---|
| Governance | 2,4 | 2,3 | ↓ |
| Organisatie | 2,3 | 2,3 | ↔ |
| Risicobeheer | 1,8 | 1,8 | ↔ |
| Personeelsbeheer | 2,3 | 2,3 | ↔ |
| Configuratiebeheer | 2,3 | 2,2 | ↓ |
| Incident-/probleembeheer | 2,6 | 2,4 | ↓ |
| Wijzigingsbeheer | 2,2 | 2,1 | ↓ |
| Systeemontwikkeling | 2,0 | 1,9 | ↓ |
| Gegevensbeheer | 2,2 | 2,0 | ↓ |
| Identiteits- en toegangsbeheer | 2,1 | 1,9 | ↓ |
| Beveiligingsbeheer | 2,2 | 2,2 | ↔ |
| Fysieke beveiliging | 2,5 | 2,4 | ↓ |
| IT-operatie | 2,7 | 2,3 | ↓ |
| Bedrijfscontinuïteitsbeheer | 2,4 | 2,2 | ↓ |
| Ketenbeheer | 2,3 | 2,2 | ↓ |
| **Gemiddelde van alle domeinen** | **2,3** | **2,2** | |

**Opmerkingen bij tabel 5**
- We houden de sectorbrede SURFaudit-benchmark eens in de twee jaar, vandaar dat de meest recente resultaten uit 2021 komen. Volgend jaar publiceren we de resultaten over 2023.
- Tot nu toe deden alleen instellingen in het hoger onderwijs mee aan de SURFaudit-benchmark. Vanaf 2023 doet ook de mbo-sector mee. De resultaten van de laatste mbo-specifieke benchmark vind je in het rapport Benchmark IBP-E 2021[18].

*Adoptie van informatieveiligheidsstandaarden*

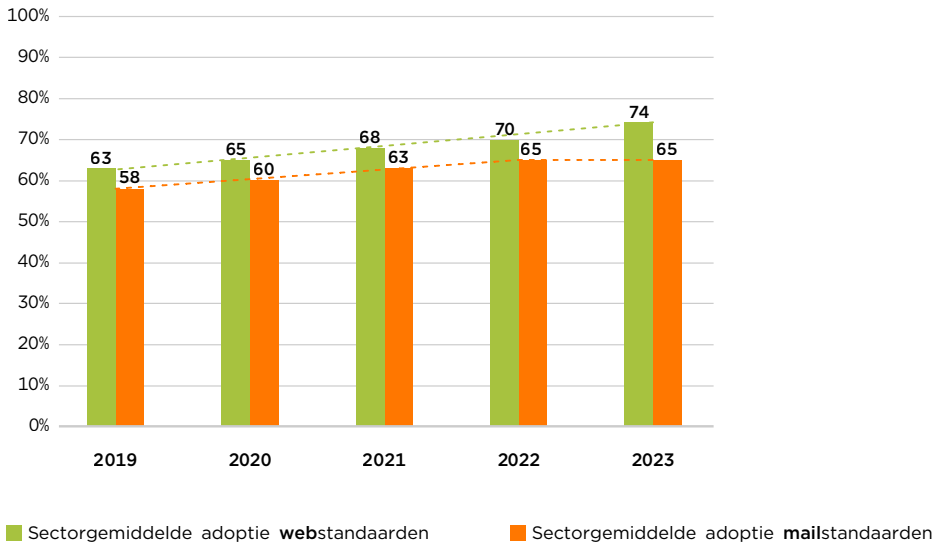
Het Forum Standaardisatie[19] adviseert de publieke sector over het gebruik van open standaarden voor internetveiligheid. Dit zijn breed gedragen afspraken over de manier waarop gegevens worden uitgewisseld. De afspraken omvatten web- en mailbeveiligingsprotocollen om de veiligheid en integriteit van de communicatie van gebruikers te waarborgen, wat ook bijdraagt aan hun privacy-bescherming. Als SURF stimuleren we het gebruik van deze standaarden. Elke organisatie kan zelf haar scores controleren[20] maar SURF meet ook ieder kwartaal[21] in hoeverre instellingen de standaarden hebben geïmplementeerd.

Het laatste jaar wordt er matig vooruitgang geboekt, zie figuur 6. Dit komt deels doordat instellingen afhankelijk zijn van leveranciers die ook hun bijdrage moeten leveren, maar ook doordat ze onvoldoende specifieke kennis hebben en er niet voldoende prioriteit aan geven. Eén op de drie instellingen in onze sector heeft de mailstandaarden niet volledig geïmplementeerd en één op de vier heeft de webstandaarden niet volledig geïmplementeerd. Bovendien onderschatten deze cijfers het werkelijke probleem aanzienlijk. De metingen van SURF richten zich immers op de hoofddomeinen van de instellingen. In de praktijk hebben instellingen echter tientallen, zo niet honderden domeinen waarvan de beveiligingsprotocollen mogelijk nog niet op het vereiste niveau zijn.

**Dialoogvragen Weerbaarheid**

- **Hebben we voldoende in kaart wat onze kroonjuwelen zijn en wie de eigenaren zijn?**
- **Meten we hoe we ervoor staan?**
- **Zijn we in staat de juiste beheersmaatregelen af te wegen?**
- **Voldoen we aan compliance-eisen zoals het volwassenheidsniveau van 3 op het SURFaudit toetsingskader informatiebeveiliging, AVG of de aanbevolen standaarden voor internetveiligheid?**

Figuur 6 **Adoptie e-mail- en webstandaarden voor de hoofddomeinen van de sector onderwijs en onderzoek**




*Awarenessmeting*

BDO heeft in 2022 in opdracht van SURF bij 26 instellingen een security- en privacy-awarenessmeting gedaan[22]. De awareness van de deelnemende medewerkers blijkt vergelijkbaar te zijn. De gemiddelde score is 5,9, terwijl 7 of hoger voldoende is om privacybewust en informatieveilig te werken. Er is dus nog enige verbetering nodig.

Opvallend is dat docenten en onderzoekers achterblijven bij medewerkers in ondersteunende functies, zowel in deelname aan deze meting als in resultaten. Dit zou door de hoge werkdruk kunnen komen. Een andere oorzaak kan zijn dat de werksituatie, vooral bij onderzoekers, minder eenduidig is te vatten in een set regels of richtlijnen. Onderzoekers werken vaak in instellingsoverstijgende samenwerkingsverbanden, die bijvoorbeeld software gebruiken die niet toegestaan is volgens de richtlijnen van de eigen instelling.

## 4.4 Conclusie

### Risicobeheer nog weinig toegepast

Nog heel weinig instellingen hebben risicobeheer opgenomen in hun plannings- en controlcyclus. Functionarissen die risico-eigenaren moeten ondersteunen zijn vaak nog niet goed in positie gebracht en worden gehinderd door capaciteitsproblemen. Toch zien we dat bestuurders steeds meer betrokken zijn en worden in de hele sector verbeterprogramma's uitgevoerd.

### Risico's en dreigingen zijn permanent aanwezig en weerbaarheid blijft aandachtspunt

De risico's en dreigingen die we voorgaande jaren zagen zijn nog steeds relevant. Daarnaast zijn instellingen bezorgd over gebrek aan bewustzijn en onveilig gedrag binnen instellingen. De metingen die SURF uitvoert op procesvolwassenheid, internetveiligheid en awareness laten zien dat dit aandachtspunten zijn. Bovendien loopt het aantal incidenten op en aanvalsmethoden ontwikkelen zich sneller dan de weerbaarheid van instellingen.

### Informatie over incidenten delen

Dat in 2022 relatief weinig incidenten de media haalden betekent niet dat ze er niet zijn. We moeten binnen de sector informatie blijven delen over incidenten. Een incident bij de een leidt bijna altijd tot vragen of zelfs een incident bij een andere instelling of partnerorganisatie. Alleen als we de handen ineenslaan kunnen we het hele ecosysteem van onze sector weerbaar maken.

# Zo werkt de mbo-sector aan cyberweerbaarheid: boven alles sámen

**Controle en logging, maar ook leveranciersmanagement. Dat zijn volgens Martijn Bijleveld, adviseur informatiebeveiliging en privacy binnen MBO Digitaal, de belangrijkste uitdagingen op het gebied van cyberveiligheid voor mbo-instellingen.**

*'We benchmarken binnen het mbo al sinds 2015 op het gebied van informatiebeveiliging en privacy. We weten dus heel goed waar onze risico's liggen en deze aandachtspunten komen steeds weer terug', stelt hij.*

*Programma Cyberveiligheid mbo*

*Tot voor kort had de mbo-sector niet de noodzakelijke, centrale beschikking over middelen om de problemen op te lossen. Sinds oktober vorig jaar is daar verandering in gekomen, met de start van het programma Cyberveiligheid mbo. Met goedkeuring van het programma door de MBO Raad en het ministerie van OCW kwam er namelijk ook een subsidie van in totaal 24 miljoen euro voor vijf jaar. Om daarmee de digitale weerbaarheid van mbo-instellingen te vergroten.*

*'Dat laatste lukt alleen door samen te werken en dat weten we binnen het mbo allang', stelt Bijleveld. 'Je zit in een wedloop met cybercriminelen en die kun je als individuele instelling niet winnen.' Precies de reden waarom het programma Cyberveiligheid mbo in zijn woorden 'samenwerking ademt'. 'We doen het niet voor, maar mét alle 55 mbo-instellingen en daar ben ik als programmamanager supertrots op.'*

*‘Je zit in een wedloop met cybercriminelen en die kun je als individuele instelling niet winnen’*

### *Meteen stappen gezet*

*Een van de eerste zaken die binnen het programma is opgepakt, is het probleem van de logging. Zo is vrijwel meteen besloten dat MBO Digitaal vanuit de subsidie voortaan de kosten vergoedt voor de aansluiting van mbo’s bij SURFsoc. ‘We merkten dat de financiële drempel hiervoor voor mbo-instellingen vrij hoog was’, legt Bijleveld uit. ‘Een hobbel die we op deze manier hebben weggenomen. Met succes, want inmiddels zit een groot aantal mbo’s in het implementatietraject of bereiden ze dit voor.’ Ook op het leveranciersmanagement is meteen doorgepakt. ‘Alle eisen die wij ons als mbo’s opleggen, gelden ook voor onze (cloud)leveranciers. Zij vormen dus een risico’, licht de programmamanager toe. ‘We zijn daarom gestart met de centrale beoordeling van verwerkersovereenkomsten van applicaties die veel in het mbo worden gebruikt.’*

*Het gaat daarbij vooral om de beoordeling van de gegeven veiligheids-waarborgen, waarbij je ook de werking ervan wilt kunnen controleren aan de hand van DPIA’s, audits en pentests. De eerste DPIA’s zijn al uitgevoerd en hier zal de mbo-sector volgens Bijleveld de komende jaren fors verder op inzetten. Zodra de ‘compliancedienst’ van SURF beschikbaar is, sluit de sector hier daarom bij aan. Waarbij de ledenbijdrage voor deze dienst vanuit de subsidie wordt vergoed.*

### *Hoog ambitieniveau*

*Allemaal met als doel om over vijf jaar als mbo-sector cyberweerbaar te zijn. Wat vanuit OCW betekent dat een instelling een gemiddelde volwassenheids-score van 3 op het nieuwe SURFaudit Toetsingskader Informatiebeveiliging moet scoren. ‘Maar als mbo-sector ligt ons ambitieniveau met een gewenste score van 3,3 zelfs nog iets hoger’, weet Bijleveld op basis van een nulmeting bij de start van het programma.*

*Waarbij je volgens hem niet genoeg kunt benadrukken dat het scoren van je volwassenheid geen doel op zich moet zijn, maar veel meer een resultaat van een risicogebaseerde afweging van maatregelen. Voor MBO Digitaal aanleiding om samen met SURF een aanbestedingstraject te starten voor de aanschaf van een mbo-brede Governance Risk & Compliance (GRC)-applicatie. Tooling die volgens Bijleveld in het najaar beschikbaar zal komen.*

### *Uitdaging*

*Snelle stappen dus als je het hem vraagt. ‘En daar zit meteen een risico’, realiseert de programmamanager zich. ‘We lopen hard, maar alle 55 instellingen moeten het wel bij kunnen houden. Dat vraagt om goede communicatie en community-building vanuit het programmateam van MBO Digitaal.’*

*Precies de reden waarom MBO Digitaal momenteel hard op zoek is naar de juiste beleidsadviseurs en communicatieprofessionals om dit proces te stroomlijnen. Gezien de huidige krappe arbeidsmarkt volgens Bijleveld ‘misschien wel de belangrijkste uitdaging van dit moment’.*

# 5 HANDELINGS- EN TOEKOMSTPERSPECTIEF

In dit hoofdstuk kijken we vooruit. We bieden handelingsperspectieven voor de korte termijn en we gaan in op vraagstukken van de toekomst.

## 5.1 Handelingsperspectief: op weg naar weerbaarheid

**Zorg dat de basis op orde is**

*Technische basismaatregelen implementeren*
Voer technische basismaatregelen door, zoals multifactorauthenticatie en het maken en testen van back-ups. Het Nationaal Cyber Security Centrum (NCSC) adviseert acht basismaatregelen te implementeren: de minimale maatregelen die elke organisatie op orde moet hebben[23]. Met dergelijke basismaatregelen kan een organisatie de meeste cyberaanvallen afweren.

Microsoft's Digital Defense Report 2022[24] stelt dat 98% van de aanvallen voorkomen kunnen worden door:
- Multifactorauthenticatie
- Toepassen van zero trust-principes
- Het gebruik van detectie- en anti-malware systemen
- Tijdig patchen
- Implementatie van gegevensbeschermingcontrols

*Aandacht voor veilig gedrag en kennisvergroting*
Er moet permanente aandacht zijn voor veilig gedrag en het vergroten van kennis van medewerkers en studenten. Het is belangrijk om structureel te investeren in voorlichting, training en duidelijke procedures voor vragen en voor het melden van incidenten. Beleg de verantwoordelijkheid voor awareness breed in de organisatie. Bijvoorbeeld door iets te organiseren voor studenten of onderzoeksgroepen die met dit onderwerp bezig zijn. Hoe breder dit onderwerp gedragen wordt, des te groter het effect op de weerbaarheid van de instelling. Medewerkers hebben daarnaast behoefte aan korte en bondige richtlijnen, opgesteld in heldere taal en makkelijk te vinden.

*Promoot aantrekkelijke werkomgeving*
Het capaciteitstekort voor informatiebeveiligings- en privacyprofessionals is niet uniek voor onze sector. Dat in heel Nederland vacatures lastig zijn te vervullen heeft niet alleen te maken met het tekort aan talent: organisaties kunnen zelf ook meer doen om het wervingsproces te verbeteren, een aantrekkelijke werkgever te zijn en de medewerkers die al in dienst zijn te ontwikkelen en te behouden[25]. Daarbij helpen marktconforme arbeidsvoorwaarden, permanente educatie, professionele certificeringen en het uitwerken van carrièrepaden met behulp van competentieprofielen.

**Richt governance, risicobeheer en compliance in**

*Risicogebaseerd werken*
Organisaties die voldoende weerbaar zijn, werken risicogebaseerd[26].
Om op volwassenheidsniveau 3 te komen voor het domein risicobeheer uit de SURFaudit-benchmark, moeten instellingen het volgende inrichten:
- Risicoanalyses hebben een centrale plek en gestructureerde aanpak in de primaire processen[27].
- Het beleid moet alle relevante elementen van risicobeheer bevatten zoals risicobereidheid, eigenaarschap, risicoproces en het bepalen, mitigeren en accepteren van risico's.
- Het senior management is eigenaar van risico's en bijbehorende actieplannen[28].

Instellingen die in 2024 via de Wet beveiliging netwerk- en informatiesystemen (Wbni) onder de NIS 2-richtlijn gaan vallen, kunnen overwegen om hun bestuursleden en medewerkers alvast laten deelnemen aan een opleiding. Dit staat beschreven in artikel 20, lid 2 van de NIS 2-richtlijn[29]. Op die manier kunnen zij voldoende kennis en vaardigheden verwerven om risico's te kunnen identificeren en risicobeheerspraktijken op het gebied van cyberbeveiliging te kunnen beoordelen. Daarnaast is het verstandig om alvast budget en capaciteit te reserveren om evenuele extra inspanningen uit te voeren die de Wbni mogelijk

gaat vereisen. SURF houdt informatie over de NIS 2-richtlijn bij op een FAQ pagina waar leden de laatste ontwikkelingen in de gaten kunnen houden[30].

### Capaciteit effectief gebruiken

Om efficiënt gebruik te maken van de schaarse capaciteit, kunnen veiligheids-functionarissen binnen organisaties de samenwerking versterken en proces-eigenaren ondersteunen. Organiseer bijvoorbeeld informatiebeveiliging integraal met andere veiligheidsgebieden zoals in de toolkit voor integrale veiligheid[31]. Met name in de gebieden beleid, risicobeheersysteem en rapportage processen kan samenwerking leiden tot efficiënter gebruik van mensen en middelen.

### Weet hoe je ervoor staat

Er bestaan diverse indicatoren om inzicht te krijgen in weerbaarheid[32, 33]. Een paar voorbeelden daarvan staan in tabel 6. Het meten van de weerbaarheid van processen, technologie en mensen vereist een combinatie van meet-instrumenten die elk inzicht geven in een deelgebied. De bekende SURFaudit benchmark meet hoofdzakelijk de volwassenheid van informatiebeveiligings-processen, evenals de mate van integratie van informatiebeveiliging in de overkoepelende bedrijfsprocessen. Door deelname aan OZON meet je of het businesscalamiteitenplan en/of het crisismanagementteam goed functioneert. Maar aanvullend op business continuity is het raadzaam om ook op regelmatige basis de back-ups en recovery te testen.

Tabel 6 **Overzicht voorbeelden van meetinstrumenten van weerbaarheid**

| Instrument | Meet processen? | Meet technologie? | Meet mensen (kennis en gedrag)? |
|---|---|---|---|
| SURFaudit (externe) assessment | Ja | Deels | Deels |
| Compliance aan wet- en regelgeving | Ja | Deels | Deels |
| Crisisoefeningen (zoals OZON) | Deels | Deels | Ja |
| SOC/SIEM | Deels | Ja | Deels |
| Back-up/recovery test | Ja | Ja | Nee |
| Coordinated Vulnerability Disclosurebeleid (zoals SURF HALON) | Deels | Ja | Deels |
| Red Teaming | Deels | Ja | Deels |
| (SURF) awarenessmeting | Deels | Nee | Ja |
| Periodieke risicobeoordelingen | Ja | Deels | Deels |
| Incident response KPI's, bijvoorbeeld, Mean Time To Detect, Mean Time To Response, Recovery Point Objective en Recovery Time Objective | Deels | Deels | Deels |
| Percentage IT-middelen waarop geautomatiseerde scans van kwetsbaarheden zijn uitgevoerd en middelen die zijn vrijgesteld van ernstige kwetsbaarheden | Deels | Ja | Deels |
| Internetveiligheidsmetingen | Deels | Ja | Nee |

SURF ontwikkelt samen met de sector nieuwe meetinstrumenten. Zo brengen we in 2023 een privacy toetsingskader uit voor de bescherming van persoonsgegevens. Daarnaast werken we aan een weerbaarheidsdienst om de doeltreffendheid van technische beveiligingsmaatregelen te toetsen en een leveranciers compliancy-dienstverlening om te garanderen dat de diensten en producten van onze leveranciers voldoen aan de gestelde eisen op het gebied van informatiebeveiliging en privacy.

**Deel kennis en informatie**

Instellingen kunnen zich via SURF aanmelden voor diverse informatiebeveiligings- en privacy-community's, zoals SCIPR en SCIRT, om op de hoogte te blijven en om kennis te delen over activiteiten die bij de eigen instelling goed werken.

Registreer incidenten en deel informatie met SURFcert en andere instellingen. Door elkaar te waarschuwen worden incidenten voorkomen en komt hulp sneller op gang. Cyberschaamte, het cybersecuritywoord van het jaar 2022[34], is niet nodig: incidenten komen overal voor en je staat er als instelling niet alleen voor. Een van de respondenten beschreef in de survey dat door het snel delen van informatie over een incident in hun instelling, een andere instelling op tijd kon ingrijpen en het ergste heeft kunnen voorkomen. Dat is precies het doel van het delen van informatie over incidenten. Daarnaast kunnen we door het delen van data beter inzicht krijgen in de aard en omvang van incidenten in de sector. Daardoor kunnen we gerichte maatregelen nemen en de weerbaarheid vergroten.

## 5.2 Toekomstperspectief

**Inspelen op snelle ontwikkelingen**

Het cyberdreigingsbeeld is traditioneel een samenvatting van de inzichten van het afgelopen jaar. Kennis van het recente verleden is een belangrijk element voor het plannen van acties op korte termijn. Maar we moeten ook over de toekomst nadenken: technologische ontwikkelingen gaan snel en daar moeten we op inspelen. Hoe snel de ontwikkelingen gaan, blijkt bijvoorbeeld uit de open brief van een aantal prominenten[35] waarin zij ervoor pleiten om grote AI-ontwikkelingen tijdelijk te stoppen, totdat de risico's voldoende beheersbaar zijn. Aan wet- en regelgeving op dat vlak wordt momenteel wel gewerkt, maar dat verloopt langzamer dan de ontwikkeling van de technologie. We moeten dus nu zelf actie nemen om keuzes te maken hoe we ermee willen omgaan.

**Nieuwe technologie biedt kansen maar leidt tot zorgen**

Momenteel zien we zorgen binnen de privacy- en cybersecuritycommunity's over makkelijk toegankelijke taalmodellen zoals ChatGPT. Er wordt bijvoorbeeld gesproken over het verzamelen en verwijderen van persoonsgegevens, de mogelijkheden die ChatGPT biedt voor het verbeteren van teksten van phishingmails, en het genereren van programmacode (malware) of het verbeteren van social-engineeringmethodes. Door de ontwikkelingen op het gebied van generative AI in tekst, beeld en spraak zijn er grote zorgen over de impact van deepfakes op sociale veiligheid. Een ander voorbeeld zien we bij projecten met extended reality. Daar zijn veel vraagstukken met betrekking tot privacy en security. Bij veel projecten worden privacy- en security officers niet (tijdig) betrokken.

Daartegenover staan mogelijkheden om arbeidsintensieve processen voor security officers te verlichten, zoals het trainen van spam- en phishingfilters, het vinden van oplossingen voor malware, snelle toegang tot kennis, of het schrijven van documenten.

**SURF Tech Trendrapport**

In februari 2023 heeft SURF een rapport gepubliceerd over de trends binnen zes belangrijke technologieën voor onderwijs en onderzoek[36]. Het rapport is een startpunt voor instellingen om het gesprek aan te gaan over de strategie van de toekomst, keuzes te maken op welke trends de focus moet liggen en deze uit te werken in mogelijke scenario's. Tijdens die gesprekken kun je het volgende dialoogkaartje gebruiken om in je eigen instelling de relevante vraagstukken rondom informatiebeveiliging en privacy te bespreken.

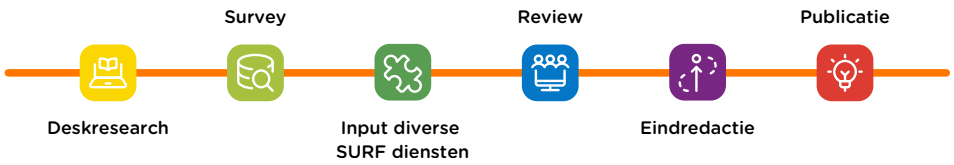
## Dialoogvragen Toekomstperspectief

- Hebben we de expertise in huis om trends te signaleren en te duiden?
- Houden we in onze strategie voldoende rekening met gevolgen van innovatie voor informatieveiligheid?
- Is onze enterprise architectuur klaar voor nieuwe ontwikkelingen?
- Zijn huidige normen- en toetsingskaders geschikt voor nieuwe technologie?
- Welke scenario's kunnen ontstaan?
- Kan nieuwe technologie de weerbaarheid versterken en de werkdruk van cybersecurity analisten verlichten?
- Gaan aanvalsmethoden veranderen?
- Neemt ketenafhankelijkheid toe?
- Welke dilemma's zien we over surveillance, privacy, ethiek, controleerbaarheid, best practices, sociale normen, sociale veiligheid, regelgeving, toezicht?
- Hoe beschermen we onze nieuwe technologie en algoritmes, en de kennis daarover, als kroonjuwelen?

# BIJLAGE 1 **TOTSTANDKOMING EN METHODE**

Het cyberdreigingsbeeld is een samenvatting van kennis die we gedurende het hele jaar opbouwen. We houden daarvoor relevante publicaties bij, bijvoorbeeld die van internationale kennisorganisaties, de Rijksoverheid, de onderwijskoepels, openbare bronnen over incidenten, en dreigingsbeelden uit andere sectoren. Met die publicaties schetsen we de context en de omgeving waarin wij ons bevinden.

Figuur 7 **Totstandkoming Cyberdreigingsbeeld 2023**




Naast de deskresearch gebruiken we data uit diverse bronnen:

- **Survey**

In januari 2023 hebben we een survey uitgezet onder de SURF-leden met vragen over governance, risico's, incidenten en weerbaarheid. De survey is ingevuld door 87 personen uit 69 instellingen. De respondenten bestonden voornamelijk uit CIO's en IT-directeuren, CISO's, IT-managers, ISO's, IBP-adviseurs, en een aantal IT-auditors en FG's.

| Respondenten per sector | Aantal instellingen | Aantal respondenten |
|---|---|---|
| Wo | 11 | 18 |
| Hbo | 22 | 24 |
| Mbo | 32 | 40 |
| Umc | 2 | 2 |
| Research & overige | 2 | 3 |
| **Totaal** | **69** | **87** |

Respondenten konden zelf bepalen voor welke primaire processen ze de vragenlijst wilden invullen.

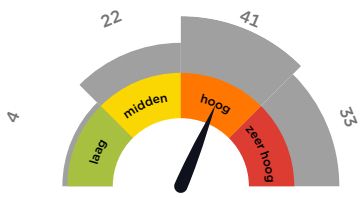
| Aantal vragenlijsten ingevuld over processen | |
|---|---|
| Onderwijs | 83 |
| Onderzoek | 42 |
| Bedrijfsvoering | 70 |

- **Awarenessmeting**
- **De geaggregeerde resultaten van de SURFaudit-benchmark**
- **Internetveiligheidsmetingen**
- **Gesprekken met experts binnen en buiten de sector**

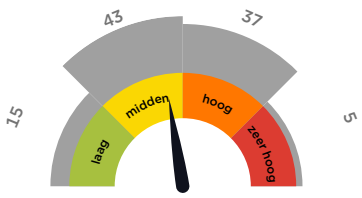
We brengen alle verzamelde kennis samen in dit document. Teksten worden meegelezen en besproken door diverse betrokkenen binnen SURF, en besproken met de leden. De publicatie is daarmee een interdisciplinaire teaminspanning waar veel mensen aan hebben bijgedragen. Wij bedanken iedereen voor hun inbreng.

# BIJLAGE 2 **RESULTATEN RISICOPERCEPTIE PER PROCES**

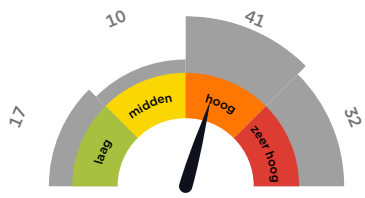
Figuur 8 **Risicobeeld Onderwijs** (%)



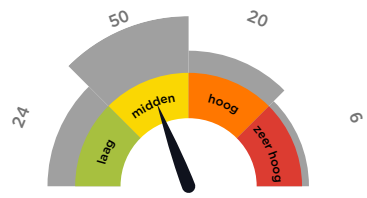

Verkrijging en openbaarmaking van informatie



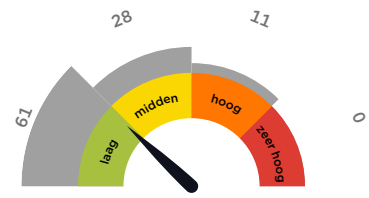

Identiteitsfraude



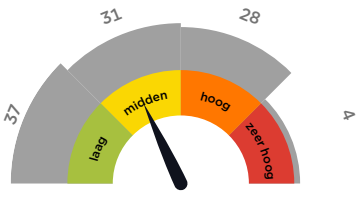

Verstoring ict



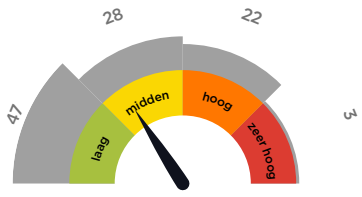

Manipulatie van data



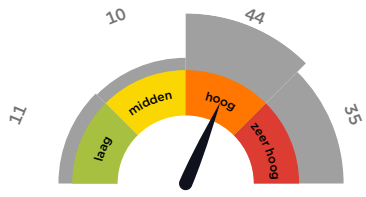

Spionage



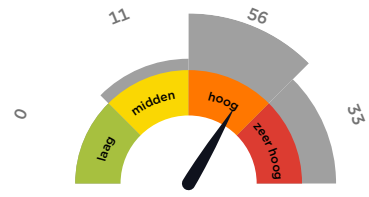

Overname en misbruik ict



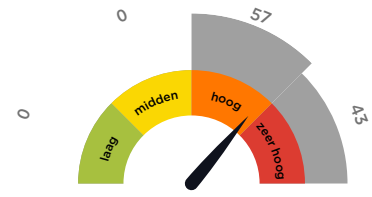

Bewust beschadigen imago




Ketenafhankelijkheid



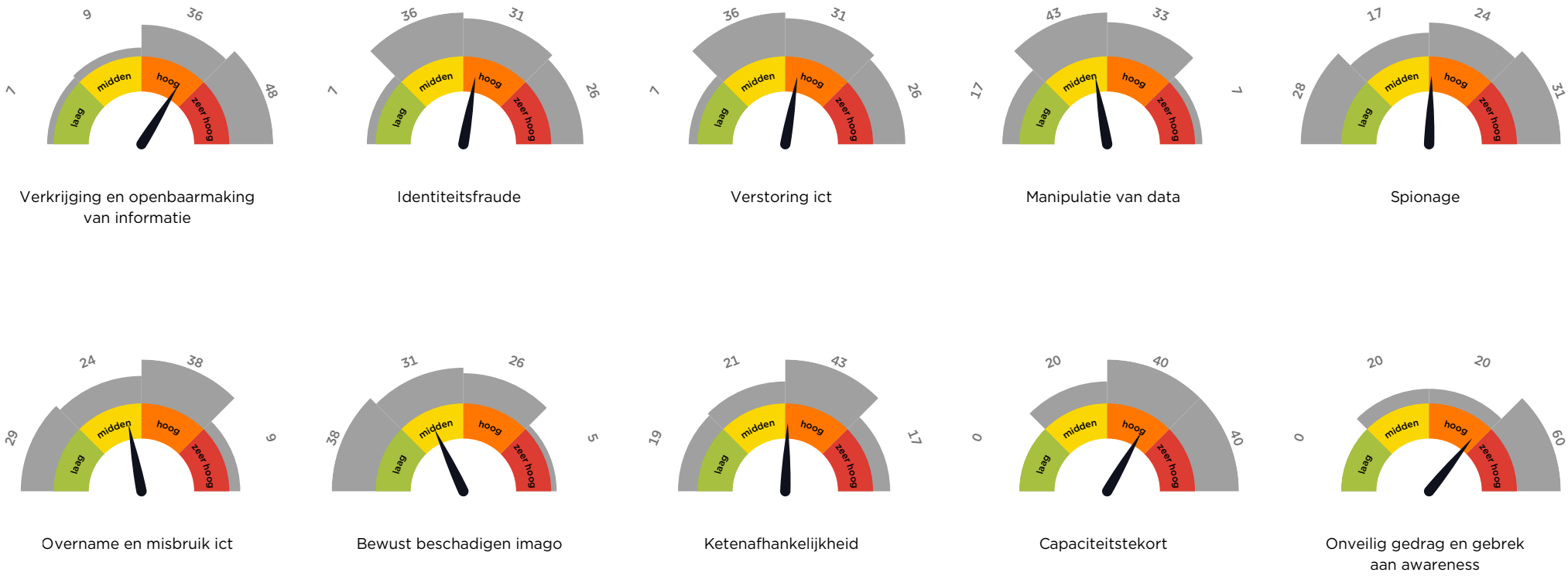

Capaciteitstekort



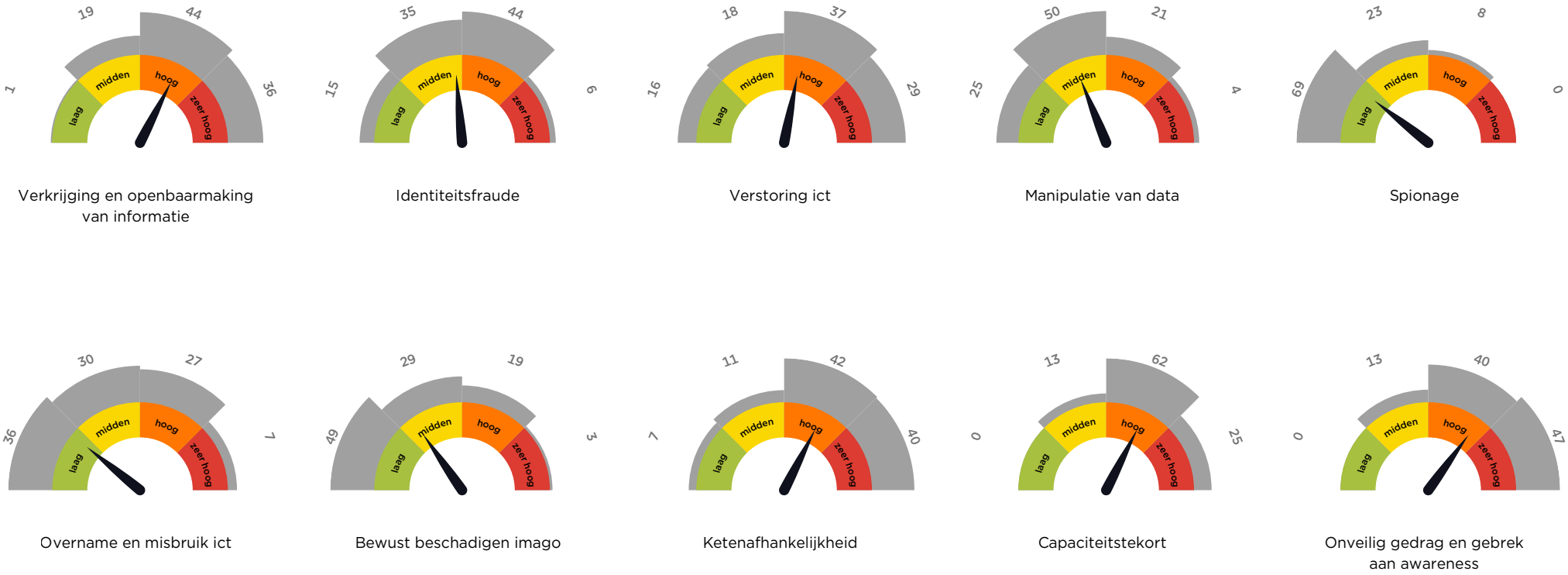

Onveilig gedrag en gebrek aan awareness

- Laag
- Midden
- Hoog
- Zeer hoog
- Deelnemers in %

Figuur 9 **Risicobeeld Onderzoek** (%)



Figuur 10 **Risicobeeld Bedrijfsvoering** (%)



# BIJLAGE 3 **MAPPING RISICOCATEGORIEËN NAAR INTERNATIONALE TAXONOMIEËN**

Organisaties hanteren verschillende terminologieën en definities. Daarom geven we hieronder de relatie aan tussen de door ons gehanteerde categorieën en de internationaal geaccepteerde ISO 27005. Dit bestaat uit de threat-taxonomie van ENISA[37], de incidenttaxonomie van ENISA[17] en de hoofdcategorieën van het MITRE ATT&CK framework[38]. Zo kunnen instellingen de categorieën relateren aan hun eigen classificaties.

| SURF-risicocategorieën | ENISA threat taxonomy | ENISA incident taxonomy | ISO27005 Table A.10 | Mitre ATT&CK |
|---|---|---|---|---|
| **Verkrijging en openbaarmaking van informatie** \| Gevoelige gegevens zoals persoonsgegevens, onderzoeksgegevens en intellectueel eigendom komen in verkeerde handen en/of worden openbaar gemaakt. | Information leaks | Mitre ATT&CK | Disclosure of information | Exfiltration |
| **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. Daarnaast zien instellingen ook statelijke actoren die proberen onderwijsaccounts te bemachtigen en gebeurtenissen met onderzoekers uit hoog risicolanden. | Masquerading of identity | Fraud | Theft of digital identity or credentials | Resource development |
| **Verstoring ict** \| Verstoringen van ict-voorzieningen door DDoS-aanvallen, malware (ransomware en virussen) zijn aan de orde van de dag, ook voor onderwijs- en onderzoeksinstellingen. | Denial of services | Availability<br>Malicious code | Technical failures | Impact |
| **Manipulatie van 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. | Deliberate alteration of information | Information content security | Corruption of data | Impact |
| **Spionage** \| Spionage wordt bij onderwijs en bedrijfsvoering al jaren laag ingeschat en is daarom voor die processen minder van toepassing. Voor onderzoek wordt deze dreiging wel hoog ingeschat en zelfs hoger dan vorig jaar. De AIVD, MIVD en NCTV waarschuwden in 2022 nadrukkelijk dat kennisinstellingen en wetenschappers op grote schaal doelwit zijn van statelijke actoren die uit zijn op hoogwaardige technologie. De respondenten voor wie deze dreiging relevant is, geven aan dat ze deze dreiging als zeer reëel beschouwen. | Eavesdropping | Information gathering | Remote spying<br>Eavesdropping<br>Social engineering | Alle categorieën |

## BIJLAGE 3 **MAPPING RISICOCATEGORIEËN NAAR INTERNATIONALE TAXONOMIEËN** (VERVOLG)

| SURF-risicocategorieën | ENISA threat taxonomy | ENISA incident taxonomy | ISO27005 Table A.10 | Mitre ATT&CK |
|---|---|---|---|---|
| **Overname en misbruik 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. Onder de instellingen zijn grote zorgen over software kwetsbaarheden en andere zwakke plekken in de weerbaarheid waardoor deze dreiging relevant blijft. | Misuse | Intrusion | Compromise of functions or services | Impact |
| **Bewust beschadigen imago** \| Dit is een categorie die al meerdere jaren door respondenten op gemiddelde urgentie wordt geschat. Toch blijft waakzaamheid geboden. De eerste reden is de evolutie van de modus operandi van cybercriminelen. Ransomware-aanvallen worden soms ook gecombineerd met direct publieke openbaring van de gijzeling. De tweede reden is dat hacktivisme in het veranderende geopolitieke en maatschappelijke klimaat mogelijk een comeback zou kunnen maken. Instellingen met banden met bepaalde bedrijven, landen of sectoren die in het maatschappelijk debat gevoelig liggen, kunnen te maken krijgen met pogingen tot verstoring door activisten. | Enemy overrun | Abusive content | Damage to public trust of reputation | Impact |
| **Ketenafhankelijkheid (afhankelijkheden van partners en (cloud)leveranciers)** \| Instellingen verplaatsen hun data en applicaties steeds meer naar de cloud en hebben daardoor minder regie over de kwaliteit van de informatiebeveiliging door de leverancier. Het is lastig de staat van informatiebeveiliging te bepalen bij cloud-diensten. Door een beperkt aantal leveranciers van clouddiensten is overstappen naar een alternatief moeilijk. Daarnaast hebben instellingen in samenwerkings-verbanden een afhankelijkheid van de weerbaarheid van hun partners in de keten. | Loss of governance<br>Data protection risks<br>Lock-in | Niet van toepassing | Failure of service providers | Niet van toepassing |
| **Capaciteitstekort** \| Het wereldwijde gebrek aan cybersecurityspecialisten is ook in onze sector actueel. Dit vormt een kwetsbaarheid om de weerbaarheid tegen risico's goed in te richten en heeft grote impact op andere risicocategorieën en compliance. | Staff shortage<br>Breach of personnel availability | Niet van toepassing | Lack of staff | Niet van toepassing |
| **Onveilig gedrag en gebrek aan awareness** \| Instellingen maken zich zorgen over bewustzijn, kennis en gedrag van medewerkers en studenten omdat veel incidenten beginnen bij onbedoeld risicovol gebruik van ict-middelen. | User error<br>Information leaks | Niet van toepassing | Human acts or omissions | Niet van toepassing |

# BRONDOCUMENTEN


1 https://www.nctv.nl/documenten/publicaties/2021/06/28/cybersecuritybeeld-nederland-2021
2 https://www.nctv.nl/onderwerpen/nederlandse-cybersecuritystrategie-2022-2028
3 https://www.surf.nl/files/2022-09/surfaudit-benchmark-informatiebeveiliging-2021.pdf
4 https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos
5 https://www.rabobank.nl/kennis/d011268958-it-sector-staat-op-een-kruispunt-rechtdoor-of-terug
6 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
7 https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
8 https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-dutch.pdf
9 https://www.politie.nl/nieuws/2023/januari/19/politie-registreert-minder-cybercrime.html
10 https://www.aivd.nl/documenten/jaarverslagen/2023/04/17/aivd-jaarverslag-2022
11 https://www.rijksoverheid.nl/documenten/jaarverslagen/2023/04/19/openbaar-jaarverslag-2022-mivd
12 https://www.nctv.nl/actueel/nieuws/2022/07/04/nctv-risico-op-ontwrichting-groter-door-scheefgroei-dreiging-en-weerbaarheid
13 https://www.rijksoverheid.nl/documenten/kamerstukken/2022/07/06/tk-aanbieden-samenhangend-inspectiebeeld-cybersecurity-vitale-processen
14 https://www.rdi.nl/onderwerpen/wet-beveiliging-netwerk--en-informatiesystemen/melden-incident-door-aanbieders-van-essentiele-diensten
15 https://www.rtlnieuws.nl/economie/artikel/5341242/datalek-tu-eindhoven-hogeschool-utrecht-ransomware-id-ware-pashouders
16 https://www.nbip.nl/nieuws/ddos-aanvallen-q4-2022/
17 https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
18 https://mbodigitaal.nl/2022/01/benchmark-ibp-e-2021-gepubliceerd/
19 https://www.forumstandaardisatie.nl
20 https://www.internet.nl/
21 https://wiki.surfnet.nl/pages/viewpage.action?spaceKey=SCIPR&title=2023+Q1
22 https://www.surf.nl/security-en-privacy-awarenessmeting-in-onderwijs-en-onderzoek-2022-maak-awareness-minder
23 https://www.ncsc.nl/onderwerpen/basismaatregelen
24 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022
25 https://www.pvib.nl/actueel/ib-magazines/ib-magazine-2022-2/downloaden
26 https://integraalveilig-ho.nl/instrument/position-paper-governance-van-cybersecurity-privacy-kennisveiligheid/
27 https://www.ncsc.nl/documenten/publicaties/2020/juli/21/factsheet-risicobeheersing
28 https://www.integraalveilig-ho.nl/nieuws/advies-cybersecurity-en-kennisveiligheid-handreiking-governance-privacy/
29 https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32022L2555&qid=1684827320290#d1e3342-80-1
30 https://www.surf.nl/nieuws/richtlijn-netwerk-en-informatiebeveiliging-nis2-wat-betekent-het-voor-de-leden-van-surf

## BRONDOCUMENTEN (VERVOLG)


31 https://integraalveilig-ho.nl/wp-content/uploads/Toolkit-implementatie-framework-integrale-veiligheid-hoger-onderwijs.pdf

32 https://www.digitaleoverheid.nl/wp-content/uploads/sites/8/2023/03/75856-BZK-Keuzekaart-securitytesten-Rijksoverheid_PDFUA.pdf

33 https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf

34 https://www.nederlanddigitaal.nl/actueel/nieuws/2022/11/22/cyberschaamte-is-cybersecuritywoord-van-het-jaar-voor-2022

35 https://futureoflife.org/open-letter/pause-giant-ai-experiments/

36 https://www.surf.nl/techtrends

37 https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox

38 https://attack.mitre.org

# COLOFON

**Auteurs**
Nicole van Deursen (SURF)
Abdul Altawekji (SURF)

**Redactie**
Jan Michielsen (SURF)

**Interviews**
Sanscript Tekstproducties

**Survey**
Bureau de Uitkomst

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



Juni 2023

Samen aanjagen van vernieuwing