mbo digitaal

MEMO

Praktische vertaling Cyberdreigingsbeeld 2023

Datum
12 oktober 2023

Auteur
Mick Deben CISSP CRISC CGEIT CCSP

Wat betekent het Cyberdreigingsbeeld 2023 voor mbo-instellingen? Hoe geef je er als verantwoordelijke IBP'er praktisch invulling aan? In dit memo geven we praktische tips en vertellen we welke zaken we vanuit het programma Cyberveiligheid oppakken.

Het onlangs door SURF gepubliceerde Cyberdreigingsbeeld 2023 is net als vergelijkbare publicaties gebaseerd op gebeurtenissen en trends uit het verleden. Het biedt het dus geen garanties voor de toekomst. En hoewel we helaas geen invloed kunnen uitoefenen op het dreigingslandschap, kunnen we er samen wel voor zorgen dat we onze zaken op orde brengen en houden. Zo kunnen we de impact van cyberaanvallen beperken, onze informatie beschermen en de continuïteit van de bedrijfsvoering en het onderwijs waarborgen. Daarbij gebruiken we het Cyberdreigingsbeeld als input om sectorbrede risico's te definiëren. Ook koppelen we het rapport aan de NBA-modelaanpak, bijvoorbeeld door op basis van de cyberdreigingen de streefvolwassenheid voor NBA-beheerdoelstellingen te bepalen.

Prioriteit van de risico's

Op basis van de in het Cyberdreigingsbeeld 2023 genoemde ontwikkelingen in het dreigingslandschap, risicoperceptie van de instellingen en incidenten die zich hebben voorgedaan, kunnen we het aanpakken van de risico's prioriteren volgens het schema in de volgende kolom. Aanvullend op deze risico's benoemt het Cyberdreigingsbeeld governance en risicomanagement als belangrijke aandachtspunten. In dit memo behandelen we deze twee punten daarom ook als categorie 'prioriteit 1'.

Omdat het spionagerisico dusdanig laag wordt ingeschaald, besteden we er in dit memo geen aandacht aan.

Stapsgewijs risico's verkleinen

Op de volgende pagina's hebben we voor ieder risico en 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 NBA-toetsingskader gelegd. Deze verwijzingen herken je 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 van cyberaanvallen.

Relatie met programma Cyberveiligheid en dienstverlening SURF
We sluiten dit memo af met een tabel waarin we de relaties van de in het Cyberdreigingsbeeld 2023 genoemde risico's en aandachtspunten met initiatieven vanuit het programma Cyberveiligheid mbo, dienstverlening van SURF en het NBA-model overzichtelijk in kaart brengen. Instellingen kunnen van de dienstverlening en initiatieven gebruikmaken om de risico's uit het Cyberdreigingsbeeld te adresseren.

Wat doen we verder om cyberrisico's te verkleinen?
Vanuit het programma Cyberveiligheid ondernemen we nog veel meer initiatieven om de in het Cyberdreigingsbeeld geïdentificeerde risico's en aandachtsgebieden te adresseren. Dat doen we onder meer met de volgende acties:

1. Beoordelen hoe de 11 use cases van SURFsoc zich verhouden tot de risico's uit het Cyberdreigingsbeeld. We onderzoeken of SURFsoc de TTP's (tactics, techniques and procedures) adequaat afdekt.
2. Instellingen stimuleren om van de (netwerk)diensten van SURF gebruik te maken (anti-DDoS-maatregelen en geavanceerde monitoring).
3. Onderzoeken of de generieke processen van mbo's centraal geclassificeerd kunnen worden, inclusief het beleggen van het eigenaarschap (RASCI). ROSA dient hiervoor als bron.
4. Bijdragen aan het verbeteren en aanvullen van beschikbare content in het Security Expertise Centrum.
5. Onderzoeken hoe we instellingen verder kunnen ondersteunen bij vulnerability management.
6. Verder ontwikkelen van de CISO-as-a-Service-dienstverlening.
7. De website MBO Digitaal verder uitbreiden.

We communiceren updates over de voortgang van bovengenoemde zaken via de nieuwsbrieven en het netwerk IBP. Mochten er naar aanleiding van dit memo vragen of opmerkingen zijn, neem dan contact op met m.deben@mbodigitaal.nl of stuur een (chat)bericht via het netwerk IBP.

mbo digitaal

MEMO

RISICO'S SURF CYBERDREIGINGSBEELD 2023: 1 – VERKRIJGING EN OPENBAARMAKING VAN INFORMATIE / 8 – BEWUST BESCHADIGEN IMAGO

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
☐ Identificeer politiek gevoelige samenwerkingen en projecten (3.1, 3.2, 3.3).	☐ Identificeer alle domeinen in eigendom van de instelling (5.1, 5.2).	☐ Gebruik SURFmailfilter (11.7, 11.11, 11.12).
☐ Monitor het internet en darkweb op relevante zoektermen passend daarbij (3.1, 3.2, 3.3).	☐ Lever een lijst met alle domeinen aan bij SURF t.b.v. IV-metingen (niet nodig met SURFdomeinen) (5.1, 5.2).	☐ Controleer minimaal wekelijks geautomatiseerd zowel de buitenkant als de binnenkant van netwerken op bekende kwetsbaarheden en misconfiguraties (11.6, 11.7, 11.11, 11.12, 11.13).
☐ Neem in het patchbeleid ook contentmanagementsystemen (CMS) en plug-ins van websites op (1.2).	☐ Bevorder de bewustwording rondom het herkennen van phishingberichten (4.6).	☐ Prioriteer patches op basis van de ernst van de kwetsbaarheid en overige factoren (11.6).
☐ Krijg grip op de risico's in de toeleveringsketen (3.1, 3.2, 3.3).	☐ Monitor proactief op de registratie van en wijzigingen aan domeinen die lijken op die van instelling (5.2).	☐ Test patches voordat deze in productieomgevingen worden doorgevoerd (11.6).
	☐ Hanteer een 'deny-by-default'-beleid en sta alleen goedgekeurde verbindingen toe (11.1).	☐ Segmenteer de securityfunctie van de rest van het netwerk (monitoring, authenticatie en administratie) (11.11).
	☐ Zorg ervoor dat medewerkers en studenten geen of beperkt (whitelist) software kunnen installeren[1] (10.1, 11.1).	☐ Segmenteer web- en mailservers van de rest van het netwerk (DMZ) (11.11, 11.12, 11.13).
	☐ Schakel macro's in Office-bestanden uit of sta alleen ondertekende macro's toe (11.1).	☐ Definieer de richting van verkeer tussen segmenten en toegestane protocollen (11.11, 11.12, 11.13).
	☐ Schakel ActiveX in Office-bestanden uit (11.1).	☐ Investeer in geavanceerde endpointdetectie- en responsoplossingen (11.3, 11.4, 11.7, 11.11, 11.12, 11.13).
	☐ Schakel automatisch afspelen uit ('AutoPlay' en 'AutoRun')[2] (11.1).	☐ Leid uitgaand verkeer via een proxy naar buiten toe of gebruik DNS-filtering[3] om malafide domeinen en IP-adressen te blokkeren (Spamhaus, Barracuda, AbuseIPDB, etc.) (11.11).
	☐ Zet USB-poorten dicht en blokkeer USB-opslag, tenzij noodzakelijk (beperk gebruik) (11.1).	☐ Implementeer een Web Application Firewall (WAF) op alle publieke websites (11.7, 11.11, 11.12).
	☐ Definieer hersteltijden voor verschillende soorten informatie (Recovery Point Objective) (14.1).	
	☐ Maak back-ups volgens de 3-2-1-regel (3 back-ups, 2 verschillende media, 1 offline) (14.3, 14.4).	
	☐ Implementeer de security headers op alle (sub)domeinen (11.1).	

[1] Let ook op browser-extensies en M365-plugins

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

[3] In de toekomst mogelijk een onderdeel van SURFdomeinen

RISICO SURF CYBERDREIGINGSBEELD 2023: 2 - 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
☐ Koppel intern eigenaren aan leveranciers (2.1). ☐ Stel beleid voor leveranciersmanagement vast (1.2). ☐ Neem de evaluatie van leveranciers ten aanzien van informatiebeveiliging op in de planning en zie toe op de uitvoering en opvolging daarvan (1.3).	☐ Identificeer alle leveranciers en partners en classificeer ze ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid (laag, midden of hoog) (15.3). ☐ Evalueer leveranciers aan de hand van hun classificatie en risico voor de instelling, bijvoorbeeld via audits, penetratietesten, certificeringen en prestatiegesprekken (SLA)[4] (15.1, 15.2, 15.3, 15.4). ☐ Stel standaard clausules voor informatiebeveiliging op, passend bij de classificatie (11.1). ☐ Gebruik de SURF Security Baseline om minimale eisen aan leveranciers op te leggen (11.1). ☐ Gebruik STITCH en OWASP als minimale eisen voor applicaties (11.1). ☐ Neem deel aan de SURF-aanbesteding voor vendor risk management (15.3). ☐ Bereid je voor op incidenten in de keten, stel een bedrijfscontinuïteitsplan op (14.1). ☐ Stem continuïteitsplannen en bijhorende contactpersonen regelmatig met elkaar af (14.1, 14.2). ☐ Regel escrow in met belangrijke leveranciers (15.3). ☐ Definieer en implementeer gecontroleerde toegang tot informatie(systemen) door leveranciers (10.1, 10.2, 10.3, 10.4, 10.5).	

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

RISICO SURF CYBERDREIGINGSBEELD 2023: 3 – 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
☐ Zie risico 'ketenafhankelijkheid'.	☐ Zorg ervoor dat IT-beheer uitgevoerd wordt volgens best practices (zoals ITIL) (5.1, 5.2, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6).	☐ Maak gebruik van SURFcert om DDoS-aanvallen te mitigeren (11.8, 11.11).
☐ Identificeer, documenteer, rapporteer en monitor IT-continuïteitsrisico's (3.1, 3.2, 3.3).	☐ Inventariseer of ICT-leveranciers anti-DDoS maatregelen geïmplementeerd hebben (15.3, 15.4).	☐ Implementeer redundantie voor kritieke systemen (failover) om de beschikbaarheid te verhogen en de impact van een falend systeem te verminderen (11.8, 11.9).
☐ Stel beleid voor incident response vast, met in het bijzonder aandacht voor incidenten buiten kantoortijden en op feestdagen (1.2, 1.3).	☐ Stel vast of gemaakte afspraken (met leveranciers) over beschikbaarheid, zoals een Service Level Agreement (SLA), in lijn zijn met de eisen[5] (15.1, 15.2). ☐ Volg de adviezen van het Nationaal Cyber Security Centrum (NCSC) op (14.1, 14.2, 14.3, 14.4, 14.5). ☐ Stel incident response procedures op en test ze minimaal jaarlijks[6] (6.1, 6.2, 6.3, 6.4). ☐ Stel een disaster recovery plan op en test dit minimaal semi-jaarlijks (14.1, 14.2, 14.5). ☐ Test het bedrijfscontinuïteitsplan minimaal semi-jaarlijks (6.1, 6.2, 6.3, 14.1, 14.2, 14.5).	☐ Implementeer 24/7 monitoring van ICT-infrastructuur met real-time waarschuwingen voor ongewone activiteiten of uitval van systemen (11.4, 11.7, 11.8, 11.11, 11.12, 13.3). ☐ Voer regelmatig onderhoud uit en zorg voor tijdige updates en patches van soft- en hardware om bekende kwetsbaarheden aan te pakken (11.6, 11.7, 11.9).

[5] Recovery Point Objective & Recovery Time Objective

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

RISICO SURF CYBERDREIGINGSBEELD 2023: 4 – ONVEILIG GEDRAG EN GEBREK AAN AWARENESS

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 (1.1, 1.3).	☐ Deel tips met studenten en medewerkers om zichzelf te beschermen[7] (4.6). ☐ Organiseer regelmatig bewustwordingstrainingen en -campagnes om medewerkers en studenten te informeren over actuele cyberdreigingen en passend handelingsperspectief. Maak bijvoorbeeld gebruik van Cybersave Yourself (4.6). ☐ Geef duidelijk aan dat berichten afkomstig zijn van buiten de organisatie (4.6). ☐ Implementeer data loss prevention in Microsoft 365 (9.1, 9.2, 9.3, 9.4, 9.5). ☐ Maak het mogelijk om laagdrempelig incidenten te kunnen melden (6.1). ☐ Voer bij incidenten oorzaakanalyses uit en deel de geleerde lessen (6.3, 6.4). ☐ Voer regelmatig social engineering simulaties uit (4.6). ☐ Implementeer veilig sessiemanagement (11.1). ☐ Implementeer het least privilege principe (10.1, 10.5). ☐ Informeer medewerkers en studenten over nieuwe aanmeldingen op accounts (4.6). ☐ Beoordeel regelmatig de toegangsrechten om te voorkomen dat men onnodig toegang heeft (10.5). ☐ Informeer medewerkers en studenten over de risico's en veilige alternatieven[8] (4.6). ☐ Train personeel in het herkennen van verdachte activiteiten en maak duidelijk hoe en waar ze dat kunnen melden (4.6, 6.1). ☐ Zorg voor gescheiden omgevingen voor ontwikkelen, testen en productie (7.1, 7.4). ☐ Voer voorafgaand aan wijzigingen altijd een impact assessment uit (7.2). ☐ Hanteer altijd het 4-ogenprincipe voordat wijzigingen worden doorgevoerd (7.6). ☐ Zorg voor een rollback procedure voor grote wijzigingen en migraties (7.1, 7.6).	☐ Monitor op uitgelekte gegevens van studenten en medewerkers (11.7). ☐ Maak gebruik van Safe Links in Microsoft 365 (11.7). ☐ Implementeer Microsoft Defender for endpoints (11.4, 11.7, 11.12). ☐ Maak gebruik van SURFconext daar waar mogelijk (11.2). ☐ Zorg ervoor dat MFA overal wordt afgedwongen (11.2, 11.3). ☐ Tref daar waar MFA niet mogelijk is compenserende maatregelen, zoals automatisch account lock-out, monitoring en een sterk wachtwoordbeleid (11.2, 11.3). ☐ Implementeer conditionele toegang in Microsoft 365 (11.3). ☐ Maak gebruik van SURFsoc (11.4, 11.7, 11.11, 11.12, 11.13). ☐ Implementeer de browser extensie Cookie Autodelete (11.7). ☐ Monitor en analyseer DNS-verzoeken en firewallrapportages op het gebruik van schaduw-IT (11.4, 11.7).

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

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

RISICO SURF CYBERDREIGINGSBEELD 2023: 5 – 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 het bestuur strategie en beleid vast om competent personeel te werven, op te leiden en te behouden (1.1, 1.2).	☐ Inventariseer en documenteer beschikbare kennis en expertise over informatiebeveiliging (4.2). ☐ Identificeer hiaten in benodigde kennis en expertise over informatiebeveiliging (4.1, 4.2, 4.3). ☐ Identificeer capaciteitstekorten en kaart deze aan bij het management/bestuur/CISO-as-a-service (4.1, 4.2, 4.3). ☐ Maak gebruik van de SCIPR, SCIRT en overige communities van SURF (4.5). ☐ Maak gebruik van het Security Expertise Centrum (4.5). ☐ Maak gebruik van de SURFacademy om ontbrekende kennis en expertise in te vullen (4.2). ☐ Maak gebruik van het Netwerk IBP (4.5). ☐ Laat systeem- en netwerkbeheerders deelnemen aan de TRANSITS trainingen (4.2). ☐ Stel ambassadeurs voor informatiebeveiliging en privacy aan en laat hen kleine taken uitvoeren (zoals controle op vergrendelen werkplekken of verhogen awareness) (4.6). ☐ Maak gebruik van de CISO-as-a-Service dienst van het programma Cyberveiligheid (4.1, 4.3, 4.5, 4.6). ☐ Documenteer kennis om opleiding voor nieuwe medewerkers te versnellen (4.2). ☐ Zet stages en traineeships op om jong talent aan te trekken (4.1, 4.2). ☐ Zet interne trainingen op om huidige medewerkers verder te ontwikkelen (4.2). ☐ Sluit aan bij beroepsverenigingen zoals het Platform voor Informatiebeveiliging of ISACA (4.4, 4.6).	

AANDACHTSPUNT SURF CYBERDREIGINGSBEELD 2023: 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 behouden. 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 (2.1). ☐ Positioneer de CISO (of vergelijkbare functionaris) op een onafhankelijke positie en zorg voor een directe verantwoordingslijn richting de portefeuillehouder informatiebeveiliging (2.1, 2.2). ☐ Stel voldoende middelen (tijd en geld) beschikbaar voor informatiebeveiliging (de Cybersecurity raad adviseert om minimaal 10% van het ICT-budget te alloceren) (1.1, 1.3). ☐ Stel taken, verantwoordelijkheden en bevoegdheden voor informatiebeveiliging vast[9] (1.2, 2.1). ☐ Stel een proces voor het managementsysteem voor informatiebeveiliging (ISMS) vast[10] (1.2, 1.3, 2.1, 2.2). ☐ 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 (1.1, 1.2, 1.5, 2.1).	☐ Identificeer tenminste de kritieke bedrijfsprocessen en -middelen, classificeer ze en koppel er eigenaren aan (5.1, 5.2). ☐ Zorg voor continue bijscholing en training voor het bestuur en management over nieuwe trends, ontwikkelingen en best practices met betrekking tot informatiebeveiliging (4.5, 4.6).	

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

mbo digitaal

MEMO

AANDACHTSPUNT SURF CYBERDREIGINGSBEELD 2023: 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
☐ Implementeer en gebruik de mbo-brede GRC-applicatie zo snel mogelijk ter ondersteuning van risicomanagement (1.2, 1.3, 2.1, 3.1, 3.2, 3.3). ☐ Stel een risicoregister op (bijvoorbeeld in Excel of in mbo-brede GRC-applicatie) en registreer daarin alle risico's (3.3). ☐ Voorzie alle risico's van een eigenaar (op MT/CvB niveau) (2.1, 3.1, 3.2, 3.3). ☐ Evalueer alle hoog geclassificeerde risico's minimaal jaarlijks (3.2). ☐ Integreer risicomanagement in projectplannen (3.1, 3.2, 3.3). ☐ Integreer risicomanagement in inkooptrajecten (3.1, 3.2, 3.3). ☐ Richt een 'tolpoort' in zodat de informatiebeveiligingsspecialist(en) altijd worden betrokken (3.1, 3.2, 3.3). ☐ Rapporteer ieder kwartaal over de status van risico's aan het CvB (3.1, 3.2, 3.3).	☐ Maak gebruik van de beschikbaar gestelde templates op het Security Expertise Centrum (4.5). ☐ Integreer risicomanagement in de wijzigingsprocedure (7.2).	

RISICO SURF CYBERDREIGINGSBEELD 2023: 6 – 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
☐ Zie risico 'onveilig gedrag medewerkers en gebrek aan awareness'.	☐ Instrueer medewerkers over impersonatietechnieken (spoofing (e-mail, SMS, instant messaging, social media), doppelgänger domeinen, etc.) (4.5, 4.6). ☐ Instrueer medewerkers om alert te zijn op verzoeken en deze altijd te verifiëren (4.5, 4.6). ☐ Geef medewerkers en studenten tips om fraude te herkennen en te voorkomen[11] (4.5, 4.6). ☐ Zie 'autorisatiebeheer' onder risico 4.	☐ 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) (11.4, 11.7, 11.11, 11.12).

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

RISICO SURF CYBERDREIGINGSBEELD 2023: 7 – OVERNAME EN MISBRUIK ICT

Er zijn twee dreigingen verbonden aan dit risico: cryptomining en kwetsbaarhedenmanagement.[12] Kwetsbaarhedenmanagement is een belangrijk aandachtspunt. Het aantal meldingen door SURFcert is het afgelopen jaar gestegen naar 1741 ten opzichte van 891 het jaar daarvoor. Dat is een toename van liefst 95%! Het is dus belangrijk om hier extra alert op te zijn.

GOVERNANCE	PROCESSEN	TECHNIEK
☐ Verkrijg voor belangrijke systemen periodiek onafhankelijke assurance over de informatiebeveiliging (1.5).	☐ 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[14] (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[15] (11.1). ☐ Maak gebruik van het centrale coordinated vulnerability disclosure (CVD) beleid van MBO Digitaal en neem het security.txt op in alle publieke websites[16] (11.1, 11.7).	☐ Monitor op algemene procesnamen die kunnen wijzen op misbruik[13] (11.4, 11.7). ☐ Monitor prestaties van CPU en geheugen en wees alert op pieken in verbruik (13.3). ☐ Pas zero-trust principes toe, ga ervan uit dat dreigingen zowel binnen als buiten het netwerk kunnen bestaan en verifieer elke toegangspoging (11.2, 11.3, 11.7, 11.11, 11.12, 11.13). ☐ Beperk externe toegang door het gebruik van eduVPN en sterke authenticatie om externe toegang te beveiligen (11.2, 11.3). ☐ Verricht regelmatig penetratietesten om bekende kwetsbaarheden en mogelijke aanvalspaden te identificeren (11.5).

[12] Zie voor kwetsbaarheden management 'verkrijging en openbaarmaking van informatie'
[13] Bijvoorbeeld child/fork processen
[14] https://ublockorigin.com/, https://github.com/xd4rker/MinerBlock, https://chrome.google.com/webstore/detail/easy-redirect-prevent-cry/kceciaijnoaceceljkggfocngjleimem
[15] We adviseren dit een vast onderdeel te maken van de leveranciersbeoordelingen
[16] Publiceer het security.txt bestand onder het /.well-known/ pad (https://instelling.nl/.well-known/security.txt)

RISICO SURF CYBERDREIGINGSBEELD 2023: 9 – MANIPULATIE VAN DATA

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.

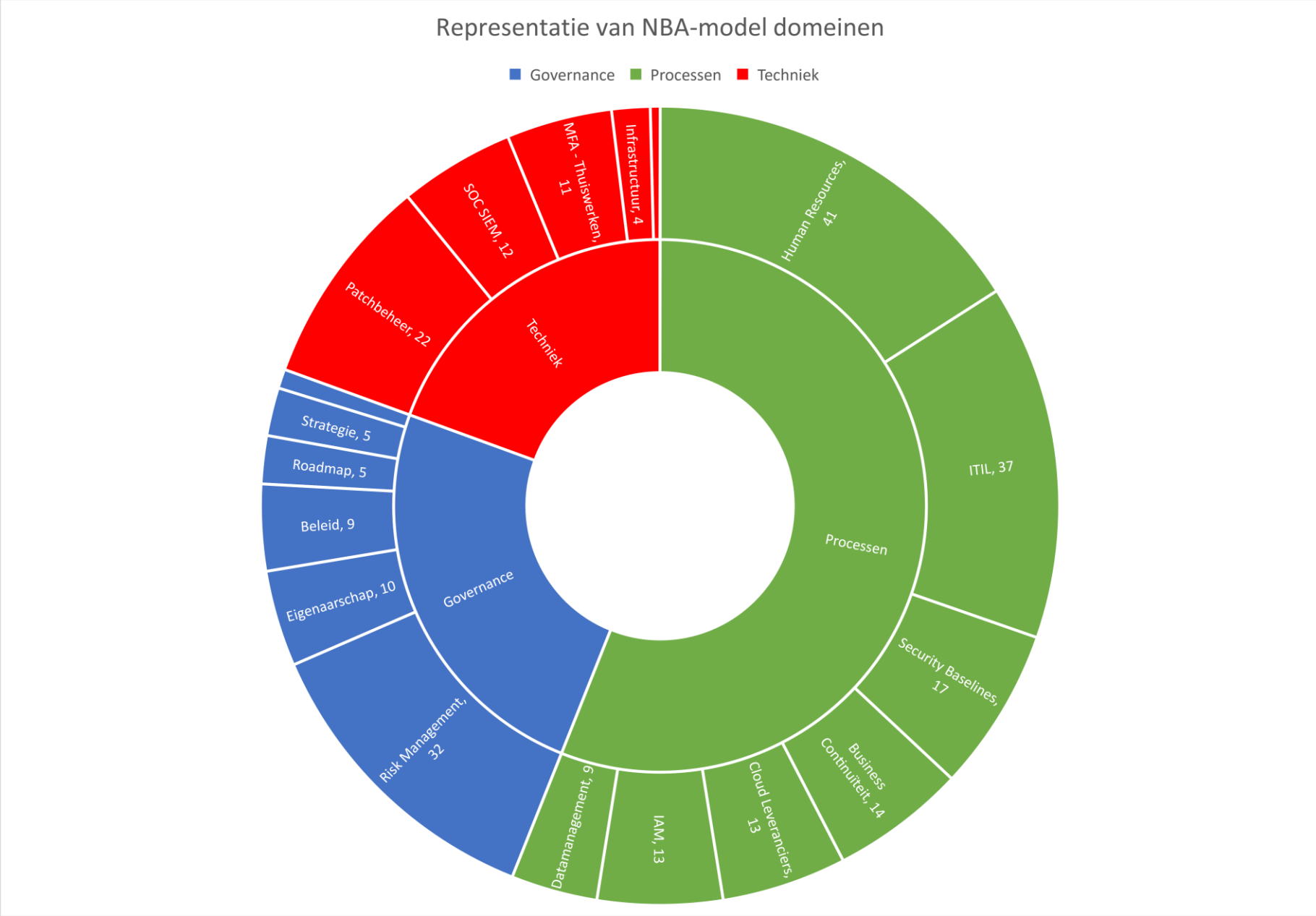
GOVERNANCE	PROCESSEN	TECHNIEK
☐ Stel een gedragscode vast (1.2).	☐ Stel een procedure voor de omgang met informatie vast (9.1, 9.3).	☐ Log en monitor de toegang tot en het muteren of exfiltreren van informatie (11.4).
	☐ In- en uitvoer van informatie is genormaliseerd, gevalideerd en gelimiteerd (11.1).	☐ Verifieer altijd de checksums van software(updates) voordat deze worden gebruikt (11.6).
	☐ Maak uitsluitend gebruik van versleutelde verbindingen (11.1)	☐ Verifieer of logging is geactiveerd en voldoende retentie heeft (11.4).
	☐ Overweeg aanvullende maatregelen om data integriteit te waarborgen (9.3).	☐ Verifieer of logging beschermd is tegen manipulatie (11.4).
	☐ Maak gebruik van een data integriteit security checklist (9.3).	☐ Implementeer file integrity monitoring in Microsoft Defender (11.7).

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 2023 te adresseren. Deze tabel geeft de relaties tussen de risico's, het programma Cyberveiligheid mbo, dienstverlening van SURF en het NBA-model weer.

Cyberdreigingsbeeld 2023	Relatie NBA	SURF-dienstverlening		Programma Cyberveiligheid
1. Verkrijging en openbaarmaking van informatie	6.1, 6.2, 6.3, 6.4, 11.1, 11.5, 11.6, 11.7, 11.11, 14.3,	Capture the Flag HALON NBA Microsoft policy templates SURFcert SURFdomeinen SURFfirewall	SURFinternet SURFlichtpaden SURFmailfilter SURFsoc SURFwireless	CISO-as-a-Service GRC-applicatie Red Teaming Riskpooling Aanbesteding pentesting
2. Ketenafhankelijkheid	15.1, 15.2, 15.3, 15.4	Aansluiting dislocatie HPC Cloud ICT-inkoop Regie Office 365	SURFcumulus SURFdashboard SURFdomeinen Vendor risk management	Applicatiecatalogus Centrale DPIA's CISO-as-a-Service GRC-applicatie
3. Verstoring ict	6.1, 6.2, 6.3, 6.4, 11.5, 14.1, 14.2, 14.3, 14.4, 14.5	(N)OZON Capture the Flag HALON	SURFcert SURFdashboard SURFopzichter	CISO-as-a-Service GRC-applicatie Red Teaming Risk pooling Aanbesteding pentesting
4. Onveilig gedrag en gebrek aan awareness	4.5, 4.6, 6.1, 6.2, 6.3, 6.4, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6	Consultancy Cybersave Yourself eduVPN Security Expertise Centrum	SURFacademy SURFconext SURFsecureID SURFsoc	0-meting awareness 0-meting governance CISO-as-a-Service GRC-applicatie Netwerk IBP Red Teaming
5. Capaciteitstekort	4.1, 4.2, 4.3, 13.3	Consultancy Security Expertise Centrum	SURFacademy SURFcommunities (SCIPR/SCIRT)	Centrale DPIA's CISO-as-a-Service GRC-applicatie Netwerk IBP
6. Governance	1.1, 1.2, 1.3, 1.4, 1.5	(N)OZON Security Expertise Centrum	SURFaudit SURFcommunities (SCIPR/SCIRT)	0-meting governance CISO-as-a-Service Cyberconvenant GRC-applicatie
7. Risicomanagement	1.3, 1.5, 3.1, 3.2, 3.3, 11.5	(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 Risk Management	Centrale DPIA's CISO-as-a-Service GRC-applicatie Red Teaming Security Audits Toetsingskader privacy Aanbesteding pentesting

8. Identiteitsfraude	4.5, 4.6	eduVPN SURFconext	SURFsecureID	CISO-as-a-Service GRC-applicatie Riskpooling
9. Overname en misbruik ict	Zie #1	Zie '1. Verkrijging en openbaarmaking van informatie'.		CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting
10. Bewust beschadigen imago	Zie #1	Zie '1. Verkrijging en openbaarmaking van informatie'.		CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting
11. Manipulatie van data	1.2, 2.1, 2.2, 8.1, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 11.1, 11.4	SURFcertificaten SURFconext	SURFdomeinen	CISO-as-a-Service GRC-tool Riskpooling Aanbesteding pentesting


Representatie van NBA-model domeinen
Governance
Processen
Techniek
Human Resources, 41
ITIL, 37
Security Baselines, 17
Business Continuïteit, 14
Cloud Leveranciers, 13
IAM, 13
Datamanagement, 9
Risk Management, 32
Eigenaarschap, 10
Beleid, 9
Roadmap, 5
Strategie, 5
Patchbeheer, 22
SOC SIEM, 12
MFA - Thuiswerken, 11
Infrastructuur, 4
Techniek
Processen
Governance

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