mbo digitaal

Update praktische vertaling Educatief Cyberdreigingsbeeld 2025

Het door SURF gepubliceerde Cyberdreigingsbeeld 2024 betrof een terugblik op de afgelopen tien jaar en bood geen nieuwe inzichten ten opzichte van eerdere SURF dreigingsbeelden. Desondanks is er een hoop gaande in de (cybersecurity) wereld en vonden wij het noodzakelijk om de praktische vertaling bij te werken. Alle cyberdreigingen zijn herzien en daar waar nodig bijgewerkt. Aanvullend daarop is aandacht geschonken aan de volgende (cyber) trends en ontwikkelingen: geopolitieke spanningen, (digitale) spionage, Living-of-the-Land (LOTL) technieken, edge devices, kunstmatige intelligentie (AI), quantum computing, Operational Technology (OT) en de Cyberbeveiligingswet (NIS2). Op verzoek van diverse instellingen zijn alle handreikingen uit deze praktische vertaling ook beschikbaar gesteld in Excel formaat. Voor de mbo's zullen deze ook in Trustbound beschikbaar gesteld worden.

Prioriteit van de risico's
De prioriteitstelling van risico's is niet aangepast, echter kan er gediscussieerd worden of *ketenafhankelijkheid* niet op nummer één zou moeten staan vanwege de huidige geopolitieke spanningen. Governance en risicomanagement waren al toegevoegd aan de categorie 'prio-1' en de aanwijzing van het hoger onderwijs (HO, WO) onder de Cyberbeveiligingswet (NIS2) benadrukt het belang van beide domeinen. Ondanks dat het spionagerisico voor de meeste instellingen dusdanig laag wordt ingeschaald, is er in deze versie toch een uitwerking voor gemaakt. Met name ook omdat dit voor een deel van de sector wel waardevol kan zijn.

Stapsgewijs risico's verkleinen
Op de volgende pagina's hebben we voor ieder risico en/of aandachtspunt een handelingsperspectief uitgewerkt als 1-page checklist. Hiermee kunnen instellingen stapsgewijs werken aan het verkleinen van de risico's. Voor iedere maatregel hebben we de relatie met de beheerdoelstellingen uit het SURFaudit toetsingskader gelegd. Deze verwijzingen herkennen de mbo's aan de kleuren voor **Governance**, **Processen** en **Techniek**.

Let op! De gepresenteerde maatregelen bieden geen garantie dat een instelling geheel veilig is voor cyberdreigingen. Maar gezamenlijk dragen ze zeker bij aan het voorkomen, tijdig detecteren en beperken van de impact daarvan.

Relatie met programma Cyberveiligheid en dienstverlening SURF
We sluiten dit memo af met een tabel waarin we de relaties van de in het Cyberdreigingsbeeld genoemde risico's en aandachtspunten met initiatieven vanuit het programma Cyberveiligheid mbo, dienstverlening van SURF en het SURFaudit toetsingskader overzichtelijk in kaart brengen. Instellingen kunnen van de dienstverlening en initiatieven gebruikmaken om de risico's uit het Cyberdreigingsbeeld te adresseren. Samen met SURF is een document gemaakt met daarin de relatie tussen SURF diensten, het NIST Cyber Security Framework en het SURFaudit toetsingskader. Mochten er vragen of opmerkingen zijn, neem dan contact op met Mick Deben.

Prio-1 Korte termijn	**Prio-2** Middellange termijn	**Prio-3** Lange termijn
Informatielekken	Identiteitsfraude	Spionage
Ketenafhankelijkheid	Misbruik IT/OT	
Verstoring ICT	Imagoschade	
Onveilig gedrag	Datamanipulatie	
Capaciteitstekort		
Governance		
Risicomanagement		

mbo digitaal

Versiebeheer

Versie	Datum	Auteur(s)	Omschrijving
1.0	26 september 2023	Mick Deben	Eerste versie met dank aan Abdul Altawekji, Nicole van Deursen en het Programmateam Cyberveiligheid van MBO Digitaal.
1.1	12 oktober 2023	Mick Deben	Wijzigingen: - 2 maatregelen toegevoegd aan governance m.b.t. hacktivisme (risico 1 en 8) - Sunburst toegevoegd met representatie van NBA-model domeinen in dit document (met dank aan Yuverta voor het idee). - Versiebeheer toegevoegd
1.2	April 2025	Mick Deben	Wijzigingen: - Verwijzingen aangepast naar ID's van het SURFaudit toetsingskader - Dreigingsbeeld IACS 2023-2024 verwerkt - Cybersecuritybeeld Nederland 2024 verwerkt - Dashboard Cybersecurity verwerkt - Trends check tot hack verwerkt - Updates m.b.t. NIS2 - Spionage dreiging toegevoegd - Eigenaarschap aangepast naar verantwoordelijkheid om discussies met onze geliefde community te voorkomen ;) - Versiebeheer naar begin verplaatst - Dit document in Excel en Trustbound beschikbaar gesteld - Meer verwijzingen naar nuttige bronnen toegevoegd - Naamgeving risico's compacter gemaakt - Document geneutraliseerd (Geen MS)

mbo digitaal

RISICO'S SURF CYBERDREIGINGSBEELD: INFORMATIELEKKEN & IMAGOSCHADE

Op dit moment is het afpersen van organisaties door informatie ontoegankelijk te maken de grootste dreiging. Om hier weerstand tegen te kunnen bieden is een gelaagde beveiliging noodzakelijk

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Monitor het internet en darkweb op relevante zoektermen passend bij de instelling, bijvoorbeeld via Google Alerts of AI geplande taken (SM.07). ☐ Neem in het patchbeleid ook contentmanagementsystemen (CMS) en plug-ins van websites op (SM.06). ☐ Krijg grip op de risico's in de toeleveringsketen (GO.02, SC.03, SC.04). ☐ Kijk niet alleen naar risico's in je eigen keten, maar kijk ook naar de rol van je instelling in de keten van anderen (GO.02, SC.03, SC.04) ☐ Bepaal op basis van een risico-afweging welke informatie(systemen) toegankelijk mogen zijn vanaf onbeheerde apparatuur, en onder welke condities (DM.02)	☐ Identificeer met behulp van OSINT alle (sub)domeinen in eigendom van de instelling (CO.01). ☐ Lever een lijst met alle (sub)domeinen aan bij SURF t.b.v. IV-metingen (niet nodig met SURFdomeinen) (CO.02). ☐ Bevorder de bewustwording rondom het herkennen van phishingberichten (HR.06). ☐ Monitor proactief op de registratie van en wijzigingen aan domeinen die lijken op die van instelling. Let hierbij ook op subdomeinen van cloudoplossingen (SM.07). ☐ Hanteer een 'deny-by-default'-beleid en sta alleen goedgekeurde verbindingen toe (SM.11). ☐ Zorg ervoor dat medewerkers en studenten geen of beperkt (lokaal, in de browser en cloud) software kunnen installeren (allowlisting) (SM.01). ☐ Schakel macro's in Office-bestanden uit of sta alleen ondertekende macro's toe (SM.01). ☐ Schakel ActiveX in Office-bestanden uit (SM.01). ☐ Schakel automatisch afspelen uit ('AutoPlay' en 'AutoRun')[1] (SM.01). ☐ Zet USB-poorten dicht en blokkeer USB-opslag, tenzij noodzakelijk (beperk gebruik) (SM.01). ☐ Definieer hersteltijden voor verschillende soorten informatie (Recovery Point Objective) (OP.02). ☐ Maak back-ups volgens de 3-2-1-regel (3 back-ups, 2 verschillende media, 1 offline) (OP.02, BC.03, BC.04). ☐ Implementeer de security headers op alle (sub)domeinen (SM.06).	☐ Implementeer mailfiltering (SM.12). ☐ Controleer minimaal wekelijks geautomatiseerd zowel de buitenkant als de binnenkant van netwerken op bekende kwetsbaarheden en misconfiguraties (SM.12). ☐ Prioriteer patches op basis van de ernst van de kwetsbaarheid en overige factoren (SM.06). ☐ Test patches voordat deze in productieomgevingen worden doorgevoerd (CO.04, CO.05). ☐ Segmenteer de securityfunctie van de rest van het netwerk (monitoring, authenticatie en administratie) (SM.11, SM.13). ☐ Segmenteer web- en mailservers van de rest van het netwerk (DMZ) (SM.11). ☐ Definieer de richting van verkeer tussen segmenten en toegestane protocollen (SM.12). ☐ Investeer in geavanceerde endpointdetectie- en responsoplossingen (SM.12). ☐ Leid uitgaand verkeer via een proxy naar buiten toe of gebruik DNS-filtering om malafide domeinen en IP-adressen te blokkeren (zoals Spamhaus, Barracuda, AbuseIPDB, etc.) (SM.12). ☐ Volg de best practices om weerstand te bieden tegen ransomware aanvallen (SM.07) ☐ Implementeer een Web Application Firewall (WAF) op alle publieke websites (SM.08). ☐ Monitor het externe aanvalsoppervlak om wijzigingen en hiaten in de beveiliging tijdig te detecteren (EASM) (SM.07) ☐ Zorg ervoor dat (grootschalige) data-exfiltratie gedetecteerd kan worden (SM.07) ☐ Gebruik honeytokens voor vroegtijdige detectie van AitM-aanvallen (SM.05) ☐ Gebruik tools zoals PassfieldGuard en Linkshield om de impact van menselijke fouten en het succes van phishing te reduceren (SM.07)

[1] Group Policy: ...\Computer Configuration\Policies\Administrative Templates\Windows Components\AutoPlay Policies

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: KETENAFHANKELIJKHEID

Dreigingen strekken zich niet alleen uit over cloudleveranciers, maar in de gehele keten (leveranciers, partners en overheden). Een incident in de keten kan leiden tot negatieve impact bij instellingen en vice versa.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Maak een afweging over de mate waarin afhankelijkheden wenselijk of acceptabel zijn, bijvoorbeeld voor gevoelige informatie of kritieke infrastructuur (SC.03) ☐ Koppel intern verantwoordelijken aan leveranciers (SC.01) ☐ Stel beleid voor leveranciersmanagement vast (SC.01) ☐ Versterk de weerbaarheid van leveranciers (SC.04) ☐ Neem de evaluatie van leveranciers ten aanzien van informatiebeveiliging op in de planning en zie toe op de uitvoering en opvolging daarvan, bijvoorbeeld door terugkerende taken te automatiseren (SC.03) ☐ Plan een exit strategie voor kritieke IT-leveranciers (SM.07) ☐ Maak gebruik van SURF Vendor Compliance en de centrale DPIA's (SC.03)	☐ Identificeer alle leveranciers en partners en classificeer ze ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid (laag, midden of hoog) (SC.03). ☐ Evalueer leveranciers aan de hand van hun classificatie en risico voor de instelling, bijvoorbeeld via audits, penetratietesten, CCV-keurmerken, certificeringen en prestatiegesprekken (SLA)[2] (SC.03, SC.04). ☐ Stel standaard clausules voor informatiebeveiliging op, passend bij de classificatie (SC.03) ☐ Gebruik bijvoorbeeld de SURF Security Baseline om minimale eisen aan leveranciers op te leggen (11.1). ☐ Gebruik STITCH en OWASP als minimale eisen voor applicaties (SD.01) ☐ Bereid je voor op incidenten in de keten, stel een bedrijfscontinuïteitsplan op (BC.01) ☐ Stem continuïteitsplannen en bijhorende contactpersonen regelmatig met elkaar af (BC.01) ☐ Regel escrow in met belangrijke leveranciers (BC.01) ☐ Definieer en implementeer gecontroleerde toegang tot informatie(systemen) door leveranciers (SM.02, ID.01, ID.02, ID.03, ID.04, ID.05) ☐ Stel een security baseline per classificatieniveau vast voor leveranciers (SC.03, SC.04)	

[2] Laag = wanneer nodig, medium = 1x per 3 jaar en hoog = jaarlijks

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: VERSTORING ICT

Verstoringen in ICT kunnen bewust en onbewust veroorzaakt worden. Ondanks alle getroffen maatregelen kan het fout gaan en is een goede voorbereiding belangrijk.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Identificeer, documenteer, rapporteer en monitor IT-continuïteitsrisico's (RM.02). ☐ Stel beleid voor incident response vast, met in het bijzonder aandacht voor incidenten buiten kantoortijden en op feestdagen (IM.01, IM.03). ☐ Voer Business Impact Assessments (BIA) uit (RM.01)	☐ Zorg ervoor dat IT-beheer uitgevoerd wordt volgens best practices (zoals ITIL) (IM.01). ☐ Inventariseer of ICT-leveranciers anti-DDoS maatregelen geïmplementeerd hebben (SC.03). ☐ Stel vast of gemaakte afspraken (met leveranciers) over beschikbaarheid, zoals een Service Level Agreement (SLA), in lijn zijn met de eisen[3] (SC.01). ☐ Volg de adviezen van het Nationaal Cyber Security Centrum (NCSC) op (SM.07). ☐ Stel incident response procedures op en test ze minimaal jaarlijks[4], bijvoorbeeld met (N)OZON (IM.01, IM.03). ☐ Stel een disaster recovery plan op en test dit minimaal semi-jaarlijks, bijvoorbeeld met (N)OZON (BC.01, BC.02). ☐ Test het bedrijfscontinuïteitsplan minimaal semi-jaarlijks (BC.02).	☐ Maak gebruik van SURFcert om incidenten, zoals DDoS-aanvallen, te mitigeren (SM.08). ☐ Implementeer redundantie voor kritieke systemen (failover) om de beschikbaarheid te verhogen en de impact van een falend systeem te verminderen (BC.01). ☐ Implementeer 24/7 monitoring van ICT-infrastructuur (SOC/SIEM) met real-time waarschuwingen voor ongewone activiteiten of uitval van systemen (SM.04, SM.08). ☐ Voer regelmatig onderhoud uit en zorg voor tijdige updates en patches van soft- en hardware om bekende kwetsbaarheden aan te pakken (SM.06). ☐ Zorg ervoor dat je externe aanvalsoppervlak, en in het bijzonder edge devices, bekend en adequaat beschermd zijn (CO.01) ☐ Gebruik een reverse proxy voor je publieke website(s) om deze via het SURF netwerk te beschermen tegen DDoS-aanvallen (SM.08)

[3] Recovery Point Objective & Recovery Time Objective

[4] Ter inspiratie: https://github.com/certsocietegenerale/IRM & https://www.incidentresponse.org/playbooks/

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: ONVEILIG GEDRAG

Veilig gedrag kan tot op zekere hoogte technisch worden afgedwongen, maar nooit helemaal. Het is daarom van belang om continu aandacht te besteden aan de bewustwording van medewerkers en studenten. En om hen te ondersteunen in het vertonen van veilig gedrag.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Verkrijg commitment en ondersteuning van het bestuur voor het structureel verhogen en stimuleren van veilig gedrag (GO.01). ☐ Zorg voor een no-blame cultuur waarin fouten maken mag en er lering getrokken wordt uit (bijna) incidenten (IM.01) ☐ Pas threat modeling toe om de gelaagdheid van weerbaarheidsmaatregelen te bepalen, het mag niet mogelijk zijn dan één onveilige menselijke handeling direct leidt tot majeure schade (GO.04, RM.02) ☐ Stel KPI's vast om het effect van investeringen in het verhogen van de veiligheidscultuur meetbaar te maken (GO.03)	☐ Deel tips met studenten en medewerkers om zichzelf te beschermen[5] (HR.06) ☐ Organiseer regelmatig bewustwordingstrainingen en -campagnes om medewerkers en studenten te informeren over actuele cyberdreigingen en passend handelingsperspectief. Maak bijvoorbeeld gebruik van Cybersave Yourself (HR.06). ☐ Geef duidelijk aan dat berichten afkomstig zijn van buiten de organisatie (RM.02). ☐ Implementeer data loss prevention (DM.05). ☐ Maak het mogelijk om laagdrempelig incidenten te kunnen melden (IM.01). ☐ Voer bij incidenten oorzaakanalyses uit en deel de geleerde lessen (IM.01). ☐ Voer regelmatig social engineering simulaties uit (SM.05). ☐ Implementeer veilig sessiemanagement (SM.01). ☐ Implementeer het least privilege principe (ID.01). ☐ Informeer medewerkers en studenten over nieuwe aanmeldingen op accounts (SM.02). ☐ Beoordeel regelmatig de toegangsrechten om te voorkomen dat men onnodig toegang heeft (ID.05). ☐ Informeer medewerkers en studenten over de risico's en veilige alternatieven, bijvoorbeeld zoals de universiteit Utrecht[6] (RM.02). ☐ Train personeel in het herkennen van verdachte activiteiten (HR.06). ☐ Voer voorafgaand aan wijzigingen altijd een impact assessment uit (SM.06, SM.08, CH.01). ☐ Hanteer altijd het 4-ogenprincipe voordat wijzigingen worden doorgevoerd (CH.01). ☐ Zorg voor een rollback procedure voor grote wijzigingen en migraties (CH.01). ☐ Zorg voor gescheiden omgevingen voor ontwikkelen, testen en productie (CH.04).	☐ Monitor op uitgelekte gegevens van studenten en medewerkers (RM.02). ☐ Maak gebruik van URL scanning om de betrouwbaarheid van links te verifiëren (SM.12). ☐ Maak gebruik van SURFconext daar waar mogelijk (SM.02). ☐ Zorg ervoor dat MFA overal wordt afgedwongen en bepaal de sterkte daarvan op basis van een risico-afweging (ID.02). ☐ Tref daar waar MFA niet mogelijk is compenserende maatregelen, zoals automatisch account lock-out, monitoring en een sterk wachtwoordbeleid (ID.02). ☐ Implementeer conditionele toegang (ID.01). ☐ Maak gebruik van een Security Operations Center, zoals SURFsoc (SM.04). ☐ Implementeer de browser extensie Cookie Autodelete (SM.11). ☐ Monitor en analyseer DNS-verzoeken en firewallrapportages op het gebruik van schaduw-IT (SM.12). ☐ Implementeer endpoint protection (SM.12)

[5] https://laatjeniethackmaken.nl/, https://veiliginternetten.nl/, https://www.checkjelinkje.nl/, https://www.fixjeprivacy.nl/, https://github.com/Lissy93/personal-security-checklist

[6] Mooi voorbeeld: https://tools.uu.nl/tooladvisor/

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: CAPACITEITSTEKORT

Personeel capaciteitstekort in ICT en informatiebeveiliging is wereldwijd een groot probleem. Het vinden en zeker ook behouden van geschikte mensen is en blijft een uitdaging.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Stel met HR, met mandaat van het bestuur, strategie en beleid vast om competent personeel te werven, op te leiden en te behouden (HR.01, HR.02). ☐ Werk nauw(er) samen met omliggende instellingen om elkaars capaciteitstekorten op te lossen en om van elkaars expertise optimaal gebruik te maken (HR.05)	☐ Inventariseer en documenteer beschikbare kennis en expertise over informatiebeveiliging (HR.03). ☐ Identificeer hiaten in benodigde kennis en expertise over informatiebeveiliging (HR.03). ☐ Identificeer capaciteitstekorten en kaart deze aan bij het management/bestuur/CISO-as-a-service (HR.01). ☐ Maak gebruik van de SCIPR, SCIRT en overige communities van SURF (HR.05). ☐ Maak gebruik van het Security Expertise Centrum (HR.05). ☐ Maak gebruik van de SURFacademy om ontbrekende kennis en expertise in te vullen (HR.05). ☐ (MBO-only) Maak gebruik van het Netwerk IBP (HR.05). ☐ Laat systeem- en netwerkbeheerders deelnemen aan de TRANSITS trainingen (HR.02). ☐ Stel ambassadeurs voor informatiebeveiliging en privacy aan en laat hen kleine taken uitvoeren (zoals controle op vergrendelen werkplekken of verhogen awareness) (HR.05). ☐ (MBO-only) Maak gebruik van de CISO-as-a-Service dienst van het programma Cyberveiligheid (HR.05). ☐ Documenteer kennis om opleiding voor nieuwe medewerkers te versnellen (HR.05). ☐ Zet stages en traineeships op om jong talent aan te trekken (HR.01, HR.02). ☐ Zet interne trainingen op om medewerkers verder te ontwikkelen (HR.02). ☐ Sluit aan bij beroepsverenigingen zoals het Platform voor Informatiebeveiliging of ISACA (HR.05).	☐ Zet AI in om capaciteitstekorten te compenseren, bijvoorbeeld voor het automatiseren van terugkerende taken (chatbots, eerste lijn support, isoleren endpoints, etc.) (HR.03)

mbo digitaal

AANDACHTSPUNT SURF CYBERDREIGINGSBEELD: GOVERNANCE

Governance kan beschouwd worden als de motor van het managementsysteem voor informatiebeveiliging ('ISMS'). Zonder effectieve governance is het niet mogelijk om de informatiebeveiliging op orde te brengen en te houden. Zorg er daarom voor dat dit staat als een huis.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Beleg de eindverantwoordelijkheid voor informatiebeveiliging bij een lid van het College van Bestuur (OR.01). ☐ Positioneer de CISO (of vergelijkbare functionaris) op een onafhankelijke positie en zorg voor een directe verantwoordingslijn richting de portefeuillehouder informatiebeveiliging (OR.01). ☐ Stel voldoende middelen (tijd en geld) beschikbaar voor informatiebeveiliging (de Cybersecurityraad adviseert om minimaal 10% van het ICT-budget te alloceren) (GO.03). ☐ Stel taken, verantwoordelijkheden en bevoegdheden voor informatiebeveiliging vast en breng deze regelmatig op begrijpbare wijze onder de aandacht[7] (OR.01, GO.03). ☐ Stel een proces voor het managementsysteem voor informatiebeveiliging (ISMS) vast[8] (RM.01). ☐ Leg periodiek verantwoording af over informatiebeveiliging door middel van zelfevaluaties en audits (via de mbo-brede GRC-applicatie) om de effectiviteit van het (governance) beleid te beoordelen (GO.05).	☐ Identificeer tenminste de kritieke bedrijfsprocessen en -middelen, classificeer ze en koppel er verantwoordelijken aan (OR.01, RM.02). ☐ Zorg voor continue bijscholing en training voor het bestuur (NIS2) en management over nieuwe trends, ontwikkelingen en best practices met betrekking tot informatiebeveiliging (HR.02).	

[7] Voorbeeld: https://www.iso27000.es/assets/files/ISO27k%20RASCI%20table%20v5.xlsx
[8] https://www.ictrecht.nl/kennis/factsheets/isms-implementatieplan

mbo digitaal

AANDACHTSPUNT SURF CYBERDREIGINGSBEELD: RISICOMANAGEMENT

'Risicomanagement staat nog in kinderschoenen' is een statement dat geen nadere toelichting behoeft. Het is de kunst om risicomanagement te integreren in alle processen en activiteiten van de instelling.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Gebruik een GRC-applicatie ter ondersteuning van risicomanagement (RM.02). ☐ Stel een risicoregister op (bijvoorbeeld in Excel of in een GRC-applicatie) en registreer daarin alle risico's (RM.02). ☐ Voorzie alle risico's van een verantwoordelijke (op MT/CvB niveau) (RM.03). ☐ Evalueer alle hoog geclassificeerde risico's minimaal jaarlijks (RM.02). ☐ Integreer risicomanagement in projectplannen (RM.02). ☐ Integreer risicomanagement in inkooptrajecten (RM.02). ☐ Integreer risicomanagement in wijzigingen aan de fysieke omgeving (PH.01, PH.02) ☐ Pas Crime Prevention Through Environmental Design (CPTED) principes toe (PH.01, PH.02) ☐ Richt een 'tolpoort' in zodat de informatiebeveiligingsspecialist(en) altijd worden betrokken, zonder dat dit vertragend werkt (RM.01). ☐ Rapporteer ieder kwartaal over de status van risico's aan het CvB (RM.01). ☐ Maak gebruik van KPI's en KRI's (RM.03)	☐ Maak gebruik van de beschikbaar gestelde templates op het Security Expertise Centrum (HR.05). ☐ Integreer risicomanagement in de wijzigingsprocedure (CH.01).	☐ Hanteer security baselines voor hardware, software, firmware en cloudomgevingen op basis van een risico-afweging[9] (SM.01) ☐ Verifieer de effecten van updates op security baselines en stel die zo nodig bij (SM.01) ☐ Pas threat modeling toe om hiaten en kwetsbaarheden in de technische beveiliging te identificeren en op te lossen (GO.04, RM.02) ☐ Bepaal de ernst en daarmee oplosprioriteit van kwetsbaarheden op basis van de specifieke context te berekenen (CVSS)[10] (RM.01) ☐ Maak gebruik van Canarytokens om (mogelijke) inbreuken snel te detecteren (SM.07) ☐ Monitor Certificate Transparency (CT) logs om uitgegeven certificaten voor (typosquat) (sub)domeinen te detecteren (SM.10) ☐ Implementeer een DNS Certificate Authority Authorization (CAA) record voor alle TLD's (SM.10) ☐ Geef wildcard certificaten alleen uit voor subdomeinen en niet voor TLD's, dwing dit af in je CAA-record (SM.01)

[9] https://www.cisecurity.org/cis-benchmarks, https://ncp.nist.gov/repository, https://www.semperis.com/purple-knight/, https://www.pingcastle.com/, https://github.com/cisagov/ScubaGear, https://maester.dev/, https://ssl-config.mozilla.org/, Identificeren en oplossen van misconfiguraties en kwetsbaarheden in AD en M365 - versie 1.0.pdf, https://github.com/nsacyber/Hardware-and-Firmware-Security-Guidance

[10] https://www.cisa.gov/ssvc-calculator

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: IDENTITEITSFRAUDE

Van identiteitsfraude is sprake wanneer iemand zich bedient van andermans identiteit of een gecreëerde, fictieve identiteit om daarmee geld en/of goederen te verwerven. De identiteit kan voor uiteenlopende doeleinden worden mis- of gebruikt. Bijvoorbeeld om online bestellingen te plaatsen, leningen af te sluiten, een geldstroom af te buigen naar een andere bankrekening of mensen te benaderen met een zogenaamde hulpvraag. Identiteitsfraude kan verregaande gevolgen hebben voor slachtoffers. Daarom is het nodig om preventief maatregelen te treffen.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Identificeer sleutelfiguren en maak hen ervan bewust dat zij een hogere attractiviteit voor (cyber)criminaliteit hebben (HR.06) ☐ Voer regelmatig een kwetsbaarhedenanalyse op basis van openbare informatie (OSINT) uit om vast te stellen welke informatie over sleutelfiguren publiekelijk vindbaar zijn en acteer daar indien nodig op (RM.02) ☐ Maak sleutelfiguren extra bewust van de gevaren en train ze daarin (HR.06)	☐ Instrueer medewerkers over impersonatie technieken (spoofing (e-mail, SMS, instant messaging, social media, doppelgänger domeinen, etc.) (HR.06). ☐ Instrueer medewerkers om alert te zijn op verzoeken en deze altijd te verifiëren, met name door het toenemende gebruik van Deepfake technologie is het onderscheid maken tussen de werkelijkheid en oplichting veel lastiger (HR.06). ☐ Geef medewerkers en studenten tips om fraude te herkennen en te voorkomen[11] (HR.06).	☐ Maak gebruik van geavanceerde monitoringtools om ongebruikelijke activiteiten te detecteren en te waarschuwen, zoals (herhaalde) mislukte inlogpogingen of pogingen vanuit ongebruikelijke locaties (of blokkeer dit preventief) (SM.04) ☐ Implementeer maatregelen om weerstand te bieden tegen AitM-aanvallen (SM.07) ☐ Hanteer een Level of Assurance (LoA) dat past bij de risico's van identiteitsfraude (SM.02) ☐ Implementeer de e-mail beveiligingsstandaarden (SPF, DKIM, DMARC) voor alle beheerde (sub)domeinen (SM.07) ☐ Implementeer phishing bestendige MFA tenminste voor sleutelfiguren (SM.02)

[11] Fraudehelpdesk, Rijksoverheid, Slachtofferwijzer, Identiteitsfraude voorkomen en Consumentenbond

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: MISBRUIK IT/OT

Er zijn twee dreigingen verbonden aan dit risico: cryptomining en kwetsbaarhedenmanagement.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Verkrijg voor belangrijke systemen periodiek onafhankelijke assurance over de informatiebeveiliging (SM.05). ☐ Publiceer een coordinated vulnerability disclosure (CVD) beleid inclusief security.txt. MBO's kunnen aansluiten op het centrale CVD-beleid. (SM.05). ☐ Implementeer afwijkingsdetectie voor kostenanalyse in cloudomgevingen om onverwachte kosten snel te detecteren (SM.01) ☐ Monitor Operational Technology (OT) gerelateerde kwetsbaarheden (SM.07)	☐ Instrueer medewerkers alert te zijn op traagheid en het warm worden of blazen van hun apparaten (4.5, 4.6). ☐ Implementeer browserextensies om cryptomining tegen te gaan[12] (11.1). ☐ Services dienen hun eigen account met minimale privileges te gebruiken. Dit verkleint de risico's wanneer een enkele service wordt gecompromitteerd (10.1, 10.2, 10.3, 10.5). ☐ Valideer of de instellingen in overeenstemming zijn met security baselines (11.1). ☐ Valideer of leveranciers gebruik maken van security baselines en dat zelf (laten) valideren[13] (11.1). ☐ Implementeer basismaatregelen voor slimme apparaten (IoT) ☐ Harden Operational Technology (OT) assets[14]	☐ Monitor op algemene procesnamen die kunnen wijzen op misbruik[15] (SM.01, SM.04). ☐ Monitor prestaties van CPU en geheugen en wees alert op pieken in verbruik (SM.01, SM.04). ☐ Pas zero-trust principes toe, ga ervan uit dat dreigingen zowel binnen als buiten het netwerk kunnen bestaan en verifieer elke toegangspoging (SM.02). ☐ Beperk externe toegang door het gebruik van eduVPN en sterke authenticatie om externe toegang te beveiligen (SM.02). ☐ Verricht regelmatig penetratietesten om bekende kwetsbaarheden en mogelijke aanvalspaden te identificeren (SM.07). ☐ Identificeer, monitor en beperk het gebruik van Living-of-the-Land binaries en scripts (LOLBins)[16] (SM.01) ☐ Voorkom misconfiguraties in netwerken (SM.01) ☐ Identificeer infecties in je netwerk (SM.12) ☐ Waarborg de integriteit van backups (immutable) (OP.02) ☐ Beperk laterale communicatie tot het strikt noodzakelijke in (draadloze) netwerken (host/client isolation) (SM.11)

[12] https://ublockorigin.com/, https://github.com/xd4rker/MinerBlock, https://chrome.google.com/webstore/detail/easy-redirect-prevent-cry/kceciaijnoaceceljkggfocngjleimem

[13] We adviseren dit een vast onderdeel te maken van de leveranciersbeoordelingen

[14] https://www.dragos.com/blog/ot-cybersecurity-best-practices-for-smbs-system-hardening-an-ot-environment/ https://www.ncsc.nl/wat-kun-je-zelf-doen/technologische-ontwikkelingen/iacs-ot/aan-de-slag-met-het-beveiligen-van-ot-iacs, https://www.ncsc.nl/binaries/ncsc/documenten/publicaties/2019/mei/01/checklist-beveiliging-ics-scada/FS2012-02-Checklist-beveiliging-van-ICS-SCADA-systemen_archief.pdf

[15] Bijvoorbeeld child/fork processen

[16] https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/identifying-and-mitigating-living-off-the-land-techniques https://gtfobins.github.io/, https://www.loobins.io/, https://www.loldrivers.io/, https://lolbas-project.github.io/#

RISICO SURF CYBERDREIGINGSBEELD: DATAMANIPULATIE

Aantasting van de integriteit van informatie, hetzij bewust of onbewust, kan vervelende gevolgen hebben voor instellingen. Zorg er daarom voor dat er op verschillende niveaus maatregelen getroffen zijn om de integriteit te waarborgen.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Stel een gedragscode voor bezoekers, studenten en medewerkers vast (GO.02).	☐ Stel een procedure voor de omgang met informatie vast (DM.01, DM.02). ☐ In- en uitvoer van informatie is genormaliseerd, gevalideerd en gelimiteerd (DM.05). ☐ Maak uitsluitend gebruik van versleutelde verbindingen (DM.03, DM.05) ☐ Overweeg aanvullende maatregelen om data integriteit te waarborgen (DM.03). ☐ Maak gebruik van een data integriteit security checklist (DM.03).	☐ Log en monitor de toegang tot en het muteren of exfiltreren van informatie (DM.05). ☐ Verifieer altijd de checksums van software(updates) voordat deze worden gebruikt (RM.02). ☐ Verifieer of logging is geactiveerd en voldoende retentie heeft (min. 60 dagen) (SM.04). ☐ Verifieer of logging beschermd is tegen manipulatie (SM.04). ☐ Implementeer file integrity monitoring in Microsoft Defender (SM.04). ☐ Gebruik Canarytokens om datamanipulatie te detecteren (DM.03) ☐ Volg best practices voor event logging[17] (SM.04)

17 https://www.ic3.gov/CSA/2024/240822.pdf
https://sec.surf.nl/controls/sb-10-004-logging-events/
https://cheatsheetseries.owasp.org/cheatsheets/Logging_Cheat_Sheet.html#introduction

mbo digitaal

RISICO SURF CYBERDREIGINGSBEELD: SPIONAGE

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.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Identificeer politiek gevoelige projecten en samenwerkingen (RM.01) ☐ Identificeer de te beschermen belangen (TBB), bijvoorbeeld via de KWAS-methodiek (RM.01, CO.01) ☐ Overweeg (aanvullende) screening voor individuen die in aanraking komen met TBB (HR.01) ☐ Volg good practices om de risico's van insider threats te reduceren (HR.01) ☐ Monitor het darkweb en criminele fora op pogingen tot het rekruteren van studenten en medewerkers (RM.01)	☐ Implementeer taakroulatie en verplichte vakanties zodat men periodiek elkaars taken moet overnemen (HR.03, HR.04) ☐ Maak studenten en medewerkers bewust van de monitoringspraktijken bij de instelling, oftewel dat handelingen worden gelogd en dat daar vragen over gesteld kunnen worden (SM.04)	☐ Zie alle voorgaande technische aanbevelingen.

Relatie Cyberdreigingsbeeld met dienstverlening SURF en het programma Cyberveiligheid mbo

Instellingen kunnen gebruikmaken van de dienstverlening van SURF en initiatieven vanuit het programma Cyberveiligheid mbo om de risico's en aandachtspunten uit het Cyberdreigingsbeeld te adresseren. Deze tabel geeft de relaties tussen de risico's, het programma Cyberveiligheid mbo, dienstverlening van SURF en het SURFaudit toetsingskader weer. Samen met SURF hebben we een mooi overzicht gemaakt van de relatie tussen haar diensten, het SURFaudit toetsingskader en het NIST Cyber Security Framework 2.0.[18]

Cyberdreigingsbeeld 2023	Relatie SURFaudit toetsingskader	SURF-dienstverlening		Programma Cyberveiligheid
1. Informatielekken	BC.03 BC.04 CO.01 CO.02 CO.04 CO.05 DM.02 GO.02 HR.06 OP.02 SC.03 SC.04 SM.01 SM.05 SM.06 SM.07 SM.07 SM.08 SM.11 SM.12 SM.13	Capture the Flag HALON SURFcert SURFdomeinen SURFfirewall	SURFinternet SURFlichtpaden SURFmailfilter SURFsoc SURFwireless	CISO-as-a-Service GRC-applicatie Red Teaming Riskpooling Aanbesteding pentesting Check tot hack
2. Ketenafhankelijkheid	SC.01 SC.03 SC.04 SD.01 BC.01 SM.02 ID.01 ID.02 ID.03 ID.04 ID.05	Aansluiting dislocatie HPC Cloud ICT-inkoop Regie Office 365	SURFcumulus SURFdashboard SURFdomeinen Vendor Compliance	Applicatiecatalogus Centrale DPIA's CISO-as-a-Service GRC-applicatie Check tot hack
3. Verstoring ICT	BC.01	(N)OZON	SURFcert	CISO-as-a-Service

[18] https://sec.surf.nl/wp-content/uploads/2024/10/Cyberweerbaarheid-en-SURF-diensten.pdf

	BC.02 CO.01 IM.01 IM.03 RM.01 RM.02 SC.01 SC.03 SM.04 SM.06 SM.07 SM.08	Capture the Flag HALON	SURFdashboard SURFopzichter	GRC-applicatie Red Teaming Risk pooling Aanbesteding pentesting Check tot hack
4. **Onveilig gedrag**	CH.01 CH.04 DM.05 GO.01 GO.03 GO.04 HR.06 ID.01 ID.02 ID.05 IM.01 RM.02 SM.01 SM.02 SM.04 SM.05 SM.06 SM.08 SM.11 SM.12	Consultancy Cybersave Yourself eduVPN Security Expertise Centrum Privacy Expertise Centrum	SURFacademy SURFconext SURFsecureID SURFsoc	0-meting awareness 0-meting governance CISO-as-a-Service GRC-applicatie Netwerk IBP Red Teaming MBOKS
5. Capaciteitstekort	HR.01 HR.02 HR.03 HR.05	Consultancy Security Expertise Centrum Privacy Expertise Centrum	SURFacademy SURFcommunities (SCIPR/SCIRT)	Centrale DPIA's CISO-as-a-Service GRC-applicatie Netwerk IBP
6. Governance	GO.03 GO.05 HR.02 OR.01 RM.01 RM.02	(N)OZON Security Expertise Centrum Privacy Expertise Centrum	SURFaudit SURFcommunities (SCIPR/SCIRT)	0-meting governance CISO-as-a-Service Cyberconvenant GRC-applicatie
7. Risicomanagement	CH.01 GO.04 HR.05 PH.01 PH.02 RM.01 RM.02	(N)OZON Capture the Flag Cyberdreigingsbeeld HALON ICT-inkoop IV-metingen NBA Microsoft policy templates	Regie Office 365 Security Expertise Centrum SURFaudit SURFcommunities (SCIPR/SCIRT) SURFsoc Vendor Compliance	Centrale DPIA's CISO-as-a-Service GRC-applicatie Red Teaming Security Audits Toetsingskader privacy Aanbesteding pentesting

	RM.03 SM.01 SM.07 SM.10			Check tot hack
8. Identiteitsfraude	HR.06 RM.02 SM.02 SM.04 SM.07	eduVPN SURFconext	SURFsecureID	CISO-as-a-Service GRC-applicatie Riskpooling
9. Misbruik IT/OT	HR.06 ID.01 OP.02 SC.03 SM.01 SM.02 SM.04 SM.05 SM.07 SM.11 SM.12	Zie '1. Verkrijging en openbaarmaking van informatie'.		CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting Check tot hack
10. Imagoschade	Zie #1	Zie '1. Verkrijging en openbaarmaking van informatie'.		CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting
11. Datamanipulatie	DM.01 DM.02 DM.03 DM.05 GO.02 RM.02 SM.04	SURFcertificaten SURFconext	SURFdomeinen	CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting Check tot hack
12. Spionage	CO.01 HR.01 HR.03 HR.04 RM.01 SM.04			