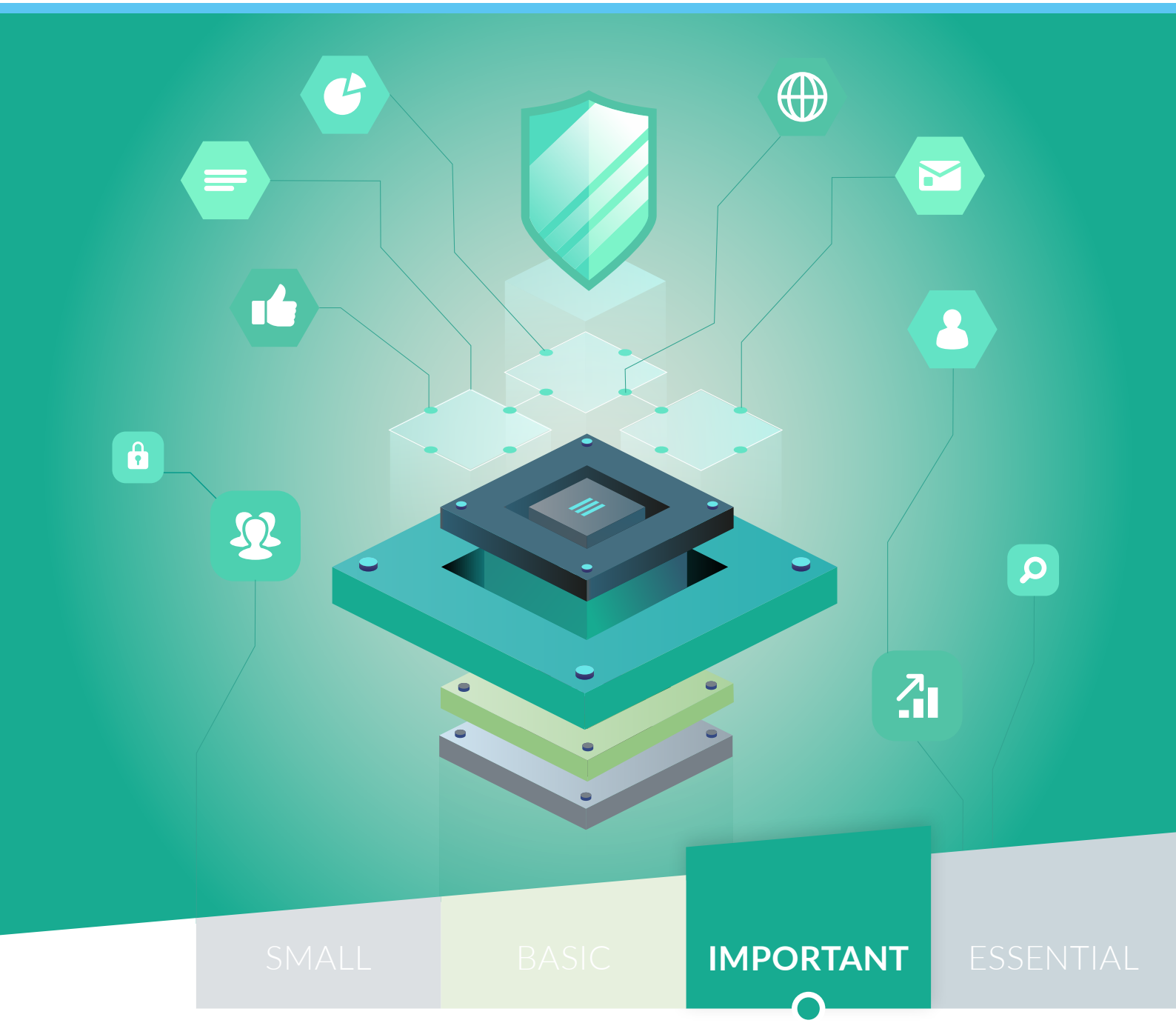
CyFun®



SMALL BASIC **IMPORTANT** ESSENTIAL

CyberFundamentals 2025

Nederlands

Version 2025-10-01

INHOUD

IDENTIFICEREN 27

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.

In het zekerheidsniveau **Important** worden de basis beveiligingsmaatregelen versterkt om bekende cyberrisico's te helpen verminderen en de impact van aanvallen door bedreigers met beperkte middelen en vaardigheden te beperken.

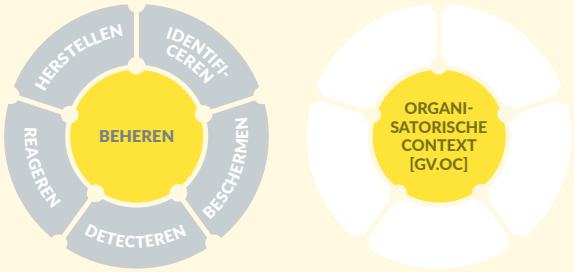
Controles met betrekking tot managementaspecten moeten tijdens elke certificeringsaudit worden beoordeeld – ongeacht of het gaat om een initiële audit, een surveillance-audit of een hercertificeringsaudit – wanneer het CyFun®-zekerheidsniveau Essential wordt geaudit. Deze controles sluiten aan bij de managementsysteemprincipes die certificeringsinstanties verplicht moeten toepassen conform ISO/IEC 17021-1, ongeacht het type managementsysteem dat wordt gecertificeerd.

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.


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-01 De missie van de organisatie wordt begrepen en vormt de basis voor het cyberbeveiligingsrisicobeheer

GV.OC-01.1 De missie van de organisatie moet worden vastgesteld, gecommuniceerd en vormt de basis voor informatie- en cyberbeveiligingsrisicobeheer.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat de missie van de organisatie duidelijk is gedefinieerd en gecommuniceerd, en dat deze als basis dient voor het beheer van informatie- en cyberbeveiligingsrisico's. Inzicht in de missie helpt bij het identificeren van risico's die het bereiken van strategische doelstellingen kunnen belemmeren.

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

- De missie van de organisatie zou kunnen worden gecommuniceerd via bv. visie- en missieverklaringen, dienstverleningsstrategieën of marketingdocumenten. Dit zou kunnen helpen bij het identificeren en prioriteren van risico's.
- Bij de ontwikkeling van bedrijfsprocessen en strategische doelstellingen zou rekening kunnen worden gehouden met informatiebeveiliging en cyberbeveiliging. Dit zou kunnen omvatten dat er inzicht wordt verkregen in hoe risico's van invloed kunnen zijn op activiteiten, assets, personen, partners of bredere maatschappelijke belangen.
- De noodzaak om gevoelige informatie, waaronder persoonsgegevens, te beschermen, zou kunnen worden beoordeeld op basis van de missie van de organisatie en de manier waarop haar systemen en diensten functioneren.
- De missie en de daarmee samenhangende bedrijfsprocessen zouden regelmatig, bijvoorbeeld eenmaal per jaar, kunnen worden geëvalueerd om ervoor te zorgen dat ze relevant blijven en effectief risicobeheer blijven ondersteunen.

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

GV.OC-03.2 Wettelijke, regelgevende en contractuele verplichtingen met betrekking tot informatie en cyberbeveiliging moeten continu worden beheerd om ervoor te zorgen dat ze accuraat en up-to-date blijven en effectief worden toegepast.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat wettelijke en regelgevende vereisten met betrekking tot informatie en cyberbeveiliging continu worden beheerd, up-to-date worden gehouden en effectief worden toegepast in de hele organisatie.

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

- Er zou een gestructureerd proces kunnen worden ingericht om wettelijke en regelgevende vereisten met betrekking tot informatie- en cyberbeveiliging continu te beheren.
- Deze vereisten zouden kunnen worden gedocumenteerd, regelmatig worden herzien en bijgewerkt om wijzigingen in wet- en regelgeving weer te geven.
- De aanpak van de organisatie op het gebied van compliance zou duidelijk kunnen worden gedefinieerd, met inbegrip van rollen, verantwoordelijkheden en verantwoordingsplicht.
- Er zouden mechanismen kunnen worden geïmplementeerd om veranderingen in het wettelijke en regelgevende kader te monitoren. Dergelijke veranderingen zouden aanleiding kunnen geven tot een herziening van relevante beleidslijnen, procedures en controles om permanente naleving te waarborgen.
- Bewijs van compliance-activiteiten zou kunnen worden bewaard ter ondersteuning van audits en om aan te tonen dat de nodige zorgvuldigheid in acht is genomen.

GV.OC-04 Kritieke doelstellingen, capaciteiten en diensten waarvan externe belanghebbenden afhankelijk zijn of die ze van de organisatie verwachten, worden begrepen en gecommuniceerd

GV.OC-04.1 **De organisatie moet vaststellen, documenteren en communiceren welke capaciteiten, diensten en doelstellingen voor externe belanghebbenden het meest belangrijk zijn. Deze moeten op prioriteit worden gerangschikt en meegenomen in de risicoanalyse.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de organisatie begrijpt welke kritieke diensten, capaciteiten (wat de organisatie kan) en doelstellingen essentieel zijn voor externe belanghebbenden, deze op basis van hun belang prioriteert en ze opneemt in het risicobeoordelingsproces.

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

- De focus van deze controle ligt op wat de organisatie aan anderen levert, met andere woorden, de diensten en functies waarvan externe stakeholders afhankelijk zijn (de downstream supply chain, zoals klanten, partners of eindgebruikers).
- De organisatie zou kritieke diensten en de interne functies die deze ondersteunen duidelijk kunnen identificeren.
- Er zouden criteria kunnen worden gedefinieerd om te bepalen hoe belangrijk elke dienst of capaciteit is, zowel vanuit intern als extern perspectief.
- Een bedrijfsimpactanalyse zou kunnen helpen bepalen welke assets en activiteiten van vitaal belang zijn voor het bereiken van belangrijke doelstellingen, en wat de gevolgen zouden zijn als deze zouden worden verstoord.
- Er zouden veerkrachtdoelstellingen kunnen worden vastgesteld en gecommuniceerd, zoals hoe snel kritieke diensten tijdens verstoringen zouden moeten herstellen.

GV.OC-04.2 **De organisatie moet cyberbeveiligingsvereisten voor essentiële activiteiten definiëren en documenteren, deze valideren door middel van tests en audits, de resultaten en eventuele corrigerende acties bijhoudenen de vereisten regelmatig bijwerken op basis van veranderende risico's.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat essentiële activiteiten worden beschermd door duidelijk omschreven en geteste beveiligingsmaatregelen, en dat deze maatregelen effectief en actueel blijven naarmate de risico's evolueren.

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

- **Identificatie en documentatie**
  - Het uitvoeren van een gestructureerde risicobeoordeling om kritieke diensten en hun afhankelijkheden (bijvoorbeeld systemen, leveranciers) te definiëren.
  - Het documenteren van beveiligings- en operationele vereisten, inclusief regelgevende en branchespecifieke behoeften (bijv. CyFun®, ISO/IEC 27001, IEC 62443)
- **Validatie en goedkeuring**
  - Het opzetten van governanceprocessen voor het beoordelen en goedkeuren van geïdentificeerde beveiligingsvereisten.
  - Het toewijzen van verantwoordelijkheden aan relevante belanghebbenden (bijv. beveiligingsteams, compliance officers, hoger management).

- Testen en borging
  - Het uitvoeren van penetratietesten, kwetsbaarheidsbeoordelingen en incidentensimulaties om de implementatie te valideren.
  - Het uitvoeren van audits om de effectiviteit te beoordelen en hiaten in de beveiligingsmaatregelen te identificeren.
  - Het uitvoeren van corrigerende maatregelen wanneer tekortkomingen worden vastgesteld, om zo continue verbetering te waarborgen.
- Registratie en compliance
  - Het bijhouden van gedetailleerde documentatie van testprocedures, resultaten, goedkeuringen en corrigerende maatregelen.
  - Het afstemmen van beveiligingsraamwerken op wettelijke verplichtingen om compliance en toezicht op het bestuur te waarborgen.
- Voortdurende evaluatie en aanpassing
  - Het regelmatig evalueren van de vereisten in reactie op veranderende bedreigingen, incidenten en wijzigingen in de regelgeving.
  - Het houden van toezicht door bestuursorganen op updates en verbeteringen om de cyberweerbaarheid op lange termijn te behouden.

GV.OC-05 De resultaten, capaciteiten en diensten waarvan de organisatie afhankelijk is, worden begrepen en gecommuniceerd

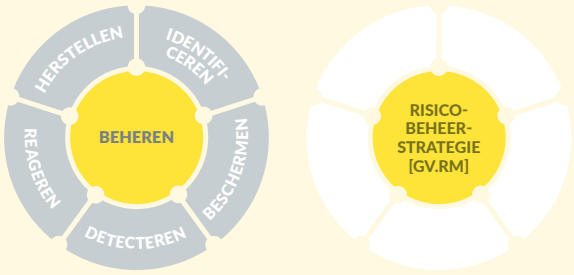
GV.OC-05.1 De organisatie moet duidelijk vastleggen welke rol zij speelt in de toeleveringsketen. Daarbij moet ze ook beschrijven en communiceren van welke externe diensten, middelen en afhankelijkheden ze gebruikmaakt (upstream), en hoe ze samenwerkt met partijen verderop in de keten (downstream).

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de organisatie haar rol binnen de toeleveringsketen identificeert, documenteert en communiceert door inzicht te krijgen in de externe diensten, middelen en afhankelijkheden waarvan ze gebruikmaakt (upstream), en hoe ze samenwerkt met partijen verderop in de keten (downstream).

Deze controle richt zich voornamelijk op de upstream-toeleveringsketen, dat wil zeggen waar de organisatie van anderen afhankelijk is, terwijl deze in overeenstemming blijft met GV.OC-04, die betrekking heeft op wat de organisatie aan anderen levert. Samen bieden ze een volledig beeld van de afhankelijkheden en verantwoordelijkheden in de toeleveringsketen.

Ter ondersteuning van deze controle kan het volgende worden overwogen:
- De rol van de organisatie in de toeleveringsketen zou duidelijk kunnen worden gedefinieerd, met inbegrip van zowel wat aan anderen wordt geleverd (downstream) als wat van externe bronnen wordt ontvangen (upstream).
- Afhankelijkheden van externe middelen, zoals faciliteiten, cloudproviders en leveranciers van diensten, producten of capaciteiten, zouden kunnen worden geïdentificeerd en gedocumenteerd.
- Deze afhankelijkheden zouden in kaart kunnen worden gebracht in relatie tot de betreffende bedrijfsfuncties en organisatorische middelen om inzicht te krijgen in hun impact op de bedrijfsvoering.
- Er zou bijzondere aandacht kunnen worden besteed aan externe afhankelijkheden die potentiële storingspunten vormen voor kritieke diensten of capaciteiten.
- Deze informatie zou kunnen worden gedeeld met relevant personeel en belanghebbenden ter ondersteuning van risicomanagement, continuïteitsplanning en gecoördineerde respons.
- Communicatiekanalen zouden kunnen worden opgezet om ervoor te zorgen dat de rollen en afhankelijkheden in de toeleveringsketen duidelijk worden begrepen binnen de organisatie en bij belangrijke partners.



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

GV.RM-01 Doelstellingen voor risicobeheer worden vastgesteld en overeengekomen door de belanghebbenden van de organisatie

GV.RM-01.1 Doelstellingen voor informatie- en cybersecurity moeten op coherente wijze binnen de hele organisatie worden vastgesteld en goedgekeurd door het senior management.

Implementatierichtlijnen

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

- De risicobeheerprincipes volgen die zijn uiteengezet in ISO/IEC 27005, die richtlijnen bieden voor het identificeren, beoordelen en beperken van informatiebeveiligingsrisico's. Meer specifiek:
  - Clausule 6.1 zou kunnen worden gebruikt om een gestructureerd risicobeoordelingsproces op te zetten.
  - Clausule 6.3 zou als leidraad kunnen dienen voor het definiëren van passende strategieën voor risicobeheersing.
- De informatie- en cyberbeveiligingsdoelstellingen voor de korte en lange termijn zouden kunnen worden bijgewerkt tijdens de jaarlijkse strategische planning en in reactie op belangrijke organisatorische veranderingen.
- In organisaties in de OT-sector zou het senior management bij het identificeren van risico's rekening kunnen houden met gezondheids-, veiligheids- en milieufactoren.
- Meetbare (SMART) doelstellingen voor informatie- en cyberbeveiliging zouden kunnen worden vastgesteld (bijvoorbeeld het verbeteren van de kwaliteit van de gebruikersopleiding, het waarborgen van adequate bescherming voor industriële controlesystemen). Deze doelstellingen zouden kunnen worden gebruikt om risico's en prestaties binnen de hele organisatie te meten en te beheren.

GV.RM-02 Verklaringen over risicobereidheid en risicotolerantie worden opgesteld, gecommuniceerd en onderhouden

GV.RM-02.1 Verklaringen over risicobereidheid en risicotolerantie moeten worden gedefinieerd, gedocumenteerd, goedgekeurd door het senior management, gecommuniceerd en onderhouden.

Implementatierichtlijnen

Het doel van GV.RM-02.1 is ervoor te zorgen dat een organisatie een duidelijk en bruikbaar inzicht heeft in haar risicogrenzen, wat helpt bij het sturen van besluitvorming en risicobeheerpraktijken.

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

- Risicobereidheid is de hoeveelheid en het type risico dat een organisatie bereid is te nemen of te accepteren, en is strategisch/kwalitatief (bron: ISO/IEC 27005).
- Risicotolerantie is de aanvaardbare afwijking van het niveau dat is vastgesteld door de risicobereidheid en de bedrijfsdoelstellingen, en is tactisch/kwantitatief (bron: ISACA).
- De risicobereidheid van de organisatie zou rekening kunnen houden met haar rol in kritieke infrastructuur en haar sector.
- Organisaties in de OT-sector zouden bij het bepalen van hun risicobereidheid rekening kunnen houden met prioriteiten op het gebied van gezondheid, veiligheid en milieu.
- Risicobereidheidsverklaringen zouden kunnen worden omgezet in specifieke, meetbare en algemeen begrijpelijke afspraken over hoeveel risico aanvaardbaar is (SMART).
- De doelstellingen en risicobereidheid van de organisatie zouden periodiek kunnen worden bijgesteld op basis van de bekende risicoblootstelling en het restrisico.
- Met AR-in-a-Box biedt ENISA, het Agentschap van de Europese Unie voor cyberbeveiliging, organisaties essentiële tools en middelen om de bewustmaking rond cyberbeveiliging binnen hun activiteiten effectief te vergroten. Deze ENISA-doe-het-zelf-toolbox bevat een gids voor het C-level.

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.

GV.RM-03.2 **Informatie- en cyberbeveiligingsrisico's moeten worden gedocumenteerd als onderdeel van de bedrijfsrisicobeheerprocessen, formeel worden goedgekeurd door het senior management en worden bijgewerkt wanneer zich wijzigingen voordoen.**

Implementatierichtlijnen

Deze controle moet ervoor zorgen dat de strategie via gestructureerde processen in praktijk wordt gebracht. De controle richt zich op het operationele en governanceniveau, zorgt voor verantwoordingsplicht en traceerbaarheid van risico's en legt de nadruk op formele processen en toezicht.

Bij de implementatie van deze controle kunnen de volgende uitvoerbare componenten worden overwogen:

Systematische risico-identificatie

- Doel: proactief identificeren van informatie- en cyberbeveiligingsrisico's binnen de hele organisatie.
- Acties:
  - Er zouden regelmatig risicobeoordelingen kunnen worden uitgevoerd met behulp van methoden zoals dreigingsmodellering, risicoworkshops en kwetsbaarheidsscans.
  - Risico's met betrekking tot alle digitale en fysieke assets (hardware, software, gegevens, netwerken) zouden kunnen worden opgenomen in de inventaris van assets, samen met belangrijke metagegevens (locatie, eigenaar, gebruik).
  - Gebruik zou kunnen worden gemaakt van bronnen zoals:
    - Logboeken van beveiligingsincidenten
    - Resultaten van penetratietests
    - Wettelijke vereisten
    - Bedreigingsinformatie uit de sector
  - Overweeg om multifunctionele teams (IT/OT, juridische afdeling, compliance, bedrijfsonderdelen) bij het proces te betrekken.
  - Te overwegen tools:
    - Risicobeoordelingstemplates
    - Platforms voor informatie over bedreigingen (bijv. MISP, Recorded Future)
    - Inventarissen van bedrijfsmiddelen en gegevensstroomdiagrammen

Risicodocumentatie in het ERM-raamwerk

- Doel: ervoor zorgen dat cyberbeveiligingsrisico's worden geïntegreerd in het bredere Enterprise Risk Management (ERM)-proces.
- Acties:
  - Overweeg het gebruik van een gecentraliseerd risicoregister of GRC-tool om het volgende te documenteren:
    - Risicobeschrijving
    - Waarschijnlijkheid en impact
    - Risico-eigenaar
    - Bestaande controles
    - Resterend risico
    - Behandelingsplan
  - Cybersecurityrisicobeheer zou kunnen worden afgestemd op strategische bedrijfsdoelstellingen om relevantie en ondersteuning te garanderen.
- Te overwegen tools:
  - GRC-platforms
  - Excel/SharePoint (voor kleinere organisaties)

Formele goedkeuring en betrokkenheid van het senior management

- Doel: zorgen voor toezicht en verantwoordingsplicht van het management bij risicobeslissingen.
- Acties:
  - Risicobeoordelingen en behandelingsplannen zouden kunnen worden voorgelegd aan een risicocomité of raad van bestuur.
  - Overweeg om cyberbeveiligingsrisico's op te nemen in kwartaalrapportages over risico's.
  - Er zou formele goedkeuring kunnen worden verkregen voor:
    - Risicoacceptatie
    - Mitigatieplannen
    - Budgettoewijzingen

- Te overwegen tools:
  - Templates voor rapportage aan de raad van bestuur
  - Risicodashboards
  - Notulen van vergaderingen met gedocumenteerde goedkeuringen

Communicatie en bewustmaking
- Doel: ervoor zorgen dat alle relevante belanghebbenden worden geïnformeerd en betrokken.
- Acties:
  - Er zouden duidelijke communicatielijnen kunnen worden opgezet voor cyberbeveiligingsrisico's, inclusief die van leveranciers en derde partijen.
  - Goedgekeurde risico's en risicobeperkende strategieën zouden kunnen worden gecommuniceerd aan de relevante teams.
  - Bewustwording zou kunnen worden bevorderd door middel van opleidingen, briefings en interne communicatie.
- Te overwegen tools:
  - Interne communicatieplatforms (bijv. Teams, Slack)
  - Risicocommunicatieplannen
  - Stakeholderkaarten

Voortdurende monitoring en updates
- Doel: risico-informatie actueel houden en inspelen op veranderingen.
- Acties:
  - Er zou continu toezicht kunnen worden gehouden om veranderingen in het dreigingslandschap of de organisatorische omgeving op te sporen.
  - Overweeg om triggers voor updates te definiëren, zoals:
    - Nieuwe bedreigingen of kwetsbaarheden
    - Veranderingen in bedrijfsprocessen of IT-systemen
    - Wijzigingen in de regelgeving
- Er zou een proces voor veranderingsmanagement kunnen worden opgezet dat het bijwerken van cyberbeveiligingsdocumentatie omvat.
- Er zouden regelmatig evaluaties kunnen worden uitgevoerd (bijvoorbeeld elk kwartaal of twee keer per jaar) van gedocumenteerde risico's.
- Te overwegen tool:
  - Veranderingsmanagementsystemen
  - Tools voor continue monitoring
  - Risicobeoordelingskalenders

Deze controle maakt GV.RM-03.1 operationeel door cyberbeveiligingsrisico's te integreren in het Enterprise Risk Management (ERM)-raamwerk en governance en verantwoording te waarborgen.

GV.RM-04 Er wordt een strategische koers vastgesteld en gecommuniceerd waarin passende opties voor risicorespons worden beschreven

GV.RM-04.1 **Er moet een formeel globaal plan of een duidelijke visie worden opgesteld en gecommuniceerd aan alle betrokkenen over hoe risico's moeten worden beheerd, met inbegrip van de verschillende strategieën die de organisatie kan toepassen om geïdentificeerde risico's aan te pakken, rekening houdend met de mate van risicobereidheid of risicotolerantie.**

Implementatierichtlijnen

Het doel van deze controle is het leggen van de strategische basis voor risicobeheer, met inbegrip van:
- Risicotolerantie en risicobereidheid,
- Strategische richting voor het beheer van risico's (bijv. beperken, overdragen, accepteren),

- Zorgen voor afstemming tussen afdelingen.
- Ervoor zorgen dat iedereen in de organisatie begrijpt hoe risico's worden benaderd en beheerd

De controle richt zich op:
- Strategisch en organisatorisch risicobeheer.
- Het opstellen van een formele, overkoepelende visie of plan.
- Communiceren van risicobeheerstrategieën (bijv. vermijden, beperken, overdragen, accepteren).
- Dit geldt voor alle soorten risico's, niet alleen voor cyberbeveiliging.

In relatie tot de controles GV.RM-03.1, GV.RM-03.2 en GV.RM-05.1 is deze controle het uitgangspunt; deze definieert de risicobeleidsfilosofie van de organisatie, inclusief risicobereidheid en risicotolerantie, die als leidraad dient voor alle andere activiteiten.

GV.RM-05 Er worden communicatielijnen binnen de organisatie opgezet voor cyberbeveiligingsrisico's, inclusief risico's van leveranciers en andere derde partijen.

GV.RM-05.1 **Om de overkoepelende visie op risicobeheer te ondersteunen, moet de organisatie zorgen voor duidelijke afspraken over hoe informatie over cyberrisico's wordt gedeeld, ook wanneer die risico's afkomstig zijn van leveranciers of andere externe partijen.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat informatie over cyberbeveiligings- en informatiebeveiligingsrisico's effectief wordt gedeeld binnen de organisatie en met externe partijen.

Deze controle richt zich op operationele en tactische communicatie die specifiek is voor cyberbeveiligingsrisico's en benadrukt communicatiekanalen (bijv. rapportage, escalatie, coördinatie), inclusief externe risico's van leveranciers en derde partijen.

Bij de implementatie van deze controle, kan rekening gehouden worden met de volgende elementen:
- Communicatierollen en -verantwoordelijkheden definiëren
  Er zouden duidelijke verantwoordelijkheden kunnen worden toegewezen voor het rapporteren, escaleren en reageren op cyberbeveiligingsrisico's binnen afdelingen en met derde partijen.
- Communicatiekanalen opzetten
  Er zouden gestructureerde kanalen kunnen worden gebruikt zoals e-mailgroepen, ticketsystemen, incidentresponsplatforms of samenwerkingstools (bijv. Teams, Slack) voor tijdige risicocommunicatie.
- Derde partijen betrekken
  Leveranciers en partners zouden kunnen worden betrokken bij het communicatieproces door middel van contractuele bepalingen, gedeelde rapportageprotocollen of gezamenlijke incidentresponsplannen.
- Documenteren en opleiden
  Er zou een communicatieprotocol of draaiboek kunnen worden bijgehouden en relevante medewerkers zouden kunnen worden opgeleid.
- Evalueren en verbeteren
  De effectiviteit van de communicatie zou periodiek kunnen worden getest en geëvalueerd door middel van tabletop-oefeningen of evaluaties na incidenten.

Deze controle ondersteunt de implementatie van GV.RM-03.2 door ervoor te zorgen dat geïdentificeerde en gedocumenteerde risico's worden gecommuniceerd aan de juiste belanghebbenden, waardoor tijdige respons en coördinatie mogelijk wordt.

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

GV.RR-02 Rollen, verantwoordelijkheden en bevoegdheden met betrekking tot cyberbeveiligingsrisicobeheer worden vastgesteld, gecommuniceerd, begrepen en gehandhaafd.

GV.RR-02.1 De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging voor medewerkers, leveranciers, klanten en partners moeten worden vastgelegd, regelmatig beoordeeld en goedgekeurd, actueel gehouden, duidelijk gecommuniceerd en zowel intern als extern afgestemd.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat alle interne en externe partijen hun rollen, verantwoordelijkheden en bevoegdheden op het gebied van cyberbeveiliging begrijpen en nakomen, waardoor hiaten, overlappingen en vertragingen bij incidentrespons en naleving ('compliance') worden verminderd.

Om dit doel te bereiken kan het volgende worden overwogen:

- De rollen, verantwoordelijkheden en bevoegdheden op het gebied van beveiliging zouden kunnen worden beschreven: wie binnen de organisatie zou kunnen worden geraadpleegd, geïnformeerd, verantwoordelijk gehouden en aansprakelijk gesteld voor alle of een deel van de bedrijfsmiddelen. Het gebruik van het RACI-model zou kunnen worden overwogen. Richtlijnen zijn ook te vinden in de ENISA European Cybersecurity Skills Framework Role Profiles (https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles)
- Risicobeheerrollen, verantwoordelijkheden en bevoegdheden zouden kunnen worden opgenomen.
- Verantwoordelijkheden en prestatie-eisen op het gebied van informatie/cyberbeveiliging zouden kunnen worden opgenomen in personeelsbeschrijvingen.
- Er zou duidelijk kunnen worden aangegeven wat de verantwoordelijkheden op het gebied van informatie/cyberbeveiliging zijn binnen de bedrijfsvoering, risicofuncties en interne auditfuncties.
- Een of meer specifieke rollen of functies zouden kunnen worden geïdentificeerd die verantwoordelijk en aansprakelijk zijn voor het plannen, toewijzen van middelen en uitvoeren van activiteiten op het gebied van informatie-/cyberbeveiligingsrisicobeheer in de toeleveringsketen.
- Interne beveiligingsfuncties, verantwoordelijkheden en bevoegdheden zouden kunnen worden uitgebreid naar de functies, verantwoordelijkheden en bevoegdheden op het gebied van informatie-/cyberbeveiliging in de toeleveringsketen.
- Rollen, verantwoordelijkheden en bevoegdheden voor leveranciers, klanten en zakenpartners zouden kunnen worden ontwikkeld om gezamenlijke verantwoordelijkheden voor toepasselijke informatie-/cyberbeveiligingsrisico's aan te pakken, en deze zouden kunnen worden geïntegreerd in het beleid van de organisatie en toepasselijke overeenkomsten met derden.
- De rollen en verantwoordelijkheden van derden op het gebied van informatie-/cyberbeveiligingsrisicobeheer in de toeleveringsketen zouden intern kunnen worden gecommuniceerd.

- Regels en protocollen voor het delen van informatie en rapportageprocessen tussen de organisatie en haar leveranciers zouden kunnen worden opgesteld.
- Overweeg een duidelijk onderscheid tussen IT (informatietechnologie) en OT (operationele technologie) bij de implementatie van deze controle, waarbij rekening wordt gehouden met het volgende:
  - Rollen en verantwoordelijkheden
    - IT: definieer rollen zoals systeembeheerder, netwerkbeveiligingsanalist, incidentresponder.
    - OT: definieer rollen zoals controlesysteemingenieur, OT-cybersecurityverantwoordelijke, fabrieksoperator.
  - Documentatie en beoordeling
    - Zorg ervoor dat zowel IT- als OT-rollen afzonderlijk worden gedocumenteerd, maar op elkaar zijn afgestemd.
    - Beoordelingscycli kunnen verschillen: IT (per kwartaal/jaarlijks), OT (afgestemd op onderhoudsperiodes).
  - Autorisatie en updates
    - Zorg ervoor dat zowel IT- als OT-documentatie is goedgekeurd door de relevante leidinggevenden (bijv. de CIO voor IT, de Plant Manager voor OT).
    - Updates in OT kunnen vanwege veiligheidsimplicaties wijzigingscontroleprocedures vereisen.
  - Communicatie en coördinatie
    - Intern: zorg ervoor dat IT- en OT-teams gezamenlijke incidentresponsplannen hebben.
    - Extern: betrek leveranciers en partners die specifiek zijn voor OT (bijv. ICS-leveranciers) en IT (bijv. cloud-providers).

GV.RR-03 Er worden voldoende middelen toegewezen in overeenstemming met de cyberbeveiligingsrisicostrategie, rollen, verantwoordelijkheden en beleidslijnen

GV.RR-03.1 Er moeten voldoende middelen worden toegewezen in overeenstemming met de cyberbeveiligingsrisicostrategie, rollen, verantwoordelijkheden en beleid.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat cyberbeveiliging effectief wordt ondersteund door de toewijzing van middelen (kan personeel, budget, technologie omvatten) af te stemmen op strategische prioriteiten, rollen en beleid.

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

- Er zouden periodieke managementbeoordelingen kunnen worden uitgevoerd om ervoor te zorgen dat degenen die verantwoordelijk zijn voor het beheer van cyberbeveiligingsrisico's over de nodige bevoegdheden beschikken.
- De toewijzing van middelen en investeringen zou kunnen worden bepaald in overeenstemming met de risicobereidheid van de organisatie.
- Er zou kunnen worden gezorgd voor voldoende en adequate mensen, processen en technische middelen om de cyberbeveiligingsstrategie te ondersteunen.
- Deskundig personeel zou kunnen beschikken over de specialistische kennis en vaardigheden die nodig zijn voor OT-beveiliging, zodat ze kunnen samenwerken met OT-technici. Zo worden waarschuwingen nauwkeurig geïnterpreteerd en wordt er effectief gereageerd op bedreigingen.

GV.RR-03.2 **De organisatie moet rollen en verantwoordelijkheden toewijzen voor het regelmatig herzien en bijwerken van respons- en herstelplannen, zodat deze blijven aansluiten bij veranderingen in het risicolandschap en effectief blijven functioneren.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat respons- en herstelplannen effectief blijven door rollen en verantwoordelijkheden toe te wijzen voor de regelmatige herziening en aanpassing ervan aan veranderende risico's.

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

- **Verantwoordelijkheden definiëren en toewijzen**
  - Wijs duidelijke rollen toe voor het onderhouden, beoordelen en bijwerken van respons- en herstelplannen.
  - Zorg ervoor dat de verantwoordelijke personen de bevoegdheid en middelen hebben om op geïdentificeerde veranderingen te reageren.
  - Wijs een centrale coördinator of team aan om toezicht te houden op het updateproces en de verantwoordingsplicht te waarborgen.
- **De organisatorische context begrijpen en monitoren**
  Beoordeel regelmatig interne en externe factoren, zoals:
  - Organisatiestructuur en kritieke systemen
  - Opkomende bedreigingen en kwetsbaarheden
  - Veranderingen in regelgeving en marktdynamiek
  - Lessen die zijn geleerd uit incidenten, tests of oefeningen
- **Plannen bijwerken op basis van contextuele veranderingen**
  - Herzie plannen om rekening te houden met:
    - Nieuwe of zich ontwikkelende bedreigingen
    - Veranderingen in technologie of infrastructuur
    - Operationele uitdagingen of hiaten die tijdens het testen zijn vastgesteld
  - Updates kunnen betrekking hebben op contactlijsten, communicatieprotocollen, escalatieprocedures en toewijzing van middelen.
- **Communiceren en opleidingen**
  - Zorg ervoor dat alle relevante belanghebbenden op de hoogte zijn van updates.
  - Geef opleiding of briefings om de rollen en verantwoordelijkheden in de herziene plannen te verduidelijken.
- **Testen en verbeteren**
  - Voer regelmatig oefeningen en simulaties uit om de effectiviteit van bijgewerkte plannen te valideren.
  - Gebruik de resultaten om hiaten te identificeren en continue verbetering te stimuleren.
- **Continue evaluatiecyclus**
  - Stel een evaluatieschema op (bijvoorbeeld per kwartaal of na grote veranderingen).
  - Integreer planupdates in bredere risicobeheer- en governanceprocessen.

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.

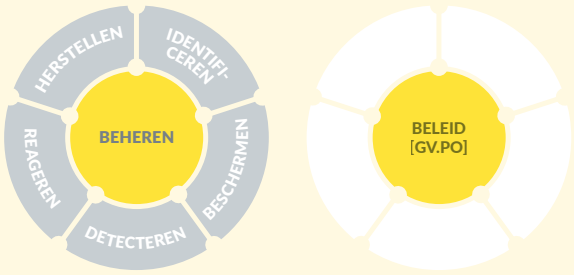
GV.RR-04.2 Er moet een cyberbeveiligingsproces voor human resources worden ontwikkeld en onderhouden dat van toepassing is bij werving, tijdens het dienstverband en bij beëindiging van het dienstverband.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat cyberbeveiligingsrisico's gedurende de hele levenscyclus van de werknemer worden beheerd door beveiliging te integreren in HR-processen, van aanwerving tot beëindiging van het dienstverband.

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

- Overwegingen met betrekking tot cyberbeveiligingsrisicobeheer moeten worden geïntegreerd in human resources-processen (bijv. personeelsscreening, onboarding, kennisgeving van wijzigingen, offboarding).
- Het cyberbeveiligingsproces voor human resources moet toegang tot kritieke informatie of technologie omvatten, evenals achtergrondcontroles, een gedragscode, rollen, bevoegdheden en verantwoordelijkheden.
- De verplichtingen voor personeel om op de hoogte te zijn van en zich te houden aan het beveiligingsbeleid dat relevant is voor hun rol, moeten duidelijk worden gedefinieerd en worden gehandhaafd.



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:

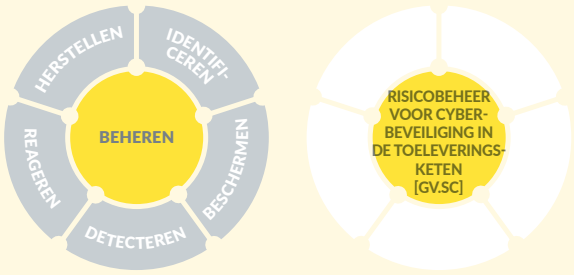
- Duidelijke en praktische beleidsregels, processen en procedures ontwikkelen die:
  - Aanvaardbaar gedrag en verwachtingen definiëren voor de bescherming van de informatie en systemen van de organisatie.
  - Beschrijven hoe het management verwacht dat werknemers de bedrijfsmiddelen gebruiken en beschermen.
- 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.

GV.PO-01.2 **Organisatiebrede beleidsregels en procedures op het gebied van informatie- en cyberbeveiliging moeten het gebruik van cryptografie en, indien van toepassing, encryptie omvatten, rekening houden met veranderingen in vereisten, bedreigingen, technologie en organisatorische rollen, en worden goedgekeurd door het senior management, dat toezicht houdt op de implementatie ervan.**

Deze controle bouwt voort op GV.PO-01.1 en richt zich op de inhoud en het toezicht op het cyber- en informatiebeveiligingsbeleid zelf. Het zorgt ervoor dat specifieke technische onderwerpen (zoals cryptografie en encryptie) aan bod komen, dat het beleid inspeelt op veranderingen en dat het senior management actief betrokken is bij de goedkeuring en het toezicht.

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

- **Omvang en doelstellingen definiëren**
  Zorg ervoor dat het beleid binnen de hele organisatie wordt toegepast en aansluit bij de zakelijke en risicoprioriteiten.
- **Cryptografie en encryptie opnemen**
  - Behandel encryptie in rust/tijdens transport, sleutelbeheer en goedgekeurde algoritmen.
  - Geef aan waar encryptie vereist is (bijvoorbeeld persoonlijke gegevens, externe toegang).
- **Het beleid actueel houden**
  Werk het beleid bij om veranderingen weer te geven in:
  - Wettelijke/regelgevende vereisten
  - Bedreigingslandschap
  - Technologie
  - Organisatiestructuur
- **Toezicht door het senior management**
  - Formele goedkeuring door het senior management vereist.
  - Wijs een beleidsverantwoordelijke (bijv. CISO) aan om toezicht te houden op de implementatie en naleving.
- **Rollen en verantwoordelijkheden toewijzen**
  - Gebruik ENISA ECSF-rolprofielen https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles) om:
    - Cybersecurityrollen te definiëren (bijv. beleidsmedewerker, risicomanager)
    - Taken, vaardigheden en competenties op elkaar af te stemmen
- **Communiceren en opleiden**
  Verspreid beleid en bied rolspecifieke opleiding.
- **Bewaken en handhaven**
  Gebruik technische controles en audits om naleving te garanderen.



Processen voor cyberrisicobeheer in de toeleverings-keten worden geïdentificeerd, vastgesteld, beheerd, gecontroleerd en verbeterd door belanghebbenden binnen de organisatie

GV.SC-02 Cybersecurityrollen en -verantwoordelijkheden voor leveranciers, klanten en partners worden intern en extern vastgesteld, gecommuniceerd en gecoördineerd.

GV.SC-02.1 Externe dienstverleners moeten de organisatie informeren over elke overdracht, beëindiging of overgang van personeel dat fysieke of digitale toegang heeft tot bedrijfskritieke onderdelen van de systemen.

Implementatierichtlijnen

Het doel van deze controle is om de continuïteit en veiligheid van kritieke systemen te waarborgen door externe leveranciers te verplichten personeelswijzigingen die van invloed zijn op de toegang te melden.

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

- Externe leveranciers zijn bijvoorbeeld dienstverleners, aannemers en andere organisaties die systeemontwikkeling, technologische diensten, uitbestede applicaties of netwerk- en beveiligingsbeheer leveren.
- Regels en protocollen voor het delen van informatie tussen de organisatie en haar leveranciers en subleveranciers zouden kunnen worden vastgelegd in contractuele overeenkomsten.

GV.SC-05 Er worden vereisten vastgesteld om cyberbeveiligingsrisico's in toeleveringsketens aan te pakken, deze worden geprioriteerd en geïntegreerd in contracten en andere soorten overeenkomsten met leveranciers en andere relevante derde partijen

GV.SC-05.1 Er moeten duidelijke eisen worden vastgesteld voor het aanpakken van cyberbeveiligingsrisico's en het delen van gevoelige informatie in de toeleveringsketen. Deze eisen moeten worden geprioriteerd, geïntegreerd in contracten en andere soorten formele overeenkomsten, en gehandhaafd.

Implementatierichtlijnen

Het doel van deze maatregel is om vereisten voor cyberbeveiliging en de omgang met gevoelige gegevens vast te stellen en te handhaven in overeenkomsten met de toeleveringsketen, door deze te integreren in contracten en te prioriteren op basis van risico.

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

- Contractuele overeenkomsten en andere soorten formele overeenkomsten met leveranciers en andere relevante derde partijen zouden verwachtingen, verantwoordelijkheden en beveiligingsvereisten kunnen definiëren.
- Belangrijke elementen van deze overeenkomsten zouden onder meer kunnen zijn: het delen van informatie tussen de organisatie en haar leveranciers en subleveranciers, beveiligingsmaatregelen, incidentrespons en de vereiste naleving van normen en voorschriften.
- Er zouden beveiligingsvereisten kunnen worden vastgesteld voor leveranciers, producten en diensten die in verhouding staan tot de kriticiteit en de mogelijke gevolgen als deze worden geschonden.
- Alle cyberbeveiligings- en toeleveringsketenvereisten waaraan derden zouden moeten voldoen, zouden kunnen worden opgenomen in standaardcontractuele bepalingen (d.w.z. vooraf opgestelde, veelgebruikte termen en clausules die consistentie, naleving en duidelijkheid garanderen). In het contract zou ook kunnen worden gespecificeerd hoe de naleving van deze vereisten zal worden gecontroleerd.
- Er zou kunnen worden overwogen om in de handhaving op te nemen dat externe leveranciers en gebruikers (bijv. leveranciers, klanten, partners) zouden kunnen aantonen dat ze hun rollen en verantwoordelijkheden begrijpen.
- Er zou kunnen worden overwogen om beveiligingsvereisten te definiëren in Service Level Agreements (SLA's) voor het monitoren van leveranciers op acceptabele beveiligingsprestaties gedurende de hele levenscyclus van de leveranciersrelatie.
- Er zou kunnen worden overwogen om leveranciers contractueel te verplichten hun werknemers te screenen en zich te wapenen tegen bedreigingen van binnenuit.
- Er zou kunnen worden overwogen om leveranciers contractueel te verplichten om bewijs te leveren van het uitvoeren van aanvaardbare beveiligingspraktijken door middel van bijvoorbeeld zelfevaluatie (bijv. CyFun®), naleving van bekende normen, verificaties (bijv. CyFun®), certificeringen (bijv. CyFun®) of inspecties.
- Houd er rekening mee dat aan de GDPR-vereisten moet worden voldaan wanneer bedrijfsinformatie persoonsgegevens bevat (dit geldt op alle niveaus). Dit betekent dat er onder meer passende waarborgen in het contractuele kader moeten worden opgenomen.

GV.SC-07 De risico's die een leverancier, zijn producten en diensten en andere derde partijen met zich meebrengen, worden begrepen, vastgelegd, geprioriteerd, beoordeeld, aangepakt en gemonitord gedurende de hele relatie

GV.SC-07.1 **De risico's die een leverancier, zijn producten en diensten en andere derde partijen met zich meebrengen, moeten worden geïdentificeerd, gedocumenteerd, geprioriteerd, beperkt en minstens jaarlijks beoordeeld, en ook bij wijzigingen tijdens de samenwerking.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat risico's met betrekking tot leveranciers, hun producten en diensten en andere derde partijen gedurende de hele relatie continu worden geïdentificeerd, beoordeeld, geprioriteerd en beheerd, vooral wanneer er veranderingen optreden in kritieke systemen.

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

- **Risicobeoordelingen op maat**
  De beoordelingsformats en -frequenties zouden kunnen worden aangepast op basis van de reputatie van de leverancier en de kriticiteit van de geleverde producten of diensten, met inbegrip van OT-componenten.
- **Bredere risico-overwegingen**
  Risicobeoordelingen zouden rekening kunnen houden met mogelijke dienstonderbrekingen en concentratierisico's die van invloed kunnen zijn op de bedrijfsvoering of OT-omgevingen.

- **Bewijs van naleving**
  Leveranciers zouden bewijs kunnen leveren van naleving van contractuele cyberbeveiligings (e.g. CyFun®), certificeringen, garanties, testresultaten, labels of auditrapporten van derden.
- **Voortdurende monitoring**
  Kritieke leveranciers zouden gedurende de hele relatie kunnen worden gecontroleerd door middel van inspecties, audits, tests of andere evaluatiemethoden om ervoor te zorgen dat aan de beveiligingsverplichtingen wordt voldaan.
- **Updates van risicoprofielen**
  Veranderingen in de diensten, producten of prestaties van leveranciers zouden aanleiding kunnen geven tot een herbeoordeling van hun risicoprofiel en kriticiteit, vooral wanneer OT-systemen betrokken zijn.
- **Bedrijfscontinuïteitsplanning**
  Er zou een actieplan kunnen zijn om onverwachte verstoringen bij leveranciers op te vangen en de bedrijfscontinuïteit te waarborgen.

GV.SC-08 Relevante leveranciers en andere derde partijen worden betrokken bij incidentplanning, respons en herstelactiviteiten

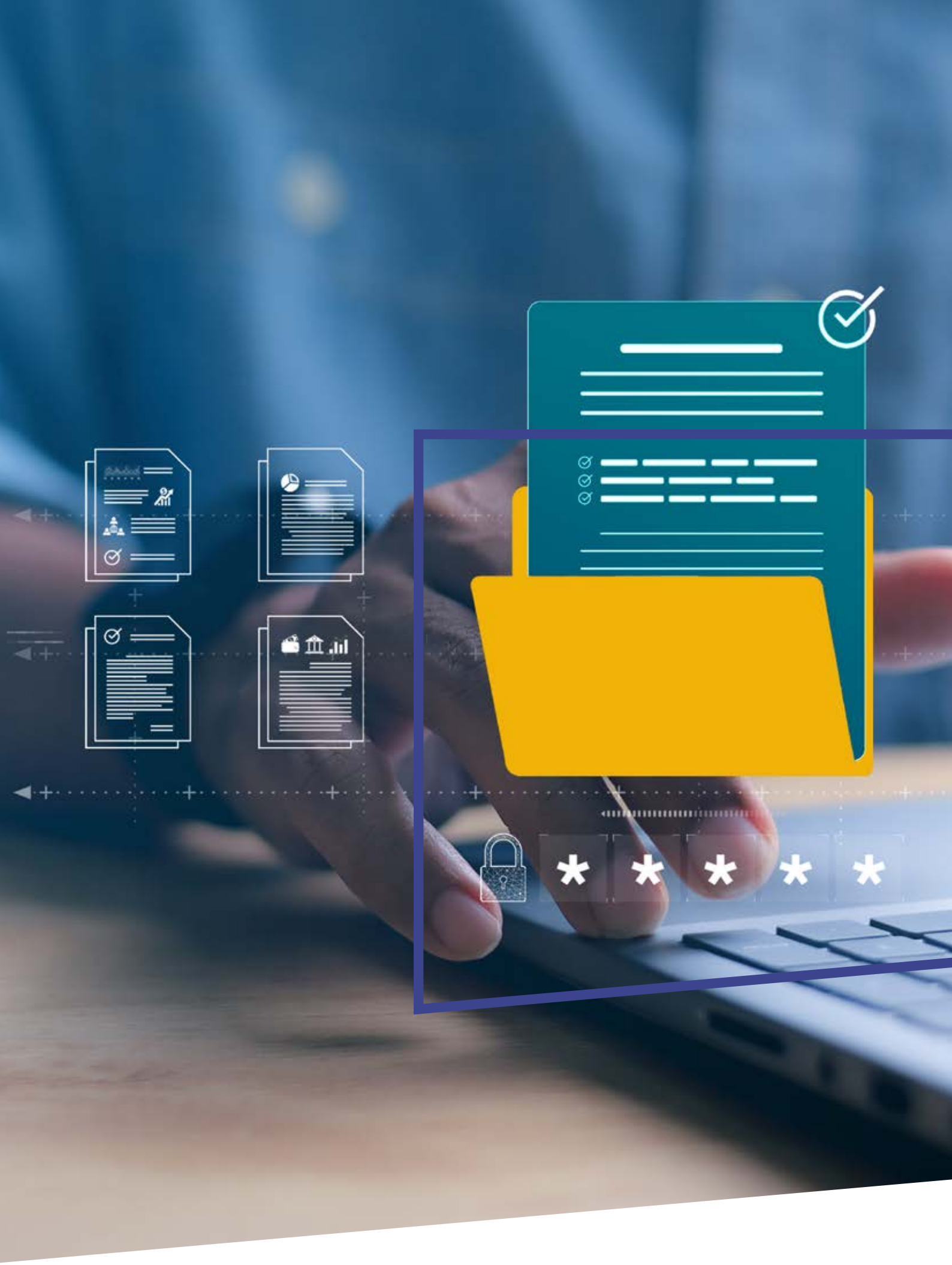
GV.SC-08.1 De organisatie moet sleutelpersonen van relevante leveranciers en andere derde partijen identificeren en documenteren om hen te betrekken bij incidentplanning, respons en herstelactiviteiten.

Implementatierichtlijnen

Het doel van deze maatregel is het versterken van de paraatheid en het herstel bij incidenten door ervoor te zorgen dat sleutelpersonen van kritieke leveranciers en derde partijen worden geïdentificeerd en actief worden betrokken bij de planning en uitvoering van de aanpak van incidenten.

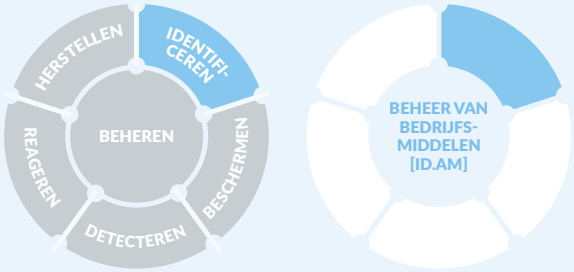
Om dit doel te bereiken, kan het volgende worden overwogen:

- **Communicatieprotocollen opstellen**
  Er zouden duidelijke regels en procedures kunnen worden vastgesteld voor het rapporteren van de status van incidenten en het coördineren van respons- en herstelactiviteiten tussen de organisatie en haar bedrijfskritieke leveranciers.
- **Rollen en verantwoordelijkheden definiëren**
  De rollen, verantwoordelijkheden en bevoegdheden voor incidentrespons zouden kunnen worden gedocumenteerd voor zowel interne teams als externe deelnemers, inclusief degenen die OT-systemen en -infrastructuur ondersteunen.
- **Gezamenlijk leren bevorderen**
  Na grote incidenten zouden er gezamenlijke sessies kunnen worden gehouden met kritieke leveranciers en derde partijen om lessen te trekken en de toekomstige coördinatie en veerkracht te verbeteren.



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-01.2 De inventaris van bedrijfsassets die verband houden met informatie en informatieverwerkingsfaciliteiten moet wijzigingen in de context van de organisatie weerspiegelen en alle informatie bevatten die nodig is voor een effectieve verantwoording.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de inventaris van bedrijfsmiddelen de operationele transparantie ondersteunt, verantwoordelijk eigendom mogelijk maakt en zich aanpast aan veranderingen in de structuur, technologie en risicolandscape van de organisatie.

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

- **Neem essentiële details van assets op**
  Inventarissen zouden belangrijke specificaties kunnen bevatten, zoals fabrikant, apparaattype, model, serienummer, machinenaam, netwerkadres en fysieke locatie. OT-assets kunnen worden opgenomen waar dit van toepassing is.
- **Ondersteun verantwoording**
  Registraties van assets zouden traceerbaarheid van acties en beslissingen mogelijk kunnen maken, zodat verantwoordelijke partijen kunnen worden geïdentificeerd en ter verantwoording kunnen worden geroepen voor de resultaten.
- **Weerspiegel organisatorische wijzigingen**
  Inventarissen zouden tijdig kunnen worden bijgewerkt om wijzigingen binnen de organisatie accuraat weer te geven.

ID.AM-01.3 Wanneer ongeautoriseerde hardware wordt gedetecteerd, moet deze in quarantaine worden geplaatst voor mogelijke uitzonderingsafhandeling, worden verwijderd of vervangen, en moet de inventaris dienovereenkomstig worden bijgewerkt.

Implementatierichtlijnen

Het doel van deze controle is het verminderen van veiligheidsrisico's door ervoor te zorgen dat ongeautoriseerde hardware onmiddellijk wordt geïdentificeerd, geïsoleerd en aangepakt, terwijl een nauwkeurige en verantwoordelijke inventaris van assets wordt bijgehouden.

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

- **Ongeautoriseerde hardware definiëren**
  Alle hardware die niet is goedgekeurd of waarvoor geen gedocumenteerde uitzonderingen gelden, zou kunnen worden aangemerkt als ongeautoriseerd.
- **Reageren op detectie**
  Ongeautoriseerde hardware zou in quarantaine geplaatst kunnen worden voor beoordeling, worden verwijderd of vervangen, al naargelang het geval. De inventaris van bedrijfsmiddelen zou dienovereenkomstig bijgewerkt kunnen worden.
- **Rekening houden met OT-overwegingen**
  Ongeautoriseerde apparaten in OT-omgevingen zouden met extra voorzichtigheid kunnen worden behandeld vanwege mogelijke gevolgen voor de veiligheid en de bedrijfsvoering.

Voorbeelden van ongeautoriseerde hardware zijn onder meer:

- **Niet-goedgekeurde eindpunten**: persoonlijke of niet-geregistreerde laptops, desktops of mobiele apparaten die zonder toestemming op het netwerk zijn aangesloten.
- **Externe opslagapparaten**: USB-sticks of externe harde schijven die niet zijn goedgekeurd voor gebruik en die risico's op malware of gegevenslekken met zich mee kunnen brengen.
- **Niet-gecontroleerde IoT- en OT-apparaten**: slimme apparaten, sensoren of industriële componenten die zonder de juiste controle zijn aangesloten en risico's vormen voor zowel IT- als OT-omgevingen.
- **Ongeautoriseerde netwerkapparatuur**: draadloze toegangspunten of switches die zonder goedkeuring zijn geïnstalleerd en mogelijk de netwerkbeveiligingscontroles omzeilen.

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-02.2 **De inventaris die weergeeft welke software, diensten en systemen in de organisatie worden gebruikt, moet wijzigingen in de context van de organisatie weerspiegelen en alle informatie bevatten die nodig is voor effectieve verantwoording.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat inventarissen van software, diensten en systemen actueel en volledig blijven, zodat traceerbaarheid, verantwoordelijk eigendom en afstemming op veranderingen in de operationele en risicocontext van de organisatie mogelijk zijn.

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

- **Neem essentiële details van assets op**
  Inventarissen zouden relevante kenmerken kunnen bevatten, zoals de titel van de software, de uitgever, de datum van de eerste installatie of het eerste gebruik, het zakelijke doel, de versie, de implementatiemethode en de datum van buitengebruikstelling. URL's of app store-bronnen zouden kunnen worden opgenomen indien van toepassing.
- **Ondersteun verantwoording**
  Inventarisgegevens zouden de traceerbaarheid van acties en beslissingen kunnen mogelijk maken, zodat verantwoordelijke rollen kunnen worden geïdentificeerd en aanspreekbaar (verantwoordingsplicht) kunnen worden gesteld voor het gebruik en beheer van software en diensten.
- **Weerspiegel organisatorische wijzigingen**
  Inventarissen zouden kunnen worden bijgewerkt om wijzigingen weer te geven, zoals nieuwe implementaties, upgrades of verwijderingen, inclusief die welke van invloed zijn op OT-systemen en ingebouwde software-componenten.

ID.AM-02.3 **De personen die verantwoordelijk en aanspreekbaar zijn voor het beheer van softwareplatforms en -applicaties binnen de organisatie moeten formeel worden geïdentificeerd.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat softwareplatforms en -applicaties goed worden beheerd, door duidelijk aan te geven wie verantwoordelijk is voor de dagelijkse werkzaamheden en wie eindverantwoordelijk (aanspreekbaar – verantwoordingsplicht) is voor het algemene toezicht en de resultaten.

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

- **Rollen duidelijk definiëren**
  De personen die verantwoordelijk zijn voor het beheer van software zouden formeel kunnen aangewezen worden. Dit zijn de personen die het werk uitvoeren, technische beslissingen nemen en operationele taken uitvoeren (bijv. ontwikkelaars, systeembeheerders, testers).
- **Aanspreekbaarheid toewijzen**
  Er zou formeel een aparte rol kunnen worden toegewezen om toezicht te houden op en goedkeuring te verlenen voor de succesvolle voltooiing van software gerelateerde taken. Dit kunnen projectmanagers, product-eigenaren of teamleiders zijn.
- **Toepassen op alle omgevingen**
  Deze rollen zouden kunnen worden gedefinieerd voor zowel IT- als OT-omgevingen, zodat ook de software die in industriële systemen wordt gebruikt, goed kan worden beheerd.

ID.AM-02.4	**Wanneer ongeautoriseerde software wordt gedetecteerd, moet deze in quarantaine worden geplaatst voor mogelijke uitzonderingsafhandeling, worden verwijderd of vervangen, en moet de inventaris dienovereenkomstig worden bijgewerkt.**

Implementatierichtlijnen

Het doel van deze controle is om beveiligings-, operationele en compliance-risico's te minimaliseren door ervoor te zorgen dat ongeautoriseerde software snel wordt geïdentificeerd, op de juiste manier wordt behandeld en correct wordt opgenomen in de software-inventaris van de organisatie.

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

- **Definieer ongeautoriseerde software**
  Software die is geïnstalleerd of wordt gebruikt zonder de juiste licentie, goedkeuring of gedocumenteerde uitzonderingen zou kunnen worden geclassificeerd als ongeautoriseerd.
- **Begrijp de risico's**
  Ongeautoriseerde software kan leiden tot:
  - **Beveiligingskwetsbaarheden** (bijv. malware of achterdeuren)
  - **Risico's voor gegevensbescherming** (bijv. niet-goedgekeurde gegevensverwerking)
  - **Operationele inefficiënties** (bijv. compatibiliteitsproblemen)
  - **Verlies van controle** over softwaregebruik en updates
- **Stel procedures op voor het reageren op incidenten**
  Ongeautoriseerde software zou in quarantaine kunnen worden geplaatst voor mogelijke uitzonderings-afhandeling, worden verwijderd of vervangen. De software-inventaris zou dienovereenkomstig kunnen worden bijgewerkt.
- **Ondersteun met gecentraliseerd beheer**
  Er zou een gecentraliseerd softwarebeheerproces kunnen worden opgezet om toezicht te houden op de selectie van leveranciers, verouderde software en beveiligingsmaatregelen.
- **Gebruik SBOM's waar van toepassing**
  Software Bills of Materials (SBOM's) zouden kunnen worden gebruikt om alle onderdelen, bibliotheken en modules van software bij te houden. Dit helpt om te voldoen aan licentievereisten en om kwetsbaarheden beter te beheren, vooral in omgevingen met operationele technologie (OT) en ingebedde systemen.

ID.AM-03 Weergaven van de geautoriseerde netwerkcommunicatie en interne en externe netwerkgegevensstromen van de organisatie worden bijgehouden

ID.AM-03.2	**De netwerkcommunicatie en interne gegevensstromen van de organisatie moeten in kaart worden gebracht, gedocumenteerd, geautoriseerd en bijgewerkt wanneer er wijzigingen optreden.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat interne netwerkcommunicatie en gegevensstromen duidelijk worden begrepen, goed worden gedocumenteerd en up-to-date worden gehouden om veilige operaties en wel-overwogen besluitvorming in ICT- en OT-omgevingen te ondersteunen.

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

- **Netwerkreferentiepunten vaststellen**
  Communicatie en gegevensstromen via bekabelde, draadloze en cloudgebaseerde infrastructuur (bijv. IaaS) zouden in kaart kunnen worden gebracht, gedocumenteerd en geautoriseerd. Bij wijzigingen zouden updates uitgevoerd kunnen worden.
- **Technische details documenteren**
  Verwachte netwerkpoorten, protocollen en diensten die tussen geautoriseerde systemen worden gebruikt, zouden geregistreerd kunnen worden om monitoring en probleemoplossing te ondersteunen.
- **Integratie met configuratiebeheer**
  Configuratiebeheerprocessen zouden het onderhoud en de validatie van documentatie over netwerkstromen kunnen ondersteunen.
- **Zorgen voor veerkrachtige documentatie**
  Documentatie over netwerkstromen zou veilig kunnen worden opgeslagen en niet alleen op het netwerk dat het beschrijft. Er zou een beveiligde offline kopie (bijvoorbeeld een versleutelde externe schijf of papieren kopie) kunnen worden bewaard om de beschikbaarheid tijdens storingen of incidenten te garanderen.

ID.AM-04 Inventarissen van door leveranciers geleverde diensten worden bijgehouden

ID.AM-04.1 Organisaties moeten een duidelijke en actuele lijst bijhouden van alle externe diensten die ze gebruiken, inclusief hoe deze verbinding maken met hun systemen. Deze diensten moeten vóór gebruik worden beoordeeld en goedgekeurd, en de lijst moet worden bijgewerkt wanneer er wijzigingen plaatsvinden.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle externe diensten die door de organisatie worden gebruikt, duidelijk worden geïdentificeerd, beoordeeld en bijgewerkt om het risico van ongeoorloofde toegang, onbeheerde afhankelijkheden van derden of dienstonderbrekingen in ICT- en OT-omgevingen te verminderen.

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

- **Een inventaris van externe diensten bijhouden**
  Alle externe services waarop de organisatie vertrouwt, zouden kunnen worden geïdentificeerd en gedocumenteerd. Dit kan ook services omvatten die in zowel IT- als OT-omgevingen worden gebruikt. De inventaris zou kunnen worden bijgewerkt wanneer services worden toegevoegd, gewijzigd of verwijderd.
- **De verbindingen tussen diensten beschrijven en in kaart brengen**
  De manier waarop elke externe dienst verbinding maakt met interne systemen zou duidelijk beschreven en vastgelegd kunnen worden. Dit omvat tools voor externe toegang, cloudgebaseerde SCADA-platforms en door leveranciers beheerde OT-systemen.
- **Diensten goedkeuren en controleren voor gebruik**
  Externe diensten zouden kunnen worden gecontroleerd en goedgekeurd voordat ze worden gebruikt. Tijdens dit proces zou kunnen worden nagegaan of de dienst voldoet aan de interne beveiligings-, nalevings- en operationele vereisten.
- **Diensten categoriseren en classificeren**
  Externe diensten zouden kunnen worden gecategoriseerd op type (bijv. IaaS, SaaS, API's) en geclassificeerd op basis van hun kriticiteit en gegevensgevoeligheid. Dit kan helpen bij het prioriteren van toezicht en risicobeheer.
- **Integreren met risico- en veranderingsbeheer**
  De inventaris zou kunnen worden geïntegreerd in bredere risicobeheer- en veranderingsbeheerprocessen. Elke wijziging in externe diensten zou aanleiding kunnen geven tot een beoordeling van de bijbehorende risico's en vereiste controles.

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-07.2 **Inventarissen van gegevens en bijbehorende metagegevens moeten worden bijgehouden voor aangewezen datatypes.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat er overzichten worden bijgehouden van gegevens en hun kenmerken (metadata) voor alle datatypes die expliciet zijn geselecteerd of aangewezen door beleid of richtlijnen (bijvoorbeeld klantgegevens, financiële informatie of productiegegevens). Dit ondersteunt veilig gegevensbeheer, naleving van wet- en regelgeving en een betrouwbare werking (operationele integriteit) van ICT- en OT-omgevingen.

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

- **Een gegevensclassificatieschema definiëren**
  Er zou een classificatieschema kunnen worden opgesteld om gegevenstypen te categoriseren op basis van gevoeligheid en gebruik. Dit schema zou als leidraad dienen voor de manier waarop gegevens worden behandeld, beschermd en bewaard.
- **Beveiligingsmaatregelen toepassen op basis van classificatieniveau**
  Voor elk classificatieniveau zouden passende beveiligingsmaatregelen kunnen worden geïmplementeerd. Deze kunnen bestaan uit versleuteling, op rollen gebaseerde toegangscontroles en op maat gemaakte beleidsregels voor het bewaren van gegevens.
- **Gevoelige gegevenstypen identificeren en beschermen**
  Inventarissen zouden gevoelige gegevens kunnen bevatten, zoals:
  - Persoonlijk identificeerbare informatie (PII)
  - Financiële en gezondheidsinformatie
  - Vertrouwelijke bedrijfsgegevens
  - Intellectueel eigendom
  - Overheids- en personeelsdossiers
    OT-omgevingen zouden ook operationele gegevens kunnen bevatten die cruciaal zijn voor de veiligheid en betrouwbaarheid.
- **Metadata voor elke gegevensinstantie bijhouden**
  Metadata zouden bijgehouden kunnen worden om gegevensbeheer te ondersteunen. Dit omvat:
  - Beschrijvende metadata (bijv. titel, auteur, trefwoorden)
  - Structurele metadata (bijv. formaat, schema)
  - Administratieve metadata (bijv. toegangsrechten, bewaarbeleid)
  - Technische metadata (bijv. codering, checksum)
- **De herkomst en locatie van gegevens monitoren**
  De oorsprong, eigendom en geolocatie van elke gegevensinstantie zou gedocumenteerd kunnen worden. Dit helpt om te begrijpen waar en hoe gegevens worden opgeslagen en verwerkt, met name in gedistribueerde of OT-systemen.
- **Ad-hocgegevens continu ontdekken en analyseren**
  Er zouden processen kunnen zijn om nieuwe gevallen van gevoelige gegevens te identificeren die niet in de eerste inventarisaties zijn opgenomen. Dit helpt om hiaten in de gegevensstroom in kaart te brengen en ondersteunt de voortdurende gegevensbescherming.
- **Het gebruik van het Traffic Light Protocol (TLP) overwegen**
  TLP zou beschouwd kunnen worden als een methode om gegevens met betrekking tot cyberbeveiliging te classificeren en te delen, met name in de context van incidentrespons en dreigingsinformatie.

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.

ID.AM-08.3 De organisatie moet verantwoordingsplicht afdwingen voor al haar bedrijfskritische middelen gedurende de volledige levenscyclus van het systeem, inclusief verwijdering, overdracht en buitengebruikstelling.

Implementatierichtlijnen

Het doel van deze controle is om de verantwoordingsplicht voor alle bedrijfskritieke assets gedurende hun hele levenscyclus, inclusief implementatie, verplaatsing en verwijdering, te waarborgen om het risico van ongeoorloofde toegang, gegevenslekken of operationele verstoringen in ICT- en OT-omgevingen te verminderen.

Om dit doel te bereiken, zou het volgende in overweging kunnen worden genomen:

- **Assets beveiligen vóór implementatie**
  Systemen, hardware, software en diensten zouden correct kunnen worden geconfigureerd en beveiligd voordat ze in productieomgevingen worden geïntroduceerd.
- **Overtollige assets identificeren en verwijderen**
  Overbodige of ongebruikte systemen, software en diensten die het aanvalsoppervlak vergroten, zouden periodiek kunnen worden geïdentificeerd en verwijderd.
- **Bewegingen van assets monitoren en documenteren**
  Verplaatsingen van bedrijfskritieke assets zouden kunnen worden bijgehouden en er zou documentatie kunnen worden bijgehouden om traceerbaarheid en verantwoordingsplicht te waarborgen.
- **Overdrachten van assets autoriseren**
  Bedrijfskritieke assets zouden alleen met de juiste autorisatie faciliteiten kunnen binnenkomen of verlaten, vooral in OT-omgevingen waar fysieke controle van assets van cruciaal belang kan zijn.
- **Assets veilig buiten gebruik stellen**
  Het buiten gebruik stellen van bedrijfskritieke assets zou op een veilige, verantwoorde en controleerbare manier kunnen gebeuren om gegevenslekken of ongeoorloofd hergebruik te voorkomen.
- **Inventarissen tijdig bijwerken**
  De inventaris van assets zou kunnen worden bijgewerkt wanneer systemen, hardware, software of diensten worden verplaatst, overgedragen, verwijderd of buiten gebruik gesteld.

ID.AM-08.4 De organisatie moet ervoor zorgen dat de nodige maatregelen worden genomen om verlies, misbruik, beschadiging of diefstal van assets aan te pakken.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat er passende maatregelen zijn getroffen om verlies, misbruik, beschadiging of diefstal van assets te voorkomen en hierop te reageren, om de bedrijfsvoering te beschermen en de veiligheidsrisico's in ICT- en OT-omgevingen te verminderen.

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

- **Fysieke beveiligingsmaatregelen toepassen**
  Fysieke beveiligingen zoals sloten, bewakingscamera's en alarmen zouden kunnen worden gebruikt om faciliteiten en kritieke assets te beveiligen, ook in OT-omgevingen.
- **Technische beveiligingsmaatregelen implementeren**
  Technische controles zoals versleuteling, veilige gegevensverwijdering en regelmatige back-ups zouden kunnen worden toegepast om gegevens en systemen te beschermen tegen ongeoorloofde toegang of verlies.
- **Organisatorische controles instellen**
  Er zouden beleidsregels, procedures en gebruikersovereenkomsten kunnen worden opgesteld om verantwoordelijkheden en verwachtingen te definiëren. Mobile Device Management (MDM) en andere administratieve tools zouden kunnen worden gebruikt om het gebruik van assets te beheren.

- **Regelmatig audits en inventariscontroles uitvoeren**
  Er zouden periodieke audits en inventarisaties van bedrijfsmiddelen kunnen worden uitgevoerd om te controleren of alle bedrijfsmiddelen worden verantwoord en correct worden beheerd.
- **De toegang tot gevoelige assets beperken**
  De toegang tot kritieke systemen, gegevens en fysieke ruimtes zou kunnen worden beperkt tot bevoegd personeel, vooral in omgevingen waar operationele continuïteit essentieel kan zijn.
- **De medewerkers bewustmaken en opleiden**
  Medewerkers zouden kunnen worden opgeleid in het beschermen van assets en worden aangemoedigd om verdachte activiteiten of incidenten met betrekking tot misbruik of verlies van assets te melden.
- **Zorgen voor een passende verzekeringsdekking**
  Er zouden verzekeringen kunnen worden afgesloten om financiële verliezen als gevolg van diefstal, beschadiging of andere incidenten met assets te helpen beperken.

ID.AM-08.6 De organisatie moet preventief onderhoud en reparaties aan haar kritieke systeemcomponenten plannen, uitvoeren en documenteren volgens goedgekeurde processen en tools.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat preventief onderhoud en reparaties aan kritieke systeemcomponenten op een veilige en consistente manier worden gepland, uitgevoerd en gedocumenteerd om de betrouwbaarheid van het systeem te behouden en operationele risico's in ICT- en OT-omgevingen te verminderen.

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

- **Procedures voor documentonderhoud**
  Het onderhoudsbeleid en de onderhoudsprocedures zouden duidelijk kunnen worden omschreven en opgenomen in de cyberbeveiligings- en operationele plannen van de organisatie. Het toezicht op deze procedures zou deel kunnen uitmaken van de verantwoordelijkheden van het management.
- **Onderhoudspersoneel autoriseren**
  Er zou een proces kunnen worden opgezet om personen of externe leveranciers die onderhoud uitvoeren te autoriseren. Er zou een lijst van goedgekeurd personeel of organisaties kunnen worden bijgehouden en regelmatig worden herzien.
- **Onderhoudsactiviteiten plannen en registreren**
  Preventief onderhoud en reparaties zouden kunnen worden gepland, uitgevoerd en gedocumenteerd volgens de vereisten van de organisatie en de specificaties van de leverancier. De registraties zouden kunnen worden gecontroleerd om de volledigheid en nauwkeurigheid ervan te garanderen.
- **Alle onderhoudsactiviteiten controleren**
  Alle onderhoudswerkzaamheden, zowel ter plaatse als op afstand, zouden vooraf kunnen worden goedgekeurd en tijdens de uitvoering kunnen worden gecontroleerd. Dit kan ook het onderhoud van onderdelen omvatten die uit de faciliteit zijn verwijderd.
- **Zorgen voor veilig en betrouwbaar OT-onderhoud**
  Het onderhoud van OT-systemen moet worden gepland en uitgevoerd op een manier die de veiligheid van de bedrijfsvoering waarborgt, onnodige stilstand voorkomt en voldoet aan alle specifieke instructies of vereisten van leveranciers van apparatuur.

ID.AM-08.8 **De organisatie moet onderhoudstools voor gebruik op haar kritieke systemen vooraf goedkeuren, controleren en handhaven.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat onderhoudstools die op kritieke systemen worden gebruikt, vooraf worden goedgekeurd, gecontroleerd en afgedwongen om de integriteit, veiligheid en operationele continuïteit van het systeem te beschermen. In OT-omgevingen kan onjuist gebruik van tools fysieke processen verstoren, waardoor controle over de goedkeuring en het gebruik van tools essentieel is voor de operationele veiligheid en betrouwbaarheid.

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

- **Kritieke systemen identificeren**
  Systemen die van invloed zijn op de veiligheid, kwaliteit, naleving van regelgeving of operationele doorvoer zouden als kritiek kunnen worden geclassificeerd. Metrieken zoals Mean Time to Repair (MTTR) en Mean Time Between Failures (MTBF) zouden deze classificatie kunnen ondersteunen.
- **Onderhoudstools vooraf goedkeuren**
  Op kritieke systemen mogen alleen onderhoudstools worden gebruikt die vooraf zijn gecontroleerd en goedgekeurd. Dit kan zowel apparaten als programma's zijn, zoals diagnoseapparaten, netwerkcontroletools en laptops.
- **Het gebruik monitoren**
  Het gebruik van onderhoudstools op kritieke systemen zou actief kunnen worden gemonitord om ongeoorloofde of onveilige activiteiten op te sporen.
- **Controles afdwingen**
  Er zouden beleidsregels en technische controles kunnen worden ingesteld om het gebruik van niet-goedgekeurde tools te voorkomen en om naleving van interne procedures en toepasselijke wet- en regelgeving te waarborgen.

ID.AM-08.11 **Onderhouds- en diagnoseactiviteiten op afstand van bedrijfsmiddelen van de organisatie moeten vooraf worden goedgekeurd en de uitvoering ervan moet worden geregistreerd.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat onderhouds- en diagnoseactiviteiten op afstand geautoriseerd, traceerbaar en veilig zijn. In OT-omgevingen moet onderhoud op afstand streng worden gecontroleerd, aangezien ongeautoriseerde wijzigingen rechtstreeks van invloed kunnen zijn op de veiligheid en stabiliteit van fysieke systemen.

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

- **Activiteiten vooraf goedkeuren**
  Alle onderhouds- en diagnoseactiviteiten op afstand zouden vóór uitvoering kunnen worden beoordeeld en goedgekeurd.
- **Prestaties registreren**
  Elke sessie op afstand zou gedetailleerd kunnen worden geregistreerd, inclusief tijdstip, duur, betrokken personeel en ondernomen acties.
- **Logboekprocedures vaststellen**
  Logboek- en monitoringprocedures zouden kunnen worden gedocumenteerd, goedgekeurd, gecommuniceerd, toegepast en regelmatig worden beoordeeld, idealiter op jaarbasis.
- **Ongeautoriseerde wijzigingen voorkomen**
  Er zouden technische en procedurele maatregelen kunnen worden geïmplementeerd om ongeautoriseerde wijzigingen aan systemen, configuraties, applicaties of infrastructuur tijdens externe toegang te detecteren of te voorkomen.
- **Zorgen voor conformiteit en naleving**
  Alle activiteiten zouden in overeenstemming kunnen zijn met het interne beleid.

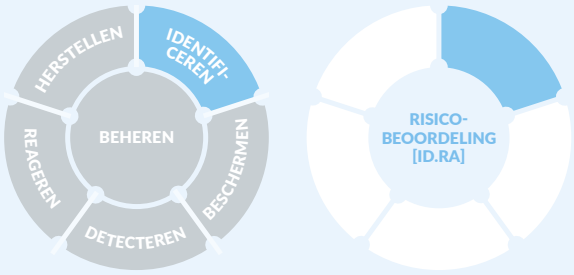
ID.AM-08.12	**Voor het opzetten van niet-lokale onderhouds- en diagnosesessies via externe netwerkverbindingen zijn sterke authenticatiemiddelen vereist en dergelijke verbindingen moeten worden beëindigd wanneer het niet-lokale onderhoud is voltooid.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat niet-lokale onderhouds- en diagnosesessies veilig worden opgezet en correct worden beëindigd om ongeoorloofde toegang of aanhoudende verbindingen te voorkomen. In OT-omgevingen zijn het veilig opzetten en beëindigen van sessies essentieel om te voorkomen dat er blijvende toegangspaden ontstaan die kunnen worden misbruikt om fysieke activiteiten te verstoren.

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

- **Sterke authenticatie gebruiken**
  Externe sessies zouden kunnen worden beveiligd met sterke authenticatiemiddelen die bestand zijn tegen replay-aanvallen. Waar mogelijk zou multifactorauthenticatie kunnen worden gebruikt.
- **Communicatie beveiligen**
  Er zouden cryptografische mechanismen kunnen worden geïmplementeerd om de vertrouwelijkheid en integriteit van communicatie voor onderhoud op afstand te waarborgen.
- **Sessies beëindigen**
  Externe verbindingen zouden onmiddellijk na voltooiing van het onderhoud kunnen worden beëindigd om de blootstelling aan potentiële bedreigingen te verminderen.
- **De verbreking van de verbinding verifiëren**
  Verificatie van verbreking van de verbinding op afstand zou kunnen worden gebruikt om te bevestigen dat sessies volledig zijn afgesloten en niet langer toegankelijk zijn.
- **Zorgen voor conformiteit en naleving**
  Alle activiteiten op afstand zouden kunnen voldoen aan interne beveiligingsprocedures en aan de toepasselijke wet- en regelgeving en industrienormen.



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-01.2 **Er moet een proces worden opgezet om de kwetsbaarheden van de bedrijfskritieke systemen van de organisatie continu te monitoren, te identificeren en te documenteren.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat kwetsbaarheden in bedrijfskritieke systemen continu worden geïdentificeerd, gemonitord en gedocumenteerd om tijdige risicobeperking te ondersteunen en de operationele veerkracht te behouden.

Om dit doel te bereiken, zou de organisatie:

- **Kwetsbaarheidsscans gebruiken waar dat veilig is**
  Kwetsbaarheidsscans zouden kunnen worden toegepast op IT- en OT-systemen wanneer dit de bedrijfsvoering niet verstoort en de veiligheid niet in gevaar brengt. In OT-omgevingen zou passieve of niet-intrusieve methoden de voorkeur kunnen hebben.
- **Tools voor kwetsbaarheidsbeheer gebruiken**
  Er zouden tools kunnen worden gebruikt om niet-gepatchte software, verkeerde configuraties en verouderde firmware in zowel IT- als OT-middelen op te sporen.
- **Architecturen beoordelen op zwakke punten**
  Netwerk- en systeemarchitecturen, inclusief segmentatie, paden voor externe toegang en verouderde componenten, zouden kunnen worden gecontroleerd op ontwerpfouten die OT-systemen kunnen blootstellen aan cyberdreigingen.
- **Bronnen van dreigingsinformatie bewaken**
  Openbare en particuliere bronnen van cyberdreigingsinformatie zouden kunnen worden gecontroleerd op kwetsbaarheden die van invloed zijn op OT-producten, industriële controlesystemen (ICS) en leverancierspecifieke technologieën.
- **Door de organisatie ontwikkelde software beoordelen**
  Aangepaste applicaties, waaronder die welke worden gebruikt in OT-omgevingen (bijv. HMI's, PLC-logica), zouden kunnen worden geanalyseerd en getest op onveilige coderingspraktijken en standaardconfiguraties.
- **Operationele procedures evalueren**
  Processen en procedures, met name die welke betrekking hebben op externe toegang, onderhoud en noodoperaties, zouden kunnen worden beoordeeld op kwetsbaarheden die kunnen worden misbruikt en die de integriteit van OT-systemen kunnen aantasten.

ID.RA-01.3 De organisatie moet een gedocumenteerd proces opstellen en onderhouden dat zorgt voor een continue beoordeling, analyse en verhelpen van kwetsbaarheden, en dat voorziet in het delen van informatie waar van toepassing.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat kwetsbaarheden continu worden beoordeeld, geanalyseerd en verholpen via een gedocumenteerd proces dat ook voorziet in het delen van informatie, indien van toepassing.

Om dit doel te bereiken, zou de organisatie:

- **Lessen uit het verleden en opkomende bedreigingen integreren**
  Het proces zou kunnen worden bijgewerkt op basis van incidenten, technologische veranderingen en nieuwe bedreigingen, waaronder bedreigingen die gericht zijn op OT-systemen en industriële protocollen.
- **Gebruikmaken van interne feedback en indicatoren**
  Auditresultaten, prestatie-indicatoren en feedback van operators zouden kunnen worden gebruikt om het kwetsbaarheidsbeheerproces te verfijnen, vooral wanneer handmatige processen gebruikelijk zijn.
- **Gebruikmaken van softwarecomponentenlijst (SBOM's)**
  SBOM's zouden kunnen worden gebruikt om kwetsbare componenten in zowel IT- als OT-softwarestacks te identificeren, inclusief ingebedde systemen en firmware.
- **Bronnen van dreigingsinformatie monitoren**
  Betrouwbare bronnen zoals adviezen van leveranciers, ICS-CERT en ENISA zouden kunnen worden gecontroleerd op kwetsbaarheden die van invloed zijn op OT-producten, besturingssystemen en veldapparatuur.
- **Processen en procedures herzien**
  Operationele procedures, met name die welke betrekking hebben op externe toegang, onderhoud en veiligheidskritieke functies, zouden kunnen worden gecontroleerd op kwetsbaarheden die kunnen worden misbruikt.
- **Coördineren met engineering en operations**
  Herstelmaatregelen zouden kunnen worden gepland in samenwerking met OT- en engineeringteams.

ID.RA-01.5 Het scannen op kwetsbaarheden mag geen nadelige invloed hebben op de systeemfuncties.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat kwetsbaarheidsscans de prestaties van bedrijfskritieke systemen niet verstoren of verslechteren, met name in Operational Technology (OT)-omgevingen waar de stabiliteit en beschikbaarheid van het systeem van cruciaal belang zijn.

Om dit doel te bereiken, kan de organisatie:

- **Scans plannen tijdens periodes van laag gebruik**
  Scans zouden kunnen worden uitgevoerd tijdens daluren of geplande onderhoudsperiodes om de operationele impact te minimaliseren.
- **Niet-intrusieve scantools gebruiken**
  Tools zouden kunnen worden geselecteerd op basis van hun vermogen om te scannen zonder de systeembronnen te overbelasten of realtime activiteiten te verstoren.
- **Eerst testen in testomgevingen**
  Scans zouden kunnen worden getest in niet-productieomgevingen om mogelijke problemen te identificeren voordat ze in live systemen worden geïmplementeerd.
- **Incrementele scans toepassen**
  Scans zouden kunnen worden opgedeeld in kleinere, beheersbare segmenten om de systeembelasting te verminderen en te voorkomen dat kritieke componenten overbelast raken.
- **De systeemprestaties tijdens scans monitoren**
  Het systeemgedrag zou tijdens het scannen actief kunnen worden gecontroleerd om prestatieverlies of afwijkingen op te sporen en hierop te reageren.

Onderscheid met ID.RA-01.4 (CyFun® Essential)

Terwijl ID.RA-01.4 zich richt op testactiviteiten zoals penetratie- en belastingstests, die doorgaans gepland zijn, niet vaak voorkomen en vaak worden uitgevoerd in gecontroleerde omgevingen, richt ID.RA-01.5 zich op de veilige uitvoering van kwetsbaarheidsscans, die vaker voorkomen, vaak geautomatiseerd zijn en zorgvuldig moeten worden beheerd om onbedoelde verstoringen in live OT-systemen te voorkomen.

ID.RA-01.6 Kwetsbaarheden moeten worden geïdentificeerd en beheerd in alle relevante assets, waaronder software, netwerk- en systeemarchitecturen en faciliteiten.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat kwetsbaarheden systematisch worden geïdentificeerd en beheerd in alle relevante assets, waaronder software, netwerk- en systeemarchitecturen en fysieke faciliteiten. Dit bouwt voort op controle ID.RA-01.1, die zich richt op het identificeren van zowel bedreigingen als kwetsbaarheden om risicobeperking te ondersteunen.

Om dit doel te bereiken, kan de organisatie:

- **Het toepassingsgebied van kwetsbaarheidsbeheer uitbreiden**
  Het identificeren en verhelpen van kwetsbaarheden zou betrekking kunnen hebben op alle relevante assets, waaronder IT- en OT-systemen, applicaties, netwerkontwerpen en faciliteiten die kritieke activiteiten ondersteunen.
- **Een speciaal proces voor kwetsbaarheidsbeheer onderhouden**
  Het zou waardevol zijn om een gestructureerd proces te hebben waarmee kwetsbaarheden continu worden gevolgd, beoordeeld en verholpen, los van activiteiten rond dreigingsinformatie.

- **Onderscheid maken tussen dreigingsinformatie en kwetsbaarheidsbeheer**
  Er zou onderscheid kunnen worden gemaakt door afzonderlijke processen of bewijsmateriaal bij te houden voor het identificeren van externe bedreigingen (bijv. bedreigingsactoren, campagnes) en het beheren van interne zwakke punten (bijv. niet-gepatchte systemen, verkeerde configuraties).
- **Integreren met breder risicobeheer**
  Het kwetsbaarheidsbeheerproces zou kunnen aansluiten bij het algemene risicobeheerkader van de organisatie en tijdige besluitvorming ondersteunen.
- **Zorgen voor OT-specifieke overwegingen**
  In OT-omgevingen zou kwetsbaarheidsbeheer rekening kunnen houden met verouderde systemen, afhankelijkheid van leveranciers en operationele beperkingen die de mogelijkheden voor patchen of scannen beperken.

ID.RA-02 Cyberdreigingsinformatie wordt ontvangen van fora en bronnen voor het delen van informatie

ID.RA-02.1 **Er moet een programma voor bewustmaking van bedreigingen en kwetsbaarheden worden geïmplementeerd dat de mogelijkheid biedt om informatie binnen de hele organisatie te delen.**

Implementatierichtlijnen

Het doel van deze maatregel is het versterken van het vermogen van de organisatie om te anticiperen op cyberdreigingen en hierop te reageren door een programma voor bewustmaking van dreigingen en kwetsbaarheden te implementeren dat informatie-uitwisseling tussen organisaties omvat.

Om dit doel te bereiken, kan de organisatie:

- **De tactieken van dreigingsactoren en opkomende kwetsbaarheden monitoren**
  Cyberdreigingsinformatie zou actuele inzichten kunnen bevatten over dreigingsactoren, hun tactieken, technieken en procedures (TTP's), evenals kwetsbaarheden in opkomende technologieën (bijv. AI-aangedreven aanvallen, data-vergiftiging bij machinaal leren).
- **Zorgen voor voortdurende externe betrokkenheid**
  De organisatie zou actief kunnen deelnemen aan beveiligingsgroepen, forums en beroepsverenigingen om waarschuwingen, adviezen en inzichten van collega's te ontvangen die relevant zijn voor zowel IT- als OT-omgevingen.
- **Informatie-uitwisseling mogelijk maken**
  Het programma zou het delen van niet-geclassificeerde en, indien van toepassing, geclassificeerde informatie over kwetsbaarheden en incidenten tussen afdelingen en met vertrouwde externe partners kunnen ondersteunen.
- **OT-specifieke bewustmaking ondersteunen**
  Threat intelligence zou OT-specifieke bronnen kunnen omvatten (bijv. ICS-CERT, adviezen van leveranciers) om kwetsbaarheden in industriële controlesystemen, verouderde apparaten en sectorspecifieke technologieën aan te pakken.
- **Een onderscheid maken tussen dreigingsinformatie en kwetsbaarheidsbeheer**
  Het bewustmakingsprogramma zou een aanvulling kunnen vormen op, maar onderscheiden blijven van, kwetsbaarheidsbeheerprocessen door zich te richten op externe dreigingsontwikkelingen en strategische inzichten.

ID.RA-03 Interne en externe bedreigingen voor de organisatie worden geïdentificeerd en geregistreerd

ID.RA-03.1 Bedreigingen moeten worden geïdentificeerd en beoordeeld in relatie tot alle relevante assets, waaronder software, netwerk- en systeemarchitecturen en faciliteiten.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat bedreigingen systematisch worden geïdentificeerd en beoordeeld in relatie tot alle relevante assets, waaronder software, netwerk- en systeemarchitecturen en faciliteiten. Dit bouwt voort op ID.RA-01.1, dat de basis legt voor het identificeren van zowel bedreigingen als kwetsbaarheden in kritieke assets.

Om dit doel te bereiken, kan de organisatie:

- **De identificatie van bedreigingen uitbreiden naar alle assets**
  Bedreigingen zouden kunnen worden beoordeeld met betrekking tot alle relevante assets, waaronder IT- en OT-systemen, applicaties, netwerkontwerpen en fysieke faciliteiten die kritieke activiteiten ondersteunen.
- **Een speciaal proces voor dreigingsinformatie onderhouden**
  Het zou nuttig zijn om een gestructureerd proces te hebben waarmee dreigingsinformatie uit interne en externe bronnen wordt verzameld, geanalyseerd en beoordeeld, inclusief sectorspecifieke adviezen en OT-gerichte dreigingsfeeds.
- **Bedreigingsinformatie onderscheiden van kwetsbaarheidsbeheer**
  Bedreigingsinformatie zou apart van kwetsbaarheidsbeheer kunnen worden beheerd, met duidelijke processen en bewijsmateriaal om helderheid en focus te garanderen. Bedreigingen verwijzen naar potentiële actoren of gebeurtenissen, terwijl kwetsbaarheden verwijzen naar zwakke punten die kunnen worden misbruikt.
- **De identificatie van bedreigingen integreren in het bredere risicoanalyseproces**
  Geïdentificeerde bedreigingen zouden kunnen worden gekoppeld aan bekende kwetsbaarheden en vastgelegd in een centraal risicoregister om prioritering en mitigatieplanning te ondersteunen, zoals beschreven in ID.RA-01.1.
- **OT-specifieke bedreigingen opnemen**
  Bij dreigingsbeoordelingen zou rekening kunnen worden gehouden met OT-specifieke risico's, zoals compromittering van de toeleveringsketen, ongeoorloofde toegang op afstand en misbruik van verouderde systemen of eigen protocollen.

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.

ID.RA-05.2 De organisatie moet risicobeoordelingen uitvoeren en documenteren, waarbij het risico wordt bepaald aan de hand van bedreigingen, kwetsbaarheden, de impact op bedrijfsprocessen en assets, en de waarschijnlijkheid dat deze zich voordoen.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat risicobeoordelingen worden uitgevoerd en gedocumenteerd aan de hand van een gestructureerde aanpak waarbij rekening wordt gehouden met bedreigingen, kwetsbaarheden, bedrijfsimpact en waarschijnlijkheid. Dit ondersteunt weloverwogen besluitvorming en prioritering van cyberbeveiligingsinspanningen in zowel IT- als OT-omgevingen.

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

- **Interne en externe bedreigingen meenemen**
  Risicobeoordelingen zouden zowel bedreigingen van binnen de organisatie als van externe actoren kunnen meenemen.
- **Erkende risicoanalysemethoden toepassen**
  Het zou zinvol zijn om kwalitatieve en/of kwantitatieve methoden te gebruiken, zoals het MAPGOOD-model, ISO/IEC 27005 of de CIS-risicobeoordelingsmethode. Deze methoden zouden kunnen worden ondersteund door risicobeheersoftwaretools.
- **Prioriteiten stellen op basis van waarschijnlijkheid en impact**
  Cybersecuritymiddelen en -investeringen zouden kunnen worden toegewezen op basis van de geschatte waarschijnlijkheid van bedreigingen en de potentiële impact op bedrijfsprocessen en kritieke assets.
- **Zorgen voor OT-specifieke risico-overwegingen**
  Bij risicobeoordelingen zou rekening kunnen worden gehouden met OT-specifieke factoren, zoals veiligheidsimplicaties, systeembeschikbaarheid, verouderde technologieën en operationele beperkingen.

ID.RA-06 Risicoresponsen worden geselecteerd, geprioriteerd, gepland, bijgehouden en gecommuniceerd

ID.RA-06.1 Maatregelen om risico's aan te pakken moeten worden geïdentificeerd, geprioriteerd, gepland, opgevolgd en gecommuniceerd.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat de organisatie duidelijk bepaalt welke acties nodig zijn om risico's te beheersen. Deze acties moeten worden geïdentificeerd, geprioriteerd, gepland, opgevolgd en gecommuniceerd, zodat effectieve risicobeperking en weloverwogen besluitvorming in de hele organisatie worden ondersteund.

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

- **Criteria voor het bepalen van risicobeheersmaatregelen toepassen**
  Beslissingen om risico's te accepteren, over te dragen, te verhelpen of te vermijden zouden in overeenstemming kunnen zijn met de criteria voor kwetsbaarheidsbeheer van de organisatie, zoals vermeld in ID.RA-08.1.
- **Zorgvuldig compenserende controles selecteren**
  Wanneer directe mitigatie niet haalbaar is, zou het verstandig kunnen zijn om compenserende controles te selecteren op basis van dezelfde criteria om een consistente risicoreductie te garanderen.
- **Acties baseren op bevindingen van risicobeoordelingen**
  Alle beslissingen over risicorespons zouden kunnen worden gebaseerd op de resultaten van gedocumenteerde risicobeoordelingen, zodat deze aansluiten bij de daadwerkelijke bedreigingen, kwetsbaarheden en bedrijfsimpact.
- **De voortgang van de implementatie volgen**
  Risicoresponsmaatregelen zouden kunnen worden gevolgd met behulp van gestructureerde tools, zoals een risicoregister, een actieplan en mijlpalen, of gedetailleerde risicorapporten.
- **Communiceren in volgorde van prioriteit**
  Geplande risicoresponsmaatregelen zouden in volgorde van prioriteit kunnen worden gecommuniceerd aan de betrokken belanghebbenden, zodat tijdige bewustmaking en coördinatie worden gewaarborgd.
- **OT-specifieke overwegingen meenemen**
  Risicorespons in OT-omgevingen zou rekening kunnen houden met operationele beperkingen, veiligheidseisen en systeembeschikbaarheid, vooral bij het plannen van mitigerende of compenserende maatregelen.

ID.RA-08 Processen voor het ontvangen, analyseren en reageren op meldingen van kwetsbaarheden worden opgezet

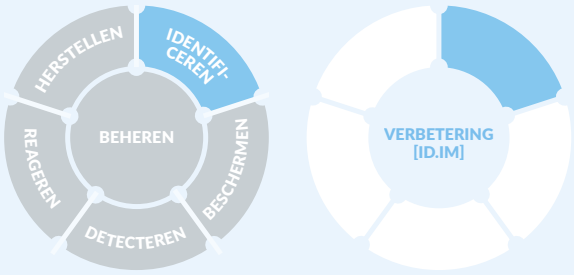
ID.RA-08.1 De organisatie moet een kwetsbaarheidsbeheerplan opstellen en implementeren om alle soorten kwetsbaarheden te identificeren, analyseren, beoordelen, mitigeren en communiceren, onder meer in de vorm van een gecoördineerde kwetsbaarheidsmelding (CVD) volgens de toepasselijke wettelijke modaliteiten.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle soorten kwetsbaarheden systematisch worden geïdentificeerd, geanalyseerd, beoordeeld, beperkt en gecommuniceerd via een gedocumenteerd kwetsbaarheidsbeheerplan. Dit omvat het afhandelen van meldingen in overeenstemming met de praktijken voor gecoördineerde kwetsbaarheidsmeldingen (CVD) en de toepasselijke wettelijke vereisten.

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

- **Een uitgebreid kwetsbaarheidsbeheerplan opstellen**
  Het plan zou kwetsbaarheden kunnen omvatten die zijn vastgesteld door interne tests, externe bronnen zoals beveiligingsbulletins en meldingen van onderzoekers, leveranciers, partners of overheidsinstanties op het gebied van cyberbeveiliging.
- **Verantwoordelijkheden toewijzen en de uitvoering opvolgen**
  Er zouden duidelijke rollen kunnen worden vastgelegd voor het verwerken, analyseren en afhandelen van gemelde kwetsbaarheden. De uitvoering van deze procedures zou kunnen worden opgevolgd om te zorgen voor een tijdige en effectieve aanpak.
- **Gecoördineerde kwetsbaarheidsmeldingen (CVD) ondersteunen**
  Het plan zou procedures kunnen bevatten voor het ontvangen van en reageren op kwetsbaarheidsrapporten van externe partijen. CVD-praktijken zouden in overeenstemming kunnen zijn met de richtlijnen van het CVD-kader van ENISA, waarin juridische, technische en communicatieaspecten worden beschreven.
- **Zorgen voor OT-specifieke dekking**
  Het plan zou kwetsbaarheden in OT-omgevingen kunnen aanpakken, waaronder verouderde systemen, door leveranciers beheerde componenten en ingebouwde firmware, waarvoor voor het aanbrengen van patches of het nemen van mitigerende maatregelen mogelijk afstemming met engineeringteams nodig is.



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

ID.IM-02 Verbeteringen worden geïdentificeerd aan de hand van beveiligingstests en -oefeningen, waaronder die welke in samenwerking met leveranciers en relevante derden worden uitgevoerd.

ID.IM-02.1 Beveiligingstests en -oefeningen, inclusief die welke worden uitgevoerd met leveranciers en relevante derde partijen, moeten worden gebruikt om verbeterpunten te identificeren.

IMPLEMENTATIERICHTLIJNEN

Het doel van deze controle is om mogelijkheden te identificeren voor het verbeteren van de beveiliging, incidentrespons en veerkracht door het uitvoeren van beveiligingstests en -oefeningen, zowel intern als in samenwerking met leveranciers en derde partijen. In Operational Technology (OT)-omgevingen zijn deze activiteiten essentieel om voorbereid te zijn op incidenten die van invloed kunnen zijn op fysieke activiteiten, veiligheid of continuïteit van de dienstverlening.

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

- De paraatheid voor incidentrespons beoordelen
  Beveiligingstests zoals tabletop-oefeningen, simulaties, interne beoordelingen en audits zouden kunnen worden gebruikt om verbeteringen in procedures voor het afhandelen van beveiligingsincidenten te identificeren.
- Coördineren met externe partijen
  Er kunnen oefeningen worden georganiseerd waarbij kritieke dienstverleners en belangrijke leveranciers betrokken zijn, om de bedrijfscontinuïteit, het herstel na calamiteiten en het vermogen om beveiligingsincidenten effectief af te handelen te versterken.
- Interne belanghebbenden betrekken
  Relevante interne functies, waaronder senior executives, juridische afdeling en HR, zouden bij oefeningen kunnen worden betrokken om te zorgen voor een brede bewustmaking en afstemming binnen de organisatie.
- Penetratietests uitvoeren
  Systemen met een hoog risico zouden kunnen worden onderworpen aan penetratietests om kwetsbaarheden te identificeren. Deze tests zouden vooraf kunnen worden goedgekeurd door het management.
- Noodplannen testen
  Plannen voor het reageren op ongeautoriseerde of gemanipuleerde producten of diensten zouden kunnen worden getest en verfijnd om een effectief herstel te garanderen.
- Zorgen voor conformiteit en naleving
  Alle testactiviteiten zouden in overeenstemming kunnen zijn met interne procedures en voldoen aan de toepasselijke wet- en regelgeving en industrienormen.

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.

ID.IM-03.2 **De organisatie moet de lessen die zijn geleerd uit incidentafhandeling opnemen in aangepaste of nieuwe processen en/of procedures voor incidentafhandeling. Deze moeten, na beoordeling, goedkeuring en testen, worden omkaderd door passende training.**

Implementatierichtlijnen

Het doel van deze maatregel is om de incidentafhandelingscapaciteit van de organisatie te verbeteren door lessen uit eerdere incidenten op te nemen in aangepaste of nieuwe processen en procedures. In omgevingen met Operationele Technologie (OT), waar incidenten directe gevolgen kunnen hebben voor fysieke systemen en de operationele continuïteit, helpt het toepassen van praktijkervaring om de effectiviteit van de respons te vergroten en de kans op herhaalde storingen te verkleinen.

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

- **De volledige levenscyclus van incidenten bestrijken**
  Er zouden lessen kunnen worden getrokken uit alle fasen van de incidentafhandeling, waaronder identificatie, categorisering, prioritering, onderzoek, oplossing, herstel, afsluiting en evaluatie na het incident.
- **Procesoptimalisatie aantonen**
  Updates van incidentafhandelingsprocedures zouden een weerspiegeling kunnen zijn van de inzichten die zijn opgedaan bij eerdere incidenten en duidelijk worden gedocumenteerd.
- **Samenwerken met leveranciers**
  Sessies om lessen te trekken zouden samen met belangrijke leveranciers kunnen worden gehouden om de coördinatie en respons in de hele toeleveringsketen te verbeteren.
- **Prestatie-indicatoren gebruiken**
  Indicatoren zouden kunnen worden gebruikt om de effectiviteit van incidentafhandeling in de tijd te volgen en te beoordelen, en om verbeteringen te sturen.
- **Zorgen voor conformiteit en naleving**
  Alle updates van processen en procedures zouden kunnen voldoen aan interne governancevereisten en aan de toepasselijke wet- en regelgeving en industrienormen.

ID.IM-03.3 **De organisatie moet verbeterpunten identificeren op basis van monitoring, metingen, beoordelingen en geleerde lessen, en deze omzetten in verbeterde processen, procedures en technologieën om de cyberweerbaarheid te versterken (continue verbetering).**

Implementatierichtlijnen

Het doel van deze controle is het verbeteren van de cyberweerbaarheid van de organisatie door verbeteringen te identificeren op basis van monitoring, metingen, beoordelingen en geleerde lessen, en deze te vertalen naar bijgewerkte processen, procedures of technologieën. In omgevingen met Operationele Technologie (OT), waar systeembetrouwbaarheid en veiligheid nauw verbonden zijn met cyberprestaties, helpt continue verbetering om de operationele integriteit te behouden en zich aan te passen aan evoluerende dreigingen.

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

- **Cyberweerbaarheidsindicatoren gebruiken**
  Indicatoren kunnen worden ingezet om het vermogen van de organisatie om cyberincidenten te weerstaan en ervan te herstellen te beoordelen, ter ondersteuning van onderbouwd risicobeheer en besluitvorming.
- **Effectiviteitsmaatregelen (MOE's) toepassen**
  MOE's kunnen worden gebruikt om de effectiviteit van verschillende strategieën voor cyberweerbaarheid te evalueren en te vergelijken, en om investerings- of ontwerpbeslissingen te ondersteunen.

- **Doelgerichte indicatoren implementeren**
  De indicatoren moeten aspecten omvatten zoals paraatheid, operationele continuïteit tijdens aanvallen, beperking van schade en het vermogen tot herstel en het opnieuw in werking brengen van systemen.
- **Onafhankelijke beoordelingen uitvoeren**
  Er zouden onafhankelijke teams kunnen worden ingeschakeld om beoordelingen uit te voeren en objectieve inzichten te verschaffen in verbeterpunten.
- **Gestructureerde scoresystemen gebruiken**
  Scoremethodologieën zoals MITRE's SSM-CR (Situated Scoring Methodology for Cyber Resiliency) zouden kunnen worden overwogen om gestructureerde evaluatie en prioritering van verbeteringen te ondersteunen.
- **Zorgen voor conformiteit en naleving:**
  Alle verbeteringen zouden in overeenstemming kunnen zijn met interne governancevereisten en voldoen aan de toepasselijke wet- en regelgeving en industrienormen.

ID.IM-03.4 De organisatie moet samenwerken en informatie over beveiligingsincidenten en mitigerende maatregelen met betrekking tot haar kritieke systemen delen met aangewezen partners.

Implementatierichtlijnen

Het doel van deze controle is het versterken van de cyberweerbaarheid door informatie over beveiligingsincidenten en mitigerende maatregelen met betrekking tot kritieke systemen te delen met aangewezen partners. In Operational Technology (OT)-omgevingen helpt tijdige en gecoördineerde informatie-uitwisseling de verspreiding van bedreigingen te voorkomen, ondersteunt het een sneller herstel en verbetert het de collectieve verdediging van onderling verbonden systemen.

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

- **Rollen en bevoegdheden definiëren**
  Het incidentresponsplan zou duidelijk de rollen, verantwoordelijkheden en bevoegdheden kunnen beschrijven voor het delen van incident gerelateerde informatie met aangewezen partners.
- **Het responsteam opleiden**
  Incidentresponspersoneel zou regelmatig kunnen worden opgeleid in procedures voor communicatie met externe partners tijdens en na incidenten.
- **Coördineren met partners**
  Het delen van informatie zou details kunnen omvatten over incidenten, mitigerende maatregelen en geleerde lessen, met name met leveranciers en dienstverleners die betrokken zijn bij kritieke systeemoperaties.
- **Betrouwbare richtlijnen raadplegen**
  Relevante praktijken zouden kunnen worden gebaseerd op betrouwbare bronnen zoals ENISA/CERT-EU Security Guidance 22-001, dat aanbevolen maatregelen tegen kritieke bedreigingen bevat.
- **Zorgen voor conformiteit en naleving**
  Alle samenwerkings- en uitwisselingsactiviteiten kunnen plaatsvinden in overeenstemming met het interne beleid en voldoen aan de geldende wet- en regelgeving en relevante industrienormen.

ID.IM-03.5 De effectiviteit van beschermingstechnologieën moet worden gecommuniceerd aan relevante belanghebbenden.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de effectiviteit van beschermingstechnologieën duidelijk wordt gecommuniceerd aan relevante belanghebbenden. In operationele technologieomgevingen (OT), waar beschermingsinstrumenten kritieke fysieke systemen beveiligen, ondersteunt zinvolle communicatie weloverwogen beslissingen, risicobewustzijn en afstemming tussen technische en niet-technische teams.

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

- **Communicatie afstemmen op belanghebbenden**
  Informatie zou kunnen worden aangepast aan de behoeften van verschillende doelgroepen; technische teams hebben mogelijk gedetailleerde logboeken nodig, terwijl leidinggevenden wellicht behoefte hebben aan samenvattingen op hoog niveau die verband houden met bedrijfsrisico's.
- **Verder gaan dan technische indicatoren**
  Communicatie zou niet alleen gegevens kunnen bevatten (zoals geblokkeerde bedreigingen of gedetecteerde incidenten), maar ook inzichten in de risicopositie, opkomende trends en aanbevolen acties.
- **Alle relevante rollen betrekken**
  Stakeholders zoals CISO's, IT-beveiligingsteams, compliance officers, interne auditors en leidinggevenden zouden de informatie kunnen ontvangen die nodig is om hun verantwoordelijkheden te kunnen uitoefenen.
- **Prestaties monitoren en rapporteren**
  De prestaties van beveiligingstechnologieën (zoals antivirus, firewalls, inbraakpreventie, eindpuntdetectie en preventie van gegevensverlies) zouden continu kunnen worden gemonitord en gerapporteerd.
- **Continue verbetering ondersteunen**
  Communicatie zou kunnen helpen bij het identificeren van hiaten, het nemen van strategische beslissingen en het bevorderen van een cultuur van transparantie en veerkracht.
- **Zorgen voor conformiteit en naleving**
  Alle communicatiepraktijken zouden in overeenstemming kunnen zijn met het interne beleid en voldoen aan de toepasselijke wet- en regelgeving en industrienormen.

ID.IM-03.6 De organisatie moet, waar mogelijk, geautomatiseerde mechanismen implementeren om het proces van informatie-uitwisseling en samenwerking te vergemakkelijken.

Implementatierichtlijnen

Het doel van deze maatregel is om de efficiëntie, nauwkeurigheid en veiligheid van het delen van informatie en samenwerking te verbeteren door waar mogelijk geautomatiseerde mechanismen te implementeren. In operationele technologieomgevingen (OT) helpt automatisering om handmatige fouten te verminderen, toegangscontroles af te dwingen en tijdige besluitvorming tussen onderling verbonden systemen te ondersteunen.

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

- **Toegangsautorisaties afstemmen**
  Geautomatiseerde tools zouden kunnen controleren of de toegangsrechten van partners die informatie delen in overeenstemming zijn met de gevoeligheid van de informatie. Afwijkingen zouden kunnen worden gemarkeerd voordat de informatie wordt gedeeld.
- **Het handhaven van beleid automatiseren**
  Systemen zouden automatisch kunnen beoordelen of informatie kan worden gedeeld op basis van de classificatie ervan en de toegangsrechten van de ontvanger. Deze controles zouden kunnen worden geïntegreerd met identiteits- en toegangsbeheersystemen (IAM) om te zorgen voor actuele autorisatiegegevens.
- **Zoeken en ophalen controleren**
  Zoek- en ophaaltools zouden toegangsbeperkingen kunnen afdwingen met behulp van metadata tagging en classificatie, zodat gebruikers alleen toegang hebben tot geautoriseerde informatie.

- **Activiteiten monitoren en controleren**
  Geautomatiseerde logboekregistratie en monitoring zouden alle acties op het gebied van informatie-uitwisseling kunnen bijhouden. Logboeken zouden regelmatig kunnen worden gecontroleerd om ongeoorloofde toegang of schendingen van het beleid op te sporen.
- **Gebruiksvriendelijkheid en opleiding bevorderen**
  Geautomatiseerde tools zouden gebruiksvriendelijk kunnen zijn om correct gebruik te stimuleren. Er zou opleiding kunnen worden gegeven om ervoor te zorgen dat gebruikers begrijpen hoe ze deze tools effectief en verantwoord kunnen gebruiken.
- **Zorgen voor conformiteit en naleving**
  Alle geautomatiseerde mechanismen zouden in overeenstemming kunnen zijn met het interne beleid en voldoen aan de toepasselijke wet- en regelgeving en industrienormen.

ID.IM-04 Incidentresponsplannen en andere cyberbeveiligingsplannen die van invloed zijn op de bedrijfsvoering worden opgesteld, gecommuniceerd, onderhouden en verbeterd.

ID.IM-04.1 **Nood- en continuïteitsplannen moeten worden opgesteld, gecommuniceerd, onderhouden, getest, gevalideerd en verbeterd.**

Implementatierichtlijnen

Het doel van deze maatregel is het waarborgen van de veerkracht van de organisatie door nood- en continuïteitsplannen op te stellen, bij te houden en te verbeteren, zodat effectief kan worden gereageerd op verstoringen en het herstel kan worden ingezet.

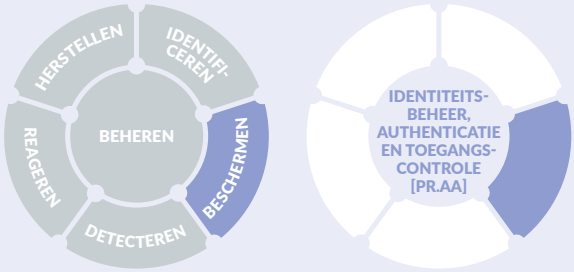
Om dit doel te bereiken, kan het volgende worden overwogen:

- **Uitgebreide plannen opstellen**
  Plannen zouden het volgende kunnen omvatten:
  - **Incidentresponsplan (IRP)**
  - **Bedrijfscontinuïteitsplan (BCP)**
  - **Rampenherstelplan (DRP)**
    Deze kunnen betrekking hebben op operationele verstoringen, datalekken en missiekritieke storingen.
- **Een duidelijke planinhoud definiëren**
  Plannen zouden het volgende kunnen bevatten:
  - Contact- en communicatiegegevens
  - Rollen, verantwoordelijkheden en bevoegdheden (in overeenstemming met GV.RR-02.1)
  - Procedures voor veelvoorkomende scenario's
  - Criteria voor prioritering, escalatie en besluitvorming
  - IRP's zouden betrekking kunnen hebben op detectie, beheersing, respons en herstel van cyberincidenten.
- **Communiceren en opleiden**
  Plannen zouden kunnen worden gedeeld met alle relevante medewerkers. Er zou een crisismanagementteam kunnen worden opgericht met vertegenwoordigers van belangrijke afdelingen (zoals IT, juridische zaken, HR en PR) en worden opgeleid om te handelen tijdens crises.
- **Plannen onderhouden en herzien**
  Plannen zouden ten minste eenmaal per jaar of na grote veranderingen of incidenten kunnen worden herzien. Updates zouden rekening kunnen houden met geleerde lessen en veranderende risico's.
- **Regelmatig testen en valideren**
  Plannen zouden kunnen worden getest aan de hand van realistische scenario's. Validatie zou kunnen bevestigen dat de procedures werken zoals bedoeld en voldoen aan de operationele behoeften. De resultaten zouden kunnen worden gedocumenteerd.
- **Voortdurend verbeteren**
  Feedback uit tests, incidenten en beoordelingen zou aanleiding kunnen geven tot verbeteringen. Verbeteringen zouden kunnen worden geprioriteerd op basis van risico en impact om de continuïteit van essentiële functies te waarborgen.
- Voorbeelden van sjablonen voor beleidsdocumenten zijn beschikbaar op www.cyfun.eu


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.

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-01.2 Identiteiten en authenticatiemiddelen voor geautoriseerde gebruikers, diensten en hardware moeten waar mogelijk worden beheerd via geautomatiseerde mechanismen.

Implementatierichtlijnen

Het doel van deze controle is het risico op misbruik van authenticatiemiddelen en ongeoorloofde toegang te verminderen door identiteits- en authenticatiemiddelenbeheerprocessen te automatiseren, waardoor consistentie, schaalbaarheid en veiligheid in IT- en OT-omgevingen worden gewaarborgd.

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

- **Het beheer van authenticatiemiddelen automatiseren**
  Geautomatiseerde systemen zouden kunnen worden gebruikt voor het uitgeven, verifiëren, intrekken en auditen van authenticatiemiddelen voor gebruikers, diensten en hardware. Dit vermindert handmatige fouten en verhoogt de operationele efficiëntie.
- **Sterke authenticatiemechanismen implementeren**
  In overeenstemming met controle PR.AA-03.2 is MFA vereist voor alle externe toegang tot de netwerken van de organisatie. Multifactorauthenticatie (MFA) moet ten minste twee onafhankelijke factoren gebruiken:
  - *Kennis* (bijv. wachtwoord of pincode)
  - *Bezit* (bijv. token of smartphone)
  - *Inherentie* (bijv. vingerafdruk of gezichtsherkenning)

  Deze factoren moeten onafhankelijk zijn om ervoor te zorgen dat het compromitteren van één factor geen invloed heeft op de andere.
- **Cryptografische en op tokens gebaseerde oplossingen gebruiken**
  Digitale certificaten en identiteitstokens zouden kunnen worden gebruikt om gebruikers, apparaten en diensten te authentiseren, vooral in OT-omgevingen waar handmatige verwerking van authenticatiemiddelen onpraktisch kan zijn.
- **Zorgen voor OT-specifieke integratie**
  Oplossingen voor identiteits- en toegangsbeheer zouden OT-systemen kunnen ondersteunen, inclusief verouderde apparaten en door leveranciers beheerde componenten, met minimale verstoring van de bedrijfsvoering.
  Wanneer individuele gebruikersaccounts niet haalbaar zijn (bijvoorbeeld gedeelde toegang tot PLC's of HMI's), zou de toegang kunnen worden gerouteerd via beveiligde jumpservers met logboekregistratie en extra authenticatielagen. Voor externe toegang tot OT-systemen zouden beveiligde protocollen kunnen worden gebruikt (zoals VPN, SSH, TLS), zou de toegang in de tijd beperkt kunnen zijn (Just-In-Time) en volledig kunnen worden bewaakt.

PR.AA-02 Identiteiten worden gecontroleerd en gekoppeld aan authenticatiemiddelen op basis van de context van interacties

PR.AA-02.1 De organisatie moet gedocumenteerde procedures implementeren voor het verifiëren van de identiteit van personen voordat authenticatiemiddelen worden verstrekt die toegang geven tot de systemen van de organisatie.

Implementatierichtlijnen

Het doel van deze controle, die voortbouwt op GV.RR-04.1, is ervoor te zorgen dat alleen geverifieerde personen authenticatiemiddelen krijgen, waardoor het risico op identiteitsfraude, ongeoorloofde toegang en bedreigingen van binnenuit wordt verminderd.

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

- **Gedocumenteerde procedures voor identiteitsverificatie opstellen**
  Er zou een formeel proces kunnen worden ontwikkeld en goedgekeurd om identiteiten te verifiëren voordat authenticatiemiddelen worden verstrekt. Dit proces zou kunnen zorgen voor verantwoordingsplicht, traceerbaarheid en controleerbaarheid.
- **Identiteit verifiëren met behulp van betrouwbare bronnen**
  Identiteitsverificatie zou gebaseerd kunnen zijn op officiële documenten, zoals door de overheid uitgegeven identiteitskaarten, paspoorten of rijbewijzen. Voor onboarding op afstand of digitale onboarding zouden de praktijken in overeenstemming kunnen zijn met de goede praktijken van ENISA voor identiteitscontrole op afstand.
- **Identiteitsfraude en misbruik voorkomen**
  Procedures zouden controles kunnen omvatten om identiteitsdiefstal of identiteitsfraude op te sporen en te voorkomen. Dit zou helpen het risico op financieel verlies, reputatieschade en ongeoorloofde toegang te verminderen.
- **Zorgen voor OT-relevante aanpassing**
  Identiteitsverificatieprocessen zouden kunnen worden aangepast aan OT-omgevingen, met name wanneer technici van derden of personeel van leveranciers toegang zouden moeten hebben tot kritieke systemen.

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-03.3 De organisatie moet gebruiksbeperkingen, verbindingsvereisten en autorisatieprocedures voor externe toegang tot haar kritieke systemen definiëren, documenteren en implementeren. Deze controles moeten ervoor zorgen dat alleen goedgekeurde gebruikers verbinding kunnen maken met behulp van veilige methoden, waarbij de toegang beperkt blijft tot wat nodig is voor hun functie.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat externe toegang tot kritieke systemen streng wordt gecontroleerd door middel van gedefinieerde gebruiksbeperkingen, veilige verbindingsmethoden en formele autorisatieprocedures. Dit helpt ongeoorloofde toegang te voorkomen en beperkt de blootstelling aan cyberdreigingen.

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

- **Gebruiksbeperkingen definiëren**
  - Er zouden systemen kunnen worden geïdentificeerd die kritiek zijn (bijv. OT-systemen, productieservers, financiële databases).
  - Er zou kunnen worden bepaald wie er op afstand toegang mag hebben (bijv. specifieke functies, externe leveranciers).
  - De toegang zou kunnen worden beperkt tot goedgekeurde tijdsbestekken en alleen tot de systemen en functies die nodig zijn voor de functie van de gebruiker.
- **Vereisten voor veilige verbindingen vaststellen**
  - Toegang op afstand zou kunnen worden gerealiseerd met behulp van veilige methoden, zoals VPN's met sterke encryptie, TLS/SSH of jumpservers voor OT-omgevingen.
  - Alle toegang op afstand zou kunnen worden beveiligd met multifactorauthenticatie (MFA), in overeenstemming met PR.AA-03.2.
  - Apparaten die worden gebruikt voor toegang op afstand zouden kunnen voldoen aan de beveiligingsvereisten voor eindpunten (bijv. antivirus, patches)).
- **Toegang documenteren en goedkeuren**
  - In een beleid voor externe toegang zouden aanvraag- en goedkeuringsprocedures, rollen en technische vereisten kunnen worden vastgelegd.
  - Er zou een register van externe gebruikers kunnen worden bijgehouden, met daarin de toegangsrechten, goedkeuringsdata en beoordelingstermijnen.
- **Toegang controleren en beoordelen**
  - Alle externe sessies zouden kunnen worden geregistreerd, waarbij de identiteit van de gebruiker, het tijdstip, de duur en de systemen waartoe toegang is verkregen, worden vastgelegd.
  - Logboeken zouden regelmatig kunnen worden gecontroleerd op afwijkingen. Toegangsrechten en configuraties voor externe toegang zouden periodiek kunnen worden gecontroleerd.

- **OT-specifieke controles toepassen**
  - Voor OT-systemen zou de toegang kunnen worden gerouteerd via beveiligde front-end interfaces of jumpservers.
  - Als gedeelde accounts vereist zijn (bijvoorbeeld voor PLC's of HMI's), zou de toegang kunnen worden gelogd, in de tijd beperkt, beveiligd door MFA op jumpserver niveau en gevolgd.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zijn in overeenstemming met de technische implementatierichtlijnen van ENISA voor NIS2, waarin veilige beleidsregels voor externe toegang, sterke authenticatie en continue monitoring worden aanbevolen als onderdeel van het cyberbeveiligingsrisicobeheer voor kritieke systemen.

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.

mplementatierichtlijnen

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-05.5 **Waar dit technisch, operationeel en economisch haalbaar is – zonder afbreuk te doen aan de integriteit, veiligheid of naleving van het systeem – moeten geautomatiseerde mechanismen worden toegepast om gebruikersaccounts op kritieke ICT- en OT-systemen te beheren. De haalbaarheid moet worden bepaald op basis van de mogelijkheden van het systeem, het integratiepotentieel, de risicobeoordeling en de impact op het bedrijf.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat gebruikersaccounts op kritieke ICT- en OT-systemen veilig, efficiënt en consistent worden beheerd door middel van geautomatiseerde mechanismen – waar dit technisch, operationeel en economisch haalbaar is – zonder de integriteit, veiligheid of naleving van het systeem in gevaar te brengen.

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

- **De haalbaarheid van automatisering beoordelen**
  De haalbaarheid zou kunnen worden gebaseerd op de mogelijkheden van het systeem, het integratiepotentieel, de risicobeoordeling en de impact op de bedrijfsvoering.
  - Voor ICT-systemen zou de haalbaarheid kunnen afhangen van de beschikbaarheid van automatiseringstools, API's of integratieopties.
  - Voor OT-systemen zou de haalbaarheid kunnen afhangen van de leeftijd van het systeem, beperkingen van leveranciers, veiligheidseisen en het risico van verstoring van kritieke activiteiten.
- Bij de algemene haalbaarheid zou rekening kunnen worden gehouden met technische mogelijkheden, operationele veiligheid, kosteneffectiviteit en naleving van veiligheids- en regelgevingsnormen.
- **Het beheer van de levenscyclus van accounts automatiseren**
  Geautomatiseerde mechanismen zouden het aanmaken, wijzigen en verwijderen van accounts kunnen beheren op basis van vooraf gedefinieerde regels. Dit zou ervoor kunnen zorgen dat alleen geautoriseerde gebruikers toegang hebben en dat accounts onmiddellijk worden verwijderd wanneer ze niet langer nodig zijn.
- **Inactieve of niet-geautoriseerde accounts uitschakelen**
  Accounts zouden automatisch kunnen worden uitgeschakeld wanneer gebruikers de organisatie verlaten of geen toegang meer nodig hebben. Dit zou het risico op ongeautoriseerde toegang tot kritieke systemen kunnen verminderen.
- **Accountactiviteit monitoren en rapporteren**
  Geautomatiseerde tools zouden het accountgebruik continu kunnen monitoren en rapporten kunnen genereren om ongebruikelijke of ongeautoriseerde activiteiten te detecteren. Bij verdacht gedrag zouden waarschuwingen kunnen worden geactiveerd.
- **Meldingen sturen voor belangrijke gebeurtenissen**
  Geautomatiseerde meldingen zouden beheerders kunnen informeren over belangrijke gebeurtenissen, zoals het aanmaken, wijzigen of verwijderen van accounts, zodat ze tijdig toezicht kunnen houden.
- **Audittrails bijhouden voor naleving**
  Alle account gerelateerde activiteiten zouden automatisch kunnen worden geregistreerd om naleving van interne beleidsregels en externe regelgeving te ondersteunen.
- **Zorgen voor OT-specifieke haalbaarheid**
  In OT-omgevingen zou automatisering alleen kunnen worden geïmplementeerd als dit geen afbreuk doet aan de veiligheid of de operationele continuïteit. Wanneer directe automatisering niet haalbaar is, zou het accountbeheer kunnen worden afgehandeld via beveiligde interfacelagen of jumpservers.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zouden kunnen worden ondersteund door de technische implementatierichtlijnen van ENISA voor NIS2 en haar werkzaamheden op het gebied van veilig toegangsbeheer in kritieke infrastructuur omgevingen.

PR.AA-05.6 Scheiding van taken (SoD) moet worden gewaarborgd bij het beheer van toegangsrechten.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat geen enkele persoon volledige controle heeft over kritieke systemen of processen door scheiding van taken (SoD) af te dwingen. Dit moet het risico op fouten, fraude en misbruik van toegangsrechten verminderen.

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

- **Scheiding van taken definiëren**
  Verantwoordelijkheden zouden zodanig kunnen worden verdeeld dat belangrijke taken door verschillende personen worden uitgevoerd.
  SoD zou het volgende kunnen omvatten:
  - Operationele en systeemondersteunende functies zouden aan verschillende personen kunnen worden toegewezen.
  - Systeemondersteunende taken zouden toezicht of dubbele controle kunnen vereisen.
  - Eén persoon zou niet dezelfde transactie kunnen initiëren en goedkeuren.
  - Toegangscontrole en auditfuncties zouden door afzonderlijke personen kunnen worden uitgevoerd.
- **Toegangsrechten op de juiste manier beheren**
  - Role-Based Access Control (RBAC) zou kunnen worden gebruikt om machtigingen toe te wijzen op basis van functies.
  - Het principe van minimale rechten zou kunnen worden toegepast om de toegang te beperken tot wat strikt noodzakelijk is.
  - Toegangsrechten zouden regelmatig kunnen worden herzien, met name voor kritieke systemen en risicovolle functies.
  - Waar mogelijk zouden afzonderlijke tools of accounts kunnen worden gebruikt voor administratieve en auditfuncties.
- **Controles toepassen voor systeembeheerders**
  - Beheertaken zouden kunnen worden verdeeld om te voorkomen dat één persoon volledige controle heeft.
  - Beheerders zouden aparte accounts kunnen gebruiken voor reguliere en geprivilegieerde taken.
  - Alle administratieve handelingen zouden kunnen worden geregistreerd en gecontroleerd door een onafhankelijke partij.
  - Beheerders die de toegang beheren, zouden niet verantwoordelijk kunnen zijn voor het controleren van die toegang.
- **Zorgen voor haalbaarheid in OT-omgevingen**
  - In OT-systemen zou SoD kunnen worden aangepast aan operationele en veiligheidsbeperkingen.
  - Wanneer volledige scheiding niet haalbaar is, zouden compenserende maatregelen zoals dubbele goedkeuring, registratie en externe controle kunnen worden geïmplementeerd.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zouden in overeenstemming kunnen zijn met de beveiligingsmaatregelen van ENISA voor exploitanten van essentiële diensten, waarin het belang van scheiding van taken (SoD) en op rollen gebaseerde toegangscontrole (RBAC) wordt benadrukt voor het verminderen van toegangsgerelateerde risico's in ICT- en OT-omgevingen.

PR.AA-05.7 Bevoorrechte gebruikers moeten worden beheerd en bewaakt.

Implementatierichtlijnen

Het doel van deze controle is het risico van ongeoorloofde toegang, datalekken en operationele verstoringen te verminderen door ervoor te zorgen dat bevoorrechte gebruikers, die verhoogde toegang hebben tot kritieke systemen, onderworpen zijn aan strikt beheer en voortdurend toezicht.

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

- **Privilegieerde activiteiten monitoren**
  Activiteiten van bevoorrechte gebruikers zouden kunnen worden geregistreerd en routinematig of continu worden gecontroleerd, zelfs als ze worden uitgevoerd door personen die niet onafhankelijk zijn van het proces.
- **Gevoelige gegevens beschermen**
  Monitoring zou kunnen helpen voorkomen dat bevoorrechte gebruikers gevoelige informatie en systeemconfiguraties openbaar maken of misbruiken.
- **Misbruik van privileges voorkomen**
  Privileged accounts zouden kunnen worden beheerd om ongeoorloofde wijzigingen, escalatie van privileges of het omzeilen van beveiligingsmaatregelen te voorkomen.
- **Verdacht gedrag detecteren**
  Afwijkend gedrag en ongeoorloofde acties zouden kunnen worden geïdentificeerd door middel van geautomatiseerde logboekregistratie en waarschuwingsmechanismen.
- **Incidentrespons ondersteunen**
  Monitoringgegevens zouden kunnen worden gebruikt om beveiligingsincidenten met geprivilegieerde accounts te onderzoeken en erop te reageren.
- **Toegangsrechten proactief beheren**
  Toegangsrechten zouden duidelijk kunnen worden gedefinieerd, regelmatig worden herzien en worden aangepast op basis van rolveranderingen, operationele behoeften of risicobeoordelingen.
  Zorgen voor OT-specifieke haalbaarheid
  - In OT-omgevingen zou geprivilegieerde toegang kunnen worden beheerd met inachtneming van de stabiliteit en veiligheid van het systeem.
  - Wanneer volledige monitoring niet haalbaar is, zouden compenserende controles zoals logging[1] op interfaceniveau of externe beoordeling kunnen worden geïmplementeerd.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zouden in overeenstemming kunnen zijn met de technische implementatierichtlijnen van ENISA voor NIS2, waarin het belang van geprivilegieerde toegangscontrole en monitoring voor het beveiligen van essentiële diensten en kritieke infrastructuur wordt benadrukt.

1 Logging op interfaceniveau betekent het registreren van wat gebruikers doen op het moment dat ze verbinding maken met een systeem, bijvoorbeeld via een tool voor externe toegang, een jumpserver of een beveiligde gateway, zonder dat ze rechtstreeks in het systeem zelf hoeven in te loggen (bijvoorbeeld met behulp van Splunk(®)). Dit helpt bij het monitoren van geprivilegieerde activiteiten in omgevingen waar directe systeemlogging niet mogelijk is, zoals in OT-systemen.

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.

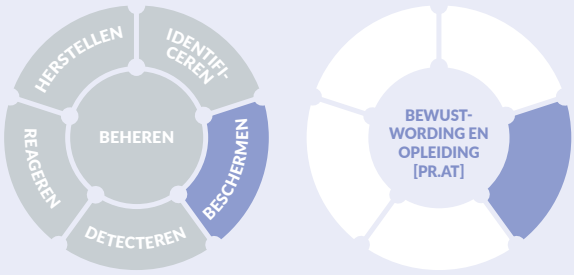
PR.AA-06.2 **Fysieke toegangscontroles moeten specifieke procedures voor noodsituaties omvatten, zodat kritieke en niet-kritieke assets tijdens dergelijke gebeurtenissen continu worden beschermd.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat fysieke toegangscontroles effectief en aanpasbaar blijven tijdens noodsituaties. Dit omvat het handhaven van de beveiliging van kritieke en niet-kritieke assets, terwijl veilige, geautoriseerde en traceerbare toegang wordt mogelijk gemaakt voor noodhulp, herstel- of beheersingsmaatregelen, met name in omgevingen waar fysieke en operationele veiligheid nauw met elkaar verbonden zijn, zoals Operational Technology (OT) en Internet of Things (IoT)-systemen.

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

- **Noodscenario's definiëren**
  Noodprocedures omvatten een reeks gebeurtenissen, waaronder:
  - Milieu- en veiligheidsincidenten (bijv. brand, overstroming, medische noodsituaties, evacuaties)
  - Infrastructuurstoringen (bijv. stroomuitval, systeemstoringen)
  - Beveiligingsincidenten (bijv. inbraken, storingen in de toegangscontrole)
  - Cyberbeveiligingsincidenten (bijv. ransomware, datalekken, bedreigingen van binnenuit)
- **Noodtoegangsprocedures handhaven**
  Noodtoegang zou kunnen:
  - Geregistreerd worden: noteer wie toegang heeft gehad tot wat, wanneer en waarom.
  - Bewaakt worden: gebruik bewakings- of toegangscontrolesystemen om activiteiten bij te houden.
  - Geëvalueerd worden: voer na afloop evaluaties uit om te controleren of er sprake is van correct gebruik en om misbruik op te sporen.
- **Paraatheid voor noodsituaties met fysieke beveiligingsmaatregelen ondersteunen**
  - Er zou een actuele lijst kunnen worden bijgehouden van personen die bevoegd zijn om in noodgevallen toegang te krijgen.
  - Er zouden identiteitsbewijzen (bijv. toegangspassen) kunnen worden gebruikt en er zouden veiligheidszones kunnen worden gedefinieerd.
  - Er zouden begeleidingsvereisten kunnen worden toegepast voor bezoekers of tijdelijk personeel.
  - Er zouden fysieke barrières kunnen worden aangebracht, zoals hekken, sloten, tourniquets en bemande controleposten.
  - Er zouden bewakingssystemen kunnen worden gebruikt om in- en uitgangen te controleren.
- **Extra veiligheidsmaatregelen toepassen**
  - Er zou kunnen worden overwogen om badgesystemen met verschillende toegangsniveaus voor verschillende zones in te voeren.
  - Fysieke toegang tot servers en netwerkcomponenten zou kunnen worden beperkt tot bevoegd personeel.
  - Alle toegang tot kritieke infrastructuur zou kunnen worden geregistreerd en regelmatig worden gecontroleerd.
  - Authenticatiemiddelen van bezoekers zouden kunnen worden bijgehouden en gecontroleerd. Indien nodig zouden corrigerende maatregelen kunnen worden genomen.
- **Zorgen voor OT-specifieke haalbaarheid**
  In OT-omgevingen zouden fysieke toegangsprocedures kunnen worden aangepast om verstoring van de veiligheid of operationele continuïteit te voorkomen. Noodtoegang zou zo kunnen worden ontworpen dat zowel snelle respons als bescherming van assets wordt ondersteund.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zouden in overeenstemming kunnen zijn met de technische implementatierichtlijnen van ENISA voor NIS2, waarin het belang van fysieke en logische toegangscontroles voor het behoud van de veerkracht tijdens noodsituaties wordt benadrukt.



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.

PR.AT-01.2 De organisatie moet bewustmaking over interne bedreigingen en meldingsprocedures opnemen in haar cybersecuritytraining, zodat medewerkers potentiële interne risico's kunnen herkennen en er op kunnen reageren. .

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat alle medewerkers worden opgeleid in het herkennen en melden van potentiële bedreigingen van binnenuit, waardoor het risico op interne cyberbeveiligingsincidenten wordt verminderd.
Deze controle bouwt voort op de algemene bewustmaking uit PR.AT-01.1 door specifieke dreigingsscenario's en responsmaatregelen te introduceren.

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

- De opleiding zou onder meer kunnen ingaan op het herkennen van gedragssignalen van bedreigingen van binnenuit, zoals ongebruikelijke toegangspatronen, het hamsteren van gegevens of plotselinge gedragsveranderingen.
- De organisatie zou bedreigingen van binnenuit duidelijk kunnen definiëren (bijv. kwaadwillende, nalatige of gecompromitteerde insiders, waaronder werknemers en aannemers).
- Het personeel zou kunnen worden opgeleid in hoe en waar verdachte activiteiten zouden kunnen worden gemeld en waarom tijdige melding belangrijk zou kunnen zijn.
- Er zouden praktijkvoorbeelden of simulaties kunnen worden gebruikt om de impact van bedreigingen van binnenuit te laten zien en het leerproces te versterken.
- Bewustwording van bedreigingen van binnenuit zou deel kunnen uitmaken van de reguliere beveiligingsopleiding en onboarding voor alle medewerkers.
- Er zou gespecialiseerde opleiding kunnen worden gegeven aan medewerkers die toegang hebben tot gevoelige gegevens of systemen, waarbij de nadruk zou kunnen liggen op hun specifieke verantwoordelijkheden.
- Er zou een functieoverschrijdende teamopleiding kunnen worden ontwikkeld met zowel IT-beveiligings- als OT-operationele expertise (cross-training).
- Er zou jaarlijks een opfriscursus kunnen worden gegeven om de belangrijkste boodschappen te versterken en updates te introduceren.
- De organisatie zou een veiligheidscultuur kunnen bevorderen waarin medewerkers zich veilig voelen om hun zorgen te melden zonder angst voor represailles.

PR.AT-01.3 Medewerkers moeten opleiding krijgen om hun specifieke rollen, verantwoordelijkheden en prioriteiten tijdens een cyber- of informatiebeveiligingsincident te begrijpen, inclusief de stappen die zij moeten volgen om effectief te reageren.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle personeelsleden hun specifieke rollen, verantwoordelijkheden en prioriteiten tijdens een cyberbeveiligings- of informatiebeveiligingsincident begrijpen, zodat ze effectief en in overeenstemming met de incidentrespons- en noodplannen van de organisatie kunnen reageren.
Deze controle bouwt voort op de dreiging specifieke bewustmaking van PR.AT-01.2 door de introductie van op rollen gebaseerde opleiding en paraatheid voor incidentrespons.

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

- De opleiding zou kunnen worden afgestemd op verschillende rollen (bijv. IT, HR, leidinggevenden), zodat elke groep zijn specifieke verantwoordelijkheden tijdens een incident begrijpt.
- Het personeel zou bekend kunnen zijn met zijn doelstellingen, herstelprioriteiten en de juiste volgorde van te nemen maatregelen tijdens een incident.
- Er zouden tabletop-oefeningen of gesimuleerde oefeningen kunnen worden gebruikt om incidentrespons te oefenen in een realistische maar gecontroleerde omgeving.
- Er zou duidelijke documentatie kunnen worden verstrekt waarin de taken en verantwoordelijkheden van elke rol tijdens een incident worden beschreven.

- De opleiding zou kunnen uitleggen hoe incidentrespons verband houdt met noodplanning, zodat het personeel begrijpt wanneer en hoe noodmaatregelen zouden kunnen worden geactiveerd (zie ook ID.IM-04.1).
- Er zouden regelmatig opfriscursussen kunnen worden gehouden om de kennis up-to-date te houden en de paraatheid te versterken.

PR.AT-02 Personen in gespecialiseerde functies krijgen bewustmaking en opleiding, zodat ze over de kennis en vaardigheden beschikken om relevante taken uit te voeren met het oog op cyberbeveiligingsrisico's

PR.AT-02.1 **Leden van bestuursorganen moeten kunnen aantonen dat ze een opleiding hebben gevolgd die hen een gedegen inzicht geeft in informatie- en cyberbeveiliging en risicobeheer, zodat ze informatie- en cyberbeveiligingsrisico's en de gevolgen daarvan kunnen beoordelen en de nodige risicobeperkende maatregelen kunnen voorstellen, rekening houdend met hun functies, verantwoordelijkheden en bevoegdheden.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat leden van leidinggevende organen in staat zijn weloverwogen beslissingen te nemen over cyberbeveiligingsrisico's en risicobeperkende strategieën door een fundamenteel begrip te ontwikkelen van informatiebeveiliging, cyberdreigingen en risicobeheerprincipes die relevant zijn voor hun leidinggevende functies.

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

- Training zou het management in staat kunnen stellen om cyberbeveiligingsrisico's te beoordelen, de mogelijke impact ervan te begrijpen en passende risicobeperkende maatregelen voor te stellen die aansluiten bij hun verantwoordelijkheden en bevoegdheden.
- De inhoud van de opleiding zou rekening kunnen houden met:
  - Kernbegrippen van informatie- en cyberbeveiliging
  - Risico-identificatie, -beoordeling en -beperking
  - Strategische besluitvorming in de context van cyberdreigingen
  - Herkennen van mogelijke beveiligingslacunes en verantwoordelijkheden op het gebied van beleid en toezicht
- De opleiding zou kunnen worden afgestemd op leidinggevende functies, waarbij gebruik zou kunnen worden gemaakt van de richtsnoeren van het Agentschap van de Europese Unie voor cyberbeveiliging (ENISA) inzake functieprofielen, met inbegrip van titels, opdrachten, taken, vaardigheden en competenties (zie European Cybersecurity Skills Framework Role Profiles).
- Er zou kunnen worden overwogen om jaarlijkse opfriscursussen te organiseren om bestaande praktijken te versterken en nieuwe ontwikkelingen op het gebied van cyberbeveiliging en risicobeheer te introduceren.

PR.AT-02.2 **Personen in gespecialiseerde functies moeten bewustmaking en opleiding krijgen voordat ze privileges krijgen, zodat ze over de kennis en vaardigheden beschikken om relevante taken uit te voeren met het oog op cyberbeveiligingsrisico's.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat personen in gespecialiseerde functies bewustmaking en opleiding op het gebied van cyberbeveiliging krijgen voordat geprivilegieerde toegang wordt verleend, zodat ze hun taken kunnen uitvoeren met een goed begrip van cyberbeveiligingsrisico's.

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

- De gespecialiseerde functies binnen de organisatie die aanvullende cybersecurityopleiding vereisen (bijv. fysiek en cybersecuritypersoneel, financieel personeel, mensen in managementfuncties en iedereen met toegang tot bedrijfskritieke gegevens) zouden formeel kunnen worden geïdentificeerd.
- Er zou op rollen gebaseerde cybersecuritybewustmaking en -opleiding kunnen worden gegeven aan iedereen in gespecialiseerde functies, inclusief aannemers, partners, leveranciers en andere derde partijen.
- Er zou voor kunnen worden gezorgd dat de opleiding wordt gegeven voordat toegang wordt verleend en dat deze is afgestemd op de specifieke risico's en verantwoordelijkheden van elke rol.
- Individuen zouden periodiek kunnen worden beoordeeld en getest op hun begrip van cyberbeveiligingspraktijken door middel van tests, simulaties of praktische evaluaties die relevant zijn voor hun functie.
- Er zou kunnen worden overwogen om jaarlijkse opfriscursussen te organiseren om bestaande praktijken te versterken en nieuwe praktijken te introduceren.
- Zowel informatietechnologie (IT) als operationele technologie (OT) zouden kunnen worden meegenomen, met name voor functies die te maken hebben met industriële systemen of kritieke infrastructuur.

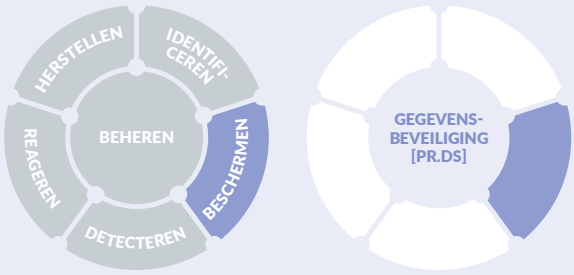
PR.AT-02.3 Bevoorrechte gebruikers moeten gekwalificeerd zijn voordat privileges worden toegekend, en deze gebruikers moeten kunnen aantonen dat ze hun rol, verantwoordelijkheden en bevoegdheden begrijpen.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat personen aan wie geprivilegieerde toegang is verleend, zowel in IT- als OT-omgevingen, aantoonbaar competent zijn en zich volledig bewust zijn van de verantwoordelijkheden, risico's en bevoegdheidsgrenzen op het gebied van cyberbeveiliging die aan hun functie verbonden zijn. Dit vermindert de kans op onopzettelijk misbruik of exploitatie van verhoogde privileges, met name in kritieke systemen waar de operationele continuïteit en veiligheid op het spel staan.

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

- Bevoorrechte gebruikers zouden op verschillende vlakken opgeleid kunnen worden om ervoor te zorgen dat ze hun verhoogde toegangsrechten op een veilige en verantwoordelijke manier gebruiken. De volgende opleidingsonderwerpen kunnen worden overwogen:
  - Beveiligingsbewustmaking: het is van cruciaal belang dat bevoorrechte gebruikers zich bewust zijn van de beveiligingsrisico's die gepaard gaan met hun verhoogde toegangsrechten. Dit omvat kennis over phishing, malware en andere cyberdreigingen.
  - Toegangsbeheer: gebruikers moeten begrijpen hoe ze hun toegangsrechten op de juiste manier kunnen beheren, onder meer door sterke wachtwoorden te gebruiken, meervoudige authenticatie toe te passen en de toegang te beperken tot wat nodig is voor hun functie.
  - Naleving en regelgeving: het is belangrijk dat bevoorrechte gebruikers op de hoogte zijn van relevante wet- en regelgeving, zoals GDPR, NIS2, DORA..., en hoe deze van invloed zijn op hun werk.
  - Incidentrespons: training in het reageren op beveiligingsincidenten is essentieel. Dit omvat het herkennen van verdachte activiteiten en weten hoe en aan wie deze moeten worden gemeld.
  - Best practices voor gegevensbeheer: gebruikers moeten worden opgeleid in het veilig opslaan, verwerken en overdragen van gevoelige gegevens.
  - Ethiek en verantwoordelijkheid: het is belangrijk dat bevoorrechte gebruikers zich bewust zijn van hun ethische verantwoordelijkheden en de mogelijke gevolgen van misbruik van hun toegangsrechten.
- Bevoorrechte gebruikers zouden periodiek kunnen worden beoordeeld en getest op hun kennis van cyberbeveiligingspraktijken voor hun gespecialiseerde functies.
- Er zou kunnen worden overwogen om jaarlijkse opfriscursussen te organiseren om bestaande praktijken te versterken en nieuwe praktijken te introduceren.



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-01.1 De organisatie moet controles uitvoeren op de integriteit van software, firmware en informatie, om ongeautoriseerde wijzigingen aan kritieke systeemcomponenten op te sporen tijdens opslag, transport, opstart en wanneer dit noodzakelijk wordt geacht.

Implementatierichtlijnen

Het doel van deze controle is om de integriteit en betrouwbaarheid van kritieke systeemcomponenten, zoals software, firmware en configuratiegegevens, te waarborgen door ongeoorloofde wijzigingen op te sporen die de operationele veiligheid, betrouwbaarheid of beveiliging in alle levensfasen, inclusief opslag, transport en opstarten, in gevaar kunnen brengen.

Om de integriteit van opgeslagen gegevens effectief te beschermen, moet de organisatie een gelaagde reeks controles implementeren die zijn ontworpen om ongeoorloofde wijzigingen aan opgeslagen gegevens, software en systeemcomponenten op te sporen en te voorkomen.

De volgende praktijken zouden overwogen kunnen worden:

- Cryptografische integriteitsmechanismen toepassen
  - Er zouden cryptografische hashes (bijv. SHA-256), digitale handtekeningen of andere cryptografische mechanismen (bijv. berichtverificatiecodes (MAC's)) kunnen worden gebruikt om de integriteit van opgeslagen gegevens en kritieke bestanden te verifiëren.
  - Integriteitswaarden zouden kunnen worden gegenereerd op het moment van opslag en geverifieerd voordat ze worden geopend of uitgevoerd.
- Geautomatiseerde integriteitsbewaking implementeren
  - Tools voor bestandsintegriteitsbewaking (FIM) zouden kunnen worden ingezet om continu wijzigingen in kritieke systeembestanden, configuraties en applicaties bij te houden.
  - Er zouden waarschuwingen kunnen worden gegenereerd voor ongeoorloofde of onverwachte wijzigingen en logboeken zouden kunnen worden bijgehouden voor controle en onderzoek.
- De integriteit van software en firmware valideren
  - Software en firmware die op systemen zijn opgeslagen, zouden vóór uitvoering kunnen worden gevalideerd met behulp van handtekeningverificatie of beveiligde opstartmechanismen.
  - Integriteitsvalidatie zou deel kunnen uitmaken van het opstartproces van het systeem en kunnen worden afgedwongen

- **Wijzigingsbeheer en toegangsbeperkingen afdwingen**
  - Schrijftoegang tot kritieke gegevens en systeemcomponenten zou kunnen worden beperkt door middel van op rollen gebaseerde toegangscontroles (RBAC) en het principe van minimale rechten.
  - Alle wijzigingen aan data-at-rest zouden kunnen worden onderworpen aan formele procedures voor wijzigingsbeheer en worden geregistreerd voor traceerbaarheid.
- **De integriteit van back-ups beschermen**
  - Back-ups zouden kunnen worden voorzien van mechanismen voor integriteitscontrole (bijv. checksums of digitale handtekeningen) om te garanderen dat ze niet zijn gemanipuleerd.
  - Er zouden regelmatig testherstelprocedures kunnen worden uitgevoerd om de integriteit en bruikbaarheid van back-upgegevens te controleren.

PR.DS-01.4 **De organisatie moet duidelijke beleidsregels en praktische maatregelen vastleggen en afdwingen om het gebruik van draagbare opslagmedia te beheren en te beperken, om zo het risico op datalekken, ongeautoriseerde toegang en het binnenbrengen van malware te verminderen.**

Implementatierichtlijnen

Het doel van deze controle is het risico op gegevenslekken, ongeoorloofde toegang en het binnenhalen van malware te verminderen door duidelijke beleidsregels en veiligheidsmaatregelen voor het gebruik van draagbare opslagmedia vast te stellen en te handhaven.

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

- **Beleid vaststellen en communiceren**
  - Er zou een gedocumenteerd beleid kunnen worden opgesteld voor het aanvaardbare gebruik van draagbare opslagmedia (bijv. USB-sticks, SD-kaarten, externe harde schijven).
  - Het beleid zou kunnen worden gecommuniceerd tijdens de introductie van nieuwe medewerkers en worden versterkt door middel van regelmatige opleidingen op het gebied van beveiligingsbewustmaking.
- **Het gebruik van apparaten controleren**
  - Alleen door de organisatie goedgekeurde draagbare opslagapparaten zouden gebruikt mogen worden.
  - Er zou een inventaris van goedgekeurde apparaten kunnen worden bijgehouden en gekoppeld aan specifieke gebruikers of afdelingen.
- **Praktische veiligheidsmaatregelen toepassen**
  - **Toegangscontrole**: apparaten zouden gebruikersauthenticatie kunnen vereisen (bijv. wachtwoordbeveiliging).
  - **Versleuteling**: gegevens op draagbare apparaten zouden kunnen worden versleuteld met behulp van hardwareversleutelde schijven of softwaretools zoals BitLocker To Go of VeraCrypt.
  - **Alleen-lezenmodus**: apparaten die worden gebruikt voor distributie (bijv. software-updates) zouden kunnen worden geconfigureerd als alleen-lezen.
  - **Malwarescans**: apparaten zouden voor en na gebruik kunnen worden gescand op malware.
  - **Fysieke beveiliging**: apparaten zouden veilig opgeborgen kunnen worden (bijvoorbeeld in afgesloten lades of kasten) wanneer ze niet worden gebruikt.
- **Gebruik controleren en registreren**
  - Op beheerde systemen zouden USB-apparaatverbindingen en bestandsoverdrachten kunnen worden geregistreerd met behulp van tools voor eindpuntbeheer.
  - Logs zouden periodiek kunnen worden gecontroleerd om ongeoorloofd gebruik of afwijkingen op te sporen.
- **Voorbeelden**
  - Een buitendiensttechnicus zou een door het bedrijf verstrekte, versleutelde USB-stick kunnen gebruiken om gegevens van externe sensoren te verzamelen. De stick zou vóór en na gebruik kunnen worden gescand en de gegevens zouden bij terugkomst naar een beveiligde server kunnen worden geüpload.
  - Een marketingteam zou een alleen-lezen USB-stick kunnen gebruiken om promotiemateriaal te verspreiden op een beurs, zodat er geen gegevens terug naar het apparaat kunnen worden gekopieerd.

PR.DS-01.5 **De organisatie mag het gebruik van verwijderbare media alleen toestaan wanneer dit absoluut noodzakelijk is en moet technische maatregelen nemen om de automatische uitvoering van bestanden vanaf deze apparaten te blokkeren.**

Implementatierichtlijnen

Het doel van deze controle is het minimaliseren van het aanvalsoppervlak in operationele en IT-omgevingen door het gebruik van verwijderbare media strikt te beperken en de automatische uitvoering van potentieel schadelijke bestanden te voorkomen.

Om het risico op malware-infecties en gegevenslekken via verwijderbare media (bijv. USB-sticks, externe schijven) te verminderen, zou de organisatie het volgende in overweging kunnen nemen:

- **Gebruik alleen toestaan wanneer dat noodzakelijk is**
  - De organisatie zou in haar beleid kunnen vermelden dat verwijderbare media alleen mogen worden gebruikt wanneer er geen veiliger alternatief beschikbaar is (bijv. beveiligde bestandsoverdracht).
  - Er zouden technische tools kunnen worden gebruikt om de toegang tot USB-poorten te beperken of om goedkeuring te vereisen voor gebruik.
- **Autorun en automatische uitvoering uitschakelen**
  - Alle systemen zouden zo kunnen worden geconfigureerd dat autorun- en autoplay-functies worden uitgeschakeld, zodat bestanden op verwijderbare media niet automatisch worden uitgevoerd.
  - Dit zou kunnen helpen voorkomen dat malware wordt uitgevoerd zonder dat de gebruiker iets doet.
- **Beveiligingstools gebruiken om de toegang te controleren**
  De organisatie zou eindpuntbeveiligingstools kunnen gebruiken om:
  - USB-toegang te blokkeren of te beperken.
  - Alleen goedgekeurde apparaten toe te staan.
  - Goedkeuring van de beheerder vereisen voor nieuwe apparaten.
- **Gebruik controleren en beoordelen**
  - Het gebruik van verwijderbare media zou kunnen worden bewaakt door apparaatverbindingen te registreren via tools voor eindpuntbeveiliging of logboeken van het besturingssysteem. In OT-omgevingen zouden handmatige registratie of gecontroleerde toegangsprocedures kunnen worden gebruikt. Logboeken zouden regelmatig kunnen worden gecontroleerd om ongeoorloofde activiteiten op te sporen.
- Voorbeeld: een financieel team zou versleutelde, door het bedrijf goedgekeurde USB-sticks kunnen gebruiken om gevoelige rapporten over te dragen. Deze sticks zouden vóór gebruik kunnen worden gescand, autorun zou op alle systemen kunnen worden uitgeschakeld en de toegang zou kunnen worden geregistreerd en gecontroleerd.

Verduidelijking van het verschil met PR.DS-01.4

- PR.DS-01.4 richt zich op het vaststellen van regels en procedures voor het gebruik van verwijderbare media (bijv. wie ze mag gebruiken, versleuteling, fysieke beveiliging).
- PR.DS-01.5 richt zich op de technische handhaving van die regels: hoe systemen moeten worden geconfigureerd om risico's te verminderen.

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.

PR.DS-11.2 De betrouwbaarheid en integriteit van back-ups moeten regelmatig worden gecontroleerd en getest.

Implementatiebegeleiding

Het doel van deze controle is ervoor te zorgen dat back-upgegevens betrouwbaar zijn en indien nodig met succes kunnen worden hersteld, ter ondersteuning van de bedrijfscontinuïteit en veerkracht.

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

- **Herstelprocedures te testen**
  Back-upherstelprocedures zouden regelmatig kunnen worden getest om te controleren of gegevens nauwkeurig en volledig kunnen worden hersteld.
- **De integriteit van back-ups te controleren**
  - Back-ups zouden vóór gebruik kunnen worden gecontroleerd op tekenen van compromittering, corruptie of manipulatie.
  - Integriteitscontroles zouden zich kunnen richten op indicatoren van beveiligingsinbreuken of gegevensverlies.
- **Testen te plannen**
  - Alle soorten gegevensbronnen zouden kunnen worden opgenomen in back-up- en hersteltests.
  - Testen zouden ten minste eenmaal per jaar kunnen plaatsvinden, of vaker op basis van steekproeven.
- **Af te stemmen op gerelateerde controles**
  Deze controle zou kunnen worden geïmplementeerd in samenwerking met RC.RP-05.1 (Herstelplanning), om consistentie in herstelstrategieën te waarborgen.

PR.DS-11.3 **De organisatie moet veilige back-ups van bedrijfskritieke gegevens bewaren op een aparte opslaglocatie om de beschikbaarheid van gegevens te garanderen in geval van systeemstoringen of gegevensverlies. Voor back-upopslag moeten dezelfde beveiligingsmaatregelen worden toegepast als voor de primaire omgeving.**

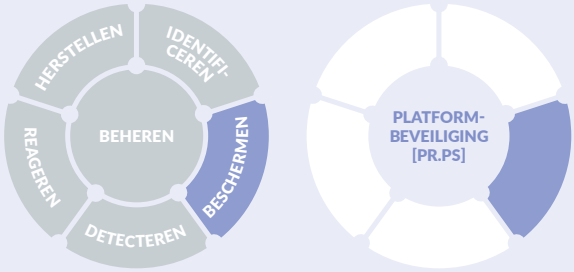
Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de organisatie haar bedrijfskritieke gegevens op betrouwbare wijze kan herstellen in twee belangrijke scenario's:

- **Natuurrampen of fysieke schade** aan de primaire locatie (waarvoor offsite of cloudgebaseerde back-ups nodig zijn).
- **Geavanceerde cyberaanvallen**, waaronder ransomware of bedreigingen van binnenuit, waarbij aanvallers kunnen proberen back-ups te beschadigen of te verwijderen (waardoor geïsoleerde of fraudebestendige back-ups nodig zijn).

Deze controle helpt ervoor te zorgen dat een organisatie haar kritieke gegevens kan herstellen als er iets misgaat. De controle is erop gericht back-ups gescheiden en net zo veilig te houden als de originele gegevens, waardoor deze vooral nuttig is voor organisaties die nog bezig zijn met het opbouwen van hun cyberbeveiligingscapaciteiten (organisaties met een minder matuur beveiligingsbeleid).

- **Te overwegen back-upstrategie**
- Om deze doelstellingen te bereiken, zou de organisatie een gediversifieerde en veerkrachtige back-upaanpak kunnen implementeren, zoals de 3-2-1-back-upregel:
  - Bewaar drie kopieën van bedrijfskritieke gegevens.
  - Sla deze kopieën op ten minste twee verschillende typen opslagmedia op (bijvoorbeeld een lokale schijf en een cloudopslag).
  - Zorg ervoor dat ten minste één kopie buiten het bedrijf of buiten het terrein wordt opgeslagen, op een fysiek gescheiden locatie.
- Om zich te beschermen tegen zowel fysieke als cyberdreigingen, zou de organisatie de volgende soorten back-ups kunnen overwegen:
  - **Offsite- of cloudback-ups:**
    Deze back-ups worden opgeslagen op een geografisch gescheiden locatie en helpen ervoor te zorgen dat gegevens kunnen worden hersteld in geval van natuurrampen of fysieke schade aan de primaire locatie.
  - **Onveranderlijke back-ups:**
    Dit zijn back-ups die gedurende een bepaalde periode niet kunnen worden gewijzigd of verwijderd. Ze zijn bijzonder effectief tegen ransomware en bedreigingen van binnenuit en kunnen worden geautomatiseerd om handmatige inspanningen te verminderen.
  - **Offline of air-gapped back-ups:**
    Dit zijn back-ups die worden opgeslagen op apparaten die volledig zijn losgekoppeld van elk netwerk, inclusief het internet. Deze isolatie zorgt ervoor dat zelfs als het netwerk van de organisatie wordt gecompromitteerd, de back-up onaangetast blijft.
- Aanvullende overwegingen
  - **Geografische scheiding**: back-uplocaties zouden zich in verschillende fysieke regio's kunnen bevinden om het risico van gelijktijdige impact van regionale rampen te verminderen.
  - **Gelijke beveiliging**: alle back-uplocaties zouden hetzelfde niveau van beveiligingsmaatregelen kunnen toepassen als de primaire omgeving (bijv. versleuteling, toegangscontrole, monitoring).
  - **Regelmatige tests**: back-up- en herstelprocedures zouden regelmatig kunnen worden getest om de integriteit van de gegevens en de operationele paraatheid te waarborgen.



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-01 Er worden configuratiebeheerpraktijken vastgesteld en toegepast

PR.PS-01.1 De organisatie moet een basisconfiguratie voor haar bedrijfskritieke systemen ontwikkelen, documenteren en onderhouden.

Implementatierichtlijnen

Deze controle zorgt ervoor dat alle bedrijfskritieke systemen in een bekende, veilige en goedgekeurde staat functioneren. Een basisconfiguratie definieert de standaardopstelling voor deze systemen, waardoor ongeoorloofde wijzigingen kunnen worden opgespoord, beveiligingsbeleid kan worden gehandhaafd en consistente bedrijfsvoering kan worden ondersteund.

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

- **Definiëren wat bedrijfskritiek is**
  Bedrijfskritieke systemen kunnen IT-, OT- (operationele technologie) en mogelijk IoT-componenten (internet of things) omvatten, mits deze essentiële bedrijfsfuncties ondersteunen:
  - IT-systemen worden doorgaans intern beheerd.
  - OT-systemen kunnen industriële controlesystemen omvatten.
  - IoT-systemen (bijv. sensoren, slimme apparaten) kunnen bedrijfskritiek zijn als hun uitval de bedrijfsvoering verstoort of veiligheidsrisico's met zich meebrengt.
- **Baselineconfiguraties vaststellen en onderhouden**
  Voor elk bedrijfskritiek systeem zou de baseline het volgende kunnen omvatten:
  - Systeemcomponenten (bijv. goedgekeurde software, hardware)
  - Versies van besturingssystemen en applicaties, inclusief patchniveaus
  - Configuratie-instellingen en parameters
  - Netwerktopologie, die laat zien hoe componenten zijn verbonden, inclusief:
    - Externe verbindingen
    - Servers die gevoelige gegevens of functies hosten
    - DNS- en beveiligingsdiensten
    - Logische plaatsing van componenten binnen de systeemarchitectuur
- **Beveiligingsprincipes toepassen**
  - Baselines zouden het principe van minimale functionaliteit kunnen afdwingen: alleen noodzakelijke functies en diensten zouden ingeschakeld worden.
  - Standaardinstellingen zouden gecontroleerd en aangepast kunnen worden om beveiligingsrisico's tijdens installatie of upgrades te verminderen.
- **Monitoren en bijwerken**
  - Systemen zouden continu kunnen worden gecontroleerd op afwijkingen van de goedgekeurde baseline.
  - Baselines zouden kunnen worden bijgewerkt wanneer systemen worden gepatcht, geüpgraded of opnieuw geconfigureerd.
- **Voor cloud- en door leveranciers beheerde systemen**
  Voor systemen die door derden worden beheerd (bijv. clouddiensten), zou ervoor gezorgd kunnen worden dat de basisverwachtingen contractueel zijn vastgelegd en dat leveranciers inzicht bieden in configuratie- en wijzigingsbeheer.

PR.PS-02 Software wordt onderhouden, vervangen en verwijderd in overeenstemming met het risico

PR.PS-02.1 De organisatie moet beperkingen opleggen aan het gebruik en de installatie van software en ervoor zorgen dat software wordt onderhouden, vervangen of verwijderd op basis van het daarmee samenhangende risico.

Implementatierichtlijnen

Het doel van deze controle is het verminderen van veiligheids- en operationele risico's door te controleren welke software wordt gebruikt, ervoor te zorgen dat deze goed wordt onderhouden en deze te verwijderen wanneer deze niet langer nodig is of wordt ondersteund.

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

- Alleen goedgekeurde software zou kunnen worden toegestaan, waarbij de toegang wordt beperkt op basis van de rollen en verantwoordelijkheden van gebruikers.
- Niet-ondersteunde of verouderde software zou kunnen worden vervangen om ongepatchte kwetsbaarheden te voorkomen.
- Ongebruikte of onnodige software, inclusief verouderde OS-hulpprogramma's, zou kunnen worden verwijderd om het aanvalsoppervlak te verkleinen.
- Patches zouden kunnen worden toegepast op basis van risico:
  - Kritieke kwetsbaarheden zouden binnen enkele uren kunnen worden gepatcht.
  - Routine-updates zouden volgens een vast schema kunnen worden uitgevoerd (bijvoorbeeld wekelijks of maandelijks).
- In containeromgevingen zouden alleen vertrouwde en up-to-date images kunnen worden gebruikt; verouderde containers zouden kunnen worden vervangen.
- Software en diensten die een onaanvaardbaar risico vormen, zoals FTP- of peer-to-peer-tools, zouden kunnen worden verwijderd of uitgeschakeld, tenzij deze expliciet vereist en beveiligd zijn.
- In ICS/OT-omgevingen zou PLC-programmering vooraf kunnen worden goedgekeurd en gepland; ad-hoc-wijzigingen zouden kunnen worden vermeden om de operationele veiligheid te beschermen.
- Een software-inventaris zou kunnen worden bijgehouden met versie- en ondersteuningsstatus.
- Procedures voor goedkeuring, patchen, vervangen en verwijderen van software zouden kunnen worden gedefinieerd.

PR.PS-03 Hardware wordt onderhouden, vervangen en verwijderd in overeenstemming met het risico

PR.PS-03.1 Hardware die wordt gebruikt in bedrijfskritieke omgevingen moet worden onderhouden, vervangen of verwijderd op basis van de bijbehorende beveiligings- en operationele risico's.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat hardware die wordt gebruikt in bedrijfskritieke omgevingen veilig, betrouwbaar en geschikt voor het beoogde doel blijft door deze te beheren op basis van operationele en veiligheidsrisico's.

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

- Hardware zou regelmatig kunnen worden beoordeeld om te controleren of deze de vereiste beveiligingsfuncties ondersteunt (bijv. versleuteling, veilig opstarten, firmware-updates); hardware die niet aan deze eisen voldoet, zou kunnen worden vervangen.
- Hardware die aan het einde van zijn levensduur is of niet meer wordt ondersteund, zou op een gecontroleerde manier kunnen worden uitgefaseerd.
- Een levenscyclusplan voor hardware zou kunnen worden opgesteld en bijgehouden, met inbegrip van:
  - Voorraadbeheer
  - Tijdschema's voor het einde van de levensduur
  - Vervangingsschema's
  - Veilige verwijderingsprocedures
- Preventief onderhoud zou kunnen worden uitgevoerd en onderdelen zouden tijdig kunnen worden vervangen om onverwachte storingen te voorkomen die van invloed kunnen zijn op de bedrijfsvoering of de veiligheid.
- Er zou voor kunnen worden gezorgd dat de hardware veilige, up-to-date software kan ondersteunen; eventuele beperkingen die dit verhinderen zouden kunnen worden aangepakt.

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-04.2 De organisatie moet ervoor zorgen dat logboekregistraties een betrouwbare tijdbron of interne kloktijdstempel bevatten die wordt vergeleken en gesynchroniseerd met een gezaghebbende tijdsbron.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat logboekregistraties in alle systemen een consistente en betrouwbare tijdsreferentie gebruiken, zodat gebeurtenissen nauwkeurig kunnen worden gevolgd en gecorreleerd.

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

- Een betrouwbare tijdsreferentie te gebruiken, zoals een GPS-klok, interne tijdserver of andere betrouwbare bron, om de systeemklokken te synchroniseren.
- Systemen zo te configureren dat hun klokken regelmatig zouden kunnen worden bijgewerkt om tijdsafwijkingen te voorkomen.
- Meerdere tijdbronnen in te stellen om redundantie en nauwkeurigheid te garanderen.
- De synchronisatiestatus te controleren en waarschuwingen te activeren als systemen niet meer synchroon lopen.
- Procedures voor tijdsynchronisatie te documenteren, inclusief serverinstellingen, update-intervallen en bewakingsprocessen.

PR.PS-04.3 Auditgegevens van de kritieke systemen van de organisatie moeten worden verplaatst naar een alternatief systeem.

Implementatierichtlijnen

Het doel van deze controle is om de integriteit van auditgegevens te beschermen door ze over te brengen van kritieke systemen naar een aparte, beveiligde locatie waar ze niet kunnen worden gewijzigd of gemanipuleerd.

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

- Auditgegevens over te zetten naar een apart systeem waar records niet kunnen worden gewijzigd door gebruikers of diensten van het oorspronkelijke systeem.
- Ervoor te zorgen dat het doelsysteem auditgegevens ongewijzigd houdt nadat ze zijn opgeslagen.
- De impact van logboekoverdrachten te monitoren om prestatieproblemen op de bronsystemen te voorkomen.
- Maatregelen te nemen die de gegevens beschermen zonder de systeemwerking te vertragen of te verstoren.

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.

PR.PS-05.2 De installatie en uitvoering van niet-geautoriseerde software moet worden voorkomen.

Implementatierichtlijnen

Het doel van deze controle is het risico op compromittering te verminderen door ervoor te zorgen dat alleen vertrouwde en goedgekeurde software op systemen wordt geïnstalleerd en uitgevoerd.

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

- De installatie en uitvoering van software zou kunnen worden beperkt tot vooraf goedgekeurde applicaties en omgevingen.
- Platforms zouden zo geconfigureerd kunnen worden dat ongeautoriseerde software wordt geblokkeerd en de uitvoering ervan wordt beperkt wanneer het risico dit rechtvaardigt.
- De bron en integriteit van alle nieuwe software zou vóór de installatie gecontroleerd kunnen worden.
- Toegang tot schadelijke websites zou kunnen worden geblokkeerd met behulp van vertrouwde en goedgekeurde internetfilterservices die zijn ontworpen om bekende online bedreigingen te detecteren en te stoppen.
- Waar mogelijk zouden systemen zo geconfigureerd kunnen worden dat alleen door de organisatie goedgekeurde software kan worden geïnstalleerd.

PR.PS-06 Veilige softwareontwikkelingspraktijken zijn geïntegreerd en hun prestaties worden gedurende de gehele softwareontwikkelingscyclus bewaakt.

PR.PS-06.1 **Beveiliging moet in aanmerking worden genomen gedurende de volledige levenscyclus van systemen en applicaties, ongeacht of deze intern zijn ontwikkeld of extern zijn aangekocht.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat beveiliging vanaf het begin in systemen en applicaties is ingebouwd en gedurende hun hele levensduur – van ontwerp tot buitengebruikstelling – wordt gehandhaafd, ongeacht of ze intern zijn ontwikkeld of extern zijn aangeschaft.

Om dit doel te bereiken:

- **Startfase**: Beveiligingsvereisten zouden in een vroeg stadium kunnen worden gedefinieerd, risico's zouden kunnen worden geïdentificeerd en relevante belanghebbenden, waaronder beveiligingsexperts, zouden vanaf het begin kunnen worden betrokken.
- **Aankoop- of ontwikkelingsfase**
  - Voor aangeschafte oplossingen: leveranciers zouden veilige ontwikkelingspraktijken kunnen volgen, bewijs van testen kunnen leveren en kunnen voldoen aan contractuele beveiligingsvereisten.
  - Voor interne ontwikkeling: er zouden veilige coderingspraktijken kunnen worden toegepast, wijzigingen zouden beheerd kunnen worden en beveiligingstests zouden kunnen worden uitgevoerd.
- **Implementatiefase**: Systemen zouden vóór de implementatie veilig geconfigureerd kunnen worden, met toegangscontroles en versleuteling om gevoelige gegevens te beschermen.
- **Exploitatie- en onderhoudsfase**: Systemen zouden gecontroleerd kunnen worden op incidenten, regelmatig kunnen worden bijgewerkt en beveiligingsmaatregelen zouden indien nodig kunnen worden herzien en verbeterd.
- **Verwijderingsfase**: Systemen zouden veilig buiten gebruik kunnen worden gesteld, gevoelige gegevens zouden verwijderd kunnen worden en geleerde lessen zouden kunnen worden gedocumenteerd om toekomstige processen te verbeteren.

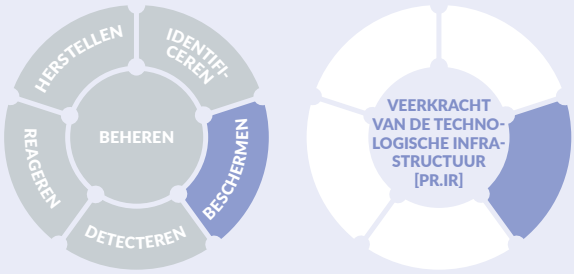
PR.PS-06.2 **Wijzigingen en uitzonderingen moeten worden getest en gevalideerd voordat ze in operationele systemen worden geïmplementeerd.**

Implementatierichtlijnen

Het doel van deze controle is het risico op verstoringen of kwetsbaarheden te verminderen door ervoor te zorgen dat alle wijzigingen en uitzonderingen naar behoren worden getest en gevalideerd voordat ze worden toegepast op operationele systemen.

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

- Alle voorgestelde wijzigingen en uitzonderingen zouden een formeel proces kunnen doorlopen dat documentatie, beoordeling, testen en goedkeuring omvat.
- De potentiële risico's van het al dan niet toepassen van een wijziging zouden kunnen worden beoordeeld en vastgelegd.
- Uitzonderingen, gedefinieerd als goedgekeurde afwijkingen van standaardbeleidsregels of -procedures, zouden kunnen worden geëvalueerd met een duidelijk inzicht in de risico's en een duidelijk plan om deze te verminderen of te beheersen.
- Geaccepteerde risico's zouden periodiek kunnen worden geëvalueerd om te bevestigen dat het oorspronkelijke besluit om ze te accepteren nog steeds geldig is, met name als de omstandigheden veranderen of als de acceptatie gebaseerd was op toekomstige acties of mijlpalen.
- Deze praktijken zouden kunnen worden aangepast aan de operationele omgeving om ongeplande downtime of veiligheidsproblemen te voorkomen, met name in OT-systemen.



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.

PR.IR-01.3 **Om de operationele stabiliteit en veiligheid te waarborgen, moet de organisatie zonder uitzondering alle verbindingen tussen onderdelen van haar kritieke systemen identificeren, documenteren en beheersen.**

Implementatierichtlijnen

Het doel van deze controle is het handhaven van operationele stabiliteit en veiligheid door ervoor te zorgen dat alle verbindingen tussen componenten van kritieke systemen bekend zijn, gedocumenteerd worden en actief worden beheerd.

In OT-omgevingen kunnen niet-gedocumenteerde of ongecontroleerde verbindingen – fysiek, draadloos of logisch – kwetsbaarheden introduceren, processen verstoren of veiligheidsmechanismen omzeilen.

Om netwerkverbindingen tussen systeemcomponenten effectief te beheren en te beveiligen, zouden de volgende praktijken in overweging genomen kunnen worden:

- **Configuratiebeheer**
  Organisaties zouden configuratiebeheerprocessen kunnen implementeren om ervoor te zorgen dat alle wijzigingen in netwerkverbindingen worden gedocumenteerd, beoordeeld en goedgekeurd. Configuratiebestanden en logboeken zouden actueel kunnen worden gehouden en veilig kunnen worden bewaard.
- **Toegangscontroles**
  Er zouden strikte toegangscontroles kunnen worden toegepast om ervoor te zorgen dat alleen bevoegd personeel de netwerkconfiguraties kan wijzigen. Er zou gebruik kunnen worden gemaakt van op rollen gebaseerde toegangscontrole (RBAC) om de toegang te beperken op basis van functieverantwoordelijkheden en operationele behoeften.
- **Regelmatige audits**
  Er zouden regelmatig audits kunnen worden uitgevoerd om te controleren of alle gedocumenteerde verbindingen nog steeds correct zijn en of er geen ongeoorloofde wijzigingen zijn aangebracht. De resultaten van de audits zouden kunnen worden gebruikt om de documentatie bij te werken en de controles te versterken.
- **Koppeling met assetbeheer (ID.AM)**
  Verbindingen tussen systeemcomponenten zouden kunnen worden gedocumenteerd onder ID.AM (Asset Management) en bewaakt onder deze vereiste (PR.IR-01.3) om consistentie, traceerbaarheid en afdwingbaarheid binnen de cyberbeveiligingsarchitectuur van de organisatie te waarborgen.

PR.IR-01.4 De organisatie moet passende maatregelen nemen om communicatie te bewaken en te controleren aan externe en belangrijke interne grenzen van kritieke systemen, inclusief de verbindingen tussen IT- en OT-domeinen, om veilige en betrouwbare werking te garanderen .

Implementatierichtlijnen

Het doel van deze controle is om veilige en betrouwbare activiteiten te garanderen door actief toezicht te houden op en controle uit te oefenen op de communicatie aan belangrijke netwerkgrenzen, met name waar kritieke systemen in contact staan met externe netwerken of minder betrouwbare interne zones.

In OT-omgevingen, waar legacy-systemen vaak geen ingebouwde beveiliging hebben, is grensbeveiliging essentieel om ongeoorloofde toegang te voorkomen, potentiële bedreigingen in te dammen en de procesintegriteit in IT- en OT-domeinen te handhaven.

Om dit doel te bereiken, zou rekening gehouden kunnen worden met het volgende:

- **Apparaten die communicatie aan netwerkgrenzen bewaken en beschermen**
  Firewalls, beveiligingsgateways en routers zouden kunnen worden ingezet op externe en interne grenzen om beleid voor het filteren en routeren van verkeer af te dwingen. Deze apparaten zouden kunnen werken volgens het model *'standaard weigeren, uitzonderingen toestaan'*.
- **Zonering en isolatie in OT-omgevingen**
  In OT-omgevingen zou grensbeveiliging een strikte scheiding tussen besturingssystemen en externe netwerken kunnen omvatten. Zones zouden kunnen worden gedefinieerd op basis van kriticiteit en vertrouwen, en de communicatie tussen zones zou streng gecontroleerd en bewaakt kunnen worden.
- **Unidirectionele gateways (datadiodes)**
  Wanneer gegevens van beveiligde OT-systemen naar externe bestemmingen (bijv. clouddiensten of regelgevende instanties) moeten worden verzonden, zouden unidirectionele gateways kunnen worden gebruikt om inkomende bedreigingen te voorkomen en tegelijkertijd uitgaande gegevensoverdracht mogelijk te maken.
- **Versleutelde communicatie**
  Communicatie over grenzen heen zou kunnen worden versleuteld met behulp van veilige protocollen (bijv. VPN's, TLS) om gegevens tijdens het transport te beschermen en de vertrouwelijkheid en integriteit te waarborgen.

- **Inbraakdetectie en -preventie**
  Inbraakdetectie - en preventiesystemen (IDPS) zouden kunnen worden ingezet op belangrijke grenzen om het verkeer te controleren op afwijkingen, ongeoorloofde toegangspogingen te detecteren en kwaadwillige activiteiten te blokkeren.
- **Handhaving van toegangscontrole**
  De toegang tot grensapparatuur en communicatiekanalen zou kunnen worden beperkt tot bevoegd personeel. Het zou overwogen kunnen worden om oplossingen voor netwerktoegangscontrole (NAC) in te zetten om apparaat- en gebruikersauthenticatie bij toegangspunten af te dwingen.
- **Continue monitoring en patching**
  Grensapparatuur en communicatiekanalen zouden continu gecontroleerd kunnen worden op verdachte activiteiten. Alle systemen die zijn blootgesteld aan externe of interzonale communicatie zouden regelmatig kunnen worden bijgewerkt en gepatcht om bekende kwetsbaarheden aan te pakken.

PR.IR-02 De technologische middelen van de organisatie worden beschermd tegen bedreigingen vanuit de omgeving

PR.IR-02.1 De organisatie moet beleid en procedures definiëren, implementeren en onderhouden met betrekking tot nood- en veiligheidssystemen, brandbeveiligingssystemen en omgevingscontroles voor haar kritieke systemen.

Implementatierichtlijnen

Het doel van deze controle is om kritieke systemen te beschermen tegen omgevingsrisico's en noodsituaties die de bedrijfsvoering kunnen verstoren, apparatuur kunnen beschadigen of de veiligheid in gevaar kunnen brengen, met name in OT-omgevingen waar fysieke omstandigheden een directe invloed hebben op de beschikbaarheid van systemen en de veiligheid van personen.

Om dit doel te bereiken, zou de organisatie het volgende kunnen overwegen:

- **Risicobeoordelingen uitvoeren** van alle locaties waar kritieke systemen zijn ondergebracht zouden kunnen worden uitgevoerd om milieurisico's en noodrisico's in kaart te brengen.
- Er zouden **beleid en procedures** kunnen worden vastgesteld voor brandbeveiliging, noodhulp en milieucontroles.
- **Bewakingssystemen** zoals sensoren voor temperatuur, vochtigheid, rook en waterlekkage zouden kunnen worden **geïnstalleerd**, met waarschuwingen voor abnormale omstandigheden.
- **Brandbeveiligingsmaatregelen zouden geïmplementeerd kunnen worden**, waaronder geschikte blussystemen (bijvoorbeeld op gasbasis voor datacenters), alarmen, detectoren en brandblussers.
- **Brandveiligheids- en milieusystemen**, waaronder HVAC en noodverlichting, zouden regelmatig kunnen worden **geïnspecteerd en onderhouden**.
- **Milieubeschermingsvereisten** zouden kunnen worden opgenomen in contracten met derden, waarbij bewijs van naleving en onderhoud wordt gevraagd.
- **Het personeel** zou **opgeleid** kunnen worden in noodprocedures en minstens één keer per jaar evacuatie- en brandbestrijdingsoefeningen kunnen uitvoeren.

PR.IR-04 Voldoende middelencapaciteit om de beschikbaarheid te waarborgen

PR.IR-04.1 **Een adequate planning van de benodigde middelen moet ervoor zorgen dat de beschikbaarheid van de kritieke systemen van de organisatie voor informatieverwerking, netwerken, telecommunicatie en gegevensopslag gewaarborgd blijft.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat kritieke systemen altijd beschikken over voldoende rekenkracht, opslagcapaciteit en netwerkbronnen, door tijdig te plannen voor zowel huidige als toekomstige capaciteitsbehoeften.

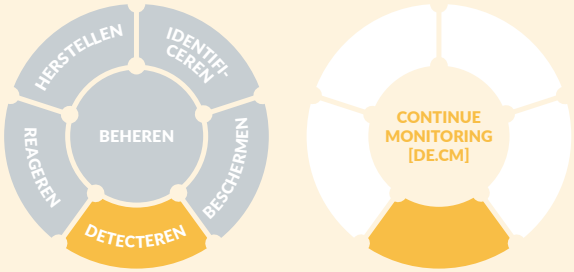
Om dit doel te bereiken, zou de organisatie het volgende kunnen overwegen:

- **Voorspellen en plannen**
  De benodigde middelen kunnen regelmatig worden voorspeld op basis van bedrijfsgroei, terugkerende piekperiodes en gebruikstrends. Toekomstige vraag naar rekenkracht, opslag en netwerkcapaciteit kan tijdig worden ingeschat om prestatieproblemen of uitval te voorkomen.
- **Rekening houden met doorlooptijden voor aankopen**
  Bij capaciteitsplanning zou rekening kunnen worden gehouden met mogelijke vertragingen in de levering van hardware of diensten als gevolg van verstoringen in de toeleveringsketen of geopolitieke ontwikkelingen. Er zou buffercapaciteit kunnen worden aangehouden om onverwachte vraag of vertragingen bij uitbreiding op te vangen.
- **Monitoren en drempels instellen**
  Systemen zouden continu gecontroleerd kunnen worden om het gebruik bij te houden. Er zouden drempels en waarschuwingen kunnen worden geconfigureerd om tijdig schaalvergrotingsmaatregelen te nemen voordat de prestaties worden beïnvloed.
- **Componenten gebruiken met hoge beschikbaarheid**
  Redundante componenten (bijv. RAID-arrays, dubbele netwerkinterfaces, noodstroomvoorziening) zouden kunnen worden ingezet om downtime als gevolg van hardwarestoringen te verminderen. Deze zouden een aanvulling kunnen vormen op capaciteitsplanning en deze niet vervangen.
- **Regelmatig controleren en aanpassen**
  Capaciteitsplannen zouden periodiek kunnen worden herzien en bijgewerkt op basis van veranderingen in de bedrijfsstrategie, technologie of externe risicofactoren.


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-01.3 De organisatie moet het ongeoorloofd gebruik van haar bedrijfskritieke systemen monitoren en identificeren door het detecteren van ongeautoriseerde lokale, netwerk- en externe verbindingen.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de organisatie ongeoorloofde toegang tot of misbruik van haar bedrijfskritieke systemen kan detecteren en hierop kan reageren. Dit omvat het identificeren van verdachte lokale, netwerk- of externe verbindingen die kunnen wijzen op een inbreuk op de beveiliging of misbruik van gevoelige systemen.

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

- Het monitoren van netwerkcommunicatie zou kunnen plaatsvinden aan de externe grens van de bedrijfskritieke systemen van de organisatie en aan belangrijke interne grenzen binnen die systemen.
- Faciliteiten zouden gecontroleerd kunnen worden op ongeoorloofde of malafide draadloze netwerken waarmee aanvallers de normale controles zouden kunnen omzeilen.
- Kritieke netwerkdiensten zoals Domain Name System (DNS – dat websitenamen vertaalt naar IP-adressen), Border Gateway Protocol (BGP – dat helpt bij het routeren van internetverkeer) en andere netwerkdiensten zouden gecontroleerd kunnen worden op tekenen van manipulatie of misbruik.
- Bij het hosten van applicaties die toegankelijk zijn vanaf het internet zou een Web Application Firewall (WAF) kunnen worden overwogen om bescherming te bieden tegen aanvallen. Als de applicatie niet web gebaseerd is, zou deze beschermd kunnen worden met behulp van andere geschikte methoden, zoals een Identity Provider (IdP) om de toegang te controleren.

DE.CM-02 De fysieke omgeving wordt gemonitord om potentieel ongewenste gebeurtenissen op te sporen.

DE.CM-02.1 De fysieke omgeving moet worden bewaakt om potentieel ongewenste gebeurtenissen op te sporen.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat de fysieke ruimtes waar kritieke systemen en gegevens zich bevinden, worden gecontroleerd op tekenen van verdachte of schadelijke activiteiten. Dit helpt bij het opsporen van potentiële bedreigingen, zoals ongeoorloofde toegang, manipulatie of andere ongebruikelijke gebeurtenissen in de fysieke omgeving.

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

- Logboeken van fysieke toegangssystemen (zoals badgelezers) zouden kunnen worden gecontroleerd om ongebruikelijke patronen op te sporen, zoals iemand die op ongebruikelijke tijdstippen probeert binnen te komen of herhaaldelijk mislukte pogingen om toegang te krijgen tot een beperkt toegankelijk gebied.
- Registraties van bezoekers (zoals inschrijfformulieren of digitale check-ins) zouden regelmatig kunnen worden gecontroleerd om ervoor te zorgen dat alleen geautoriseerde personen beveiligde zones hebben betreden.
- Fysieke beveiligingsapparatuur (zoals sloten, deursluitingen, scharnierpennen en alarmen) zou kunnen worden gecontroleerd op tekenen van manipulatie of schade die zouden kunnen wijzen op een poging tot inbraak.

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.

DE.CM-03.2 Eindpunt- en netwerkbeveiligingstools die het gedrag van eindgebruikers monitoren op gevaarlijke activiteiten moeten worden beheerd.

Implementatierichtlijnen

Deze controle bouwt voort op DE.CM-03.1 door de focus te verleggen van implementatie naar continu beheer van monitoringtools. Het doel van deze controle is ervoor te zorgen dat tools die worden gebruikt om gebruikersgedrag te monitoren en schadelijke activiteiten op apparaten en netwerken te detecteren, goed worden onderhouden en actief worden beheerd. Dit ondersteunt de voortdurende effectiviteit van de tools naarmate bedreigingen zich ontwikkelen, en zorgt ervoor dat de waarschuwingen die ze genereren nauwkeurig, relevant en nuttig zijn voor het identificeren van echte beveiligingsrisico's.

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

- Tools die apparaten zoals laptops, mobiele telefoons en servers monitoren, zouden regelmatig kunnen worden gecontroleerd om te bevestigen dat ze correct werken, worden bijgewerkt met de nieuwste informatie over bedreigingen en in staat zijn om nieuwe soorten aanvallen te detecteren.
- Er zou een centraal systeem kunnen worden gebruikt om logboeken uit verschillende bronnen te verzamelen en te analyseren. Deze logboeken zouden volledig en up-to-date moeten zijn en bruikbaar kunnen zijn voor het identificeren van verdachte activiteiten.
- Logs met betrekking tot systeemtoegang, zoals inlogpogingen of toegang buiten de normale uren, zouden regelmatig kunnen worden gecontroleerd. Er zouden waarschuwingen kunnen worden ingesteld om beveiligingsteams op de hoogte te brengen van ongebruikelijke patronen.
- Tools die het gedrag van gebruikers analyseren, zouden in de loop van de tijd kunnen worden verfijnd. Beveiligingsteams zouden waarschuwingen kunnen controleren, detectieregels aanpassen om valse alarmen te verminderen en de nauwkeurigheid verbeteren.
- Misleidende tools, zoals nep-systemen of -bestanden die zijn ontworpen om aanvallers aan te trekken, zouden nauwlettend kunnen worden gecontroleerd. Waarschuwingen van deze tools zijn vaak vroege tekenen van een echte aanval en zouden als hoge prioriteit kunnen worden behandeld.
- Beveiligingsteams zouden regelmatig kunnen beoordelen hoe goed alle monitoringtools presteren, detectieregels bijwerken en ervoor zorgen dat de tools zijn geïntegreerd in incidentresponsprocessen.
- De rollen en verantwoordelijkheden voor het monitoren van en reageren op waarschuwingen zouden duidelijk kunnen worden gedefinieerd. Het personeel zou kunnen worden opgeleid om de tools effectief te gebruiken en adequaat te reageren op incidenten.

DE.CM-06 Activiteiten en diensten van externe dienstverleners worden gemonitord om potentieel ongewenste gebeurtenissen op te sporen

DE.CM-06.1 De activiteiten en diensten van externe dienstverleners moeten worden beveiligd en gemonitord om potentieel ongewenste gebeurtenissen op te sporen.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat activiteiten die worden uitgevoerd door externe dienstverleners, zowel op afstand als ter plaatse, veilig worden beheerd en continu worden gemonitord. Dit helpt bij het opsporen van ongebruikelijke of schadelijke acties die van invloed kunnen zijn op de systemen, gegevens of diensten van de organisatie.

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

- Externe dienstverleners zouden kunnen bestaan uit aannemers, leveranciers van clouddiensten, IT-ondersteuningsteams.
- De monitoring zou zich kunnen richten op:
  - Toegangs- en inlogactiviteiten, inclusief hoe en wanneer externe gebruikers verbinding maken met systemen.
  - Gegevensoverdracht en netwerkverkeer, om ongebruikelijke of ongeoorloofde informatieverplaatsingen op te sporen.
  - Systeemwijzigingen, zoals software-updates of configuratieaanpassingen door externe partijen.
- Alle activiteiten op afstand en ter plaatse door externe leveranciers zouden kunnen worden geregistreerd en gecontroleerd om ongeoorloofde acties of risicovol gedrag te identificeren.
- Clouddiensten en internetproviders zouden kunnen worden gecontroleerd op onverwacht gedrag of prestatieproblemen die zouden kunnen wijzen op een beveiligingsprobleem.
- Er zou een gecentraliseerd registratiesysteem kunnen worden gebruikt om gegevens van alle externe diensten te verzamelen en te analyseren.
- Alle beveiligingsincidenten waarbij externe leveranciers betrokken zijn, zoals malware-infecties, phishingpogingen of ongeoorloofde toegang, zouden vroegtijdig kunnen worden gedetecteerd, snel kunnen worden gemeld en effectief kunnen worden aangepakt.

DE.CM-06.2 De naleving door externe dienstverleners van personeelsbeveiligingsbeleid, procedures en contractuele beveiligingseisen moet worden gemonitord in verhouding tot hun cyberbeveiligingsrisico's.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat externe dienstverleners het personeelsbeveiligingsbeleid en de contractvereisten van de organisatie naleven, vooral wanneer ze toegang hebben tot gevoelige systemen of gegevens. Dit helpt het risico op beveiligingsincidenten veroorzaakt door personeel van derden te verminderen en zorgt ervoor dat dienstverleners aan dezelfde normen worden gehouden als intern personeel.

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

- Externe leveranciers zouden duidelijk omschreven beveiligingsverantwoordelijkheden kunnen hebben, die zijn vastgelegd in contracten of service level agreements.
- Contracten zouden vereisten kunnen bevatten zoals:
  - Achtergrondcontroles van het personeel van de leverancier
  - Ondertekening van geheimhoudingsovereenkomsten
  - Naleving van beleid inzake aanvaardbaar gebruik
- De naleving van deze vereisten zou regelmatig kunnen worden bewaakt, met inbegrip van controles op voltooide beveiligingsopleidingen en ondertekende overeenkomsten.

- Leveranciers zouden verplicht kunnen worden om de organisatie onmiddellijk op de hoogte te stellen wanneer personeel met toegang tot het systeem wordt overgeplaatst of hun functie verlaat, zodat toegangsrechten onverwijld kunnen worden ingetrokken.
- Er zouden periodieke audits kunnen worden uitgevoerd om te controleren of providers het beveiligingsbeleid naleven. Deze zouden het volgende kunnen omvatten:
  - Het controleren van toegangslogboeken en machtigingen
  - Controle van onboarding- en offboardingprocedures
  - Ervoor zorgen dat alleen bevoegde personen toegang hebben tot kritieke systemen
- Eventuele problemen of gevallen van niet-naleving zouden kunnen worden gedocumenteerd, gemeld en aangepakt door middel van corrigerende maatregelen en vervolgcontroles.

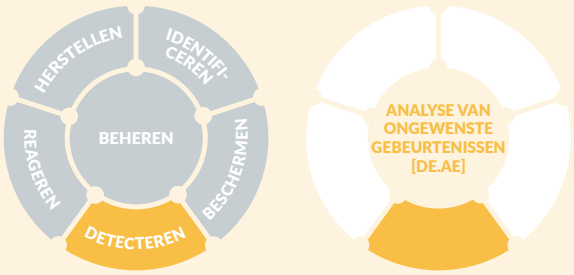
DE.CM-09 Computerhardware en -software, runtime-omgevingen en hun gegevens worden gemonitord om potentieel ongewenste gebeurtenissen op te sporen

DE.CM-09.1 **De organisatie moet computerhardware, software, runtime-omgevingen en hun gegevens monitoren om potentieel ongewenste gebeurtenissen op te sporen.**

Implementatierichtlijnen

Deze controle heeft tot doel ervoor te zorgen dat organisaties hun computersystemen en gegevens continu monitoren om potentieel schadelijke gebeurtenissen vroegtijdig op te sporen. Dit helpt om het overzicht te behouden, tijdige reacties te ondersteunen en het risico op beveiligingsincidenten te verminderen.

Om het doel van deze controle te bereiken, zou de organisatie het volgende kunnen overwegen:
- Systeemlogging zou kunnen worden ingeschakeld op computers en servers om belangrijke gebeurtenissen vast te leggen.
- Ingebouwde antivirussoftware of eindpuntbeveiliging zou kunnen worden gebruikt om bedreigingen te detecteren en waarschuwingen te genereren.
- Logboeken en waarschuwingen zouden regelmatig kunnen worden gecontroleerd om ongebruikelijke activiteiten of fouten op te sporen.
- Logboeken zouden kunnen worden opgeslagen in een gedeelde map of eenvoudige logboekviewer om ze gemakkelijker toegankelijk en te controleren te maken.
- Er zou een routine kunnen worden ingesteld (bijvoorbeeld wekelijks of maandelijks) om logboeken te controleren en monitoringtools bij te werken.
- Er zou iemand kunnen worden aangewezen die verantwoordelijk is voor de monitoring, ook al is het een parttimefunctie.



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

DE.AE-02 Potentieel ongewenste gebeurtenissen worden geanalyseerd om meer inzicht te krijgen in de bijbehorende activiteiten.

DE.AE-02.1 Cybersecurity- en informatiebeveiligingsgebeurtenissen moeten worden beoordeeld en geanalyseerd om potentiële aanvalsdoelen en -methoden te identificeren, in overeenstemming met de toepasselijke wetten, voorschriften, normen en beleidsregels.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat cyberbeveiligings- en informatiebeveiligingsgebeurtenissen worden beoordeeld en geanalyseerd om aanvalsdoelen en -methoden op te sporen. Hierdoor kunnen organisaties effectief reageren op bedreigingen en tegelijkertijd voldoen aan wettelijke, regelgevende en beleidsvereisten.

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

- Organisaties zouden bij het beoordelen van beveiligingsincidenten de relevante federale en regionale wetten, branchevoorschriften, normen en interne beleidsregels kunnen naleven.
- Logboekanalysetools zouden kunnen worden gebruikt om rapporten te genereren en verdachte activiteiten te identificeren.
- Systeem- en applicatielogboeken zouden regelmatig kunnen worden beoordeeld om tekenen van beveiligingsrisico's op te sporen, zoals herhaalde mislukte inlogpogingen of ongebruikelijke gegevensoverdrachten.
- Logs zouden kunnen worden geanalyseerd op patronen die zouden kunnen wijzen op pogingen tot of aanhoudende aanvallen.
- Er zou gebruik kunnen worden gemaakt van dreigingsinformatie om op de hoogte te blijven van nieuwe dreigingen en aanvalstechnieken, en de beveiligingsmaatregelen zouden dienovereenkomstig kunnen worden aangepast.
- Er zouden regelmatig audits en beoordelingen kunnen worden uitgevoerd om de beveiligingsstatus van de organisatie te evalueren.
- De resultaten van deze audits zouden kunnen worden gebruikt om de monitoring en analyse te verbeteren.

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.

DE.AE-03.2 De organisatie moet ervoor zorgen dat gebeurtenisgegevens van kritieke systemen worden verzameld en gecombineerd met informatie uit meerdere relevante bronnen.

Implementatierichtlijnen

Het doel van deze controle is om de organisatie in staat te stellen complexe of verspreide bedreigingen te detecteren door gebeurtenisgegevens uit verschillende systemen en bronnen te combineren en te analyseren. Door deze gegevens te correleren, kunnen patronen worden geïdentificeerd die mogelijk niet zichtbaar zijn wanneer systemen afzonderlijk worden bewaakt.

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

- Relevante bronnen van gebeurtenisgegevens zouden onder meer systeemlogboeken, auditlogboeken, netwerkmonitoringtools, fysieke toegangsregistraties en rapporten van gebruikers of beheerders kunnen zijn.
- Loggegevens zouden continu, idealiter in realtime of bijna realtime, naar een gecentraliseerd systeem kunnen worden gestuurd voor opslag en analyse. Dit zou het vermogen kunnen verbeteren om patronen te detecteren en snel te reageren op mogelijke problemen.
- Het centraliseren van logboeken op een klein aantal speciale servers of platforms, zoals een SIEM, lichte logboekbeheertools, cloudgebaseerde logboekdiensten of beheerde detectiediensten (vaak onderdeel van Managed Detection and Response, of MDR), zou een efficiënte analyse en correlatie van gebeurtenissen tussen systemen kunnen ondersteunen.
- Cyberdreigingsinformatie zou kunnen worden gebruikt om de correlatie tussen gebeurtenissen te verbeteren door context te bieden over bekende dreigingen, aanvalsmethoden en indicatoren van compromittering.
- Threat intelligence zou veilig kunnen worden geïntegreerd in detectietools en -processen om een nauwkeurigere en tijdigere identificatie van bedreigingen te ondersteunen.

DE.AE-06 Informatie over ongewenste gebeurtenissen wordt verstrekt aan bevoegd personeel en tools

DE.AE-06.1 **Informatie over ongewenste gebeurtenissen moet onmiddellijk worden doorgegeven aan bevoegde medewerkers en systemen, zodat tijdige detectie, onderzoek en reactie mogelijk zijn.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat informatie over ongewenste voorvallen onmiddellijk wordt doorgegeven aan de juiste personen en systemen, zodat zonder vertraging passende maatregelen kunnen worden genomen. Dit draagt bij aan een snellere detectie, onderzoek en reactie op mogelijke bedreigingen of verstoringen.

Om het doel van deze controle te bereiken, zou de organisatierekening kunnen houden met het volgende:

- **Soorten ongewenste gebeurtenissen**: er zouden indicatoren kunnen worden opgenomen zoals ongebruikelijke accountactiviteit, ongeoorloofde toegang, wijzigingen in de systeemconfiguratie, inbreuken op de fysieke beveiliging of malwarewaarschuwingen.
- **Detectie en waarschuwing**: er zouden cyberbeveiligingstools kunnen worden gebruikt om dergelijke gebeurtenissen te detecteren en automatisch geautoriseerd personeel (bijv. SOC-analisten, incidentresponders) te waarschuwen.
- **Integratie met ticketsystemen**: waarschuwingen zouden kunnen worden geïntegreerd in het ticketsysteem van de organisatie. Tickets zouden:
  - Automatisch kunnen worden gegenereerd voor vooraf gedefinieerde soorten waarschuwingen.
  - Handmatig kunnen worden aangemaakt wanneer technisch personeel verdachte activiteiten constateert.
- **Toegang tot logboeken en analyses**: bevoegd personeel zou continu toegang kunnen hebben tot logboekgegevens en analyseresultaten om onderzoeken te ondersteunen.
- **Beoordeling van de maturiteit en de effectiviteit**: de implementatie van de controle zou kunnen worden geëvalueerd door het volgende te controleren:
  - Documentatie van procedures voor het genereren, beoordelen en escaleren van waarschuwingen. Deze documentatie zou regelmatig kunnen worden herzien en bijgewerkt.
  - Gebruik van automatisering voor standaardwaarschuwingen, met handmatige processen als back-up.
  - Toegangscontroles voor waarschuwingen en logboeken, met periodieke beoordelingen van machtigingen (toegang tot waarschuwingen en logboeken zou beperkt kunnen blijven tot bevoegd personeel).
  - Monitoring en rapportage zouden bijvoorbeeld het aantal waarschuwingen, de responstijden en de naleving van procedures kunnen bijhouden.
  - Er zou regelmatig opleiding kunnen worden gegeven aan medewerkers die verantwoordelijk zijn voor het afhandelen van waarschuwingen, zodat ze begrijpen hoe ze deze zouden kunnen interpreteren en ernaar zouden kunnen handelen.

DE.AE-08 Incidenten worden gemeld wanneer ongewenste gebeurtenissen voldoen aan de gedefinieerde incidentcriteria.

DE.AE-08.1 **Incidenten moeten worden gemeld wanneer ongewenste gebeurtenissen voldoen aan de gedefinieerde en gedocumenteerde incidentcriteria.**

Implementatierichtlijnen

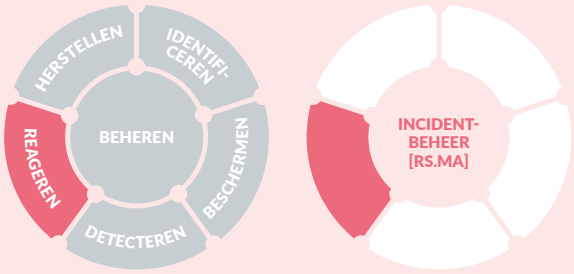
Deze controle zorgt ervoor dat ongewenste gebeurtenissen worden geïdentificeerd en gemeld wanneer ze voldoen aan duidelijk gedefinieerde en gedocumenteerde incidentcriteria. Het benadrukt het belang van consistente drempels en richtlijnen voor het vaststellen van incidenten.

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

- Incidentcriteria (regels voor wat als een incident kwalificeert) zouden duidelijk kunnen worden gedefinieerd, gedocumenteerd en regelmatig kunnen worden herzien.
- Deze criteria zouden kunnen helpen bepalen wanneer een ongewenste gebeurtenis een incident wordt dat zou moeten worden gemeld.
- De criteria zouden kunnen zijn gebaseerd op bekende patronen van normale en abnormale activiteiten, inclusief lessen die zijn geleerd uit eerdere incidenten.
- Bij het vaststellen van de criteria zou rekening kunnen worden gehouden met bekende valse positieven, om onnodige meldingen te voorkomen.
- Wanneer een gebeurtenis aan de gedefinieerde criteria voldoet, zou deze als een incident kunnen worden behandeld en gemeld volgens de procedures van de organisatie.
- Waar nodig en haalbaar zouden systemen kunnen worden geconfigureerd om dit proces te ondersteunen door waarschuwingen te genereren wanneer aan de incidentcriteria wordt voldaan. Dit zou kunnen helpen om incidenten sneller op te sporen, vooral in grotere of complexere omgevingen.

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-01.2 De organisatie moet de respons op informatie-/cyberbeveiligingsincidenten coördineren met alle vooraf gedefinieerde belanghebbenden.

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat alle relevante interne en externe belanghebbenden effectief samenwerken tijdens een cyberbeveiligings- of informatie-incident.

Om dit doel te bereiken:

- Incidentresponsmaatregelen zouden kunnen worden gecoördineerd met vooraf bepaalde belanghebbenden, waaronder bedrijfsleiders, eigenaren van IT- en OT-systemen, cyberbeveiligingsteams, leveranciers, HR, juridische afdeling, fysieke beveiliging, operations en inkoop.
- De coördinatie zou kunnen plaatsvinden volgens de gedocumenteerde incidentresponsplannen van de organisatie.
- Voor elk incident zou een leidinggevende kunnen worden aangewezen om de respons te beheren en te zorgen voor duidelijke communicatie.
- Indien nodig zouden aanvullende plannen, zoals bedrijfscontinuïteit of noodherstel, kunnen worden geactiveerd om de respons te ondersteunen.
- Informatie zou op het juiste moment met de juiste personen kunnen worden gedeeld, volgens vastgestelde communicatieprocedures.
- Verschillende soorten incidenten zouden kunnen worden herkend en dienovereenkomstig kunnen worden behandeld:
  - Informatie-incidenten (bijv. onopzettelijke blootstelling van gegevens)
  - Cyberbeveiligingsincidenten (bijv. malware, hacking)
  - OT-incidenten (bijv. verstoringen van industriële controlesystemen)
- Bij OT-incidenten moet gespecialiseerd OT-personeel worden ingeschakeld en kunnen andere responsprocedures nodig zijn om de veiligheid en de bedrijfsvoering te waarborgen.

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.

RS.MA-03 Incidenten worden gecategoriseerd en geprioriteerd

RS.MA-03.1 **Informatie-/cyberbeveiligingsincidenten moeten worden gecategoriseerd, geprioriteerd en geëscaleerd zoals bepaald in het incidentresponsplan.**

Implementatierichtlijnen

Deze controle is een voortzetting van RS.MA-02.1 en moet ervoor zorgen dat een incident, zodra het is gevalideerd, systematisch wordt geclassificeerd en beheerd op basis van de aard, urgentie en mogelijke impact ervan, zodat de organisatie efficiënt, consistent en adequaat kan reageren.

Daarom zou het volgende in overweging kunnen worden genomen:

- Incidenten zouden kunnen worden beoordeeld en geclassificeerd op basis van hun type (bijv. datalek, ransomware, DDoS, accountcompromittering) en de gevalideerde omvang van hun impact.
- De schatting en validatie van de omvang van een incident – verder uitgewerkt in RS.AN-08.1– zou als basis kunnen dienen voor de categorisering en prioritering van incidenten.
- Indicatoren zoals omvang, ernst en tijdgevoeligheid zouden als leidraad kunnen dienen bij het nemen van prioriteitsbeslissingen.
- Software Bills of Materials (SBOM) zouden de impactbeoordeling kunnen ondersteunen door de getroffen componenten en afhankelijkheden te identificeren.
- Criteria voor categorisering, prioritering en escalatie zouden kunnen worden gedocumenteerd in het incidentresponsplan en consistent kunnen worden toegepast.
- Strategieën voor incidentrespons zouden een evenwicht kunnen vinden tussen de noodzaak van snel herstel en de potentiële voordelen van het observeren van het gedrag van de aanvaller of het uitvoeren van een grondiger onderzoek.
- Escalatieprocedures zouden kunnen worden gecoördineerd met aangewezen interne en externe belanghebbenden om een tijdige en passende respons te garanderen.

RS.MA-05 De criteria voor het starten van incidentherstel worden toegepast.

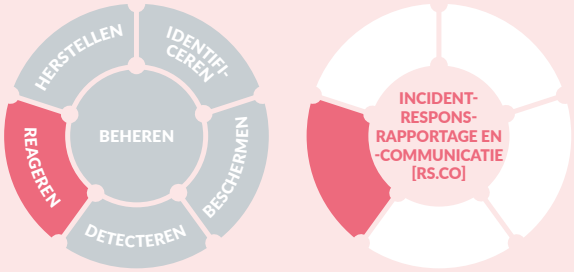
RS.MA-05.1 **Er moeten duidelijke criteria worden gedefinieerd en toegepast om te bepalen wanneer incidentherstelprocessen moeten worden gestart.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat organisaties beschikken over een duidelijk, consistent en op risico's gebaseerd besluitvormingsproces om te bepalen wanneer herstelmaatregelen moeten worden genomen na een cyberbeveiligingsincident.

Daarom kan het volgende worden overwogen:

- Criteria voor het starten van incidentherstel zouden kunnen worden gebaseerd op de bekende of veronderstelde kenmerken van het incident, zoals de ernst, de omvang en de mogelijke impact op activiteiten, gegevens of systemen.
- Bij de beslissing om met herstel te beginnen, zou ook rekening kunnen worden gehouden met de mogelijke verstoring die herstelactiviteiten zouden kunnen veroorzaken voor de lopende activiteiten.
- Herstelpuntdoelstellingen (RPO's) en hersteltijddoelstellingen (RTO's) zouden in de criteria kunnen worden opgenomen om ervoor te zorgen dat herstelmaatregelen aansluiten bij de vereisten voor bedrijfscontinuïteit en aanvaardbare drempels voor downtime of gegevensverlies.



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.

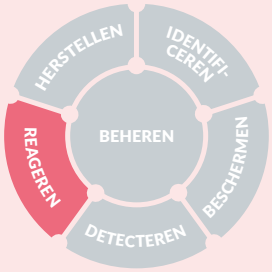
RS.CO-02.2 **Cyberbeveiligingsincidenten moeten binnen de in het incidentresponsplan vastgestelde termijnen worden gedeeld met relevante externe belanghebbenden, met inbegrip van het melden van belangrijke incidenten aan de bevoegde autoriteiten zoals wettelijk vereist.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat alle relevante externe partijen tijdig, veilig en op gepaste wijze worden geïnformeerd over cyberbeveiligingsincidenten, zodat het vertrouwen behouden blijft en aan wettelijke en contractuele verplichtingen wordt voldaan.

Om dit doel te bereiken, zou het volgende in overweging kunnen worden genomen:

- Informatie zou op een veilige manier kunnen worden gedeeld, in overeenstemming met het incidentresponsplan van de organisatie en eventuele overeenkomsten inzake het delen van informatie.
- Relevante belanghebbenden zouden kunnen zijn: aangewezen interne functies, getroffen klanten, leveranciers, externe dienstverleners en zakenpartners.
- Klanten en partners zouden op de hoogte kunnen worden gebracht als ze door een incident worden getroffen, met duidelijke instructies over de maatregelen die ze zouden kunnen nemen.
- De communicatie met externe partijen zou kunnen voldoen aan alle contractuele vereisten of overeenkomsten die van kracht zijn.
- Crisiscommunicatie zou kunnen worden gecoördineerd met kritieke leveranciers om consistente berichtgeving te garanderen.
- Bij het delen van informatie over de tactieken of technieken van aanvallers zouden alle gevoelige of identificerende gegevens kunnen worden verwijderd.
- De afdeling Human Resources zou op de hoogte kunnen worden gebracht als het incident betrekking heeft op kwaadwillige activiteiten door een insider.
- Het senior management zou regelmatig kunnen worden geïnformeerd over de status van ernstige incidenten.
- Nationale autoriteiten, zoals het CSIRT, wetshandhavingsinstanties of toezichthouders, zouden op basis van de criteria die in het IRP zijn vastgelegd en met goedkeuring van het senior management op de hoogte kunnen worden gebracht.
- Alle rapportages zouden kunnen voldoen aan de relevante nationale en EU-wetgeving, zoals de EU-uitvoeringsverordening.
- Openbare updates over incidenten zouden kunnen worden behandeld onder een afzonderlijke controle (RC.CO-04.1).



Er worden activiteiten uitgevoerd om uitbreiding van een incident te voorkomen en de gevolgen ervan te beperken.

RS.MI-01 Incidenten worden beheerst

RS.MI-01.1 Cyberbeveiligingsincidenten moeten worden ingedamd en verholpen. Elke beslissing om bepaalde cyberbeveiligingsrisico's te aanvaarden en te behouden, moet formeel worden gedocumenteerd.

Implementatierichtlijnen

Het doel van deze maatregel is om te voorkomen dat cyberbeveiligingsincidenten zich verspreiden, de oorzaak ervan weg te nemen en ervoor te zorgen dat alle aanvaarde risico's duidelijk worden vastgelegd en goedgekeurd.

Om dit te bereiken, zou het volgende in overweging kunnen worden genomen:

- Er zou een formeel risicoacceptatieproces kunnen zijn voor cyberbeveiligingsrisico's die als weinig ingrijpend worden beschouwd en geen bedreiging vormen voor kritieke bedrijfssystemen. Deze risico's zouden kunnen worden beoordeeld en goedgekeurd door de verantwoordelijke persoon of het verantwoordelijke team, op basis van de risicotolerantie van de organisatie.
- Cyberbeveiligingstools, zoals antivirussoftware of ingebouwde beveiligingsfuncties in besturingssystemen en netwerkapparatuur, zouden automatisch actie kunnen ondernemen om bedreigingen in te dammen of te verwijderen wanneer dat nodig is.
- Incidentresponsteams zouden handmatig acties kunnen kiezen en uitvoeren om incidenten te stoppen en te verwijderen wanneer dat nodig is.
- Vertrouwde derde partijen, zoals internetproviders of managed security service providers, zouden kunnen worden toegestaan om te helpen bij het indammen en elimineren van incidenten als dit deel uitmaakt van het responsplan van de organisatie.

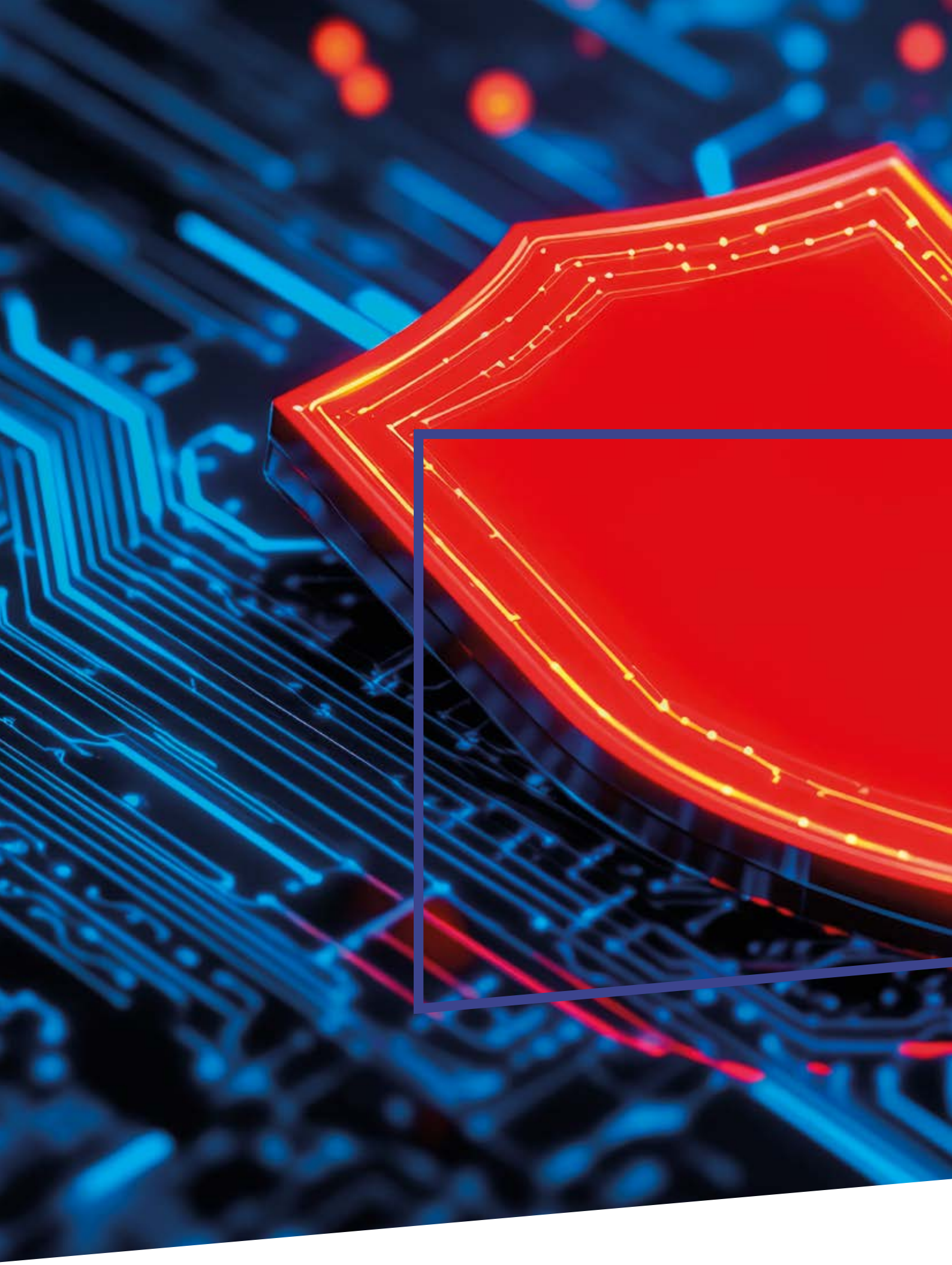
RS.MI-01.2 **De organisatie moet ongeautoriseerde toegang of datalekken detecteren en passende maatregelen nemen om deze te beperken, waaronder het monitoren van kritieke systemen aan externe grenzen en op belangrijke interne punten.**

Implementatierichtlijnen

Het doel van deze controle is om ongeoorloofde toegang en gegevenslekken tijdig te detecteren en passende maatregelen te nemen om de schade te beperken. Dit moet helpen om de vertrouwelijkheid, integriteit, beschikbaarheid en veiligheid van gegevens te beschermen, ongeacht of deze zijn opgeslagen, worden verzonden of actief worden gebruikt, zowel in IT- als OT-omgevingen (Information Technology en Operational Technology).

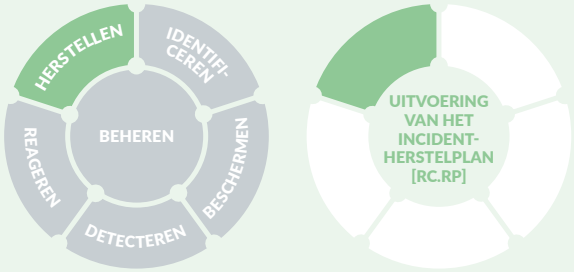
Om dit doel te bereiken, zou de organisatie het volgende in overweging kunnen nemen:

- **Kritieke systemen monitoren**
  Monitoring zou kunnen worden geïmplementeerd aan externe netwerkgrenzen en belangrijke interne punten om afwijkingen of ongeoorloofde toegangspogingen te detecteren.
- **Gegevens in alle stadia beschermen**
  Gegevens in alle stadia zouden kunnen worden beschermd met behulp van encryptie, digitale handtekeningen en cryptografische hashes om de vertrouwelijkheid en integriteit tijdens opslag, verzending en gebruik te waarborgen.
- **Uitgaande communicatie controleren**
  Uitgaande communicatie die gevoelige gegevens bevat, zou automatisch kunnen worden geblokkeerd of versleuteld op basis van gegevensclassificatie.
- **Het gebruik van persoonlijke diensten beperken**
  Toegang tot persoonlijke communicatieplatformen (zoals persoonlijke e-mail of bestandsdelingsdiensten) vanaf systemen van de organisatie moet worden beperkt om het risico op datalekken te verkleinen.
- **Hergebruik van gegevens in niet-productieomgevingen voorkomen**
  Gevoelige productiegegevens zouden niet mogen worden hergebruikt in ontwikkelings- of testomgevingen, tenzij ze op de juiste wijze zijn geanonimiseerd of gemaskeerd.
- **Tijdelijke gegevens wissen**
  Gevoelige gegevens zouden uit het geheugen of de tijdelijke opslag kunnen worden verwijderd wanneer ze niet langer nodig zijn.
- **Identiteits- en toegangsbeheer auditeren**
  Systemen zoals Microsoft Active Directory zouden kunnen worden gecontroleerd, met de nadruk op geprivilegieerde accounts en consistentie van de toegangscontrole.
- **Zorgen voor OT-specifieke haalbaarheid**
  In OT-omgevingen zouden detectie- en mitigatiemaatregelen kunnen worden aangepast om verstoring van de veiligheid of operationele continuïteit te voorkomen. Passieve monitoring en logging op interfaceniveau zouden kunnen worden gebruikt wanneer directe integratie niet haalbaar is.
- **Afstemmen op ENISA-richtlijnen**
  Deze praktijken zouden kunnen worden afgestemd op ENISA-richtlijnen, zoals de Threat Landscape Reports en Information Leakage Guidance, die aanbevelingen geven voor het detecteren en beperken van datalekken en ongeoorloofde toegang.



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 veiligheids-protocollen.
- **Toekomstige verbeteringen plannen**
  Deze controle dient als basis voor meer geavanceerde herstelplanning, zoals verder uitgewerkt in controle RC.RP-06.1 (zekerheidsniveau 'Important).

RC.RP-05 De integriteit van herstelde assets wordt gecontroleerd, systemen en diensten worden hersteld en de normale bedrijfsstatus wordt bevestigd.

RC.RP-05.1 **De integriteit van herstelde systemen en assets moet worden gecontroleerd voordat ze opnieuw in gebruik worden genomen. Systemen en diensten moeten volledig worden hersteld en de normale werking moet worden bevestigd.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat systemen en diensten na een incident niet alleen worden hersteld, maar ook worden gecontroleerd op veiligheid, integriteit en volledige functionaliteit voordat ze weer normaal worden gebruikt.

Om dit doel te bereiken, moet het volgende in overweging worden genomen:
- Herstelde systemen zouden kunnen worden gecontroleerd op tekenen van compromittering, zoals malware of ongeoorloofde toegang, voordat ze weer online worden gebracht.
- De hoofdoorzaak van het incident zou kunnen worden geïdentificeerd en aangepakt om herhaling te voorkomen.
- Alle herstelmaatregelen zouden kunnen worden gecontroleerd om er zeker van te zijn dat ze correct zijn uitgevoerd en dat er geen beveiligingslacunes zijn.
- Een laatste controle zou kunnen bevestigen dat het systeem veilig en volledig is en klaar voor normaal gebruik.

RC.RP-06 Het einde van het herstel na een incident wordt vastgesteld op basis van criteria en de documentatie met betrekking tot het incident wordt voltooid.

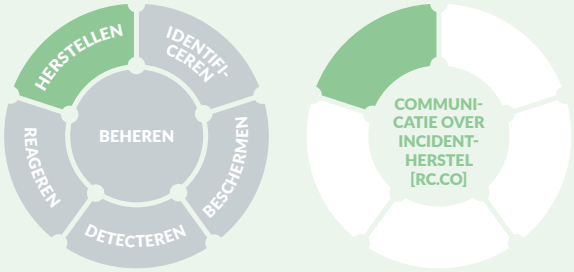
RC.RP-06.1 **Het einde van het herstelproces na een incident moet formeel worden vastgesteld op basis van vooraf gedefinieerde criteria, en alle incident gerelateerde documentatie moet worden afgerond en gecontroleerd.**

Implementatierichtlijnen

Het doel van deze controle is ervoor te zorgen dat het incidentherstelproces formeel en verantwoord wordt afgerond en dat er uitgebreide documentatie wordt opgesteld ter ondersteuning van de verantwoordingsplicht, het leerproces en de voorbereiding op toekomstige incidenten.

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

- Er zou een nabesprekingsrapport kunnen worden opgesteld met daarin:
  - Een samenvatting van het incident en de gevolgen ervan.
  - De stappen die zijn genomen om te reageren en te herstellen.
  - Geleerde lessen en aanbevelingen voor verbetering.
- Voordat de herstelfase als voltooid kan worden beschouwd, zouden de volgende criteria kunnen worden gehanteerd:
  - Alle getroffen systemen en diensten zijn volledig operationeel.
  - Er zijn geen bekende bedreigingen of kwetsbaarheden meer in de omgeving.
  - De gegevens zijn hersteld en op integriteit gecontroleerd.
  - De nodige beveiligingspatches of updates zijn toegepast.
  - Er is monitoring ingesteld om terugkerende of gerelateerde problemen op te sporen.
  - Het evaluatierapport is afgerond en beoordeeld door de relevante belanghebbenden.
  - Alle belanghebbenden zijn geïnformeerd dat het incident is opgelost.



Herstelactiviteiten worden gecoördineerd met interne en externe partijen

RC.CO-03 Herstelactiviteiten en voortgang bij het herstellen van operationele capaciteiten worden gecommuniceerd aan aangewezen interne en externe belanghebbenden

RC.CO-03.1 Herstelactiviteiten en voortgang bij het herstellen van operationele capaciteiten worden gecommuniceerd aan de aangewezen interne en externe belanghebbenden in overeenstemming met de vastgestelde communicatieprocedures.

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat herstelinspanningen en de voortgang van het herstel van operationele capaciteiten duidelijk en consistent worden gecommuniceerd aan alle relevante interne en externe belanghebbenden. Dit ondersteunt transparantie, coördinatie en weloverwogen besluitvorming tijdens de herstelfase van een incident.

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

- Updates over het herstel, inclusief de voortgang van het herstel van systemen en diensten, zouden op een veilige en consistente manier kunnen worden gedeeld met interne en externe belanghebbenden, in overeenstemming met de responsplannen en overeenkomsten voor het delen van informatie van de organisatie.
- Het senior management zou regelmatig updates kunnen ontvangen over de status van de herstelinspanningen, vooral tijdens grote incidenten.
- Communicatieprotocollen die zijn vastgelegd in contracten met leveranciers en partners zouden kunnen worden gevolgd om een tijdige en accurate uitwisseling van informatie te garanderen.
- Crisiscommunicatie met kritieke leveranciers zou kunnen worden gecoördineerd om afgestemde herstelmaatregelen te ondersteunen.
- Als er zich geen daadwerkelijke incidenten hebben voorgedaan, zouden tabletop-oefeningen kunnen worden uitgevoerd om de communicatieprocedures voor herstel en de coördinatie tussen belanghebbenden te testen en te valideren.

RC.CO-04 Openbare updates over het herstel na een incident worden gedeeld via goedgekeurde methoden en berichten.

RC.CO-04.1 **Publieke updates over het herstel na een incident moeten worden gedeeld via goedgekeurde communicatiemethoden en boodschappen, in overeenstemming met de vastgestelde procedures.**

Implementatierichtlijnen

Het doel van deze maatregel is ervoor te zorgen dat de openbare communicatie tijdens de herstelfase van een incident nauwkeurig en tijdig is en via goedgekeurde kanalen wordt verspreid, teneinde het vertrouwen te behouden, reputatierisico's te beheersen en te voldoen aan wettelijke of reglementaire verplichtingen.

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

- Goedgekeurde methoden voor openbare communicatie, zoals persberichten, officiële websites of aangewezen woordvoerders, zouden vooraf kunnen worden gedefinieerd en consistent kunnen worden gebruikt.
- Contactgegevens van relevante partijen (bijv. interne medewerkers, externe leveranciers, wetshandhavingsinstanties, cyberverzekeraars, overheidsinstanties) zouden kunnen worden vastgelegd en bijgehouden.
- Contactlijsten zouden regelmatig (bijvoorbeeld jaarlijks) kunnen worden gecontroleerd en geverifieerd om de juistheid ervan te garanderen.
- Er zouden primaire en secundaire communicatiemechanismen (bijv. telefoongesprekken, e-mails, brieven) kunnen worden vastgesteld, rekening houdend met het feit dat sommige methoden tijdens een incident mogelijk niet beschikbaar zijn.
- Communicatieprotocollen en -mechanismen zouden periodiek kunnen worden herzien of wanneer er belangrijke organisatorische veranderingen plaatsvinden.
- Als er zich geen daadwerkelijke incidenten hebben voorgedaan, zouden tabletop-oefeningen of simulaties kunnen worden uitgevoerd om de procedures voor publieke communicatie te testen en de paraatheid te waarborgen.

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.

BIJLAGE B: LIJST MET AANVULLENDE KERNMAAT-REGELEN VOOR HET ZEKERHEIDSNIVEAU 'IMPORTANT'.

De onderstaande lijst vormt een aanvulling op de kernmaatregelen voor het beveiligingsniveau 'Basic'.

Beheren

GV.RR-02 Rollen, verantwoordelijkheden en bevoegdheden met betrekking tot cyberbeveiligingsrisicobeheer worden vastgesteld, gecommuniceerd, begrepen en gehandhaafd

GV.RR-02.1 De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging voor medewerkers, leveranciers, klanten en partners moeten worden vastgelegd, regelmatig beoordeeld en goedgekeurd, actueel gehouden, duidelijk gecommuniceerd en zowel intern als extern afgestemd.

Identificeren

ID.RA-08 Processen voor het ontvangen, analyseren en reageren op meldingen van kwetsbaarheden worden opgezet.

ID.RA-08.1 De organisatie moet een kwetsbaarheidsbeheerplan opstellen en implementeren om alle soorten kwetsbaarheden te identificeren, analyseren, beoordelen, mitigeren en communiceren, onder meer in de vorm van een gecoördineerde kwetsbaarheids-melding (CVD) volgens de toepasselijke wettelijke modaliteiten.

Beschermen

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

PR.AA-03.3 De organisatie moet gebruiksbeperkingen, verbindingsvereisten en autorisatiepro-cedures voor externe toegang tot haar kritieke systemen definiëren, documenteren en implementeren. Deze controles moeten ervoor zorgen dat alleen goedgekeurde gebruikers verbinding kunnen maken met behulp van veilige methoden, waarbij de toegang beperkt blijft tot wat nodig is voor hun functie.

PR.PS-01 Er worden configuratiebeheerpraktijken vastgesteld en toegepast

PR.PS-01.1 De organisatie moet een basisconfiguratie voor haar bedrijfskritieke systemen ont-wikkelen, documenteren en onderhouden.

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

PR.IR-01.3 Om de operationele stabiliteit en veiligheid te waarborgen, moet de organisatie zonder uitzondering alle verbindingen tussen onderdelen van haar kritieke systemen identificeren, documenteren en beheersen.

PR.IR-01.4 De organisatie moet passende maatregelen nemen om communicatie te bewaken en te controleren aan externe en belangrijke interne grenzen van kritieke systemen, inclusief de verbindingen tussen IT- en OT-domeinen, om veilige en betrouwbare werking te garanderen.

Detecteren

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

DE.CM-01.3 De organisatie moet het ongeoorloofd gebruik van haar bedrijfskritieke systemen monitoren en identificeren door het detecteren van ongeautoriseerde lokale, netwerk- en externe verbindingen.

Reageren

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

RS.CO-02.2 Cyberbeveiligingsincidenten moeten binnen de in het incidentresponsplan vastgestelde termijnen worden gedeeld met relevante externe belanghebbenden, met inbegrip van het melden van belangrijke incidenten aan de bevoegde autoriteiten zoals wettelijk vereist.

RS.MI-01 Incidenten worden beheerst

RS.MI-01.2 De organisatie moet ongeautoriseerde toegang of datalekken detecteren en passende maatregelen nemen om deze te beperken, waaronder het monitoren van kritieke systemen aan externe grenzen en op belangrijke interne punten.

BIJLAGE C: LIJST MET CONTROLES MET BETREKKING TOT MANAGEMENTASPECTEN VOOR HET ZEKERHEIDSNIVEAU 'IMPORTANT'

Beheren

GV.RM-01 Doelstellingen voor risicobeheer worden vastgesteld en overeengekomen door de belanghebbenden van de organisatie

GV.RM-01.1 Doelstellingen voor informatie- en cybersecurity moeten op coherente wijze binnen de hele organisatie worden vastgesteld en goedgekeurd door het senior management.

GV.RM -02 Verklaringen over risicobereidheid en risicotolerantie worden opgesteld, gecommuniceerd en onderhouden

GV.RM-02.1 Verklaringen over risicobereidheid en risicotolerantie moeten worden gedefinieerd, gedocumenteerd, goedgekeurd door het senior management, gecommuniceerd en onderhouden.

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

GV.RM-03.2 Informatie- en cyberbeveiligingsrisico's moeten worden gedocumenteerd als onderdeel van de bedrijfsrisicobeheerprocessen, formeel worden goedgekeurd door het senior management en worden bijgewerkt wanneer zich wijzigingen voordoen.

GV.RR-02 Rollen, verantwoordelijkheden en bevoegdheden met betrekking tot cyberbeveiligingsrisicobeheer worden vastgesteld, gecommuniceerd, begrepen en gehandhaafd.

GV.RR-02.1 De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging voor medewerkers, leveranciers, klanten en partners moeten worden vastgelegd, regelmatig beoordeeld en goedgekeurd, actueel gehouden, duidelijk gecommuniceerd en zowel intern als extern afgestemd.

Identificeren

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

ID.RA-05.2 De organisatie moet risicobeoordelingen uitvoeren waarbij het risico wordt bepaald aan de hand van bedreigingen, kwetsbaarheden en de impact op bedrijfsprocessen en assets.

ID.RA-06 Risicoresponsen worden geselecteerd, geprioriteerd, gepland, bijgehouden en gecommuniceerd

ID.RA-06.1 Maatregelen om risico's aan te pakken moeten worden geïdentificeerd, geprioriteerd, gepland, opgevolgd en gecommuniceerd.

ID.IM-04 Incidentresponsplannen en andere cyberbeveiligingsplannen die van invloed zijn op de bedrijfsvoering worden opgesteld, gecommuniceerd, onderhouden en verbeterd

ID.IM-04.1 Nood- en continuïteitsplannen moeten worden opgesteld, gecommuniceerd, onderhouden, getest, gevalideerd en verbeterd.

Beschermen

PR.IR-04 Voldoende middelencapaciteit om de beschikbaarheid te waarborgen.

PR.IR-04.1 Een adequate planning van de benodigde middelen moet ervoor zorgen dat de beschikbaarheid van de kritieke systemen van de organisatie voor informatieverwerking, netwerken, telecommunicatie en gegevensopslag gewaarborgd blijft.

Herstellen

RC.CO-03 Herstelactiviteiten en voortgang bij het herstellen van operationele capaciteiten worden gecommuniceerd aan aangewezen interne en externe belanghebbenden

RC.CO-03.1 Herstelactiviteiten en voortgang bij het herstellen van operationele capaciteiten worden gecommuniceerd aan de aangewezen interne en externe belanghebbenden in overeenstemming met de vastgestelde communicatieprocedures.

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:

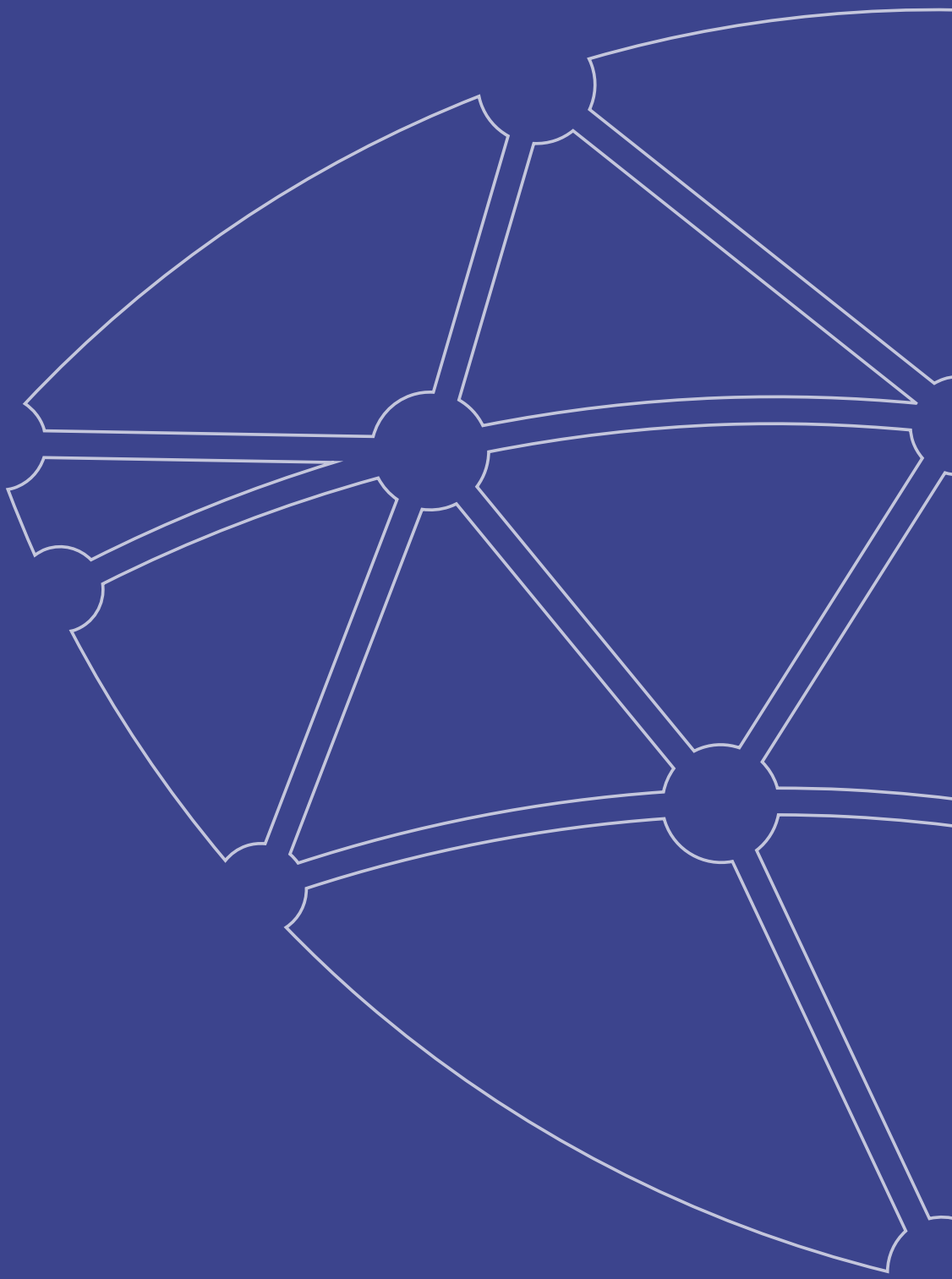
- is van algemene aard en dekt niet alle specifieke situaties.
- is niet noodzakelijkerwijs volledig, nauwkeurig of in alle opzichten actueel.

Verantwoordelijke redacteur

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

Juridisch depot

D/2025/14828/012



Centrum voor Cyberveiligheid België

Wetstraat 18

1000 Brussel