SURFAUDIT BENCHMARK INFORMATIEBEVEILIGING 2021

INHOUD

1 INLEIDING

Dit rapport bevat de resultaten van de SURFaudit benchmark informatiebeveiliging 2021. Bij de benchmark meten we de volwassenheid van de sector onderwijs en onderzoek op het gebied van cyberveiligheid aan de hand van beheersmaatregelen uit het SURFaudit Toetsingskader Informatiebeveiliging. De resultaten van de benchmark zijn gebaseerd op de externe audits die de universiteiten hebben laten uitvoeren en de self-assessments van de overige deelnemers. Met deze benchmark hebben 51 instellingen meegedaan, een toename van 50% ten opzichte van de benchmark van 2019.

Het mbo heeft in 2021 ook zijn jaarlijkse benchmark uitgevoerd. De resultaten daarvan staan in het rapport Benchmark IBP-E 2021 dat beschikbaar is op de site van MBO Digitaal[1].

Vergelijkbaarheid

Voor de benchmark is gebruik gemaakt van de gezamenlijke auditmethodiek die de CISO's in samenwerking met SURF hebben opgesteld. De universiteiten hanteren deze auditmethodiek al sinds 2020 voor hun jaarlijkse externe audits. In de auditmethodiek staat het SURFaudit Toetsingskader Informatiebeveiliging 2021 genoemd met het bijbehorende volwassenheidsmodel. Verder zijn scope, diepgang en rapportage in de methodiek beschreven. Hiermee is de vergelijkbaarheid tussen instellingen en elkaar opvolgende benchmarks gewaarborgd, en kunnen volgende benchmarks hierop voortbouwen.

Ambitie: gemiddeld volwassenheidsniveau 3

Naar aanleiding van het ernstige ransomware-incident op de Universiteit Maastricht eind 2019 hebben de instellingen en de onderwijskoepels Universiteiten van Nederland en Vereniging Hogescholen, de ambitie uitgesproken gemiddeld een volwassenheidsniveau van 3 (op een schaal van 5) voor het hele SURFaudit Toetsingskader Informatiebeveiliging te behalen. Volwassenheidsniveau 3 houdt in dat de documentatie op orde is, er in de regel **formele** goedkeuring is door het bestuur en dat **uitvoering** van de maatregelen **aantoonbaar, getest** en **effectief** is. Om deze ambitie te realiseren hebben de instellingen tijd nodig om hun informatiebeveiligingsprocessen (beter) in te regelen.

Samen weerbaarheidsverhogende maatregelen nemen

In SURF-verband – en ook bij instellingen onderling – zijn diverse initiatieven opgestart om weerbaarheidsverhogende maatregelen op het gebied van informatiebeveiliging gezamenlijk aan te pakken. Een voorbeeld daarvan is de oprichting van een SURF-breed security operations centre, SURFsoc in 2020. SURFsoc heeft als doel de cyberweerbaarheid te verbeteren en mogelijke aanvallen op de ict-infrastructuur van alle op het SURF-netwerk aangesloten instellingen te voorkomen. Verder werkt SURF samen met de instellingen aan de oprichting van het SURF Security Expertise Centrum[2]. Dit samenwerkingsverband moet – onder andere – instellingen helpen hun (cyber)volwassenheidsniveau van 2 naar 3 te verhogen. Dat gebeurt door kennis te bundelen en te ontsluiten met onder meer templates, best practices en voorbeelduitwerkingen. En tevens door instellingen te ondersteunen met specifieke expertise waar nodig. Dit soort samenwerking biedt schaalvoordelen en faciliteert uitwisseling van kennis tussen de instellingen. Zo verhogen we samen de cyberweerbaarheid van de hele sector onderwijs en onderzoek.

Leeswijzer

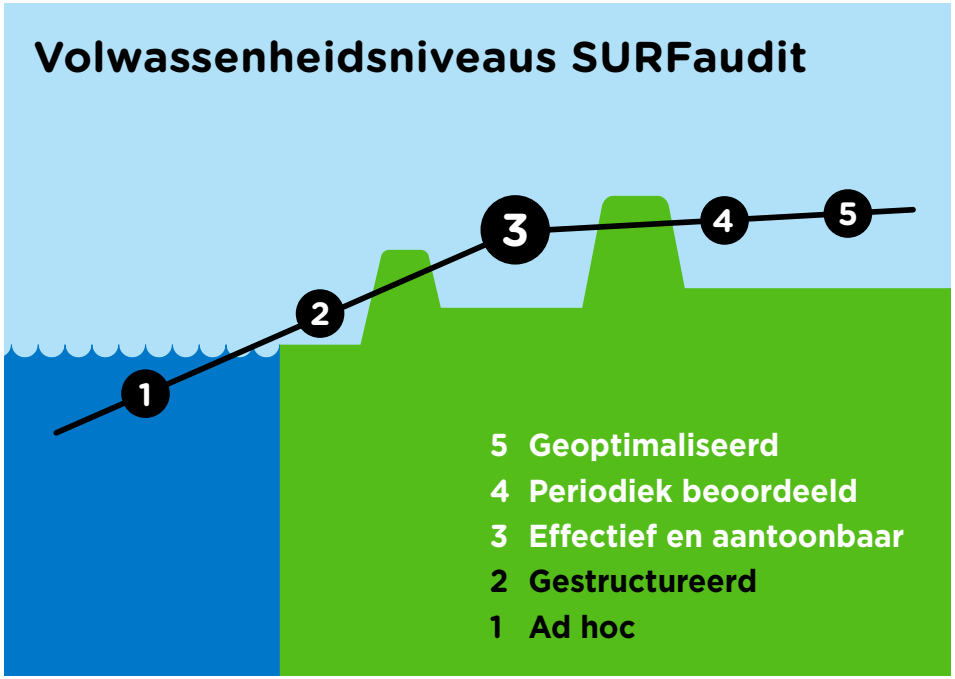
In hoofdstuk 2 vind je algemene informatie over de SURFaudit benchmark en het toegepaste volwassenheidsmodel. In hoofdstuk 3 gaan we in detail in op de resultaten van de audit en ook op de beheersmaatregelen die specifiek zijn voor de aandachtspunten naar aanleiding van het incident bij de Universiteit Maastricht. In hoofdstuk 4 vind je onze conclusies en aanbevelingen.

1 https://mbodigitaal.nl/2022/01/benchmark-ibp-e-2021-gepubliceerd/
2 https://www.surf.nl/sec

2 OVER DE SURFAUDIT BENCHMARK INFORMATIEBEVEILIGING

Het doel van SURFaudit[3] is om de bij SURF aangesloten instellingen te helpen hun informatiebeveiliging onder controle te brengen en te houden, door de procesmanagementcyclus te ondersteunen. SURFaudit biedt middelen waarmee instellingen de volwassenheid van hun informatiebeveiliging kunnen meten. Daartoe organiseert SURF eens in de twee jaar een benchmark om in kaart te brengen hoe de hele sector onderwijs en onderzoek ervoor staat op het gebied van informatiebeveiliging.

Figuur 1 **Volwassenheidsniveaus uit het SURFaudit Toetsingskader Informatiebeveiliging 2021**



3 Zie https://www.surfaudit.nl/

SURFaudit Toetsingskader Informatiebeveiliging (2021)

In de benchmark gebruiken we het SURFaudit Toetsingskader Informatiebeveiliging waarin alle beheersmaatregelen staan die een instelling moet nemen om zijn cyberweerbaarheid op peil te houden en te verbeteren. Dit toetsingskader is gebaseerd op het NBA Volwassenheidsmodel Informatiebeveiliging v2.1 (zie kader NBA Volwassenheidsmodel Informatiebeveiliging), dat ook gebruikt wordt door de Auditdienst Rijk en de grote auditbureaus in Nederland. Het model hanteert vijftien securitydomeinen.

Ieder domein bevat een aantal beheerdoelstellingen die zijn uitgewerkt in vijf volwassenheidsniveaus (zie figuur 2 en tabel 3), van ad hoc (volwassenheidsniveau 1) tot geoptimaliseerd (volwassenheidsniveau 5). Welk volwassenheidsniveau gewenst is hangt af van de hoogte van het risico dat moet worden gemitigeerd en van de risicobereidheid van de instelling. Voor de sector onderwijs en onderzoek streven we naar een gemiddeld volwassenheidsniveau van 3 voor alle beheersmaatregelen uit het toetsingskader.
De onderwijskoepels Universiteiten van Nederland (UNL) en de Vereniging Hogescholen (VH) hebben als ambitie voor de universiteiten en hogescholen om dit volwassenheidsniveau binnen één, respectievelijk twee jaar te behalen.

Tabel 1 **Volwassenheidsniveaus uit het SURFaudit Toetsingskader Informatiebeveiliging 2021**

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

* VN staat voor volwassenheidsniveau

Normenkader Informatiebeveiliging Hoger Onderwijs (2015)

De sector onderwijs en onderzoek heeft in 2015 een Normenkader Informatiebeveiliging Hoger Onderwijs vastgesteld, waarin de beheers-maatregelen zijn ingedeeld in 6 clusters (zie tabel 2).

Tabel 2 **Clusters uit het Normenkader Informatiebeveiliging Hoger Onderwijs 2015**

Cluster	
1	Beleid en organisatie
2	Personeel, studenten en gasten
3	Ruimten en apparatuur
4	Continuïteit
5	Vertrouwelijkheid en integriteit
6	Monitoring en logging

Tot 2019 is gebruik gemaakt van dit normenkader voor de benchmarks. In 2019 is de sector overgestapt naar het huidige SURFaudit Toetsingskader Informatiebeveiliging. In dit rapport staat de oude clusterindeling alleen nog voor vergelijking met eerdere benchmarks.

NBA Volwassenheidsmodel Informatiebeveiliging

De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) heeft medio 2016 een volwassenheidsmodel gepubliceerd dat tot doel heeft "de interne auditafdelingen alsmede de directies van organisaties een leidraad en handvaten te geven waarmee zij doelgericht en op pragmatische wijze hun organisaties kunnen ondersteunen bij het meten, bepalen en verbeteren van het volwassenheidsniveau van informatiebeveiliging". Begin 2019 heeft de NBA hiervan een update gepubliceerd in samenwerking met NOREA, de beroepsorganisatie van IT-auditors. Deze update dient als basis voor het huidige SURFaudit Toetsingskader Informatiebeveiliging[4]. Het model gaat uit van de risico's die relevant zijn voor een organisatie en geeft per volwassenheidsniveau de maatregelen om die risico's te mitigeren. De maatregelen zijn ook gerelateerd aan verschillende internationale standaarden, zoals bijvoorbeeld de ISO/IEC 27002:2013 standaard.

Tabel 3 **Het NBA Volwassenheidsmodel Informatiebeveiliging ingedeeld in vijftien domeinen**

#	Code	Domein	Beschrijving[5]
1	GO	Governance	Geeft richting en ondersteuning aan informatiebeveiliging in lijn met bedrijfsdoelstellingen, risicobereidheid en van toepassing zijnde wet- en regelgeving en vergewist zich van de effectieve naleving ervan.
2	OR	Organisatie	Informatiebeveiliging is op het hoogst mogelijk organisatieniveau geadresseerd en het beheer van informatiebeveiliging in lijn is met de bedrijfsdoelstellingen en van toepassing zijnde risico's en compliance eisen.
3	RM	Risicobeheer	Draagt zorg voor het op gestructureerde wijze identificeren en beheersen van informatiebeveiligingsrisico's zodanig dat de risico's in lijn zijn met de risicobereidheid en risicoraamwerk van de organisatie.
4	HR	Personeelsbeheer	Draagt zorg voor dat alle medewerkers, inhuurkrachten en derde partijen zich bewust zijn van informatiebeveiligingsrisico's en voldoende geschoold zijn om in lijn met het beveiligingsbeleid hun werkzaamheden te kunnen verrichten.
5	CO	Configuratiebeheer	Draagt zorg voor de vastlegging en ontsluiting van gegevens over de IT-middelen en IT-diensten.
6	IM	Incident-/probleembeheer	Draagt zorg voor het afhandelen van verstoringen in IT-dienstverlening en voor tijdig herstel van afgesproken dienstenniveaus. Probleembeheer draagt zorg voor het wegnemen of voorkomen van structurele fouten in de IT-dienstverlening.
7	CH	Wijzigingsbeheer	Draagt zorg voor het beheerst doorvoeren van wijzigingen in IT-middelen en IT-diensten (onder andere applicaties).
8	SD	Systeemontwikkeling	Draagt zorg voor het ontwikkelen van geautomatiseerde oplossingen in lijn met ontwerpspecificaties, ontwikkelen documentatiestandaarden en kwaliteits- en acceptatiecriteria.
9	DM	Gegevensbeheer	Draagt zorg voor het onderhouden van de volledigheid, juistheid, beschikbaarheid en bescherming van gegevens.
10	ID	Identiteits- en toegangsbeheer	Draagt zorg voor het beheren van de logische toegang tot informatie en informatiediensten (onder andere applicaties).
11	SM	Beveiligingsbeheer	Draagt zorg voor het in kaart brengen en adresseren van de risico's van beschikbaarheid, integriteit en vertrouwelijkheid die van toepassing zijn op de informatievoorziening.
12	PH	Fysieke beveiliging	Draagt zorg voor het toegangsbeheer tot ruimtes en de bescherming van personen en objecten tegen incidenten die een fysieke schade aan personen of objecten tot gevolg kunnen hebben.
13	OP	Computer operatie	Draagt zorg voor het operationeel houden van de IT-diensten.
14	BC	Bedrijfscontinuïteitsbeheer	Draagt zorg voor het herstellen en voorzetten van de bedrijfsvoering na het optreden van een calamiteit in overeenstemming met de hiervoor afgesproken dienstenniveaus.
15	SC	Ketenbeheer	Draagt zorg voor het bewaken van de levering van de afgesproken dienstverlening door (interne en externe) leveranciers.

4 https://www.nba.nl/intern-en-overheidsaccountants/volwassenheidsmodel-informatiebeveiliging/

5 bron: https://www.nba.nl/globalassets/over-de-nba/ledengroepen/lio/lio-new/nba-lio-norea-handreiking-bij-volwassenheidsmodel-informatiebeveiliging-januari-2019.pdf

3 RESULTATEN

Voor de benchmark 2021 hanteren we de gemiddelden inclusief de scores van de externe audits van de universiteiten. De scores door een onafhankelijke auditor blijken ongeveer een half volwassenheidsniveau lager uit te vallen dan bij een self-assessment. Desalniettemin dragen ze bij aan het beeld voor de hele sector onderwijs en onderzoek.

Overzicht resultaten

In tabel 4 staan de resultaten gegroepeerd naar de domeinindeling van het SURFaudit Toetsingskader Informatiebeveiliging 2021 van zowel de benchmark 2021 als die van 2019. Gemiddeld over alle maatregelen is er een kleine terug-gang ten opzichte van de resultaten in 2019.

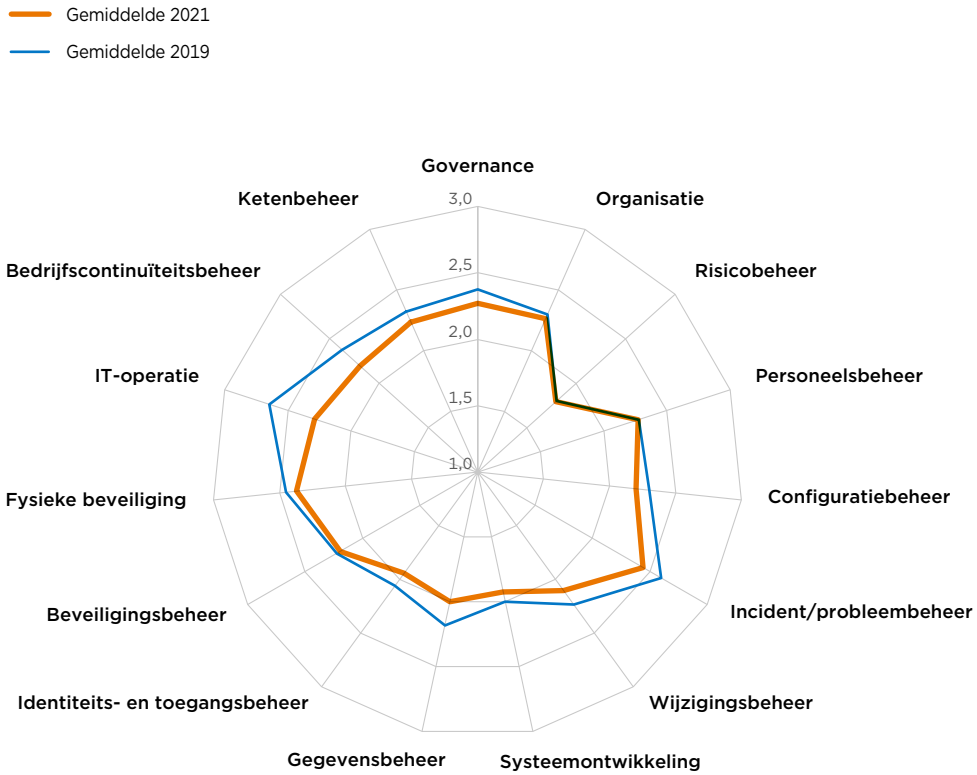
Met uitzondering van de domeinen *Organisatie, Risicobeheer, Personeelsbeheer* en *Beveiligingsbeheer* is een lichte teruggang te zien van de gemiddelden per domein. Gemiddeld komt de benchmark uit op een volwassenheidsniveau van 2,2. Een van de oorzaken voor de daling ten opzichte van de benchmark 2019 is de eerdergenoemde constatering dat een externe audit tot een verlaging van de scores leidt. Een andere oorzaak is het relatief grote aantal instellingen dat voor het eerst meedoet.

Tabel 4 **Gemiddelden per domein (Toetsingskader Informatiebeveiliging 2021)**

Domein	Benchmark 2021	Benchmark 2019
Governance	2,3	2,4
Organisatie	2,3	2,3
Risicobeheer	1,8	1,8
Personeelsbeheer	2,3	2,3
Configuratiebeheer	2,2	2,3
Incident-/probleembeheer	2,4	2,6
Wijzigingsbeheer	2,1	2,2
Systeemontwikkeling	1,9	2,0
Gegevensbeheer	2,0	2,2
Identiteits- en toegangsbeheer	1,9	2,1
Beveiligingsbeheer	2,2	2,2
Fysieke beveiliging	2,4	2,5
IT-operatie	2,3	2,7
Bedrijfscontinuïteitsbeheer	2,2	2,4
Ketenbeheer	2,2	2,3
Gemiddelde van alle statements	**2,2**	**2,3**

In figuur 2 is goed te zien dat de domeinen *Risicobeheer, Systeemontwikkeling en Identiteits- en toegangsbeheer* extra aandacht nodig hebben (gemiddelde score lager dan 2,0). Bovendien scoort *Risicobeheer* beduidend lager dan het gemiddelde van de hele benchmark. *Incident- en probleembeheer* en *IT-operatie* scoren relatief hoog.

Figuur 2 **Gemiddelden per domein (Toetsingskader Informatiebeveiliging 2021)**



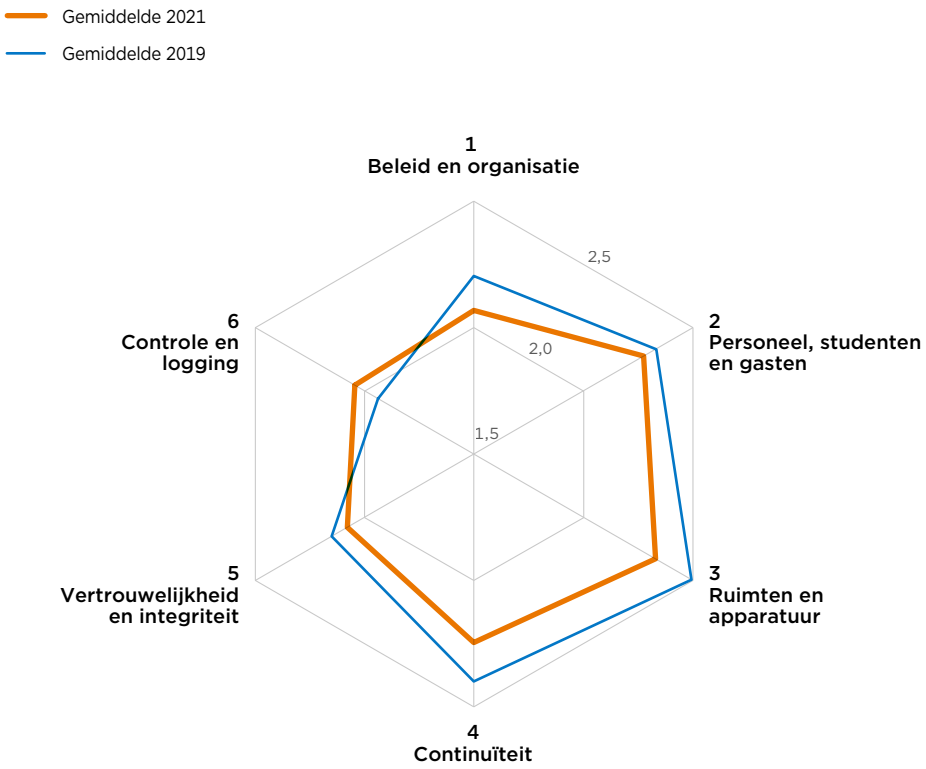
In tabel 5 staan de resultaten gegroepeerd naar de clusterindeling van het SURFaudit Normenkader Informatiebeveiliging HO 2015:

Tabel 5 **Gemiddelden per cluster (Normenkader Informatiebeveiliging HO 2015)**

Scores	Benchmark 2021	Benchmark 2019
Cluster **1** – Beleid en organisatie	2,1	2,2
Cluster **2** – Personeel, studenten en gasten	2,3	2,3
Cluster **3** – Ruimten en apparatuur	2,3	2,5
Cluster **4** – Continuïteit	2,2	2,4
Cluster **5** – Vertrouwelijkheid en integriteit	2,1	2,2
Cluster **6** – Monitoring en logging	2,0	1,9
Gemiddelde van alle statements	**2,2**	**2,3**

Hier zien we dat Cluster 6 ‘Controle en Logging’ is verbeterd ten opzichte van de benchmark van 2019. Dit hangt waarschijnlijk samen met het stijgend aantal instellingen dat gebruik maakt van een SOC/SIEM-dienst. Dat betekent echter niet dat we daar geen aandacht aan moeten blijven besteden, het blijft belangrijk het volwassenheidsniveau verder te verhogen.

Figuur 3 **Gemiddelden per cluster (Normenkader Informatiebeveiliging 2015)**



Aandachtspunten na incident bij Universiteit Maastricht

De Universiteit Maastricht heeft een aantal maatregelen opgesteld op basis van de aandachtspunten uit het rapport 'Spoedondersteuning project Fontana'[6]. De universiteiten hebben deze maatregelen extra aandacht gegeven in hun externe audits van 2020 en 2021 en zij boeken duidelijk vooruitgang op deze set maatregelen. Dit illustreert dat de benadering met jaarlijkse externe audits die de universiteiten hebben gekozen, zijn vruchten afwerpt. Hierdoor is er meer druk om cyberweerbaarheid hoog op de agenda te houden. De scores voor die set maatregelen bij de overige benchmarkdeelnemers liggen nu nog wat lager.

6 https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastrichtnl10-02pdf

4 CONCLUSIE EN AANBEVELINGEN

Conclusie

Uit de resultaten blijkt dat er enerzijds stappen zijn gezet sinds de benchmark van 2019, maar dat er ook onderdelen zijn die aandacht behoeven. De gemiddelde score van een 2,2 op de benchmark van 2021 laat zien dat de ambitie om op het hele SURFaudit Toetsingskader Informatiebeveiliging HO (2021) gemiddeld een volwassenheidsniveau van 3 te scoren, nog niet is behaald. Het lijkt eenvoudig om van 2,2 naar een 3 te komen, echter een verhoging van 1 stap in volwassenheidsniveau vergt al gauw enkele jaren. Daarbij komt ook dat de stap van niveau 2 naar 3 groot is, omdat daarbij informele processen geformaliseerd moeten worden met alle bijbehorende documentatie en bewustwording in de hele organisatie om dat aantoonbaar te maken.

Door de hoge deelname aan deze benchmark weten we als sector onderwijs en onderzoek steeds beter hoe we ervoor staan op het vlak van cyberweerbaarheid en welke verbeterpunten als eerste moeten worden aangepakt. Dat is een stevig fundament voor de toekomst.

Aanbevelingen

Om volwassenheidsniveau 3 te behalen, moet de sector onderwijs en onderzoek dus nog een stevige inspanning leveren. Daarbij ligt het voor de hand als eerste maatregelen aan te pakken die nu relatief laag scoren en waarbij snel resultaat behaald kan worden.

Een aantal onderwerpen leent zich goed om gezamenlijk op te pakken en zijn bovendien al als speerpunten vastgesteld door de CISO's van de universiteiten en de hogescholen. Ook in de SURF Innovatiezone 'State of the art Cyberveiligheid'[7] worden deze onderwerpen verder uitgewerkt in samenwerking met de instellingen. Verder ontwikkelt SURF het Security Expertise Centrum[8], een samenwerkingsverband dat de instellingen voor onderwijs en onderzoek helpt om de cyberweerbaarheid van de sector als geheel te vergroten. Zo nemen we als sector gezamenlijk eenduidig weerbaarheidverhogende maatregelen. Door – over het algemeen schaarse – specialistische kennis te bundelen en die voor de gehele sector in te zetten, wordt de gehele sector sterker. SURF speelt daarbij een belangrijke rol als aanjager en facilitator. Een overzicht van onderwerpen die zich goed lenen om gezamenlijk op te pakken zijn:

- **Risicomanagement voor informatiebeveiliging**
  Risicomanagement stelt de instellingen in staat om beter te anticiperen op mogelijke risico's, effectieve beheersmaatregelen te nemen en zo de continuïteit beter te waarborgen. De risicoprofielen van instellingen zijn echter niet per se gelijk en moeten daarom individueel worden opgesteld. Maar het biedt wel voordelen om een gemeenschappelijke visie op en methodiek voor de aanpak van risico's in de sector te ontwikkelen en risicomanagement voor informatiebeveiliging verder te professionaliseren en uiteindelijk onderdeel te maken van het organisatiebrede risicomanagement.

- **Logging en monitoring**
  Een groot aantal instellingen maakt inmiddels gebruik van SOC/SIEM-dienstverlening. SURF heeft in 2020 een security operations centre, SURFsoc, opgestart. SURFsoc zorgt voor 24/7 monitoring van de ict-infrastructuur van instellingen, signaleert bedreigingen en adviseert instellingen bij inbreuken over acties om de risico's te verlichten. Door kennis te bundelen, use cases te ontwikkelen, informatie en best practices uit te wisselen, wordt de weerbaarheid van de gehele sector vergroot. In de loop van 2020 en 2021 zijn een groot aantal instellingen aangesloten op een SOC/SIEM-dienst.

- **Regie op cloudgebruik en outsourcing**
  De beheersmaatregelen voor 'Risicobeheer van leveranciers' en 'Interne beheersing bij derden' scoren laag in de benchmark terwijl cloudgebruik

7 https://www.surf.nl/innovatiezone-state-of-the-art-cyberveiligheid
8 https://www.surf.nl/sec

en outsourcing steeds verder toenemen. Uit het Cyberdreigingsbeeld 2021-2022[9] blijkt dat 'Afhankelijkheid van clouddiensten' door de instellingen als een hoog risico wordt gezien. Vooral deze beheersmaatregelen moeten daarom snel op een hoger volwassenheidsniveau worden gebracht. Wanneer de sector hoger onderwijs en onderzoek haar onderhandelingspositie versterkt door gezamenlijk uniforme eisen op te stellen voor cloudleveranciers en outsourcingpartijen, wordt hiervoor een grote stap gezet. Dit is iets wat nu al gebeurt maar nog op te beperkte schaal. Het reikt zelfs verder dan alleen maatregelen op het vlak van informatiebeveiliging. Denk hierbij ook aan andere inkoopeisen en SLA-afspraken. Daarnaast draagt een verdere professionalisering van beheer en regie op cloudgebruik en outsourcing bij aan een hogere cyberweerbaarheid. Het gezamenlijk ontwikkelen van een best practice voor regie op cloudgebruik en outsourcing is daarvoor een goed startpunt.

Andere onderwerpen zoals 'Asset en configuratie-management' en 'Privileged account-management' lenen zich minder goed voor een gezamenlijke aanpak. De inrichting hiervan wordt namelijk sterk bepaald door de interne organisatie van een instelling. In sommige gevallen kunnen instellingen wel samen best practices ontwikkelen en met elkaar delen:

- **Asset- en configuratiemanagement**
  Goed asset- en configuratiemanagement levert een belangrijke bijdrage aan de weerbaarheid van een organisatie. Het gebrek aan inzicht op deze onderdelen van ict-beheer kan bij incidenten leiden tot vertraging en tot verkeerde beslissingen. Veel instellingen hebben al een vorm van asset- en configuratiemanagement, maar het kost vaak moeite om deze compleet en up-to-date te houden. In veel gevallen is hiervoor wel al speciale tooling ingericht. Het ontwikkelen van een best practice kan instellingen helpen om asset- en configuratiemanagement goed in te richten en te onderhouden.

- **Privileged account-management**
  Privileged account-management (PAM) regelt het gebruik van accounts met hoge rechten, zoals admin-accounts. Het is belangrijk om hiervan een goede registratie bij te houden en goed life-cycle management toe te passen. Daarnaast is het belangrijk om de activiteiten van deze accounts vast te leggen, zodat verwerkingsresultaten achteraf kunnen worden gecontroleerd. Soms is dit zelfs verplicht, bijvoorbeeld voor de AVG. Veel instellingen hebben al een vorm van PAM ingericht. We bevelen aan om ook hiervoor best practices op te stellen en mogelijk zelfs gezamenlijk tooling aan te schaffen.

9 https://www.surf.nl/files/2022-06/cyberdreigingsbeeld-onderwijs-en-onderzoek-2021-2022-lr.pdf

COLOFON

Auteurs
Bart Bosma (SURF)
René Ritzen (SURF)

Redactie
Yvonne Klaassen (SURF)
Jan Michielsen (SURF)

Ontwerp
Studio Koelewijn Brüggenwirth BNO, Den Haag

Fotografie
Foto omslag: Getty Images, Marko Geber

September 2022

Samen aanjagen van vernieuwing