CyFun®

CyberFundamentals 2025

Nederlands

Version 2025-10-01

INHOUD

INLEIDING

Het CyberFundamentals Framework is een raamwerk dat eigendom is van het Centrum voor Cybersecurity België (CCB). Het raamwerk bestaat uit een reeks concrete maatregelen en biedt een duidelijke, stapsgewijze aanpak die organisaties helpt om:

- hun gegevens te beschermen,
- het risico op de meest voorkomende cyberaanvallen aanzienlijk te verminderen,
- en hun cyberweerbaarheid te vergroten.

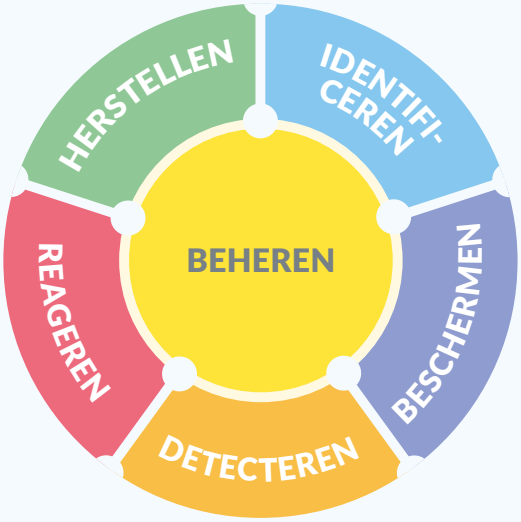
De vereisten, ook wel controles of maatregelen genoemd, worden ondersteund door relevante inzichten uit het NIST Cybersecurity Framework[1] , ISO 27001/ISO 27002, IEC 62443 en de CIS Critical Security Controls (ETSI TR 103 305-1).

Het raamwerk is opgebouwd rond **zes kernfuncties**: beheren, identificeren, beschermen, detecteren, reageren en herstellen. Deze zes functies ondersteunen duidelijke communicatie binnen alle onderdelen van de organisatie, zowel technisch als niet-technisch, waardoor cyberrisico's gemakkelijker te begrijpen, te bespreken en te beheren zijn. Door een gemeenschappelijke taal te gebruiken, helpen ze cybersecurity te integreren in bredere zakelijke beslissingen en de algehele risicobeheerstrategie.

1 De codering van de vereisten komt overeen met de codes die worden gebruikt in het NIST CSF-raamwerk. Aangezien niet alle NIST CSF-vereisten van toepassing zijn, kunnen sommige codes die wel in het NIST CSF-raamwerk voorkomen, ontbreken.

- **Beheren (Govern)**: zorgt ervoor dat cyberbeveiliging wordt behandeld als een strategische prioriteit, niet alleen als een technisch probleem. Het stelt duidelijke verwachtingen, beleidslijnen, verantwoordelijkheden en bevoegdheden vast en zorgt ervoor dat deze binnen de hele organisatie worden gecommuniceerd en geëvalueerd.

- **Identificeren (Identify)**: helpt een duidelijk beeld te krijgen van wat voor de organisatie het belangrijkst is, zoals systemen, mensen, assets, gegevens en de processen en tools die de bedrijfsvoering ondersteunen. Deze functie helpt bij het herkennen van potentiële cyberdreigingen en legt de basis voor weloverwogen beslissingen over het beheer van cyberbeveiligingsrisico's.



- **Beschermen (Protect)**: omvat het nemen van voorzorgsmaatregelen om de kans op een cyberincident te verkleinen of de impact ervan te beperken. Dit omvat technische maatregelen, processen en bewustmakingsinspanningen.

- **Detecteren (Detect)**: ondersteunt het vermogen om cyberbeveiligingsincidenten snel op te merken. Vroegtijdige detectie helpt schade te beperken en maakt een snellere reactie mogelijk.

- **Reageren (Respond)**: omvat de maatregelen die worden genomen wanneer zich een cyberbeveiligingsincident voordoet. Dit helpt het probleem in te dammen, de communicatie te coördineren en de verstoring te beperken.

- **Herstellen (Recover)**: richt zich op het herstellen van getroffen diensten en activiteiten na een incident. Het omvat ook het leren van het incident om de veerkracht in de toekomst te verbeteren.

Het CyberFundamentals Framework maakt gebruik van een proportioneel borgingsmodel met drie zekerheidsniveaus: *Basic*, *Important* en *Essential*, voorafgegaan door een instapniveau: *small*.

Het instapniveau **small** stelt een organisatie in staat een eerste beoordeling te maken. Het is bedoeld voor micro-organisaties of organisaties met beperkte technische kennis.

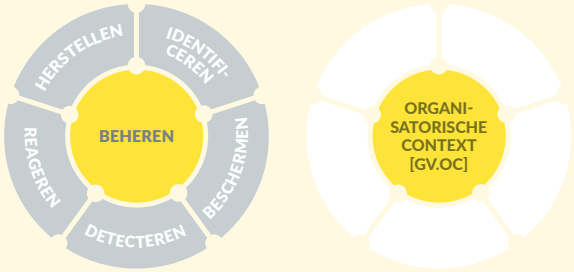
Het zekerheidsniveau **Basic** omvat informatie- en cyberbeveiligingsvereisten die van toepassing zijn op alle organisaties. Het biedt een betrouwbaar beschermingsniveau door gebruik te maken van technologieën en processen die over het algemeen al beschikbaar zijn. Waar nodig kunnen deze vereisten worden aangepast.

Op basis van veelvoorkomende soorten cyberaanvallen worden bepaalde vereisten aangemerkt als **"kernmaatregelen"** . Deze moeten op dit zekerheidsniveau worden behandeld, naast de belangrijke maatregelen die al vereist zijn op het zekerheidsniveau Basic en het zekerheidsniveau Important.


POLICIES

BEHEREN

Beheren



De omstandigheden – missie, verwachtingen van belanghebbenden, afhankelijkheden en wettelijke, regelgevende en contractuele vereisten – rondom de beslissingen van de organisatie op het gebied van cyberbeveiligingsrisicobeheer worden begrepen

GV.OC-03 Wettelijke, regelgevende en contractuele vereisten met betrekking tot cyberbeveiliging worden begrepen en beheerd

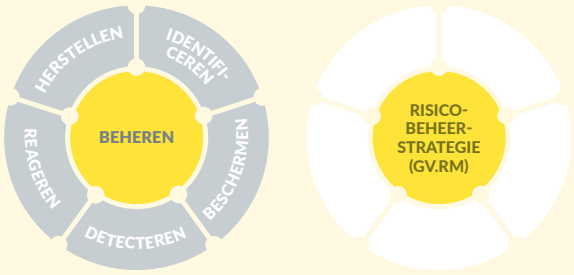
GV.OC-03.1 Wettelijke en regelgevende vereisten met betrekking tot informatie en cyberbeveiliging moeten worden geïdentificeerd en geïmplementeerd.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat wettelijke, regelgevende en contractuele vereisten met betrekking tot informatiebeveiliging en cyberbeveiliging worden geïdentificeerd, gecontroleerd en geïmplementeerd.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Er zou een proces kunnen worden opgezet om relevante wettelijke en regelgevende vereisten met betrekking tot zowel informatiebeveiliging als cyberbeveiliging bij te houden en toe te passen.
- Deze vereisten zouden kunnen worden geïntegreerd in alle relevante beleidslijnen, procedures en operationele praktijken.
- De gebieden die aan bod kunnen komen, zijn onder meer (maar niet uitsluitend):
  - Risicobeoordelingen en bescherming van informatiesystemen
  - Incidentrespons, bedrijfscontinuïteit en crisisbeheer
  - Beveiliging van de toeleveringsketen en veilige systeemontwikkeling
  - Beheer van kwetsbaarheden en veilige configuratie
  - Bewustmaking en opleiding op het gebied van beveiliging
  - Cryptografische controles en veilige communicatie
  - Noodcommunicatiesystemen
  - Toegangscontrole, assetsbeheer en meervoudige authenticatie (MFA)
  - Gecoördineerde openbaarmaking van kwetsbaarheden



De prioriteiten, beperkingen, risicotolerantie en risicobereidheid van de organisatie, evenals de aannames, worden vastgesteld, gecommuniceerd en gebruikt ter ondersteuning van operationele risicobeslissingen.

GV.RM-03 Activiteiten en resultaten op het gebied van cyberbeveiligings-risicobeheer worden opgenomen in de risicobeheerprocessen van de onderneming

GV.RM-03.1 **Als onderdeel van de organisatiebrede risicobeheerstrategie moet een uitgebreide strategie voor het beheer van informatie- en cyberbeveiligingsrisico's worden ontwikkeld en bijgewerkt wanneer zich veranderingen voordoen.**

Implementatierichtlijnen

Deze controle richt zich op het opstellen en onderhouden van een specifieke strategie voor het beheer van informatie- en cyberbeveiligingsrisico's. Deze zorgt ervoor dat de organisatie beschikt over een specifiek, uitvoerbaar plan dat mee evolueert met het dreigingslandschap.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Een organisatiebrede risicobeheerstrategie omvat een uitdrukking van de tolerantie voor beveiligingsrisico's voor de organisatie, strategieën voor het beperken van beveiligingsrisico's, methodologieën voor het beoordelen van aanvaardbare risico's, een proces voor het evalueren van beveiligingsrisico's in de hele organisatie met betrekking tot de risicotolerantie van de organisatie, en benaderingen voor het monitoren van risico's in de loop van de tijd.
- Informatie- en cyberbeveiligingsrisico's zouden kunnen worden samengevoegd en beheerd naast andere organisatierisico's (bijv. naleving, financieel, operationeel, regelgevend, reputatie, veiligheid).
- De strategie voor informatie- en cyberbeveiligingsrisicobeheer zou het identificeren en toewijzen van de nodige middelen kunnen omvatten om de bedrijfskritieke assets van de organisatie te beschermen.
- Dit is de cybersecurityspecifieke implementatie van de bredere visie die is gedefinieerd in GV.RM-04.1.

Er worden rollen, verantwoordelijkheden en bevoegdheden op het gebied van cyberbeveiliging vastgesteld en gecommuniceerd om verantwoordingsplicht, prestatiebeoordeling en voortdurende verbetering te bevorderen.

GV.RR-04 Cybersecurity is opgenomen in het personeelsbeleid

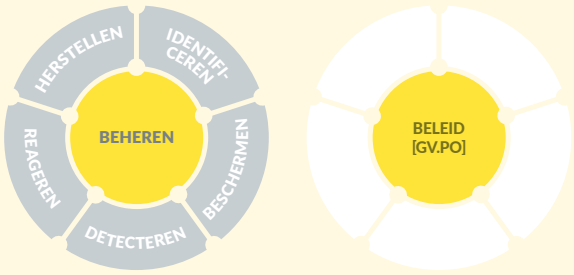
GV.RR-04.1 **Personeel dat toegang heeft tot de meest kritieke informatie of technologie van de organisatie moet worden geauthenticeerd.**

Implementatierichtlijnen

Het doel van deze controle is het beschermen van kritieke assets door ervoor te zorgen dat alleen geauthenticeerd personeel er toegang toe heeft.

Om dit doel te bereiken, kan het volgende worden overwogen:

- "Geauthenticeerd" betekent dat de gebruiker zijn identiteit technisch moet bewijzen op het moment van toegang, idealiter met behulp van MFA of sterkere methoden, en niet alleen tijdens de onboarding moet worden gevalideerd.
- De toegang tot kritieke informatie of technologie zou kunnen worden overwogen tijdens de werving, de onboarding, tijdens het dienstverband, bij een functiewijziging en bij de offboarding (beëindiging van het dienstverband).
- Voordat nieuw personeel voor gevoelige functies wordt aangenomen, zou een antecedentenonderzoek kunnen worden uitgevoerd. Voor personeel met dergelijke functies zou dit antecedentenonderzoek periodiek kunnen worden herhaald. Bij antecedentenonderzoeken zou rekening kunnen worden gehouden met de toepasselijke wet- en regelgeving en ethische normen, in verhouding tot de zakelijke vereisten, de classificatie van de informatie waartoe toegang wordt verleend en de verwachte risico's.
- Cybersecurity-expertise zou kunnen worden erkend als een waardevol bezit bij beslissingen over werving, opleiding en behoud van personeel.



Het cyberbeveiligingsbeleid van de organisatie wordt vastgesteld, gecommuniceerd en gehandhaafd.

GV.PO-01 Het beleid voor het beheer van cyberbeveiligingsrisico's wordt vastgesteld op basis van de context van de organisatie, de cyberbeveiligingsstrategie en de prioriteiten, en dit beleid wordt gecommuniceerd en gehandhaafd

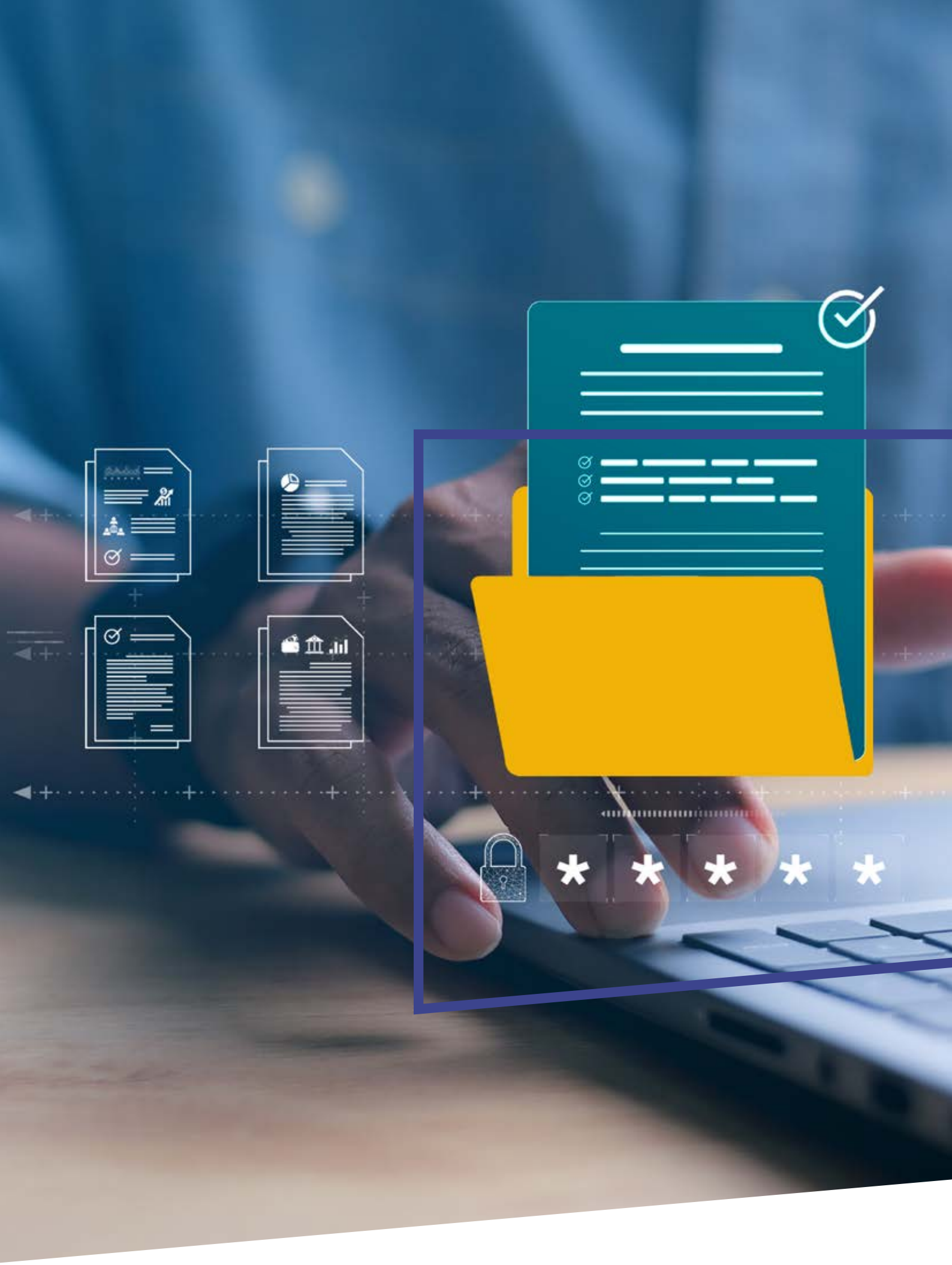
GV.PO-01.1 Beleid en procedures voor het beheer van informatie en cyberbeveiliging moeten worden vastgesteld, gedocumenteerd, beoordeeld, goedgekeurd, bijgewerkt wanneer er wijzigingen optreden, gecommuniceerd en gehandhaafd.

Implementatierichtlijnen

Deze controle vormt de basis voor het beheer van alle beleidsregels en procedures op het gebied van informatie- en cyberbeveiliging. De nadruk ligt op de governancecyclus, van opstelling tot handhaving, en zorgt ervoor dat deze aansluit bij de strategische koers van de organisatie.

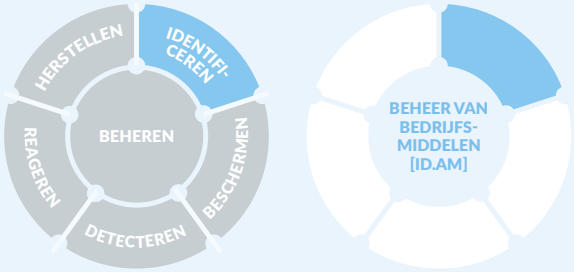
Om deze controle effectief te implementeren, zouden de volgende praktijken overwogen kunnen worden:

- Duidelijke en praktische beleidsregels, processen en procedures ontwikkelen die:
  - Aanvaardbaar gedrag en verwachtingen definiëren voor de bescherming van de informatie en systemen van de organisatie.
  - Beschrijven hoe het management verwacht dat werknemers de bedrijfsmiddelen gebruiken en beschermen.
- Ervoor zorgen dat medewerkers zich bewust zijn van deze beleidsregels, processen en procedures door deze te communiceren:
  - Tijdens de introductie van nieuw personeel.
  - Telkens wanneer er belangrijke updates of wijzigingen worden doorgevoerd.
  - Zorg ervoor dat alle relevante documenten gemakkelijk toegankelijk zijn voor werknemers.
- Regelmatig (bijvoorbeeld jaarlijks) evalueren en actualiseren om rekening te houden met:
  - Organisatorische veranderingen, zoals fusies, overnames of nieuwe contractuele verplichtingen.
  - Technologische ontwikkelingen, zoals de invoering van kunstmatige intelligentie of nieuwe beveiligingsinstrumenten.
- Risicobeoordelingscriteria binnen het risicobeheerbeleid van de organisatie definiëren:
  - De entiteit moet duidelijke criteria vaststellen en documenteren voor het bepalen van de waarschijnlijkheid en impact van risico's.
  - Deze criteria moeten worden afgestemd op de specifieke context van de organisatie en consistent worden gebruikt om cyberbeveiligingsrisico's te evalueren en te prioriteren. Dit zorgt ervoor dat risicogebaseerde beslissingen in overeenstemming zijn met de algemene strategie en risicobereidheid van de organisatie.



IDENTIFICEREN

Identificeren



Assets (bijv. gegevens, hardware, software, systemen, faciliteiten, diensten, mensen) die de organisatie in staat stellen haar bedrijfsdoelstellingen te bereiken, worden geïdentificeerd en beheerd in overeenstemming met hun relatieve belang voor de organisatiedoelstellingen en de risicostrategie van de organisatie.

ID.AM-01 Er worden inventarissen bijgehouden van de hardware die door de organisatie wordt beheerd

ID.AM-01.1 Er moet een inventaris worden opgesteld van alle fysieke en virtuele infrastructuurcomponenten – zoals hardware, netwerkapparatuur en cloudomgevingen – die informatieverwerking ondersteunen. Deze inventaris moet worden gedocumenteerd, beoordeeld en bijgewerkt zodra er wijzigingen optreden.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat kritieke systemen en diensten beschikbaar blijven door redundantie te implementeren in overeenstemming met organisatorische, wettelijke en regelgevende beschikbaarheidsvereisten.

Hoewel ID.AM-01.1 zich richt op de infrastructuurlaag, is deze controle nauw verbonden met ID.AM-02.1, die de software en diensten bijhoudt die daarop draaien, zoals applicaties, platforms en digitale tools. Samen geven ze een volledig beeld van de technologische omgeving van de organisatie.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Organisaties zouden alle fysieke en virtuele infrastructuurassets kunnen identificeren en documenteren die informatieverwerking ondersteunen, waaronder servers, werkstations, netwerkapparatuur, opslagsystemen en cloudgehoste bronnen.
- De inventaris zou belangrijke kenmerken kunnen bevatten, zoals het type asset, de locatie, de eigenaar, de configuratie en de levenscyclusstatus.
- Organisaties zouden waar mogelijk automatische tools voor het opsporen en beheren van assets kunnen overwegen om de nauwkeurigheid en realtime updates te waarborgen.
- De inventaris zou regelmatig kunnen worden gecontroleerd en bijgewerkt, vooral na wijzigingen zoals implementaties, buitengebruikstellingen of verhuizingen.
- De inventarisatie zou toegankelijk kunnen zijn voor relevante belanghebbenden en zou kunnen worden geïntegreerd met risicomanagement- en incidentresponsprocessen.

ID.AM-02 Er worden inventarissen bijgehouden van software, diensten en systemen die door de organisatie worden beheerd

ID.AM-02.1 **Een inventaris van software, digitale diensten en bedrijfssystemen die binnen de organisatie worden gebruikt, moet worden gedocumenteerd, beoordeeld en bijgewerkt wanneer er wijzigingen plaatsvinden.**

Implementatierichtlijnen

Deze controle zorgt ervoor dat alle software, digitale diensten en bedrijfssystemen die binnen de organisatie worden gebruikt, worden geïdentificeerd, bijgehouden en regelmatig bijgewerkt. De focus ligt op de functionele en immateriële onderdelen van de technologische omgeving, zoals applicaties, platforms en clouddiensten, die op de onderliggende infrastructuur draaien of daarmee communiceren. Door deze inventaris up-to-date te houden, wordt de operationele continuïteit ondersteund, de beveiliging versterkt en wordt aan compliance-eisen voldaan.

Deze controle hangt nauw samen met ID.AM-01.1, die betrekking heeft op de fysieke en virtuele infrastructuur (zoals servers, netwerkapparatuur en cloudomgevingen) die deze systemen ondersteunt.

Samen bieden beide controles een volledig beeld van het technologielandschap van de organisatie, van de fundamentele infrastructuur tot de applicaties en diensten die zakelijke waarde opleveren.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Software en diensten identificeren**
  De inventaris zou alle applicaties, clouddiensten, API's en bedrijfssystemen (bijv. ERP, CRM, HR-platforms) kunnen omvatten.
- **Belangrijke informatie vastleggen**
  Elke vermelding zou de versie, eigenaar, het doel, het licentietype en de implementatieomgeving kunnen bevatten.
- **Waar mogelijk automatiseren**
  Gebruik geautomatiseerde detectietools om software en diensten nauwkeurig te detecteren en bij te werken.
- **Een Software Bill of Materials (SBOM) bijhouden**
  Voor kritieke of intern ontwikkelde software zou een SBOM kunnen bijgehouden worden om componenten en afhankelijkheden te volgen.
- **De inventaris up-to-date houden**
  De inventaris zou regelmatig gecontroleerd en bijgewerkt kunnen worden, vooral na installaties, upgrades of verwijderingen.
- **Afstemmen op de infrastructuurinventaris (ID.AM-01.1)**
  Softwaregegevens zouden gekoppeld kunnen worden aan de infrastructuur waarop ze draaien om een volledig beeld van de technologische omgeving te geven.

ID.AM-05 Assets worden geprioriteerd op basis van classificatie, kriticiteit, middelen en impact op de missie

ID.AM-05.1 De assets van de organisatie worden geprioriteerd op basis van classificatie, kriticiteit en zakelijke waarde.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle assets van de organisatie, zoals apparaten, systemen, diensten, gegevens en bedrijfsprocessen, worden geprioriteerd op basis van hun classificatie, kriticiteit en zakelijke waarde.

Deze prioritering helpt bij het richten van beschermingsinspanningen op de belangrijkste assets, waardoor de operationele continuïteit, veiligheid en naleving worden ondersteund.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Identificatie van assets**
  Alle relevante bedrijfsmiddelen (assets), waaronder apparaten, systemen, software, clouddiensten, gegevens, medewerkers en bedrijfsprocessen, zouden geïdentificeerd en geregistreerd kunnen worden in een centrale inventaris.
- **Classificatie van assets**
  Elke asset zou geclassificeerd kunnen worden op basis van zijn rol:
  - Primaire bedrijfsmiddelen (assets) zouden kunnen worden gedefinieerd als assets die rechtstreeks de kernactiviteiten van het bedrijf ondersteunen.
  - Secundaire bedrijfsmiddelen (assets) zouden kunnen worden gedefinieerd als assets die primaire assets ondersteunen, beschermen of mogelijk maken.
- **Beoordeling van de kriticiteit**
  - De organisatie zou kunnen beoordelen hoe kritiek elk asset is voor de bedrijfscontinuïteit.
  - Bij de beoordeling zou rekening kunnen worden gehouden met mogelijke gevolgen, zoals operationele verstoring, financieel verlies, juridische of regelgevende gevolgen, veiligheidsrisico's en reputatieschade.
- **Prioriteringsmethode**
  Er zou een consistente score- of rangschikkingsmethode kunnen worden gebruikt om assets te prioriteren op basis van classificatie, kriticiteit en zakelijke waarde.
- **Toewijzing van eigenaarschap**
  Elk asset zou een toegewezen eigenaar kunnen hebben die verantwoordelijk is voor het bijhouden van accurate en actuele informatie.
- **Regelmatige evaluatie**
  De classificaties en prioriteiten van assets zouden ten minste eenmaal per jaar kunnen worden herzien, of wanneer er belangrijke veranderingen plaatsvinden (bijvoorbeeld nieuwe systemen, bedrijfsherstructurering).
- **Documentatie en bewijs**
  - Het assetsregister zou de classificatie, prioriteitscriteria, toegewezen eigenaren en bewijs van regelmatige evaluaties kunnen bevatten.
  - De definities van primaire en secundaire assets zouden duidelijk kunnen worden gedocumenteerd.

ID.AM-07 Inventarissen van gegevens en bijbehorende metadata voor specifieke gegevenstypen worden bijgehouden

ID.AM-07.1 Gegevens die de organisatie opslaat en gebruikt, moeten worden geïdentificeerd.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle gegevens die door de organisatie worden opgeslagen en gebruikt, duidelijk worden geïdentificeerd. Dit ondersteunt een goed gegevensbeheer, bescherming en afstemming op zakelijke en wettelijke vereisten.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Identificatie van gegevens**
  Alle soorten gegevens, ongeacht het formaat, de locatie of het systeem, zouden kunnen worden geïdentificeerd en geregistreerd.
- **Gegevensclassificatie**
  Geïdentificeerde gegevens zouden geclassificeerd kunnen worden aan de hand van standaardcategorieën, zoals:
  - Openbaar
  - Intern
  - Vertrouwelijk
  - Beperkt
- **Koppeling van gegevens aan assets**
  Gegevens zouden kunnen worden gekoppeld aan de assets die ze opslaan of verwerken, met inbegrip van fysieke apparaten, systemen, software en applicaties die zijn opgenomen in de inventarissen van ID.AM-01 en ID.AM-02.
- **Documentatie en onderhoud**
  Gegevenstypen, classificaties en bijbehorende assets zouden kunnen worden gedocumenteerd en regelmatig worden bijgewerkt om veranderingen in de omgeving weer te geven.

ID.AM-08 Systemen, hardware, software, diensten en gegevens worden gedurende hun hele levenscyclus beheerd

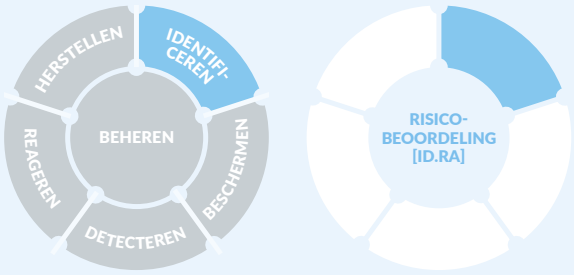
ID.AM-08.2 Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat besturingssystemen en kritieke systeemcomponenten veilig en up-to-date blijven door patches en beveiligingsupdates tijdig en op een gecontroleerde manier te installeren.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Tijdige updates**
  Patches en beveiligingsupdates zouden zo snel mogelijk geïnstalleerd kunnen worden, vooral voor kritieke systemen.
- **Industriële systemen**
  Firmware-updates voor industriële assets (bijv. PLC's, HMI's) zouden kunnen worden opgenomen in het patchproces.
- **Gecentraliseerd beheer**
  Er zou een gecentraliseerd patchbeheersysteem gebruikt kunnen worden om de implementatie van patches te automatiseren en te stroomlijnen.
- **Testen vóór implementatie**
  - Patches zouden in een gecontroleerde omgeving kunnen worden getest om verstoringen te voorkomen.
  - Een testomgeving zou de productieomgeving zo goed mogelijk kunnen weerspiegelen.
- **Gefaseerde uitrol**
  - Waar nodig zouden testgroepen, pilotgebruikers en gefaseerde implementaties gebruikt kunnen worden.
  - Er zou een terugdraaiprocedure kunnen zijn voor het geval er problemen ontstaan.
- **Alleen vertrouwde bronnen**
  - Patches zouden alleen mogen worden gedownload van geverifieerde, betrouwbare bronnen.
  - Links in e-mails of advertenties zouden vermeden kunnen worden.
- **Minimale softwarevoetafdruk**
  Er zouden alleen essentiële applicaties geïnstalleerd kunnen worden. Deze zouden regelmatig worden gepatcht en bijgewerkt.
- **Veilige updatepraktijken**
  - Automatische updates zouden ingeschakeld worden wanneer er verbinding is met vertrouwde netwerken.
  - Updates zouden niet uitgevoerd mogen worden via onbetrouwbare netwerken (bijv. openbare wifi).
- **Alleen ondersteunde software**
  - Er zou alleen door de leverancier ondersteunde en up-to-date software kunnen worden gebruikt.
  - Software die niet meer wordt ondersteund (EOL) zou zo snel mogelijk buiten gebruik kunnen worden gesteld.
- **Regelmatige controles**
  Als automatische updates niet mogelijk zijn, zou er een regelmatig schema (bijvoorbeeld maandelijks) kunnen worden opgesteld om handmatig te controleren op updates en deze te installeren.
- **Tools voor het monitoren van updates**
  Tools die melding maken van beschikbare updates zouden kunnen worden geconfigureerd om alle geïnstalleerde applicaties te monitoren.



De organisatie begrijpt het cyberbeveiligingsrisico voor de organisatie, assets en personen.

ID.RA-01 Kwetsbaarheden in assets worden geïdentificeerd, gevalideerd en geregistreerd

ID.RA-01.1 Bedreigingen en kwetsbaarheden moeten worden geïdentificeerd in alle relevante bedrijfsmiddelen, waaronder software, netwerk- en systeemarchitecturen, én de faciliteiten waarin kritieke digitale systemen en apparatuur zijn ondergebracht.

Implementatierichtlijnen

Het doel van deze maatregel is om organisaties te helpen cyberbeveiligingsrisico's te beperken door bedreigingen en kwetsbaarheden in hun kritieke assets te identificeren. Dit omvat software, netwerken, systemen en fysieke locaties die essentiële digitale activiteiten ondersteunen.

Om dit doel te bereiken, zouden organisaties het volgende in overweging kunnen nemen:

- De belangrijkste concepten begrijpen
  - Een **kwetsbaarheid** is een zwakke plek in hardware, software of procedures die kan worden misbruikt.
  - Een **bedreiging** is een gebeurtenis of actor die kan proberen misbruik te maken van een kwetsbaarheid.
  - Een **risico** is de mogelijke impact als een bedreiging met succes misbruik maakt van een kwetsbaarheid.
- Relevante assets identificeren
  Alle kritieke systemen, applicaties, netwerken en faciliteiten zouden kunnen worden geïnventariseerd en gedocumenteerd.
- Reageren op kwetsbaarheden
  - Organisaties zouden actie kunnen ondernemen tegen kwetsbaarheden die worden gemeld door betrouwbare bronnen (bijv. leveranciers, dienstverleners, overheidsadviezen).
  - Op basisniveau is actief scannen niet vereist, maar bekende kwetsbaarheden zouden onmiddellijk kunnen worden aangepakt.
- Zich bewust zijn van bedreigingen
  Organisaties zouden op de hoogte kunnen blijven van veelvoorkomende bedreigingen die relevant zijn voor hun sector (bijv. phishing, ransomware).

ID.RA-05 Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden geprioriteerd

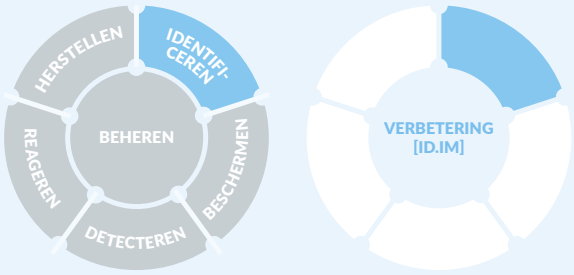
ID.RA-05.1 De organisatie moet risicobeoordelingen uitvoeren waarbij het risico wordt bepaald aan de hand van bedreigingen, kwetsbaarheden en de impact op bedrijfsprocessen en assets.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat risicobeoordelingen worden uitgevoerd door bedreigingen, kwetsbaarheden en hun potentiële impact op bedrijfsprocessen en assets te evalueren. Dit ondersteunt weloverwogen besluitvorming en effectieve risicobeperking.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Bedreigingen en kwetsbaarheden identificeren**
  Beoordelingen zouden bedreigingen en kwetsbaarheden kunnen omvatten voor software, netwerk- en systeemarchitecturen en faciliteiten waarin kritieke computerapparatuur is ondergebracht.
- **De impact op het bedrijf evalueren**
  De potentiële impact op bedrijfsactiviteiten, diensten en assets zou kunnen worden geanalyseerd om de ernst van elk risico te bepalen.
- **Rekening houden met menselijke factoren**
  Bij het ontwerpen en toepassen van beveiligingsbeleid zou rekening kunnen worden gehouden met menselijk gedrag, met name in operationele technologieomgevingen (OT).
- **Documenteren en evalueren**
  Risicobeoordelingen zouden kunnen worden gedocumenteerd, regelmatig geëvalueerd en bijgewerkt om veranderingen in systemen, activiteiten of het dreigingslandschap weer te geven.



Verbeteringen in de processen, procedures en activiteiten van de organisatie op het gebied van cyberbeveiligingsrisicobeheer worden geïdentificeerd in alle CyFun®-functies

ID.IM-03 Verbeteringen worden geïdentificeerd op basis van de uitvoering van operationele processen, procedures en activiteiten

ID.IM-03.1 De organisatie moet na elk incident evaluaties en analyses uitvoeren om lessen te trekken uit de respons en het herstel. Deze inzichten moeten worden gebruikt om processen, procedures en technologieën te verbeteren, met als doel de cyberweerbaarheid te versterken.

Implementatierichtlijnen

Het doel van deze maatregel is het verbeteren van de cyberweerbaarheid door te leren van incidenten. Na elk incident moet de organisatie analyseren wat er is gebeurd, hoe het is afgehandeld en wat er kan worden verbeterd in processen, procedures of technologieën.

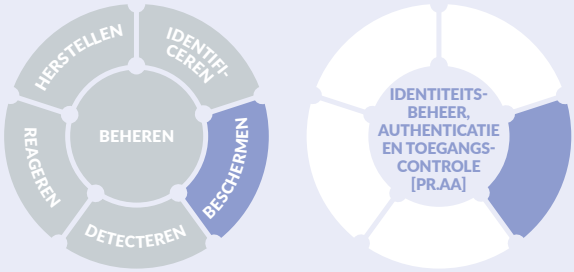
Om dit doel te bereiken, kan het volgende worden overwogen:

- **Incidenten evalueren**
  Na elk incident zou een gestructureerde evaluatie kunnen worden gehouden, waarbij alle relevante deelnemers worden betrokken.
- **Stilstaan bij belangrijke vragen**
  De evaluatie zou het volgende kunnen onderzoeken:
  - Wat er is gebeurd en waarom
  - Hoe de reactie werd beheerd
  - Wat goed werkte en wat niet
  - Welke maatregelen moeten worden genomen om herhaling te voorkomen
- **De geleerde lessen documenteren**
  De bevindingen van de evaluatie zouden kunnen worden gedocumenteerd en gedeeld met de relevante teams.
- **Beleid en procedures bijwerken**
  Het beleid, de processen en de procedures op het gebied van cyberbeveiliging zouden regelmatig, bijvoorbeeld ten minste eenmaal per jaar, kunnen worden geëvalueerd en bijgewerkt om rekening te houden met de geleerde lessen.
- **Tools en mogelijkheden verbeteren**
  Waar van toepassing zouden technologieën en responstools kunnen worden aangepast of geüpgraded op basis van de inzichten die uit het incident zijn verkregen.


Username
Password
Protected
Balance
5,367.50 $

BESCHERMEN

Beschermen



Toegang tot fysieke en logische assets is beperkt tot geautoriseerde gebruikers, diensten en hardware en wordt beheerd in overeenstemming met het beoordeelde risico van ongeoorloofde toegang.

PR.AA-01 Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware worden beheerd door de organisatie

Belangrijkste maatregel

PR.AA-01.1 Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware moeten worden beheerd.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware correct worden beheerd om ongeoorloofde toegang te voorkomen en veilige operaties in zowel ICT- als OT-omgevingen te ondersteunen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Toegangsverzoeken en autorisatie
  - Toegang zou formeel kunnen worden aangevraagd, gedocumenteerd en goedgekeurd door systeem- of gegevenseigenaren.
  - Toegangsrechten zouden het principe van minimale rechten kunnen volgen.
- Identiteits- en authenticatiemiddelenbeheer
  - Er zou gebruik kunnen worden gemaakt van individuele gebruikersaccounts; het delen van wachtwoorden zou kunnen worden vermeden.
  - Standaardwachtwoorden zouden kunnen worden gewijzigd voordat systemen worden geactiveerd.
  - Ongebruikte accounts zouden onmiddellijk kunnen worden uitgeschakeld.
  - Beheerdersaccounts zouden beperkt kunnen zijn, regelmatig worden gecontroleerd en niet worden gebruikt voor dagelijkse taken.
- Wachtwoordbeleid
  - Er zouden strenge wachtwoordregels kunnen worden gehanteerd.
  - Wachtwoorden zouden regelmatig kunnen worden gewijzigd of onmiddellijk nadat er een vermoeden bestaat dat ze zijn gecompromitteerd.
  - Er zou een formeel wachtwoordbeleid kunnen worden gehanteerd (zie ook: CyFun® Toolbox op www.cyfun.eu).
  - Rechten en privileges zouden kunnen worden toegewezen via gebruikersgroepen.
- Identiteit van apparaten en hardware

- Elk geautoriseerd apparaat zou een unieke identificatie kunnen hebben (bijvoorbeeld MAC-adres, serienummer).
- Apparaten zouden fysiek kunnen worden gelabeld om inventarisatie en onderhoud te ondersteunen.

- **Gedeelde toegang tot PLC's/HMI's (OT-specifieke maatregelen)**
  - Als individuele accounts niet haalbaar zijn, zou het principe van minimale rechten nog steeds kunnen worden toegepast.
  - Er zou een beveiligde jumpserver of HMI-front-end kunnen worden gebruikt om de toegang te controleren, activiteiten te loggen en authenticatielagen toe te voegen.
- **Veilige toegang op afstand**
  - De technische vereisten voor toegang op afstand zouden duidelijk kunnen worden gedefinieerd en gedocumenteerd.
  - Er zouden veilige methoden kunnen worden gebruikt, zoals VPN's, versleutelde protocollen (bijvoorbeeld SSH, TLS) en meervoudige authenticatie (MFA – zie ook PR.AA-03.2.
  - Toegang op afstand zou kunnen worden gecontroleerd en geregistreerd.

PR.AA-03 Gebruikers, diensten en hardware worden geauthentiseerd

PR.AA-03.1 Alle draadloze toegangspunten die door de organisatie worden gebruikt, inclusief die welke gasttoegang bieden, moeten veilig worden geconfigureerd, beheerd en bewaakt om ongeoorloofde toegang te voorkomen en de integriteit van het netwerk te waarborgen.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle draadloze toegangspunten, inclusief die voor gastgebruik, veilig worden geconfigureerd, beheerd en bewaakt om ongeoorloofde toegang te voorkomen en de integriteit van het netwerk te beschermen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Algemene draadloze beveiliging**
  - De standaard administratieve authenticatiemiddelen zouden onmiddellijk na installatie kunnen worden gewijzigd.
  - SSID-uitzendingen zouden kunnen worden uitgeschakeld, tenzij dit operationeel noodzakelijk is.
  - Er zouden sterke versleutelingsprotocollen (bijv. WPA2 of WPA3 met AES) kunnen worden gebruikt.
  - De fysieke toegang tot draadloze toegangspunten zou kunnen worden beperkt.
  - Firmware zou regelmatig kunnen worden bijgewerkt om bekende kwetsbaarheden aan te pakken.
  - Draadloze netwerken zouden kunnen worden gecontroleerd op ongeautoriseerde toegangspunten en verdachte activiteiten.
- **Beveiliging van gast-wifi**
  - Gastnetwerken zouden kunnen worden geïsoleerd van interne systemen met behulp van VLAN's of afzonderlijke SSID's.
  - Er zouden bandbreedte- en toegangsbeperkingen kunnen worden toegepast op gastnetwerken.
  - Er zouden captive portals kunnen worden gebruikt om de gebruiksvoorwaarden weer te geven en optioneel de toegang van gasten te registreren.
  - Gevoelige gegevens zouden niet kunnen worden opgeslagen of verzonden via gastnetwerken.
  - Gast-wifi zou kunnen worden uitgeschakeld wanneer deze niet wordt gebruikt of buiten kantooruren, indien mogelijk.
- **Endpoint- en gebruikerspraktijken**
  - Apparaten die verbinding maken met draadloze netwerken zouden kunnen voldoen aan het beveiligingsbeleid voor eindpunten.
  - VPN's zouden kunnen worden gebruikt bij het verbinden met onbekende of onbeveiligde netwerken.
  - Wifi-authenticatiemiddelen zouden kunnen voldoen aan een wachtwoordbeleid dat complexiteit en regelmatige updates afdwingt.

PR.AA-03.2 Multifactorauthenticatie (MFA) is vereist om op afstand toegang te krijgen tot de netwerken van de organisatie.

Implementatierichtlijnen

Het doel van deze controle is om de netwerken van de organisatie te beschermen door multifactorauthenticatie (MFA) te vereisen voor alle externe toegang, waardoor het risico op ongeoorloofde toegang en aanvallen op basis van authenticatiemiddelen wordt verminderd.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Algemene handhaving van MFA**
  MFA zou kunnen worden afgedwongen op alle systemen die in contact staan met het internet, waaronder e-mail, VPN's, RDP, clouddiensten en webportals.
  Voor alle externe toegang, inclusief toegang door externe leveranciers en aannemers, zou MFA vereist kunnen zijn.
- **Selectie van MFA-technologie**
  - MFA-methoden zouden geselecteerd kunnen worden op basis van beveiligingssterkte, weerstand tegen phishing en operationele geschiktheid.
  - Veelgebruikte opties zijn:
    - Hardware TOTP-tokens (Time-based One-Time Password) – veilig, beperkte weerstand tegen phishing
    - Authenticator-apps (software TOTP) – veel gebruikt, matige beveiliging
    - Passkeys – zonder wachtwoord, gebruiksvriendelijk, cryptografisch veilig
    - FIDO2 (platform- of hardwaregebaseerd - Fast Identity Online 2) – sterke cryptografische authenticatie
    - Push-gebaseerde apps – handig, maar mogelijk kwetsbaar voor push-moeheid
  - SMS- en e-mail gebaseerde MFA zou vermeden kunnen worden vanwege zwakke punten in de beveiliging.
- **Ondersteunende beveiligingsmaatregelen**
  - Naast MFA zou ook een sterk wachtwoordbeleid kunnen worden gehanteerd.
  - Gebruikers zouden kunnen worden opgeleid om zich expliciet af te melden bij sessies.
  - Anti-malwaretools en -platforms zouden up-to-date kunnen worden gehouden.
  - Er zou regelmatig opleiding kunnen worden gegeven om gebruikers bewust te maken van phishing.
- **OT-specifieke overwegingen met betrekking tot MFA (zie ook PR.AA-01.1)**
  - Gedeelde toegang tot PLC's/HMI's
  - Als individuele accounts niet haalbaar zijn, zou het principe van minimale rechten kunnen worden toegepast.
  - Er zou een beveiligde jumpserver of HMI-front-end kunnen worden gebruikt om de toegang te controleren, activiteiten te loggen en een authenticatielaag toe te voegen.
- **Veilige externe toegang tot OT-systemen**
  - De technische en procedurele vereisten voor toegang op afstand zouden duidelijk kunnen worden gedefinieerd.
  - Er zouden veilige protocollen (bijv. VPN, SSH, TLS) kunnen worden gebruikt.
  - MFA zou kunnen worden afgedwongen voor alle externe OT-toegang, met name voor externe leveranciers.
  - Er zou gebruik kunnen worden gemaakt van Just-In-Time (JIT)-toegangscontroles om tijdelijke, in de tijd beperkte toegang te verlenen.
  - Alle externe toegang zou kunnen worden geregistreerd en gecontroleerd.
- **Integratie en compatibiliteit**
  - De MFA-oplossing zou compatibel kunnen zijn met zowel IT- als OT-systemen.
  - De integratie zou kunnen worden getest in OT-omgevingen om verstoringen te voorkomen.
  - Wanneer directe integratie niet mogelijk is, zouden beveiligde tussenplatforms (bijv. jumpservers) kunnen worden gebruikt.

PR.AA-05 Toegangsrechten, bevoegdheden en autorisaties worden gedefinieerd in een beleid, beheerd, gehandhaafd en beoordeeld, en omvatten de principes van minimale rechten en scheiding van taken

PR.AA-05.1 Toegangsrechten, machtigingen en autorisaties moeten worden vastgesteld, beheerd, gehandhaafd en periodiek herzien.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat toegangsrechten, machtigingen en autorisaties duidelijk worden vastgelegd, correct beheerd, consequent afgedwongen en regelmatig herzien, zodat systemen en gegevens beschermd blijven tegen ongeoorloofde toegang.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Definitie en beheer van toegangsrechten
  - Toegangslijsten voor systemen (bijv. bestanden, servers, software, databases) zouden kunnen worden opgesteld en regelmatig worden herzien.
  - Beoordelingen zouden kunnen worden ondersteund door tools zoals Active Directory-analyse.
  - Procedures voor het beheer van toegangsrechten zouden kunnen worden gedocumenteerd en indien nodig worden bijgewerkt.
- Herziening en intrekking van toegangsrechten
  - Logische en fysieke toegangsrechten zouden periodiek kunnen worden gecontroleerd en telkens wanneer rollen veranderen of personen de organisatie verlaten.
  - Onnodige privileges zouden onmiddellijk kunnen worden ingetrokken.
- Richtlijnen voor het gebruik en beheer van gebruikersaccounts
  - Elke gebruiker, inclusief contractanten, zou een afzonderlijk account kunnen hebben om de verantwoordingsplicht te waarborgen.
  - Waar technisch haalbaar, zouden passende authenticatiemaatregelen kunnen worden toegepast.
  - Gastaccounts zouden kunnen worden beperkt tot de minimaal vereiste privileges (bijvoorbeeld alleen internettoegang).
  - Waar mogelijk zou Single Sign-On (SSO) kunnen worden gebruikt.
- Autorisatiecriteria
  Bij autorisatiebeslissingen zou rekening kunnen worden gehouden met kenmerken zoals geolocatie, tijdstip van toegang en de beveiligingsstatus van het apparaat waarmee de aanvraag wordt gedaan.
- OT-specifieke overwegingen
  - In omgevingen waar individuele accounts technisch niet haalbaar zijn, zoals gedeelde toegang tot PLC's of HMI's, zou de toegang kunnen worden beperkt tot alleen essentiële functies en worden afgedwongen door middel van veilige methoden, zoals een jumpserver of HMI-front-end die activiteiten registreert, de toegang beperkt op basis van rol of tijd en een extra authenticatielaag toevoegt (bijvoorbeeld een badge of pincode).
  - Authenticatiemethoden zouden kunnen aansluiten bij de mogelijkheden van OT-systemen.
  - Toegang tot OT-systemen zou waar mogelijk kunnen worden geregistreerd en gecontroleerd.

PR.AA-05.2 Er moet worden vastgesteld wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, evenals op welke manier die toegang wordt verleend.

Implementatierichtlijnen

Het doel van deze controle is vast te stellen wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, en om de veilige methoden en procedures te definiëren waarmee deze toegang wordt verleend.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Bepaling en beperking van toegangsrechten
  - Toegangsrechten zouden kunnen worden beperkt tot alleen die personen die ze nodig hebben om hun taken uit te voeren.
  - Voor zowel IT- als OT-omgevingen zou een zero trust-model kunnen worden overwogen, waarbij verificatie vereist is voordat toegang wordt verleend.
- Toegangsmethoden
  - Toegangsmethoden zouden beveiligde mechanismen kunnen omvatten, zoals sleutels, wachtwoorden, codes of beheerdersrechten.
  - Deze methoden zouden kunnen worden beheerd en gecontroleerd om misbruik te voorkomen
- Cybergezondheid van eindpunten
  - Apparaten zoals laptops, smartphones en tablets zouden aan beveiligingsnormen kunnen voldoen voordat ze verbinding maken met het productienetwerk.
  - De gezondheid van eindpunten zou kunnen worden gecontroleerd door te kijken naar:
    - Up-to-date antivirussoftware
    - Afwezigheid van malware
    - Installatie van de nieuwste beveiligingspatches
  - Alleen apparaten die aan de vereisten voldoen, zouden toegang kunnen krijgen tot kritieke systemen en gegevens.
- OT-specifieke overwegingen
  - In OT-omgevingen moet de toegang tot besturingssystemen kunnen worden beperkt tot essentieel personeel.
  - Waar individuele accounts niet haalbaar zijn, zouden veilige toegangsmethoden (bijv. jumpservers, op rollen gebaseerde beperkingen) kunnen worden gebruikt.
- Referentie

  Voor praktische tools en templates verwijzen we naar de template voor toegangsbeleid in de CyFun® Toolbox op www.cyfun.eu

PR.AA-05.3 Toegangsrechten, privileges en autorisaties moeten worden beperkt tot de systemen en specifieke informatie die nodig zijn om de taken uit te voeren (het principe van 'Least Privilege').

Implementatiebegeleiding

Het doel van deze controle is ervoor te zorgen dat toegangsrechten, privileges en autorisaties beperkt blijven tot alleen de systemen en specifieke informatie die nodig zijn om de toegewezen taken uit te voeren, volgens het principe van minimale privileges.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **'Least Privilege' toepassen**
  - Toegangsrechten zouden moeten worden beperkt tot het minimum dat nodig is voor gebruikers, systemen en diensten om de taken uit te voeren ('Least Privilege') .
  - Accounts zouden kunnen beginnen met lage privileges en alleen worden verhoogd wanneer dat gerechtvaardigd is.
  - Just-in-time-toegang zou kunnen worden gebruikt om de duur van verhoogde privileges te beperken.
- **Machtigingen definiëren en beheren**
  - Toegangsrechten ouden duidelijk kunnen worden gedefinieerd op basis van rollen en verantwoordelijkheden.
  - Er zou een inventaris van accounts en hun machtigingen kunnen worden bijgehouden en up-to-date gehouden.
  - Er zouden aparte accounts kunnen worden gebruikt voor aannemers en derde partijen om traceerbaarheid te garanderen.
- **Toegangscontroles afdwingen**
  - Waar mogelijk zouden op rollen of attributen gebaseerde toegangscontrolemodellen kunnen worden geïmplementeerd.
  - Internettoegangspunten en externe verbindingen zouden kunnen worden beperkt tot wat strikt noodzakelijk is.
- **Systemen versterken**

  Systemen zouden kunnen worden versterkt om toegangscontrole te ondersteunen door:
  - Ongebruikte poorten en diensten uit te schakelen
  - Bluetooth te beperken waar dat niet nodig is
  - Legacy-protocollen zoals FTP te beperken, tenzij deze veilig zijn geconfigureerd
- **Toegang controleren en aanpassen**
  - Toegangsrechten zouden regelmatig kunnen worden gecontroleerd en aangepast op basis van rolveranderingen, voltooiing van projecten of beveiligingsbeoordelingen.
  - Wanneer de toegang niet langer nodig is, zou deze onmiddellijk kunnen worden ingetrokken.
- **OT-specifieke overwegingen**
  - In OT-omgevingen zou toegangscontrole nog steeds het principe van minimale rechten kunnen volgen.
  - Wanneer er technische beperkingen zijn, zouden eerder gedefinieerde OT-toegangsmaatregelen (zie PR.AA-01.1 en PR.AA-05.1) kunnen worden toegepast om veilige en traceerbare toegang te garanderen.

PR.AA-05.4 Niemand mag beheerdersrechten hebben voor dagelijkse routinetaken.

Implementatierichtlijnen

Het doel van deze controle is om het gebruik van beheerdersrechten voor routinematige, dagelijkse taken te voorkomen, waardoor het risico op misbruik of exploitatie door aanvallers wordt verminderd.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Accountscheiding en beheer van privileges**
  - Beheerdersaccounts en algemene gebruikersaccounts zouden strikt gescheiden kunnen worden gehouden.
  - Speciale beheerdersaccounts zouden alleen kunnen worden gebruikt voor systeembeheer en administratieve taken.
  - Gebruikersaccounts zouden geen beheerdersrechten kunnen hebben.
- **Toegangsbeperkingen en beveiligingsmaatregelen**
  - Voor elk systeem zouden unieke lokale beheerderswachtwoorden kunnen worden aangemaakt.
  - Ongebruikte accounts zouden onmiddellijk kunnen worden uitgeschakeld.
  - Het surfen op internet vanaf beheerdersaccounts zou kunnen worden verboden om de blootstelling aan webgebaseerde bedreigingen te verminderen.
- **OT-specifieke overwegingen**
  - In OT-omgevingen zou administratieve toegang kunnen worden beperkt tot essentieel personeel en essentiële functies.
  - Wanneer gedeelde toegang noodzakelijk is, zouden veilige toegangsmethoden (bijv. jumpservers, sessielogging) kunnen worden gebruikt om verantwoordelijkheid af te dwingen en risico's te verminderen.

PR.AA-06 Fysieke toegang tot assets wordt beheerd, gecontroleerd en gehandhaafd in overeenstemming met het risico

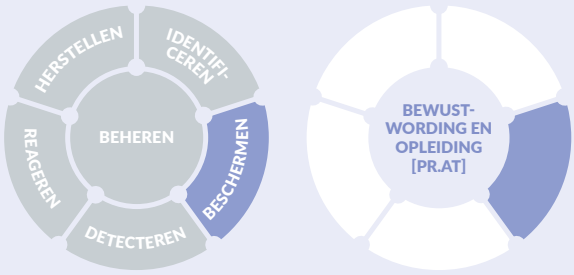
PR.AA-06.1 De fysieke toegang tot alle bedrijfsmiddelen, met inbegrip van kritieke zones, moet worden beheerd, bewaakt en gehandhaafd op basis van het risico.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de fysieke toegang tot alle bedrijfsmiddelen, met name in kritieke zones, wordt beheerd, bewaakt en gehandhaafd op basis van risico's, om ongeoorloofde toegang te voorkomen en gevoelige systemen te beschermen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Maatregelen voor toegangscontrole
  - Sleutels, badges en alarmcodes zouden strikt beheerd kunnen worden.
  - De authenticatiemiddelen van werknemers zouden onmiddellijk bij vertrek kunnen worden ingenomen.
  - Alarmcodes zouden regelmatig kunnen worden gewijzigd.
  - Externe dienstverleners (bijv. schoonmakers) zouden alleen toegang kunnen krijgen wanneer dat nodig is, en dan:
    - tijdelijk zijn met behulp van technische controles
    - elektronisch geregistreerd voor traceerbaarheid
- Verbeteringen op het gebied van fysieke beveiliging
  - Kritieke zones zouden beveiligd kunnen worden met fysieke maatregelen, zoals:
    - Bewakingscamera's
    - Beveiligingspersoneel
    - Afgesloten deuren en poorten
    - Alarmsystemen
  - Deze maatregelen zouden strategisch kunnen worden geplaatst om de toegang te controleren en te beperken.
- Netwerktoegangsbeveiliging
  Interne netwerkpoorten (bijv. Ethernet) zouden niet blootgesteld mogen worden in onbeveiligde ruimtes zoals wachtkamers, gangen of receptieruimtes.
- OT-specifieke overwegingen
  - Fysieke toegang tot OT-omgevingen (bijv. controlekamers, kasten, veldapparatuur) zou kunnen worden beperkt tot bevoegd personeel.
  - De toegang zou kunnen worden geregistreerd en gecontroleerd, en waar mogelijk kunnen fysieke barrières worden gebruikt.
- Referentie
  Voor praktische tools en templates verwijzen we naar het toegangsbeleid in de CyFun® Toolbox op www.cyfun.eu.



Het personeel van de organisatie krijgt bewustmaking en opleiding op het gebied van cyberbeveiliging, zodat ze hun taken op het gebied van cyberbeveiliging kunnen uitvoeren.

PR.AT-01 Het personeel krijgt bewustmaking en opleiding zodat het over de kennis en vaardigheden beschikt om algemene taken uit te voeren met het oog op cyberbeveiligingsrisico's

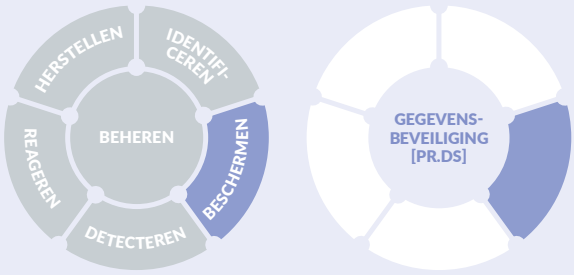
PR.AT-01.1 De organisatie moet een bewustmakings- en opleidingsprogramma op het gebied van cyberbeveiliging opzetten en onderhouden om ervoor te zorgen dat alle personeelsleden begrijpen hoe ze hun taken veilig en verantwoord kunnen uitvoeren.

Implementatierichtlijnen

Het doel van maatregel PR.AT-01.1 is ervoor te zorgen dat iedereen in de organisatie begrijpt hoe veilig te werken door regelmatig duidelijke en praktische cybersecurityopleidingen aan te bieden die menselijke risico's verminderen en veilig gedrag in zowel IT- als OT-omgevingen ondersteunen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Er zou een basisopleiding kunnen worden gegeven aan iedereen**
  Cybersecuritybewustmakingsopleiding zou kunnen worden aangeboden aan alle werknemers, aannemers, partners en leveranciers, inclusief die in operationele technologieomgevingen (OT).
- **De opleiding zou veelvoorkomende bedreigingen kunnen behandelen**
  Onderwerpen zoals phishing, zwakke wachtwoorden, social engineering en OT-specifieke risico's (bijv. misbruik van USB-sticks, bedreigingen voor externe toegang) zouden aan bod kunnen komen.
- **De opleiding zou vroeg kunnen beginnen en regelmatig worden herhaald**
  De opleiding zou kunnen worden gegeven tijdens de introductieperiode en minstens eenmaal per jaar worden herhaald. Doorlopende updates en herinneringen zouden de belangrijkste boodschappen kunnen versterken.
- **Er zouden meerdere kanalen kunnen worden gebruikt**
  De bewustmaking zou kunnen worden vergroot door middel van gestructureerde sessies, campagnes, posters, nieuwsbrieven en interactieve tools.
- **De gevolgen van niet-naleving zouden kunnen worden uitgelegd**
  De gevolgen van het overtreden van het cyberbeveiligingsbeleid zouden duidelijk kunnen worden gecommuniceerd, zowel voor individuen als voor de organisatie.
- **Training zou kunnen aansluiten bij beleid en best practices**
  De inhoud zou een afspiegeling kunnen zijn van het interne cyberbeveiligingsbeleid, het verwachte gedrag en de beschermingsmaatregelen. Erkende kaders zoals AR-in-a-Box van ENISA zouden als leidraad kunnen dienen voor het ontwerp van het programma.
- **OT-specifieke risico's zouden kunnen worden aangepakt**
  Training zou kunnen worden afgestemd op de unieke verantwoordelijkheden en risico's waarmee personeel dat met industriële controlesystemen en andere OT-middelen werkt, te maken heeft.
- **De inhoud zou up-to-date kunnen worden gehouden**
  Trainingsmateriaal zou regelmatig kunnen worden herzien en bijgewerkt om nieuwe bedreigingen en lessen die uit incidenten zijn getrokken, te weerspiegelen.



Gegevens worden beheerd in overeenstemming met de risicostrategie van de organisatie om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen.

PR.DS-01 De vertrouwelijkheid, integriteit en beschikbaarheid van opgeslagen gegevens worden beschermd

PR.DS-01.9 Bedrijfsmiddelen moeten op een veilige manier worden verwijderd.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle bedrijfsmiddelen op een veilige en gecontroleerde manier worden verwijderd, om ongeoorloofde toegang tot gevoelige zakelijke, persoonlijke of operationele gegevens te voorkomen.

Om dit doel te ondersteunen, zou de organisatie kunnen overwegen om:

- **Gegevens op te schonen vóór verwijdering**
  Gevoelige gegevens zouden veilig kunnen worden verwijderd ("gewist") van alle bedrijfsmiddelen, zoals computers, servers, harde schijven, USB-sticks, mobiele apparaten en papieren documenten, voordat deze buiten gebruik worden gesteld, worden hergebruikt, gerepareerd of vervangen.
- **Gebruik te maken van geschikte vernietigingsmethoden**
  Er zouden geschikte methoden beschikbaar kunnen zijn voor het vernietigen van papieren documenten, digitale opslagmedia en andere fysieke gegevensdragers.
- **Wissen op afstand voor mobiele apparaten mogelijk te maken**
  Op laptops, tablets, telefoons en andere mobiele apparaten zou de mogelijkheid tot wissen op afstand kunnen worden ingeschakeld om gegevens te beschermen in geval van verlies of diefstal.
- **Verlopen domeinnamen zorgvuldig te beheren**
  Verlopen domeinen zouden kunnen worden beschermd, omdat ze vaak het doelwit zijn van cybercriminelen. De volgende maatregelen zouden kunnen worden overwogen:
  - Schakel automatische verlenging in of verleng domeinen voor ten minste tien jaar.
  - Communiceer domeinwijzigingen duidelijk en beheer overgangen intern.
  - Stel automatische antwoorden in voor e-mails die naar oude domeinen worden verzonden.
  - Werk online verwijzingen en instellingen voor clouddiensten bij.
  - Wijzig of verwijder accounts die zijn geregistreerd met oude domeinen.
  - Houd e-mailadressen voor aanmeldingen actueel en schakel MFA in.
  - Het gebruik van niet-goedgekeurde cloudopslag voor gevoelige gegevens zou kunnen worden vermeden.
- **Best practices voor assetsbeheer te volgen**
  Richtlijnen van betrouwbare bronnen, zoals de template voor het beleid voor assetsbeheer in de CyFun® Toolbox op www.cyfun.eu , zouden kunnen worden gebruikt om veilige verwijdering te ondersteunen.
- **OT-assets op te nemen in de planning voor buitengebruikstelling**
  OT-systemen en -apparaten zouden kunnen worden opgenomen in de procedures voor buitengebruikstelling, waarbij ervoor wordt gezorgd dat operationele gegevens en configuraties veilig worden verwijderd voordat ze uit dienst worden genomen.

PR.DS-11 Er worden back-ups van gegevens gemaakt, beschermd, onderhouden en getest

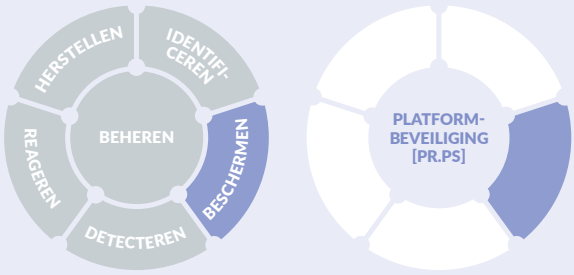
PR.DS-11.1 **Back-ups van de bedrijfskritieke gegevens van de organisatie moeten worden gemaakt en opgeslagen op een ander systeem dan het apparaat waarop de originele gegevens zich bevinden.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat bedrijfskritieke gegevens regelmatig worden geback-upt en veilig worden opgeslagen op een apart systeem om ze te beschermen tegen gegevensverlies, systeemstoringen of cyberaanvallen zoals ransomware.

Om dit doel te ondersteunen, zou de organisatie kunnen overwegen om:

- **Back-ups te maken van kritieke gegevens en systemen**
  Back-ups zouden het volgende kunnen omvatten:
  - Bedrijfskritieke gegevens (bijv. klantgegevens, financiële en operationele gegevens).
  - Systeemgegevens zoals softwareconfiguraties, apparaatinstellingen, documentatie en back-ups van applicaties.
- **Een back-upstrategie te definiëren**
  - Van kritieke gegevens zou continu of bijna in realtime een back-up kunnen worden gemaakt.
  - Van andere belangrijke gegevens zou op regelmatige, overeengekomen tijdstippen een back-up kunnen worden gemaakt.
  - Back-ups zouden kunnen worden opgeslagen op een systeem dat fysiek of logisch gescheiden is van de oorspronkelijke gegevensbron. Dit zou kunnen betekenen dat ze niet op hetzelfde apparaat, dezelfde server of dezelfde opslagarray staan als de oorspronkelijke gegevens. Idealiter zouden back-ups kunnen worden opgeslagen in een andere beveiligingszone, een ander netwerksegment of zelfs op een externe locatie, zodat ze toegankelijk en onbeschadigd blijven in geval van systeemstoringen, ransomware of andere incidenten die van invloed zijn op de primaire omgeving.
- **Te zorgen voor netwerksegmentatie**
  - Back-ups zouden niet op hetzelfde netwerk mogen worden opgeslagen als de oorspronkelijke systemen.
  - Ten minste één back-upkopie zou volledig offline of air-gapped kunnen worden bewaard om herstel te garanderen in geval van een netwerkgerelateerde cyberaanval, zoals bijvoorbeeld ransomware.
- **Herstel te plannen**
  De Recovery Time Objective (RTO – hoe snel systemen moeten worden hersteld) en de Recovery Point Objective (RPO – hoeveel gegevensverlies acceptabel is) zouden kunnen worden gedefinieerd en regelmatig geëvalueerd om een tijdig en effectief herstel te garanderen.
- **OT-omgevingen op te nemen**
  Back-upstrategieën zouden OT-systemen kunnen omvatten, waaronder configuraties van besturingssystemen, operationele gegevens en apparaatinstellingen die cruciaal zijn voor industriële activiteiten.



De hardware, software (bijv. firmware, besturingssystemen, applicaties) en diensten van fysieke en virtuele platforms worden beheerd in overeenstemming met de risicostrategie van de organisatie om hun vertrouwelijkheid, integriteit en beschikbaarheid te beschermen.

PR.PS-04 Er worden logbestanden gegenereerd en beschikbaar gesteld voor continue monitoring

PR.PS-04.1 Logbestanden moeten worden bijgehouden, gedocumenteerd en bewaakt.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat logboeken consistent worden bijgehouden, gedocumenteerd en bewaakt om de zichtbaarheid, verantwoordingsplicht en vroege detectie van afwijkingen of bedreigingen te ondersteunen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Logboekregistratie op alle systemen mogelijk maken**
  Alle besturingssystemen, applicaties, diensten (inclusief cloudgebaseerde) en beveiligingstools (bijv. firewalls, antivirusprogramma's) zouden zo geconfigureerd kunnen worden dat ze logboekrecords genereren.
- **Verschillende soorten logboeken opnemen**
  Logs zouden, indien van toepassing, het volgende kunnen omvatten: auditlogs, gebeurtenislogs, applicatielogs, beveiligingslogs, systeemlogs en onderhoudslogs.
- **Loggegevens beschermen**
  Logs zouden beschermd kunnen worden tegen ongeoorloofde toegang door middel van versleuteling en toegangscontroles.
- **Back-ups van logboeken maken en bewaren**
  Logboekback-ups zouden regelmatig kunnen worden uitgevoerd en gedurende een vooraf vastgestelde periode bewaard kunnen worden, afhankelijk van de behoeften van het bedrijf of wettelijke vereisten.
- **Logs controleren op afwijkingen**
  Logs zouden gecontroleerd kunnen worden om ongebruikelijke patronen of gedragingen op te sporen, zoals herhaalde detecties van malware of buitensporige toegang tot niet-zakelijke websites.
- **Bewaartermijnen vaststellen**
  Bewaartermijnen voor logboeken zouden duidelijk kunnen worden gedefinieerd, waarbij rekening wordt gehouden met sectorspecifieke vereisten.
- **Monitoring en verantwoordingsplicht ondersteunen**
  Er zou monitoring kunnen plaatsvinden om inzicht te krijgen in de systeemactiviteiten en om effectieve audits en incidentrespons te ondersteunen.
- **OT-systemen opnemen**
  Het bijhouden van systeemactiviteiten zou ook kunnen plaatsvinden in OT-omgevingen, inclusief industriële controlesystemen. Deze registraties helpen om afwijkingen in de werking of pogingen tot ongeautoriseerde toegang op te sporen.

PR.PS-05 De installatie en uitvoering van ongeautoriseerde software wordt voorkomen

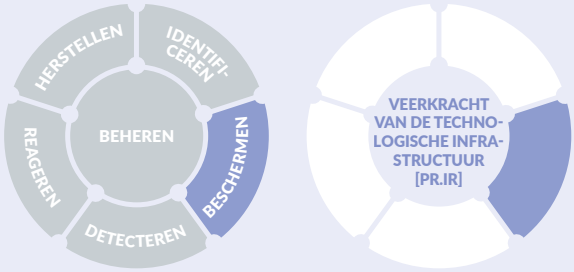
PR.PS-05.1 Er moeten web- en e-mailfilters worden geïnstalleerd en gebruikt.

Implementatierichtlijnen

Het doel van deze controle is het risico op malware-infecties, phishingaanvallen en datalekken te verminderen door effectieve web- en e-mailfilteroplossingen te implementeren en te onderhouden.

Om dit doel te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

- **Webfilters implementeren**
  Webfilters zouden gebruikt kunnen worden om de toegang tot websites te controleren op basis van:
  - Vooraf gedefinieerde lijsten met toegestane/geblokkeerde websites (bijvoorbeeld op basis van URL of domein)
  - Realtime inhoudsanalyse om schadelijke of ongepaste inhoud te detecteren
  - Technieken zoals URL-filtering, inhoudfiltering, DNS-filtering en filtering aan de client- of serverzijde
- **E-mailfiltering configureren**
  E-mailfilters zouden geconfigureerd kunnen worden om:
  - Spam, phishingpogingen en kwaadaardige bijlagen of links te blokkeren
  - Inkomende e-mails te categoriseren (bijv. nieuwsbrieven, meldingen van sociale media) om rommel te verminderen en de bewustmaking te vergroten
  - Te scannen op bekende bedreigingen en verdachte patronen om de e-mailbeveiliging te verbeteren
- **Filters up-to-date houden**
  Filterregels en bedreigingsdatabases zouden regelmatig kunnen worden bijgewerkt om te kunnen reageren op nieuwe bedreigingen.
- **Integreren met het beveiligingsbeleid**
  Web- en e-mailfiltering zouden afgestemd kunnen worden op het bredere beveiligingsbeleid en de bewustmakingsinspanningen van de organisatie.
- **Neem OT-aspecten mee in de overwegingen**
  In OT-omgevingen zou de toegang tot internet en e-mail beperkt kunnen worden tot wat operationeel noodzakelijk is. Filtering zou toegepast kunnen worden op alle systemen met externe verbindingen om blootstelling aan bedreigingen te voorkomen.



Beveiligingsarchitecturen worden beheerd met behulp van de risicostrategie van de organisatie om de vertrouwelijkheid, integriteit en beschikbaarheid van assets en de veerkracht van de organisatie te beschermen.

PR.IR-01 Netwerken en omgevingen worden beschermd tegen ongeoorloofde logische toegang en gebruik

PR.IR-01.1 Firewalls moeten worden geïnstalleerd, geconfigureerd en actief onderhouden op alle netwerken die door de organisatie worden gebruikt om bescherming te bieden tegen ongeoorloofde toegang en cyberdreigingen.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat alle netwerken die door de organisatie worden gebruikt, worden beschermd tegen ongeoorloofde toegang en cyberdreigingen door middel van de installatie, configuratie en actieve onderhoud van firewalls.

Deze controle richt zich op de installatie, configuratie en het onderhoud van netwerkgebaseerde firewalls om ongeoorloofde toegang te voorkomen door het verkeer dat het netwerk binnenkomt of verlaat te monitoren en te controleren (focus: controle en preventie). Controle DE.CM-01.1 richt zich daarentegen op hostgebaseerde firewalls, die helpen bij het detecteren van bedreigingen die de netwerkperimeter omzeilen door het verkeer van en naar individuele apparaten te monitoren (focus: zichtbaarheid en detectie).

Om dit doel te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

- De netwerkperimeter beschermen
  - Er zou een firewall kunnen worden geïnstalleerd tussen het interne netwerk en het internet. Deze zou geïntegreerd kunnen zijn in een draadloos toegangspunt, router of door de internetprovider geleverd apparaat.
  - Firewalls zouden geconfigureerd kunnen worden op basis van een basisbeveiligingsbeleid volgens het principe 'standaard alles weigeren, alleen uitzonderingen toestaan'.
- Eindapparaten beveiligen
  - Er zou een softwarefirewall kunnen worden geïnstalleerd en regelmatig bijgewerkt op alle eindapparaten, waaronder laptops, smartphones en andere netwerksystemen.
  - Lokale firewalls zouden actief kunnen blijven, zelfs bij gebruik van VPN's of clouddiensten.
- Veilige thuis- en werkomgevingen op afstand
  - Thuisnetwerken die worden gebruikt voor telewerken zouden routers met ingebouwde firewalls kunnen gebruiken, die ingeschakeld, veilig geconfigureerd en up-to-date gehouden zouden kunnen worden.
  - Op alle apparaten voor werken op afstand zouden softwarefirewalls actief kunnen zijn en regelmatig bijgewerkt kunnen worden.
  - De standaardbeheerdersgegevens van thuisrouters zouden regelmatig kunnen worden gewijzigd en bijgewerkt.

- **Operationele technologie (OT)-omgevingen beschermen**
  - Toegang op afstand tot OT-systemen zou behandeld kunnen worden als toegang door derden, niet als standaard telewerken.
  - Er zou een duidelijke scheiding tussen IT- en OT-netwerken kunnen worden gehandhaafd.
  - Wanneer toegang van IT tot OT noodzakelijk is, zou deze via een beveiligde jumphost in een speciale DMZ kunnen verlopen.
- **De detectie verbeteren met IDPS**
  Het zou overwogen kunnen worden om een Intrusion Detection and Prevention System (IDPS) in te zetten om het netwerkverkeer te monitoren en te analyseren op verdachte activiteiten en de algehele bescherming te verbeteren.

PR.IR-01.2 Om kritieke systemen te beschermen, moeten organisaties netwerksegmentatie en -scheiding toepassen, afgestemd op zones met verschillend vertrouwensniveau en de kriticiteit van systemen, zodat dreigingen zich niet kunnen verspreiden en strikte toegangscontrole wordt afgedwongen.

Implementatierichtlijnen

Het doel van deze controle is om de verspreiding van cyberdreigingen te beperken en strikte toegangscontrole af te dwingen door netwerksegmentatie en -segregatie te implementeren op basis van vertrouwensgrenzen en de kriticiteit van systemen.

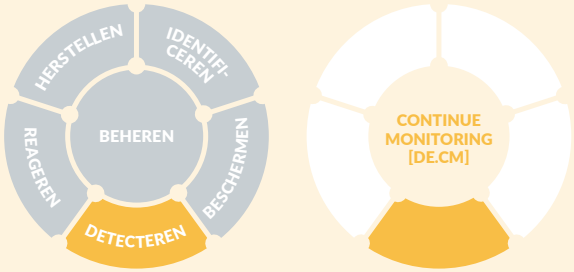
Om deze controle te implementeren, kan het volgende worden overwogen:

- **Beveiligingszones definiëren**
  Netwerken zouden kunnen worden onderverdeeld in afzonderlijke zones (bijv. kantoor, productie, gasten, mobiel). Het verkeer tussen zones zou bewaakt en beheerd kunnen worden, bijvoorbeeld met behulp van firewalls.
- **Segmentatie afstemmen op vertrouwen en kriticiteit**
  Segmentatie zou een weerspiegeling kunnen zijn van welke gebruikers en systemen vertrouwd worden en hoe kritiek elk asset is. Alleen essentiële communicatie tussen zones zou kunnen worden toegestaan, volgens het principe van minimale rechten.
- **Vlakke netwerken vermijden**
  Vlakke netwerken zouden vermeden kunnen worden, omdat het compromitteren van één systeem de hele omgeving zou kunnen blootstellen. Segmentatie zou kunnen helpen om bedreigingen binnen één zone te beperken.
- **IT- en OT-omgevingen scheiden**
  In omgevingen met industriële systemen (OT) zouden kantoor- en productienetwerken gescheiden kunnen zijn. Gast- en mobiele netwerken zouden geen directe toegang mogen hebben tot interne kantoor- of productiesystemen. Segmentatie zou kunnen voldoen aan de IEC 62443-norm, met name de vereisten SR 5.1 tot en met SR 5.3.
- **Voorzichtig zijn met het gebruik van VLAN's**
  VLAN's zouden alleen kunnen worden gebruikt als onderdeel van een bredere strategie voor diepgaande beveiliging. Ze zouden niet als enige middel mogen worden gebruikt om te voldoen aan de vereisten van beveiligingsniveau 2 volgens IEC 62443-3-3. VLAN's zouden gecombineerd kunnen worden met firewalls, toegangscontroles en monitoring.
- **Segmentatie afdwingen met firewalls**
  Firewalls zouden zo geconfigureerd kunnen worden dat ze standaard al het verkeer blokkeren en alleen specifieke, goedgekeurde verbindingen toestaan. Segmentatie en segregatie zouden kunnen worden afgedwongen door middel van goed onderhouden firewallregels, in overeenstemming met controle PR.IR-01.1.
- **Segmentatie en segregatie duidelijk onderscheiden**
  - Segmentatie zou kunnen worden gebruikt om netwerken logisch te verdelen en het verkeer tussen zones te controleren.
  - Segregatie zou kunnen worden toegepast wanneer systemen geïsoleerd moeten worden, zonder directe communicatie, tenzij dit expliciet is toegestaan.


WARNING!
SYSTEM WARNING

DETECTEREN

Detecteren



Assets worden gemonitord om afwijkingen, indicatoren van compromittering en andere potentieel nadelige gebeurtenissen op te sporen.

DE.CM-01 Netwerken en netwerkdiensten worden gemonitord om potentieel ongunstige gebeurtenissen op te sporen

DE.CM-01.1 Firewalls moeten worden geïnstalleerd en beheerd op de grenzen van het netwerk, inclusief firewalls op eindpunten.

Implementatierichtlijnen

Het doel van deze controle is het verbeteren van de zichtbaarheid en detectie van bedreigingen op apparaatniveau, met name bedreigingen die traditionele netwerkperimeterbeveiligingen kunnen omzeilen.

Deze controle richt zich op het gebruik van hostgebaseerde firewalls om bedreigingen te detecteren die de netwerkperimeter kunnen omzeilen, door het verkeer van en naar individuele apparaten te monitoren en te controleren (focus: zichtbaarheid en detectie).
Controle PR.IR-01.1 daarentegen richt zich op netwerkgebaseerde firewalls, die zijn ontworpen om ongeautoriseerde toegang te voorkomen door het verkeer dat het netwerk binnenkomt of verlaat te beheren (focus: controle en preventie).

Om dit doel te bereiken, kan het volgende worden overwogen:

- **Eindpunten in brede zin definiëren**: dit zou desktops, laptops, servers, smartphones en, waar mogelijk, OT-componenten (Operationele Technologie) zoals PLC's en HMI's, evenals IoT-apparaten kunnen omvatten.
- **Hostgebaseerde firewalls implementeren**: er zou voor gezorgd kunnen worden dat firewalls zijn geïnstalleerd, actief zijn en correct zijn geconfigureerd op alle eindpuntapparaten. Deze firewalls zouden kunnen helpen bij het detecteren en blokkeren van verdachte activiteiten direct op het apparaat, zelfs wanneer het is verbonden met beveiligde netwerken of VPN's.
- **Netwerkassets segmenteren**: systemen zouden gegroepeerd kunnen worden op basis van hun kriticiteit of functie (bijvoorbeeld openbare diensten zoals e-mail-, web- en VPN-servers in een DMZ plaatsen).
- **Vooraf gedefinieerde firewallregels gebruiken**: er zouden regels kunnen worden opgesteld om zowel inkomend als uitgaand verkeer te filteren, zodat afwijkingen of kwaadaardig gedrag kunnen worden gedetecteerd.
- **Internetgateways beperken**: het aantal verbindingspunten met het internet zou verminderd kunnen worden om de blootstelling te minimaliseren en de monitoring te vereenvoudigen.

DE.CM-01.2 Anti-virus, -spyware- en andere anti-malwareprogramma's moeten worden geïnstalleerd en bijgewerkt.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle apparaten van de organisatie (IT- en OT-middelen) worden beschermd tegen kwaadaardige software door antimalwaretools te implementeren en regelmatig bij te werken.

Om dit doel te bereiken, zou de organisatie rekening kunnen houden met het volgende:

- **Reikwijdte van de bescherming**
  - IT-apparaten: anti-malwaresoftware zou geïnstalleerd kunnen worden op alle gebruikers- en systeemapparaten, waaronder desktops, laptops, servers, smartphones en tablets.
  - OT-apparaten: de bescherming zou uitgebreid kunnen worden naar OT-middelen zoals PLC's, HMI's, SCADA-servers en technische werkstations, voor zover dit technisch haalbaar is.
- **Update- en scanpraktijken**
  - IT: antimalwaretools zouden zo geconfigureerd kunnen worden dat ze in realtime of ten minste dagelijks worden bijgewerkt, gevolgd door geautomatiseerde of geplande scans.
  - OT: updates en scans zouden zorgvuldig gepland kunnen worden om operationele verstoringen te voorkomen. Onderhoudsvensters zouden gebruikt kunnen worden en updates zouden vooraf getest kunnen worden.
- **Op maat gemaakte oplossingen voor OT**
  - Lichtgewicht of OT-specifieke antimalwaretools zouden gebruikt kunnen worden die compatibel zijn met realtime systemen.
  - Voor verouderde of resource-beperkte OT-apparaten zou het volgende overwogen kunnen worden:
    - Whitelisting van applicaties
    - Netwerkgebaseerde malwaredetectie
  - Gebruik gespecialiseerde tools die industriële systemen stil monitoren om ongebruikelijke of verdachte activiteiten op te sporen, zonder de werking van de systemen te verstoren (passieve monitoring).
- **Werken op afstand en BYOD**
  Dezelfde beschermingsnormen zouden toegepast kunnen worden op:
  - Thuiscomputers die worden gebruikt voor telewerken
  - Persoonlijke apparaten (BYOD) die worden gebruikt voor professionele taken
  - Endpointbeveiligingsplatforms zouden gebruikt kunnen worden om het beleid op alle apparaten te handhaven.
- **Gecentraliseerd beheer en monitoring**
  - Gecentraliseerde tools zouden gebruikt kunnen worden om anti-malwareconfiguraties, updates en waarschuwingen in zowel IT- als OT-omgevingen te beheren.
  - Malwarewaarschuwingen zouden geïntegreerd kunnen worden in de bredere beveiligingsmonitoring en incidentresponsprocessen van de organisatie.
- **Continue verbetering**
  - De effectiviteit van anti-malware zou regelmatig geëvalueerd en getest kunnen worden.
  - Beleid en tools zouden bijgewerkt kunnen worden op basis van nieuwe bedreigingen en lessen die uit incidenten zijn getrokken.

DE.CM-03 De activiteiten van het personeel en het gebruik van technologie worden gemonitord om potentieel ongewenste gebeurtenissen op te sporen

DE.CM-03-1 Er moeten tools voor eindpunt- en netwerkbeveiliging worden geïmplementeerd om het gedrag van eindgebruikers te monitoren op gevaarlijke activiteiten.

Implementatierichtlijnen

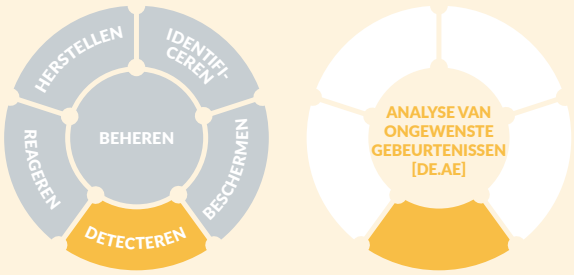
Het doel van deze controle is ervoor te zorgen dat de organisatie risicovol of verdacht gedrag van gebruikers op zowel apparaten als netwerken kan detecteren en hierop kan reageren. Dit helpt bij het identificeren van bedreigingen zoals malware-infecties, misbruik van systemen of pogingen om beveiligingsmaatregelen te omzeilen, ongeacht of deze worden veroorzaakt door externe aanvallers of insiders.

Om dit doel te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

Organisaties zouden kunnen overwegen om een combinatie van moderne beveiligingstools te gebruiken die samen een volledig beeld geven van de activiteiten van gebruikers en systemen:

- Intrusion Detection and Prevention Systems (IDPS): deze tools monitoren het netwerkverkeer en kunnen verdachte activiteiten, zoals hackpogingen of misbruik van kwetsbaarheden, blokkeren of signaleren.
- Web Application Firewalls (WAF's) en API-gateways: deze helpen online applicaties en diensten te beschermen door schadelijk verkeer te filteren en ongeoorloofde toegang te voorkomen.

- Daarnaast kan een gelaagde aanpak met geavanceerde detectie- en responstools realtime inzicht en een snellere respons bieden:
  - Endpoint Detection and Response (EDR): bewaakt activiteiten op individuele apparaten (zoals laptops of servers) om bedreigingen zoals malware of ongeoorloofde toegang te detecteren.
  - Network Detection and Response (NDR): analyseert netwerkverkeer om ongebruikelijke patronen te identificeren, zoals laterale bewegingen of verborgen aanvallen.
  - Identity Threat Detection and Response (ITDR): richt zich op het detecteren van misbruik van gebruikersaccounts, zoals gestolen authenticatiemiddelen of bedreigingen van binnenuit.
  - User and Entity Behaviour Analytics (UEBA): maakt gebruik van machine learning om normaal gedrag te begrijpen en afwijkingen te detecteren die op een bedreiging kunnen duiden.
- Deze tools maken deel uit van een moderne, gelaagde beveiligingsstrategie en worden vaak genoemd in best practices en frameworks voor de sector, zoals de Security Operations Centre (SOC) Visibility Triad die door Gartner is geïntroduceerd.



Afwijkingen, indicatoren van compromittering en andere potentieel ongewenste gebeurtenissen worden geanalyseerd om de gebeurtenissen te karakteriseren en cyberbeveiligingsincidenten op te sporen.

DE.AE-03 Informatie wordt gecorreleerd vanuit meerdere bronnen

DE.AE-03.1 De logfunctionaliteit van beschermings- en detectietools moet worden ingeschakeld. Logbestanden moeten worden geback-upt, gedurende een vooraf bepaalde periode bewaard en regelmatig gecontroleerd om ongebruikelijke of mogelijk schadelijke activiteiten te identificeren.

Implementatierichtlijnen

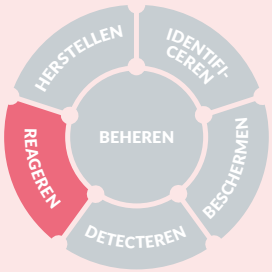
Het doel van deze controle is ervoor te zorgen dat beveiligingstools zijn ingesteld om logbestanden bij te houden, dat logbestanden gedurende een bepaalde tijd worden bewaard en dat ze regelmatig worden gecontroleerd om ongebruikelijke of schadelijke activiteiten op te sporen. Dit helpt om bedreigingen vroegtijdig te detecteren en maatregelen te nemen. Voorbeelden van dergelijke tools zijn firewalls, antivirussoftware, eindpuntdetectie en inbraakdetectiesystemen.

Om dit doel te bereiken, kan het volgende worden overwogen:

- Logs zouden veilig kunnen worden opgeslagen en bewaard volgens een vastgelegd bewaarschema, op basis van toepasselijke wettelijke, regelgevende of operationele vereisten.
- Tools en oplossingen voor gebeurtenisdetectie zouden zo kunnen worden geconfigureerd dat ze automatisch waarschuwingen genereren bij verdachte of schadelijke activiteiten.
- Er zou een gedocumenteerde procedure kunnen zijn voor het regelmatig controleren van logboeken en dashboards om tijdige detectie en reactie te ondersteunen.
- Bij het controleren van logboeken zou kunnen worden gekeken naar patronen zoals herhaalde malware-infecties, abnormaal netwerkverkeer of buitensporig veel toegang tot niet-zakelijke websites.
- Als dergelijke patronen worden vastgesteld, zouden vervolgacties kunnen worden gedefinieerd, zoals het versterken van specifieke beveiligingsmaatregelen, het bijwerken van detectieregels of het geven van gerichte bewustmakingsopleidingen.

REAGEREN

Reageren



Reacties op gedetecteerde cyberbeveiligings-incidenten worden beheerd

RS.MA-01 Het incidentresponsplan wordt uitgevoerd in samenwerking met relevante derde partijen zodra een incident is gemeld

RS.MA-01.1 Het incidentresponsplan van de organisatie moet tijdens of na een cyberbeveiligingsincident dat de kritieke systemen treft, worden uitgevoerd en duidelijke rollen, verantwoordelijkheden en bevoegdheden bevatten.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat een duidelijk omschreven incidentresponsplan wordt uitgevoerd tijdens of na een cyberbeveiligingsincident dat van invloed is op de kritieke systemen van de organisatie, zodat tijdige detectie, beheersing, communicatie en herstel mogelijk zijn.

Om het doel van deze controle te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

- **Een gedocumenteerd responsplan ontwikkelen**
  Het plan zou vooraf gedefinieerde instructies en procedures kunnen bevatten om cyberbeveiligingsincidenten te detecteren, effectief te reageren en het herstel van kritieke systemen te ondersteunen.
- **Detectiemogelijkheden opnemen**
  Er zouden detectietechnologieën aanwezig kunnen zijn om bevestigde incidenten automatisch te melden en responsmaatregelen in gang te zetten.
- **Rollen, verantwoordelijkheden en bevoegdheden definiëren**
  Het plan zou duidelijk kunnen aangeven:
  - Wie betrokken is bij de respons
  - De contactgegevens van belangrijke personen
  - Wie bevoegd is om het herstel in gang te zetten
  - Wie verantwoordelijk is voor externe communicatie (bijv. toezichthouders, partners, media)
- **Het plan regelmatig herzien en bijwerken**
  Het plan zou kunnen worden herzien en bijgewerkt om rekening te houden met veranderingen in het dreigingslandschap, de organisatiestructuur of lessen die zijn geleerd uit eerdere incidenten.
- **Het plan testen door middel van oefeningen**
  Er zouden simulaties en tabletop-oefeningen kunnen worden uitgevoerd om de effectiviteit van het plan te valideren en verbeterpunten te identificeren.
- **OT-omgevingen opnemen**
  Het plan zou betrekking kunnen hebben op de respons op incidenten in OT-systemen, inclusief coördinatie met veiligheidsprotocollen, isolatie van getroffen industriële assets en herstel van operationele processen.

RS.MA-02 Incidentrapporten worden gesorteerd en gevalideerd

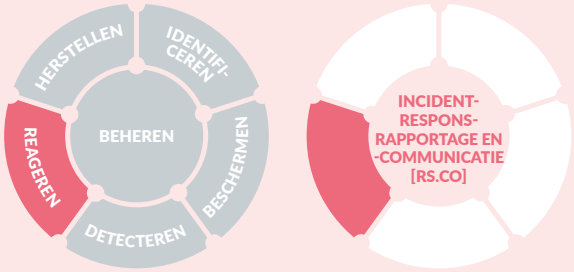
RS.MA-02.1 **Rapporten over informatie- / cyberbeveiligingsincidenten moeten worden geprioriteerd en gevalideerd volgens de incidentresponsprocedures van de organisatie.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle gemelde incidenten systematisch worden geëvalueerd voordat verdere actie wordt ondernomen.

Deze controle is een fundamentele stap in het incidentresponsproces en het volgende zou in overweging genomen kunnen worden:

- **Uitfilteren van irrelevante of valse rapporten**
  Niet elke ontvangen melding is een echt incident. Deze controle zou ervoor kunnen zorgen dat alleen legitieme, voor cyberbeveiliging relevante incidenten worden opgevolgd.
- **Zorgen voor een tijdige en passende reactie**
  Door meldingen vroegtijdig te sorteren en te valideren, zou de organisatie prioriteit kunnen geven aan echte bedreigingen en voorkomen dat middelen worden verspild aan niet-problemen.
- **Ondersteunen van consistente besluitvorming**
  Door gestructureerde sorteer- en validatiecriteria toe te passen, zou kunnen worden gezorgd dat de incidentrespons consistent, herhaalbaar en afgestemd is op het organisatiebeleid.
- **Mogelijk maken van effectieve escalatie en categorisering**
  Validatie zou een voorwaarde kunnen zijn voor het categoriseren en escaleren van incidenten (zoals vereist in RS.MA-03.1). Zonder validatie zou het responsproces verkeerd kunnen worden gestuurd of vertraging kunnen oplopen.
- **Verbeteren van het inzicht in de actuele situatie**
  Vroegtijdige validatie zou kunnen helpen een duidelijker beeld te krijgen van het dreigingslandschap en een betere coördinatie tussen teams te ondersteunen.



Responsactiviteiten worden gecoördineerd met interne en externe belanghebbenden, zoals vereist door wetten, voorschriften of beleid.

RS.CO-02 Interne en externe belanghebbenden worden op de hoogte gebracht van incidenten

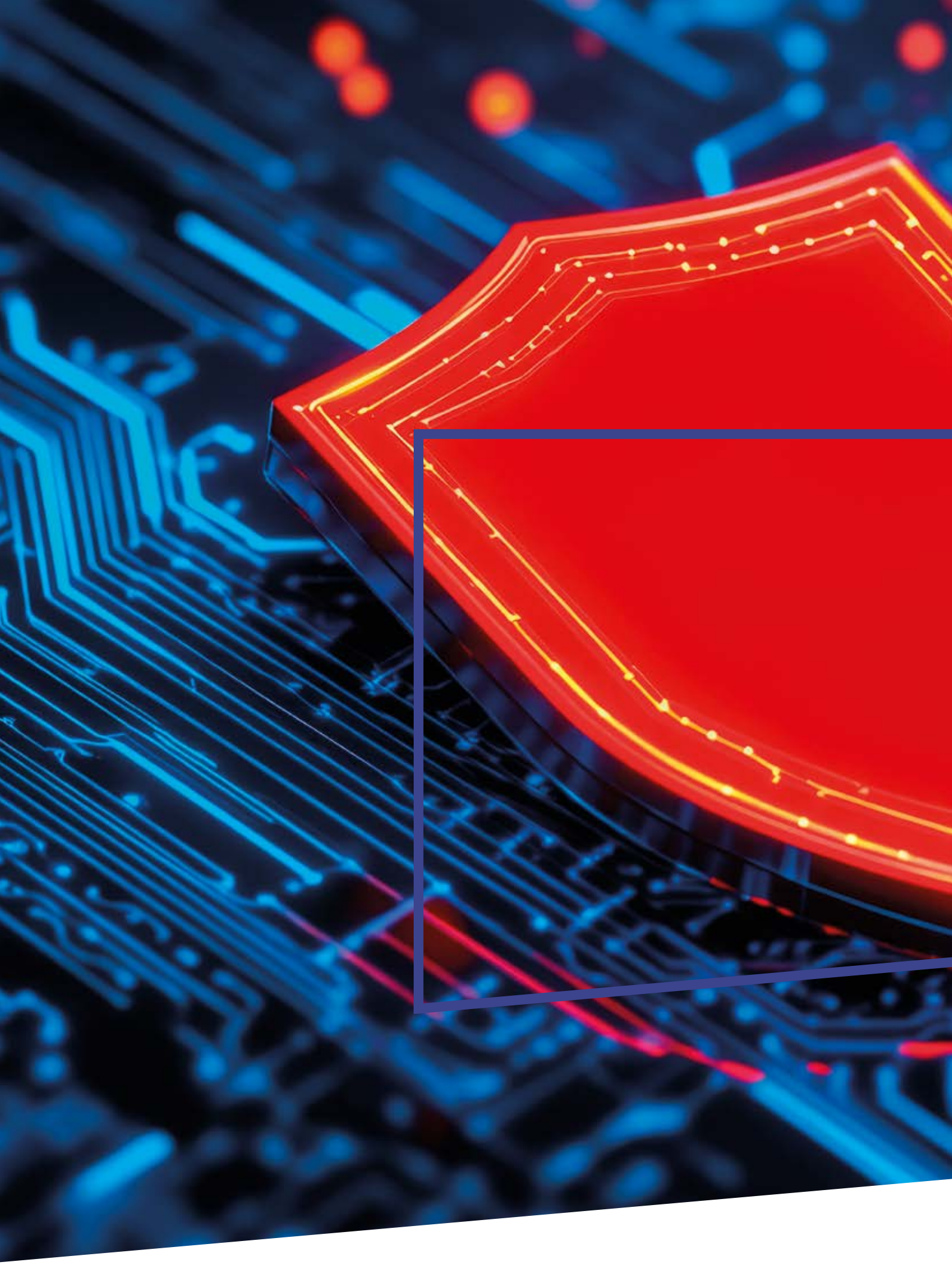
RS.CO-02.1 Informatie over cyberbeveiligingsincidenten moet aan medewerkers worden gecommuniceerd op een duidelijke en gemakkelijk te begrijpen manier.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat alle werknemers tijdig en op begrijpelijke wijze worden geïnformeerd over cyberbeveiligingsincidenten, zodat ze adequaat kunnen reageren en kunnen helpen risico's te verminderen.

Om het doel van deze controle te bereiken, kan het volgende in overweging worden genomen:

- Er zou een incidentresponsplan (IRP) kunnen worden opgesteld. In dit plan zou kunnen worden beschreven hoe de organisatie zal reageren op cyberbeveiligingsincidenten, inclusief wie waarvoor verantwoordelijk is en hoe verschillende soorten bedreigingen zouden kunnen worden geëscaleerd.
- Het IRP zou een communicatieprotocol kunnen bevatten waarin wordt uitgelegd hoe tijdens een incident snel en efficiënt accurate en relevante informatie met medewerkers zou kunnen worden gedeeld.
- Het plan zou de te gebruiken communicatiekanalen kunnen definiëren, zoals e-mail, interne berichtenplatforms, telefoongesprekken of een speciaal incidentenportaal.
- Er zouden vooraf templates voor incidentberichten kunnen worden opgesteld. Deze templates zouden belangrijke details kunnen bevatten, zoals het type incident, de ernst ervan, welke systemen zijn getroffen en welke maatregelen werknemers zouden kunnen nemen.
- Berichten zouden in duidelijke, eenvoudige taal kunnen worden geschreven, zonder technische termen, zodat alle medewerkers begrijpen wat er aan de hand is en wat er van hen wordt verwacht.
- Het senior management zou een samenvatting op hoog niveau kunnen ontvangen waarin de impact van het incident, de betrokken risico's en de genomen stappen om het op te lossen, worden uitgelegd.



HERSTELLEN

Herstellen

Herstelwerkzaamheden worden uitgevoerd om de operationele beschikbaarheid van systemen en diensten die door cyberbeveiligingsincidenten zijn getroffen, te waarborgen.

RC.RP-01 Het herstelgedeelte van het incidentresponsplan wordt uitgevoerd zodra het incidentresponsproces is gestart

RC.RP-01.1 Er moet een herstelproces voor rampen en informatie-/cyberbeveiligingsincidenten worden ontwikkeld en uitgevoerd.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de organisatie snel en effectief kan reageren op rampen, informatiebeveiligingsincidenten en cyberbeveiligingsincidenten door een gestructureerd herstelproces te ontwikkelen en uit te voeren dat mensen, systemen en gegevens beschermt.

Om dit doel te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

- **Een herstelproces ontwikkelen**: Een gedocumenteerd proces zou als leidraad kunnen dienen voor onmiddellijke acties in geval van brand, medische noodsituaties, diefstal, natuurrampen of informatie-/cyberbeveiligingsincidenten.
- **Rollen en verantwoordelijkheden definiëren**: Het herstelproces zou kunnen specificeren wie bevoegd is om herstelprocedures in gang te zetten en wie met externe belanghebbenden zal communiceren.
- **Informatie en systemen beschermen**: Het proces zou stappen kunnen bevatten om informatie en systemen te beveiligen, zoals het uitschakelen of vergrendelen van apparaten, overschakelen naar back-up locaties of het beveiligen van fysieke documenten.
- **Contactprocedures vaststellen**: Er zou een lijst met interne en externe contactpersonen kunnen worden bijgehouden en opgenomen in het herstelplan, zodat deze tijdens een incident snel toegankelijk is.
- **Zorgen voor bewustmaking en paraatheid**: Personen met herstelverantwoordelijkheden zouden bekend kunnen zijn met het herstelplan en begrijpen welke autorisaties nodig zijn om elke stap uit te voeren.
- **Integreren in het incidentresponsplan**: Het herstelproces moet deel uitmaken van of worden afgestemd op het bredere incidentresponsplan (IRP) om consistentie en coördinatie te waarborgen.
- **OT-omgevingen opnemen**: Het herstelplan zou betrekking kunnen hebben op OT-systemen, inclusief procedures voor het herstellen van industriële activiteiten, het beveiligen van besturingssystemen en het coördineren met veiligheidsprotocollen.
- **Toekomstige verbeteringen plannen**: Deze controle dient als basis voor meer geavanceerde herstelplanning, zoals verder uitgewerkt in controle RC.RP-06.1 (zekerheidsniveau 'Important).

BIJLAGE

BIJLAGE A: LIJST MET KERNMAATREGELEN VOOR HET ZEKERHEIDSNIVEAU 'BASIC'

Identificeren

ID.AM-08 **Systemen, hardware, software, diensten en gegevens worden gedurende hun hele levenscyclus beheerd**

ID.AM-08.2 Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.

Beschermen

PR.AA-01 **Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware worden beheerd door de organisatie**

PR.AA-01.1 Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware moeten worden beheerd.

PR.AA-03 **Gebruikers, diensten en hardware worden geauthentiseerd.**

PR.AA-03.2 Multifactorauthenticatie (MFA) is vereist om op afstand toegang te krijgen tot de netwerken van de organisatie.

PR.AA-05 **Toegangsrechten, bevoegdheden en autorisaties worden gedefinieerd in een beleid, beheerd, gehandhaafd en beoordeeld, en omvatten de principes van minimale rechten en scheiding van taken.**

PR.AA-05.1 Toegangsrechten, machtigingen en autorisaties moeten worden vastgesteld, beheerd, gehandhaafd en periodiek herzien.

PR.AA-05.2 Er moet worden vastgesteld wie toegang nodig heeft tot de bedrijfskritische informatie en technologie van de organisatie, evenals op welke manier die toegang wordt verleend.

PR.AA-05.3 Toegangsrechten, privileges en autorisaties moeten worden beperkt tot de systemen en specifieke informatie die nodig zijn om de taken uit te voeren (het principe van 'Least Privilege').

PR.AA-05.4 Niemand mag beheerdersrechten hebben voor dagelijkse routinetaken.

PR.DS-11 Er worden back-ups van gegevens gemaakt, beschermd, onderhouden en getest.

PR.DS-11.1 Back-ups van de bedrijfskritieke gegevens van de organisatie moeten worden gemaakt en opgeslagen op een ander systeem dan het apparaat waarop de originele gegevens zich bevinden.

PR.PS-04 Er worden logbestanden gegenereerd en beschikbaar gesteld voor continue monitoring

PR.PS-04.1 Logbestanden moeten worden bijgehouden, gedocumenteerd en bewaakt.

PR.IR-01 Netwerken en omgevingen worden beschermd tegen ongeoorloofde logische toegang en gebruik

PR.IR-01.1 Firewalls moeten worden geïnstalleerd, geconfigureerd en actief onderhouden op alle netwerken die door de organisatie worden gebruikt om bescherming te bieden tegen ongeoorloofde toegang en cyberdreigingen.

PR.IR-01.2 Om kritieke systemen te beschermen, moeten organisaties netwerksegmentatie en -scheiding toepassen, afgestemd op zones met verschillend vertrouwensniveau en de kriticiteit van systemen, zodat dreigingen zich niet kunnen verspreiden en strikte toegangscontrole wordt afgedwongen.

Detecteren

DE.CM-01 Netwerken en netwerkdiensten worden gemonitord om potentieel ongunstige gebeurtenissen op te sporen

DE.CM-01.2 Anti-virus, -spyware- en andere anti-malwareprogramma's moeten worden geïnstalleerd en bijgewerkt.

DE.AE-03 Informatie wordt gecorreleerd vanuit meerdere bronnen.

DE.AE-03.1 De logfunctionaliteit van beschermings- en detectietools moet worden ingeschakeld. Logbestanden moeten worden geback-upt, gedurende een vooraf bepaalde periode bewaard en regelmatig gecontroleerd om ongebruikelijke of mogelijk schadelijke activiteiten te identificeren.

Disclaimer

Dit document en de bijlagen ervan zijn opgesteld door het Centrum voor Cyberveiligheid België (CCB), een federale overheidsinstantie die bij koninklijk besluit van 10 oktober 2014 is opgericht en onder de bevoegdheid van de premier valt.

Dit document bevat technische informatie in het Engels. De informatie over de beveiliging van netwerken en informatiesystemen is bedoeld voor IT-dienstverleners die Engelse computerterminologie gebruiken.

Het CCB aanvaardt geen aansprakelijkheid voor de inhoud van dit document.
De verstrekte informatie:

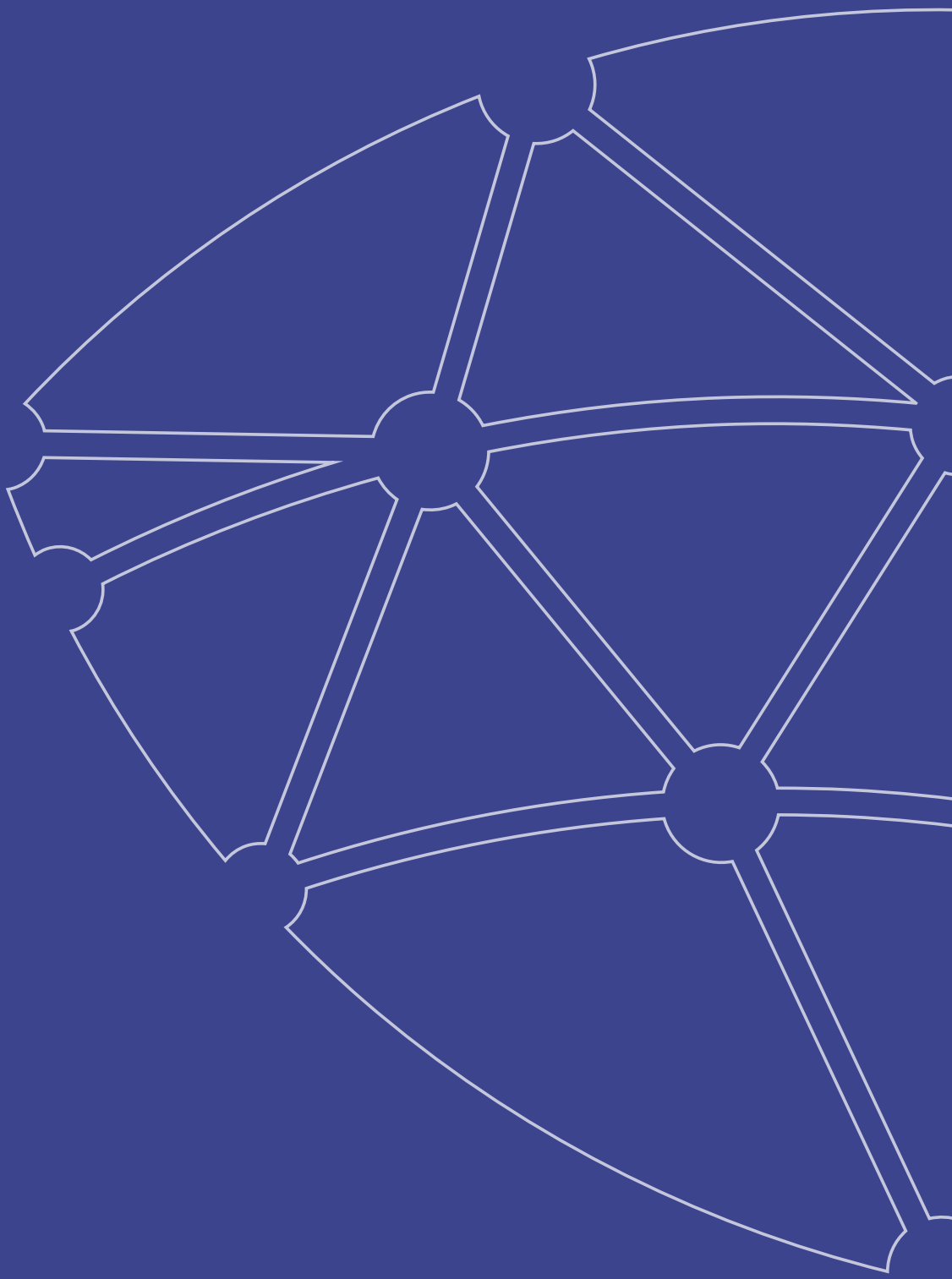
- is van algemene aard en dekt niet alle specifieke situaties.
- is niet noodzakelijkerwijs volledig, nauwkeurig of in alle opzichten actueel.

Verantwoordelijke redacteur

Centrum voor Cyberveiligheid België
De heer De Bruycker, directeur-generaal
Wetstraat 18
1000 Brussel

Juridisch depot

D/2025/14828/011



Zentrum für Cybersicherheit Belgien

Wetstraat 18

1000 Brüssel