

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-1  
Maatregel: ID.AM-1.1  
SUB-SUBCATEGORIE: Een inventaris van activa in verband met informatie en informatieverwerkingsfaciliteiten binnen de organisatie moet worden gedocumenteerd, geëvalueerd en bijgewerkt wanneer zich wijzigingen voordoen.  
RICHTLIJNEN: • Deze inventaris omvat vaste en draagbare computers, tablets, mobiele telefoons, programmeerbare logische Controllers (PLC's), sensoren, actuatoren, robots, machinegereedschappen, firmware, netwerk switches, routers, voedingen en andere netwerkcomponenten of -apparaten.  
• Er wordt aanbevolen dat deze inventaris moet alle activa omvatten, ongeacht of zij al dan niet op het netwerk van de organisatie zijn aangesloten.  
• Het gebruik van een hulpmiddel voor ICT-activabeheer kan worden overwogen

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-1  
Maatregel: ID.AM-1.2  
SUB-SUBCATEGORIE: De inventaris van activa die verband houden met informatie en informatieverwerkingsfaciliteiten moet veranderingen in de context van de organisatie weerspiegelen en alle informatie bevatten die nodig is voor een effectieve verantwoording.  
RICHTLIJNEN: • De inventarisatie kan bijvoorbeeld het volgende omvatten: fabrikant, apparaat type, model, serienummer, machinenamen en netwerkadressen, fysieke locatie...  
• Verantwoordingsplicht is de verplichting om iemands daden uit te leggen, te rechtvaardigen en er verantwoordelijkheid voor te nemen; het impliceert verantwoording voor het resultaat van de taak of het proces.  
• De veranderingen omvatten de ontmanteling van materiaal

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-1  
Maatregel: ID.AM-1.3  
SUB-SUBCATEGORIE: Wanneer niet-toegestane hardware wordt ontdekt, moet deze in quarantaine worden geplaatst voor eventuele uitzonderingsbehandeling, verwijderd of vervangen, en wordt de inventaris dienovereenkomstig bijgewerkt.  
RICHTLIJNEN: • Alle niet-ondersteunde hardware zonder uitzonderingsdocumentatie wordt aangemerkt als niet x0002 geautoriseerd.  
• Niet-toegestane hardware kan worden opgespoord tijdens inventarisaties, verzoeken om ondersteuning door de gebruiker of op andere manieren.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-1  
Maatregel: ID.AM-1.4  
SUB-SUBCATEGORIE: De mechanismen voor het detecteren van de aanwezigheid van niet-geautoriseerde hardware en firmwarecomponenten in het netwerk van de organisatie moeten worden geïdentificeerd.  
RICHTLIJNEN: • Waar dat veilig en haalbaar is, kunnen deze mechanismen worden geautomatiseerd.  
• Er zou een proces moeten zijn om niet-geautoriseerde bedrijfsmiddelen (assets) regelmatig aan te pakken; de organisatie kan ervoor kiezen het bedrijfsmiddel (asset) van het netwerk te verwijderen, het bedrijfsmiddel (asset) te verbieden op afstand verbinding te maken met het netwerk, of het bedrijfsmiddel (asset) in quarantaine te plaatsen.

```

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Asset Management
SUBCAT ID CYFUN: ID.AM-2
Maatregel: ID.AM-2.1
SUB-SUBCATEGORIE: Een inventaris die aangeeft welke softwareplatforms en -
toepassingen in de organisatie worden gebruikt, moet worden gedocumenteerd,
geëvalueerd en bijgewerkt wanneer zich wijzigingen voordoen.
RICHTLIJNEN: • Deze inventaris omvat softwareprogramma's, softwareplatforms
en databases, zelfs indien deze zijn uitbesteed (SaaS).
• Er wordt aanbevolen dat de modaliteiten van het uitbesteden deel uitmaken
van de contractuele overeenkomsten met de dienstverlener.
• De informatie in de inventaris zou bijvoorbeeld het volgende kunnen
omvatten: naam, beschrijving, versie, aantal gebruikers, verwerkte gegevens,
enz.
• Er zou een onderscheid moeten worden gemaakt tussen niet-ondersteunde
software en niet_x0002_geautoriseerde software.
• Het gebruik van een hulpmiddel voor IT-activabeheer kan worden overwogen

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Asset Management
SUBCAT ID CYFUN: ID.AM-2
Maatregel: ID.AM-2.2
SUB-SUBCATEGORIE: De inventaris van softwareplatforms en -toepassingen die
verband houden met informatie en informatieverwerking, moet veranderingen in
de context van de organisatie
weerspiegelen en alle informatie bevatten die nodig is voor een doeltreffende
verantwoording.
RICHTLIJNEN: De inventaris van softwareplatforms en toepassingen zou voor elk
item het volgende kunnen omvatten:
de titel, de uitgever, de datum van eerste installatie/gebruik en het
bedrijfsdoel; indien van toepassing, de Uniform Resource Locator (URL), de
app store(s), de versie(s), het implementatiemechanisme en de datum van
buitengebruikstelling.

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Asset Management
SUBCAT ID CYFUN: ID.AM-2
Maatregel: ID.AM-2.3
SUB-SUBCATEGORIE: De personen die binnen de organisatie verantwoordelijk en
aansprakelijk zijn voor het beheer van softwareplatforms en -toepassingen
moeten worden geïdentificeerd.
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Asset Management
SUBCAT ID CYFUN: ID.AM-2
Maatregel: ID.AM-2.4
SUB-SUBCATEGORIE: Wanneer niet-geautoriseerde software wordt ontdekt, wordt
deze in quarantaine geplaatst voor eventuele uitzonderingsbehandeling,
verwijderd of vervangen, en wordt de inventaris dienovereenkomstig
bijgewerkt.
RICHTLIJNEN: • Alle niet-ondersteunde software zonder
uitzonderingsdocumentatie wordt als niet-geautoriseerd aangemerkt.
• Niet-geautoriseerde software kan worden opgespoord tijdens inventarisatie,
verzoeken om ondersteuning door de gebruiker of andere middelen.

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Asset Management
SUBCAT ID CYFUN: ID.AM-2

```

Maatregel: ID.AM-2.5

SUB-SUBCATEGORIE: De mechanismen voor het opsporen van de aanwezigheid van niet-geautoriseerde software in de ICT/OT-omgeving van de organisatie moeten worden geïdentificeerd.

RICHTLIJNEN: • Waar dat veilig en haalbaar is, kunnen deze mechanismen worden geautomatiseerd.

- Er zou een proces moeten zijn om niet-geautoriseerde bedrijfsmiddelen (activa) regelmatig aan te pakken; de organisatie kan ervoor kiezen het bedrijfsmiddel (activa) van het netwerk te verwijderen, het bedrijfsmiddel (activa) te verbieden op afstand verbinding te maken met het netwerk, of het bedrijfsmiddel (activa) in quarantaine te plaatsen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-3

Maatregel: ID.AM-3.1

SUB-SUBCATEGORIE: Informatie die de organisatie opslaat en gebruikt, moet worden geïdentificeerd.

RICHTLIJNEN: • Begin met een lijst van alle soorten informatie die uw bedrijf opslaat of gebruikt. Definieer "informatietype" op een voor uw bedrijf zinvolle manier. U kunt uw werknemers een lijst laten maken van alle informatie die zij bij hun gewone activiteiten gebruiken. Maak een lijst van alles wat u kunt bedenken, maar u hoeft niet te specifiek te zijn. U kunt bijvoorbeeld klantnamen en e-mailadressen bewaren, ontvangstbewijzen voor grondstoffen, uw bankgegevens of andere vertrouwelijke informatie.

- Overweeg deze informatie in kaart te brengen met de bijbehorende activa die zijn geïdentificeerd in de inventarissen van fysieke apparaten, systemen, softwareplatforms en toepassingen die binnen de organisatie worden gebruikt (zie ID.AM-1 & ID.AM-2).

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-3

Maatregel: ID.AM-3.2

SUB-SUBCATEGORIE: Alle verbindingen binnen de ICT/OT-omgeving van de organisatie en met andere interne platforms van de organisatie moeten in kaart worden gebracht, gedocumenteerd, goedgekeurd en zo nodig bijgewerkt.

RICHTLIJNEN: • Verbindingsinformatie omvat bijvoorbeeld de interfacekenmerken, gegevenskenmerken, poorten, protocollen, adressen, beschrijving van de gegevens, beveiligingsvereisten en de aard van de verbinding.

- Configuratiebeheer kan worden gebruikt als ondersteunende troef.
- Deze documentatie zou niet alleen mogen worden opgeslagen op het netwerk dat zij vertegenwoordigt.
- Overweeg een kopie van deze documentatie te bewaren in een veilige offline omgeving (bv. offline harde schijf, papieren hardcopy...)

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-3

Maatregel: ID.AM-3.3

SUB-SUBCATEGORIE: De informatiestromen/gegevensstromen binnen de ICT/OT-omgeving van de organisatie en naar andere interne systemen van de organisatie moeten in kaart worden gebracht, gedocumenteerd, geautoriseerd en bijgewerkt wanneer zich wijzigingen voordoen.

RICHTLIJNEN: • Met kennis van de informatie-/gegevensstromen binnen een systeem en tussen systemen is het mogelijk te bepalen waar informatie wel en niet naartoe kan gaan.

- Overweeg:

- o Het afdwingen van controles die verbindingen beperken tot alleen geautoriseerde interfaces.
- o De systeembewaking opvoeren wanneer er een indicatie is van een verhoogd risico voor de kritische operaties en activa van de organisatie.
- o Bescherming van het systeem tegen informatielekken als gevolg van elektromagnetische signalen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-4

Maatregel: ID.AM-4.1

SUB-SUBCATEGORIE: De organisatie moet alle externe diensten en de daarmee gemaakte verbindingen in kaart brengen, documenteren, autoriseren en bij wijzigingen bijwerken.

RICHTLIJNEN: • De uitbesteding van binnen de organisatie gebruikte systemen, softwareplatforms en toepassingen wordt behandeld in ID.AM-1 & ID.AM-2.

• Externe informatiesystemen zijn systemen of onderdelen van systemen waar organisaties doorgaans geen rechtstreeks toezicht en gezag hebben over de toepassing van beveiligingseisen en -controles, of de bepaling van de doeltreffendheid van de op die systemen toegepaste controles. Dit zijn bv. diensten die worden uitgevoerd in de cloud, SaaS, hosting of andere externe omgevingen, API (Application Programming Interface) ...

• Door externe diensten en de verbindingen daarmee in kaart te brengen en vooraf te autoriseren, wordt voorkomen dat onnodig middelen worden verspild aan het onderzoeken van een zogenaamd niet\_x0002\_geauthentiseerde verbinding met externe systemen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-4

Maatregel: ID.AM-4.2

SUB-SUBCATEGORIE: De informatiestroom van en naar externe systemen moet in kaart worden gebracht, gedocumenteerd en geautoriseerd, en worden bijgewerkt wanneer zich wijzigingen voordoen.

RICHTLIJNEN: Overweeg van externe dienstverleners te verlangen dat zij de functies, poorten, protocollen en diensten die nodig zijn voor de het verlenen van diensten om te connecteren identificeren en documenteren.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Asset Management

SUBCAT ID CYFUN: ID.AM-5

Maatregel: ID.AM-5.1

SUB-SUBCATEGORIE: De middelen van de organisatie (hardware, apparaten, gegevens, tijd, personeel, informatie en software) moeten worden geprioriteerd op basis van hun classificatie, criticiteit en bedrijfswaarde.

RICHTLIJNEN:

• Bepaal de middelen van de organisatie (bijv. hardware, apparaten, gegevens, tijd, personeel, informatie en software) op basis van volgende vragen:

o Wat zou er met mijn bedrijf gebeuren als deze middelen openbaar worden gemaakt, beschadigd worden, verloren gaan...?

o Wat gebeurt er met mijn bedrijf als de integriteit van de middelen niet langer gegarandeerd is?

o Wat zou er met mijn bedrijf gebeuren als ik/mijn klanten geen toegang zouden hebben tot deze middelen? En rangschik deze middelen op basis van hun classificatie, criticiteit en bedrijfswaarde.

• De middelen moeten bedrijfsactiva omvatten.

• Er zou een classificatie voor gevoelige informatie moeten worden gemaakt door eerst categorieën te bepalen, bijv.

o Openbaar - vrij toegankelijk voor iedereen, zelfs extern

o Intern - alleen toegankelijk voor leden van de organisatie

o Vertrouwelijk - alleen toegankelijk voor diegenen die een functie hebben die toegang vereist.

- Deze categorieën zouden moeten worden gecommuniceerd en er zou moeten worden geïdentificeerd welke soorten gegevens onder deze categorieën vallen (HR-gegevens, financiële gegevens, juridische gegevens, persoonsgegevens, enz.)
- Overweeg het gebruik van het Traffic Light Protocol (TLP).
- De gegevensindeling moet van toepassing zijn op de drie aspecten: C-I-A.
- Overweeg de implementatie van een geautomatiseerd hulpmiddel, zoals host-based Data Loss Prevention (DLP) om alle gevoelige gegevens te identificeren die zijn opgeslagen, verwerkt of verzonden via bedrijfsmiddelen, met inbegrip van die welke zich ter plaatse of bij een externe dienstverlener bevinden.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-6  
Maatregel: ID.AM-6.1  
SUB-SUBCATEGORIE: De rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging binnen de organisatie moeten worden gedocumenteerd, geëvalueerd, geautoriseerd en bijgewerkt en afgestemd op de andere interne rollen van de organisatie en die van externe partners.  
RICHTLIJNEN: Het moet worden overwogen om:

- Beveiligingsrollen, -verantwoordelijkheden en -autoriteiten te beschrijven: wie in de organisatie moet worden geraadpleegd, geïnformeerd en verantwoordelijk worden gehouden voor alle of een deel van de bedrijfsmiddelen.
- Te voorzien in beveiligingsrollen, verantwoordelijkheden en bevoegdheden voor alle belangrijke functies op het gebied van informatie-/cyberbeveiliging (juridisch, opsporingsactiviteiten...).
- Informatie-/cyberbeveiligingsrollen en verantwoordelijkheden op te nemen voor derden (bijv. leveranciers, klanten, partners) met fysieke of logische toegang tot de ICT/OT-omgeving van de organisatie.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Asset Management  
SUBCAT ID CYFUN: ID.AM-6  
Maatregel: ID.AM-6.2  
SUB-SUBCATEGORIE: De organisatie zal een informatiebeveiligingsfunctionaris (Information Security Officer) aanstellen.  
RICHTLIJNEN: De informatiebeveiligingsfunctionaris zou verantwoordelijk moeten zijn voor het toezicht op de uitvoering van de informatie-/cyberbeveiligingsstrategie en -waarborgen van de organisatie.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-1  
Maatregel: ID.BE-1.1  
SUB-SUBCATEGORIE: De rol van de organisatie in de toeleveringsketen moet worden vastgesteld en gecommuniceerd.  
RICHTLIJNEN: • De organisatie zou duidelijk moeten kunnen vaststellen wie zich stroomopwaarts en stroomafwaarts van de organisatie bevindt en welke leveranciers diensten, capaciteiten, producten en artikelen aan de organisatie leveren.

- De organisatie moet haar standpunt kenbaar maken aan haar toeleveranciers en afnemers, zodat duidelijk wordt waar zij staan in termen van kritisch belang voor de activiteiten van de organisatie.

### FUNCTIONS: Identify  
FUNCTIONS: Identify

CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-1  
Maatregel: ID.BE-1.2  
SUB-SUBCATEGORIE: De organisatie moet haar ICT/OT-omgeving beschermen tegen bedreigingen vanuit de toeleveringsketen door beveiligingswaarborgen toe te passen als onderdeel van een gedocumenteerde alomvattende beveiligingsstrategie.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-2  
Maatregel: ID.BE-2.1  
SUB-SUBCATEGORIE: De plaats van de organisatie in de kritieke infrastructuur en haar bedrijfstak wordt vastgesteld en gecommuniceerd  
RICHTLIJNEN: Organisatie die onder de NIS-wetgeving vallen, hebben de verantwoordelijkheid om de andere organisaties in dezelfde sector te kennen om met hen samen te werken om de door de NIS-wetgeving voor die specifieke sector vastgestelde doelstellingen te bereiken.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-3  
Maatregel: ID.BE-3.1  
SUB-SUBCATEGORIE: Prioriteiten met betrekking tot de missie, doelstellingen en activiteiten van de organisatie worden vastgesteld en gecommuniceerd.  
RICHTLIJNEN: De behoefte aan informatiebescherming moet worden vastgesteld en de desbetreffende processen moeten zo nodig worden herzien.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-4  
Maatregel: ID.BE-4.1  
SUB-SUBCATEGORIE: De afhankelijkheden en missie-kritische functies voor de levering van kritieke diensten moeten als onderdeel van het risicobeoordelingsproces worden geïdentificeerd, gedocumenteerd en geprioriteerd op basis van hun criticiteit.  
RICHTLIJNEN: Afhangelijkheden en bedrijfskritische functies moeten ondersteunende diensten omvatten.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment  
SUBCAT ID CYFUN: ID.BE-5  
Maatregel: ID.BE-5.1  
SUB-SUBCATEGORIE: Om de cyberveerkracht te ondersteunen en de levering van kritieke diensten te beveiligen, moeten de nodige eisen worden vastgesteld, gedocumenteerd en de uitvoering ervan getest en goedgekeurd.  
RICHTLIJNEN: • Overweeg voldoende data- en netwerkredundantie (bijvoorbeeld redundante netwerkapparatuur, servers met load balancing, raid arrays, back-up diensten, 2 aparte datacentra, fail-over voor netwerkverbindingen, 2 ISP's...).

- Overweeg bescherming van kritieke apparatuur/diensten tegen stroomuitval en andere storingen als gevolg van onderbrekingen van het elektriciteitsnet (bv. UPS & NO-break, frequente tests, servicecontracten met regelmatig onderhoud, redundante stroombekabeling, 2 verschillende stroomleveranciers...)

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Business Environment

SUBCAT ID CYFUN: ID.BE-5

Maatregel: ID.BE-5.2

SUB-SUBCATEGORIE: Informatie verwerkende en ondersteunende faciliteiten moeten redundantie toepassen om te voldoen aan de beschikbaarheidseisen, zoals gedefinieerd door de organisatie en/of regelgevende kaders.

RICHTLIJNEN: • Overweeg voldoende data- en netwerkredundantie (bijvoorbeeld redundante netwerkkapparatuur, servers met load balancing, raid arrays, back-up diensten, 2 aparte datacentra, fail-over voor netwerkverbindingen, 2 ISP's...).

• Overweeg bescherming van kritieke apparatuur/diensten tegen stroomuitval en andere storingen als gevolg van onderbrekingen van het elektriciteitsnet (bv. UPS & NO-break, frequente tests, servicecontracten met regelmatig onderhoud, redundante stroombekabeling, 2 verschillende stroomleveranciers...)

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Business Environment

SUBCAT ID CYFUN: ID.BE-5

Maatregel: ID.BE-5.3

SUB-SUBCATEGORIE: Er moeten doelstellingen voor hersteltijd en herstelpunten worden vastgesteld voor het herstel van essentiële ICT/OT-systeemprocessen.

RICHTLIJNEN: • Overweeg de 3-2-1 back-upregel toe te passen om de RPO ("Recovery Point Objective") en RTO ("Recovery Time Objective") te verbeteren. Houd bijvoorbeeld ten minste 3 kopieën van uw gegevens bij, bewaar er 2 op afzonderlijke locaties en bewaar één kopie op een externe locatie.

• Overweeg mechanismen zoals hot swap, load balancing en failsafe toe te passen om de veerkracht te vergroten.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-1

Maatregel: ID.GV-1.1

SUB-SUBCATEGORIE: Beleid en procedures voor informatiebeveiliging en cyberveiligheid moeten worden opgesteld, gedocumenteerd, geëvalueerd, goedgekeurd en bijgewerkt wanneer zich wijzigingen voordoen.

RICHTLIJNEN: • Beleid en procedures worden gebruikt om aanvaardbare praktijken en verwachtingen voor de bedrijfsvoering vast te stellen, kunnen worden gebruikt om nieuwe werknemers op te leiden in uw verwachtingen op het gebied van informatiebeveiliging, en kunnen helpen bij een onderzoek in geval van een incident. Deze beleidslijnen en procedures moeten gemakkelijk toegankelijk zijn voor werknemers.

• Beleid en procedures voor informatie- en cyberbeveiliging zouden duidelijk de verwachtingen voor de bescherming van de informatie en systemen van de organisatie moeten beschrijven, en hoe het management verwacht dat de middelen van het bedrijf door alle werknemers worden gebruikt en beschermd.

• Beleid en procedures worden bij voorkeur ten minste jaarlijks worden herzien en bijgewerkt, en telkens wanneer er veranderingen zijn in de organisatie of de technologie. Telkens wanneer het beleid wordt gewijzigd, is het aangewezen de werknemers op de hoogte te brengen van die wijzigingen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-1

Maatregel: ID.GV-1.2

SUB-SUBCATEGORIE: Er moet een door het hoger management goedgekeurd informatie- en cyberbeveiligingsbeleid voor de gehele organisatie worden vastgesteld, gedocumenteerd, bijgewerkt bij wijzigingen, en verspreid.

RICHTLIJNEN: Het beleid kan bijvoorbeeld het volgende omvatten:

- De identificatie en toewijzing van rollen, verantwoordelijkheden, managementbetrokkenheid, coördinatie tussen organisatorische entiteiten, en naleving. Richtsnoeren voor rolprofielen met hun vastgestelde titels, missies, taken, vaardigheden, kennis en competenties zijn beschikbaar in de "European Cybersecurity Skills Framework Role Profiles" van ENISA. (<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>)
- De coördinatie tussen organisatorische entiteiten die verantwoordelijk zijn voor de verschillende aspecten van de beveiliging (d.w.z. technische, fysieke, personele, cyberfysische, informatie, toegangscontrole, mediabescherming, kwetsbaarheidsbeheer, onderhoud, toezicht)
- De dekking van de volledige levenscyclus van de ICT/OT-systemen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-3

Maatregel: ID.GV-3.1

SUB-SUBCATEGORIE: Wettelijke en regelgevende voorschriften over informatie-/cyberbeveiliging, met inbegrip van privacy verplichtingen, moeten worden begrepen en uitgevoerd.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-3

Maatregel: ID.GV-3.2

SUB-SUBCATEGORIE: De wet- en regelgeving inzake informatie-/cyberbeveiliging, met inbegrip van privacy verplichtingen, wordt beheerd

RICHTLIJNEN: • Er zou regelmatig moeten worden nagegaan of voortdurend wordt voldaan aan de wet- en regelgeving inzake informatie-/cyberbeveiliging, met inbegrip van privacy verplichtingen.

- Deze eis geldt ook voor aannemers en dienstverleners

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-4

Maatregel: ID.GV-4.1

SUB-SUBCATEGORIE: Als onderdeel van het algemene risicobeheer van de onderneming moet een alomvattende strategie voor het beheer van informatiebeveiliging en cyberbeveiligingsrisico's worden ontwikkeld en bijgewerkt wanneer zich veranderingen voordoen.

RICHTLIJNEN: Deze strategie zou het bepalen en toewijzen moeten omvatten van de nodige middelen om de bedrijfskritische activa van de organisatie te beschermen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Governance

SUBCAT ID CYFUN: ID.GV-4

Maatregel: ID.GV-4.2

SUB-SUBCATEGORIE: Informatie- en cyberbeveiligingsrisico's moeten worden gedocumenteerd, formeel goedgekeurd, en bij wijzigingen bijgewerkt.

RICHTLIJNEN: Overweeg het gebruik van instrumenten voor risicobeheer.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Risk Assessment

SUBCAT ID CYFUN: ID.RA-1

Maatregel: ID.RA-1.1

SUB-SUBCATEGORIE: Bedreigingen en kwetsbaarheden moeten worden geïdentificeerd.



RICHTLIJNEN: • Een kwetsbaarheid verwijst naar een zwakke plek in de hardware, software of procedures van de organisatie. Het is een gat waardoor een slechte actor toegang kan krijgen tot de activa van de organisatie. Een kwetsbaarheid stelt een organisatie bloot aan bedreigingen.

- Een bedreiging is een kwaadaardige of negatieve gebeurtenis die gebruik maakt van een kwetsbaarheid.
- Het risico is de kans op verlies en schade wanneer de dreiging zich voordoet.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Assessment  
SUBCAT ID CYFUN: ID.RA-1  
Maatregel: ID.RA-1.2  
SUB-SUBCATEGORIE: Er moet een proces worden ingesteld om kwetsbaarheden van de bedrijfskritische systemen van de organisatie voortdurend te bewaken, te identificeren en te documenteren.

RICHTLIJNEN: • Waar dat veilig en haalbaar is, zou het gebruik van kwetsbaarheidsscans moeten worden overwogen

- De organisatie zou een testprogramma kunnen opstellen en bijhouden dat past bij haar omvang, complexiteit en rijpheid.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Assessment  
SUBCAT ID CYFUN: ID.RA-1  
Maatregel: ID.RA-1.3  
SUB-SUBCATEGORIE: Om ervoor te zorgen dat de werking van de organisatie niet negatief wordt beïnvloed door het testproces, moeten prestatie-/belastingstesten en penetratietesten op de systemen van de organisatie zorgvuldig worden uitgevoerd.

RICHTLIJNEN: Overweeg het valideren van beveiligingsmaatregelen na elke penetratietest.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Assessment  
SUBCAT ID CYFUN: ID.RA-2  
Maatregel: ID.RA-2.1  
SUB-SUBCATEGORIE: Er moet een bewustmakingsprogramma in verband met bedreigingen en kwetsbaarheden worden opgezet dat een organisatie overschrijdend vermogen tot informatie-uitwisseling omvat.

RICHTLIJNEN: Een programma voor de bewustmaking van dreigingen en kwetsbaarheden moet permanente contacten omvatten met beveiligingsgroepen en -verenigingen om beveiligingswaarschuwingen en -adviezen te ontvangen. (Beveiligingsgroepen en -verenigingen zijn bijvoorbeeld belangengroepen, fora, beroepsverenigingen, nieuwsgroepen en/of 'peer groups' van beveiligingsprofessionals in soortgelijke organisaties). Dit contact kan het delen van informatie over potentiële kwetsbaarheden en incidenten omvatten. Deze uitwisselingsmogelijkheid kan niet-geclassificeerde en geclassificeerde gegevensuitwisseling omvatten.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Assessment  
SUBCAT ID CYFUN: ID.RA-2  
Maatregel: ID.RA-2.2  
SUB-SUBCATEGORIE: Er moet worden vastgesteld waar geautomatiseerde mechanismen kunnen worden toegepast om informatie over beveiligingswaarschuwingen en -adviezen ter beschikking te stellen van belanghebbenden in de organisatie.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

```

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Risk Assessment
SUBCAT ID CYFUN: ID.RA-5
Maatregel: ID.RA-5.1
SUB-SUBCATEGORIE: De organisatie moet risicobeoordelingen uitvoeren waarbij
het risico wordt bepaald aan de hand van bedreigingen, kwetsbaarheden en
gevolgen voor bedrijfsprocessen en activa.
RICHTLIJNEN: • Herinner dat bedreigingen gebruik maken van kwetsbaarheden
("vulnerability").
• Er zou in kaart moeten worden gebracht wat de gevolgen zijn van het
verliezen van vertrouwelijkheid, integriteit en beschikbaarheid voor de
activa en gerelateerde bedrijfsprocessen

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Risk Assessment
SUBCAT ID CYFUN: ID.RA-5
Maatregel: ID.RA-5.2
SUB-SUBCATEGORIE: De organisatie moet risicobeoordelingen uitvoeren en
documenteren waarin het risico wordt bepaald door bedreigingen,
kwetsbaarheden, gevolgen voor bedrijfsprocessen en activa, en de
waarschijnlijkheid dat deze zich voordoen.
RICHTLIJNEN: • De risicobeoordeling zou bedreigingen van insiders en externe
partijen moeten omvatten.
• Kwalitatieve en/of kwantitatieve risicoanalysemethoden (MAPGOOD, ISO27005,
CIS RAM, ...) kunnen samen met softwaretooling worden gebruikt

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Risk Assessment
SUBCAT ID CYFUN: ID.RA-5
Maatregel: ID.RA-5.3
SUB-SUBCATEGORIE: De resultaten van risicobeoordelingen moeten aan de
belanghebbenden worden gecommuniceerd.
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Risk Assessment
SUBCAT ID CYFUN: ID.RA-6
Maatregel: ID.RA-6.1
SUB-SUBCATEGORIE: Er moet een alomvattende strategie worden ontwikkeld en
uitgevoerd om de risico's voor de kritieke systemen van de organisatie te
beheren, die de identificatie en prioritering van
risicomaatregelen omvat.
RICHTLIJNEN: • Management en werknemers zou moeten worden betrokken bij
informatie- en cyberbeveiliging.
• Er zou moeten worden vastgesteld wat de belangrijkste activa zijn en hoe
deze worden beschermd.
• Het duidelijk moeten zijn wat de gevolgen zullen zijn als deze activa
worden gecompromitteerd.
• Er zou moeten worden vastgesteld hoe de uitvoering van adequate mitigerende
maatregelen zal worden georganiseerd.

### FUNCTIONS: Identify
FUNCTIONS: Identify
CATEGORY NAME CYFUN: Risk Management Strategy
SUBCAT ID CYFUN: ID.RM-1
Maatregel: ID.RM-1.1
SUB-SUBCATEGORIE: Een cyberrisicobeheerproces dat de belangrijkste interne en
externe belanghebbenden identificeert en het aanpakken van risico-

```

gerelateerde kwesties en informatie vergemakkelijkt, moet worden gecreëerd, gedocumenteerd, herzien, goedgekeurd en bijgewerkt wanneer zich wijzigingen voordoen.  
RICHTLIJNEN: Tot de externe belanghebbenden behoren klanten, investeerders, aandeelhouders, leveranciers, overheidsinstanties en de gemeenschap in het algemeen.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Management Strategy  
SUBCAT ID CYFUN: ID.RM-2  
Maatregel: ID.RM-2.1  
SUB-SUBCATEGORIE: De organisatie moet duidelijk haar risicobereidheid ("risk appetite") bepalen.  
RICHTLIJNEN: De bepaling en uitdrukking van de risicotolerantie (risicobereidheid) moeten in overeenstemming zijn met het beleid inzake informatiebeveiliging en cyberveiligheid, zodat de samenhang tussen beleid, risicotolerantie en maatregelen gemakkelijker kan worden aangetoond.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Risk Management Strategy  
SUBCAT ID CYFUN: ID.RM-3  
Maatregel: ID.RM-3.1  
SUB-SUBCATEGORIE: De risicotolerantie van de organisatie wordt bepaald door haar rol in de kritische infrastructuur en sectorspecifieke risicoanalyses.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-1  
Maatregel: ID.SC-1.1  
SUB-SUBCATEGORIE: De organisatie moet een risicobeheerproces voor de cybertoeleveringsketen documenteren, herzien, goedkeuren, bijwerken wanneer zich wijzigingen voordoen, en implementeren dat de identificatie, beoordeling en beperking van de risico's in verband met de gedistribueerde en onderling verbonden aard van de toeleveringsketens van ICT/OT-producten en -diensten ondersteunt.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-2  
Maatregel: ID.SC-2.1  
SUB-SUBCATEGORIE: De organisatie moet ten minste jaarlijks of bij een wijziging in de kritieke systemen, de operationele omgeving of de toeleveringsketen van de organisatie, risicobeoordelingen voor de cybertoeleveringsketen uitvoeren; Deze beoordelingen moeten worden gedocumenteerd en de resultaten moeten worden verspreid onder de relevante belanghebbenden, met inbegrip van degenen die verantwoordelijk zijn voor ICT/OT-systemen.  
RICHTLIJNEN: Deze beoordeling moet de potentiële negatieve gevolgen voor de organisatie van de risico's in verband met de gedistribueerde en onderling verbonden aard van de toeleveringsketens van ICT/OT-producten en -diensten vaststellen en prioriteren.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-2  
Maatregel: ID.SC-2.2

SUB-SUBCATEGORIE: Er moet een gedocumenteerde lijst worden opgesteld van alle leveranciers, verkopers en partners van de organisatie die bij een ernstig incident betrokken kunnen zijn; Die lijst moet worden bijgewerkt wanneer nodig en online en offline beschikbaar worden gesteld.

RICHTLIJNEN: Deze lijst zou de contactgegevens moeten bevatten van leveranciers, verkopers en partners aangevuld met de diensten die zij leveren, zodat zij kunnen worden gecontacteerd voor bijstand in geval van een storing of dienstonderbreking.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Supply Chain Risk Management

SUBCAT ID CYFUN: ID.SC-3

Maatregel: ID.SC-3.1

SUB-SUBCATEGORIE: Op basis van de resultaten van de risicobeoordeling van de cybertoeleveringsketen moet een contractueel kader voor leveranciers en externe partners worden vastgesteld om het delen van gevoelige informatie, en gedistribueerde en onderling verbonden ICT/OT-producten en - diensten, aan te pakken.

RICHTLIJNEN: • Entiteiten die niet onder de NIS-wetgeving vallen, zouden enkel bedrijfskritische leveranciers en externe partners in aanmerking mogen nemen.

• Vergeet niet dat aan de GDPR-vereisten moet worden voldaan wanneer bedrijfsinformatie persoonsgegevens bevat (van toepassing op alle niveaus), d.w.z. dat in het contractuele kader beveiligingsmaatregelen hieromtrent moeten worden genomen.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Supply Chain Risk Management

SUBCAT ID CYFUN: ID.SC-3

Maatregel: ID.SC-3.2

SUB-SUBCATEGORIE: Er moeten contractuele vereisten inzake informatie- en cyberbeveiliging voor leveranciers en externe partners worden geïmplementeerd, om te zorgen dat er een controleerbaar proces is voor het verhelpen van gebreken, en om te waarborgen dat gebreken worden verholpen die worden vastgesteld tijdens informatie- en cyberbeveiligingstesten en evaluaties.

RICHTLIJNEN: • Informatiesystemen die software (of firmware) bevatten met recentelijk aangekondigde softwaregebreken (en potentiële kwetsbaarheden als gevolg van die gebreken) zouden moeten worden geïdentificeerd.

• Nieuwe patches, service packs en hot fixes die relevant zijn voor de beveiliging zouden moeten worden geïnstalleerd, en deze patches, service packs en hot fixes zouden vóór de installatie moeten worden getest op doeltreffendheid en mogelijke neveneffecten op de informatiesystemen van de organisatie. Gebreken die worden ontdekt tijdens beveiligingsbeoordelingen, voortdurende monitoring, activiteiten in het kader van de respons op incidenten of de afhandeling van tekortkomingen in informatiesystemen, worden ook snel aangepakt. Het verhelpen van fouten zou moeten worden opgenomen in het configuratiebeheer als een noodwijziging.

### FUNCTIONS: Identify

FUNCTIONS: Identify

CATEGORY NAME CYFUN: Supply Chain Risk Management

SUBCAT ID CYFUN: ID.SC-3

Maatregel: ID.SC-3.3

SUB-SUBCATEGORIE: De organisatie moet contractuele voorschriften vaststellen die haar in staat stellen de door leveranciers en externe partners geïmplementeerde programma's voor "informatiebeveiliging en cyberveiligheid" te evalueren.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Identify

FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-4  
Maatregel: ID.SC-4.1  
SUB-SUBCATEGORIE: De organisatie moet de naleving van de contractuele verplichtingen door leveranciers en externe partners beoordelen aan de hand van routinematig nazicht van audits, testresultaten en andere evaluatie.  
RICHTLIJNEN: Entiteiten die niet onder de NIS-wetgeving vallen, zouden zich kunnen beperken tot bedrijfskritische leveranciers en partners.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-4  
Maatregel: ID.SC-4.2  
SUB-SUBCATEGORIE: De organisatie moet de naleving van de contractuele verplichtingen door leveranciers en externe partners beoordelen door regelmatig onafhankelijke audits, testresultaten en andere evaluaties van derden te bekijken.  
RICHTLIJNEN: De diepgang van de evaluatie moet afhangen van het kritieke karakter van de geleverde producten en diensten.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-5  
Maatregel: ID.SC-5.1  
SUB-SUBCATEGORIE: De organisatie moet sleutelpersoneel van leveranciers en externe partners identificeren en documenteren om hen als belanghebbenden bij de respons- en herstelplanning te betrekken.  
RICHTLIJNEN: Entiteiten die niet onder de NIS-wetgeving vallen, zouden zich kunnen beperken tot bedrijfskritische leveranciers en partners.

### FUNCTIONS: Identify  
FUNCTIONS: Identify  
CATEGORY NAME CYFUN: Supply Chain Risk Management  
SUBCAT ID CYFUN: ID.SC-5  
Maatregel: ID.SC-5.2  
SUB-SUBCATEGORIE: De organisatie moet het sleutelpersoneel van leveranciers en externe partners identificeren en documenteren om hen als belanghebbenden te betrekken bij het testen en uitvoeren van de respons- en herstelplannen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Identity Management and Access Control  
SUBCAT ID CYFUN: PR.AC-1  
Maatregel: PR.AC-1.1  
SUB-SUBCATEGORIE: Identiteiten en referenties ("credentials") voor geautoriseerde apparaten en gebruikers moeten worden beheerd.  
RICHTLIJNEN: Identiteiten en referenties voor geautoriseerde apparaten en gebruikers kunnen worden beheerd door middel van een wachtwoordbeleid. Een wachtwoordbeleid is een reeks regels die ontworpen zijn om de ICT/OT-beveiliging te verbeteren door de organisatie aan te moedigen om: (Niet limitatieve lijst en maatregelen die in voorkomend geval kunnen worden overwogen)  

- Alle standaard wachtwoorden te wijzigen.
- Ervoor te zorgen dat niemand werkt met beheerdersrechten voor dagelijkse taken.
- Een beperkte en bijgewerkte lijst van systeembeheerdersaccounts bij te houden.

- Wachtwoordregels af te dwingen, b.v. wachtwoorden moeten langer zijn dan een bepaald aantal tekens met een combinatie van soorten tekens en moeten periodiek of bij vermoeden van compromittering worden gewijzigd.
- Alleen individuele accounts te gebruiken en nooit wachtwoorden te delen.
- Ongebruikte accounts onmiddellijk uit te schakelen
- Rechten en privileges te beheren via gebruikersgroepen

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-1

Maatregel: PR.AC-1.2

SUB-SUBCATEGORIE: Identiteiten en referenties ("credentials") voor geautoriseerde apparaten en gebruikers worden beheerd, waar mogelijk via geautomatiseerde mechanismen

RICHTLIJNEN: • Geautomatiseerde mechanismen kunnen het beheer en de controle van referenties ("credentials") van informatiesystemen helpen ondersteunen.  
 • Denk aan sterke gebruikersauthenticatie, dat wil zeggen een authenticatie gebaseerd op het gebruik van ten minste twee authenticatiefactoren uit verschillende categorieën van kennis (iets wat alleen de gebruiker weet), bezit (iets wat alleen de gebruiker bezit) of inferentie (iets wat de gebruiker is) die onafhankelijk van elkaar zijn, in die zin dat het doorbreken van één ervan de betrouwbaarheid van de andere niet in gevaar brengt, en zodanig is ontworpen dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-1

Maatregel: PR.AC-1.3

SUB-SUBCATEGORIE: De systeemgegevens moeten na een bepaalde periode van inactiviteit worden gedeactiveerd, tenzij dit de veilige werking van (kritische) processen in gevaar zou brengen.

RICHTLIJNEN: • Om de veilige werking te garanderen, zouden service-accounts moeten worden gebruikt voor lopende processen en diensten.  
 • Overweeg het gebruik van een formele toegangsprocedure voor externe partijen

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-1

Maatregel: PR.AC-1.4

SUB-SUBCATEGORIE: Voor transacties binnen de kritieke systemen van de organisatie moet de organisatie het volgende implementeren:

- Multifactor-authenticatie voor eindgebruikers (MFA of "sterke authenticatie").
- Op certificaten gebaseerde authenticatie voor systeem-naar-systeem communicatie

RICHTLIJNEN: Overweeg het gebruik van SSO (Single Sign On) in combinatie met MFA voor de interne en externe kritische systemen van de organisatie.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-1

Maatregel: PR.AC-1.5

SUB-SUBCATEGORIE: De kritieke systemen van de organisatie moeten worden gecontroleerd op atypisch gebruik van systeemgegevens. Referenties "credentials" die geassocieerd worden met aanzienlijke risico's moeten worden uitgeschakeld.

RICHTLIJNEN: • Overweeg het aantal mislukte aanmeldingspogingen te beperken door een automatische blokkering toe te passen.

- Het vergrendelde account zou niet toegankelijk mogen zijn totdat het opnieuw is ingesteld of de duur van de accountvergrendeling is verstreken.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-2

Maatregel: PR.AC.2-1

SUB-SUBCATEGORIE: De fysieke toegang tot de faciliteit, de servers en de netwerkcomponenten moet worden beheerd.

RICHTLIJNEN: • Overweeg om sleutels voor toegang tot de gebouwen en alarmcodes strikt te beheren. De volgende regels moeten in overweging worden genomen:

- o Haal altijd de sleutels of badges van een werknemer terug wanneer deze het bedrijf definitief verlaat.

- o Verander de alarmcodes van het bedrijf regelmatig.

- o Geef nooit sleutels of alarmcodes aan externe dienstverleners (schoonmaakpersoneel enz.), tenzij het mogelijk is deze toegang te traceren en technisch te beperken tot bepaalde tijdstippen.

- Overweeg om interne netwerkaansluitingen niet toegankelijk te maken in openbare ruimtes. Deze openbare plaatsen kunnen wachtkamers, vergaderzalen, gangen... zijn.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-2

Maatregel: PR.AC.2-2

SUB-SUBCATEGORIE: Het beheer van fysieke toegang moet maatregelen omvatten voor de toegang in noodsituaties.

RICHTLIJNEN: • De fysieke toegangscontrole kan bijvoorbeeld bestaan uit: lijsten van bevoegde personen, identiteitsdocumenten, vereisten inzake begeleiding van bv. bezoekers, bewakers, hekken, draaihekken, sloten, monitoring van de toegang tot de faciliteit, camerabewaking.

- De volgende maatregelen kunnen worden overwogen:

- o Voer een pasjessysteem in en creëer verschillende veiligheidszones.

- o De fysieke toegang tot servers en netwerkcomponenten kan worden beperkt tot bevoegd personeel.

- o Alle toegang tot servers en netwerkcomponenten kan worden vastgelegd.

- Toegangsregisters voor bezoekers zouden moeten worden bijgehouden, geëvalueerd en zo nodig worden uitgebraat.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-2

Maatregel: PR.AC.2-3

SUB-SUBCATEGORIE: De fysieke toegang tot kritieke zones moet worden gecontroleerd boven op de fysieke toegang tot de faciliteit.

RICHTLIJNEN: Dit kan bijvoorbeeld gaan over: productie, O&O, apparatuur voor kritische systemen van de organisatie (serverruimtes...)

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-2

Maatregel: PR.AC.2-4

SUB-SUBCATEGORIE: Activa gerelateerd met kritieke zones moeten fysiek worden beschermd.

RICHTLIJNEN: • Overweeg om stroomapparatuur, stroombekabeling, netwerkbekabeling en netwerkkinterfaces te beschermen tegen toevallige schade, verstoring en fysiek geknoei.

- Overweeg redundante en fysiek gescheiden stroomsystemen te implementeren voor de kritische activiteiten van de organisatie.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Identity Management and Acces Control  
SUBCAT ID CYFUN: PR.AC-3  
Maatregel: PR.AC-3.1  
SUB-SUBCATEGORIE: De draadloze toegangspunten van de organisatie moeten worden beveiligd.  
RICHTLIJNEN: • Wijzig het administratieve wachtwoord bij de installatie van een draadloos toegangspunt.  
• Stel het draadloze toegangspunt zo in dat het zijn Service Set Identifier (SSID) niet uitzendt.  
• Stel uw router in om ten minste WiFi Protected Access (WPA-2 of WPA-3 waar mogelijk) te gebruiken, met de Advanced Encryption Standard (AES) voor encryptie.  
• Zorg ervoor dat draadloze internettoegang voor klanten gescheiden is van uw bedrijfsnetwerk.  
• Verbinding maken met onbekende of onbeveiligde/gast draadloze toegangspunten moet worden vermeden, en indien onvermijdelijk gebeuren via een versleuteld virtueel privé-netwerk (VPN).  
• Beheer alle eindpuntapparaten (vast en mobiel) volgens het beveiligingsbeleid van de organisatie.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Identity Management and Acces Control  
SUBCAT ID CYFUN: PR.AC-3  
Maatregel: PR.AC-3.2  
SUB-SUBCATEGORIE: Gebruiksbeperkingen, verbindingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot de kritieke systeemomgeving van de organisatie moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.  
RICHTLIJNEN: Overweeg het volgende:  
• Tot de methoden voor toegang op afstand behoren bijvoorbeeld draadloze, breedband-, Virtual Private Network (VPN)-verbindingen, verbindingen met mobiele apparatuur en communicatie via externe netwerken.  
• De aanmeldingsgegevens ("login credentials") moeten in overeenstemming zijn met het beleid van het bedrijf inzake de authenticatie van gebruikers.  
• Toegang op afstand voor ondersteunende activiteiten of onderhoud van organisatorische activa moet worden goedgekeurd, geregistreerd en uitgevoerd op een wijze die ongeoorloofde toegang voorkomt.  
• De gebruiker moet door een visuele indicatie worden gewezen op elke verbinding op afstand met zijn apparaat.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Identity Management and Acces Control  
SUBCAT ID CYFUN: PR.AC-3  
Maatregel: PR.AC-3.3  
SUB-SUBCATEGORIE: De toegang op afstand tot de kritieke systemen van de organisatie moet worden gecontroleerd en waar nodig moeten cryptografische mechanismen worden toegepast.  
RICHTLIJNEN: Dit houdt in dat geprivilegieerde functies enkel na autorisatie vanop afstand toegang zouden mogen krijgen.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Identity Management and Acces Control  
SUBCAT ID CYFUN: PR.AC-3  
Maatregel: PR.AC-3.4  
SUB-SUBCATEGORIE: De netwerken van de organisatie die op afstand toegankelijk zijn, moeten worden beveiligd, onder meer door middel van multifactorauthenticatie (MFA).



RICHTLIJNEN: MFA zou moeten worden afgedwongen (bv. 2FA) op internetgerichte systemen, zoals e-mail, remote desktop en Virtual Private Network (VPN's).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-3

Maatregel: PR.AC-3.5

SUB-SUBCATEGORIE: The security for connections with external systems shall be verified and framed by documented agreements.

RICHTLIJNEN:

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.1

SUB-SUBCATEGORIE: De toegangsrechten voor gebruikers tot de systemen van de organisatie moeten worden gedefinieerd en beheerd.

RICHTLIJNEN: Het volgende zou in overweging moeten worden genomen:

- Opstellen en regelmatig herzien van toegangslijsten per systeem (bestanden, servers, software, databases, enz.), eventueel via analyse van de Active Directory in op Windows gebaseerde systemen, met als doel te bepalen wie welke toegang (al dan niet geprivilegieerd) nodig heeft om zijn taken in de organisatie uit te voeren.
- Stel voor elke gebruiker (ook voor contractanten die toegang nodig hebben) een aparte account in en eis dat voor elke account sterke, unieke wachtwoorden worden gebruikt.
- Zorg ervoor dat alle werknemers computeraccounts zonder administratieve rechten gebruiken om typische werkfuncties uit te voeren. Dit houdt in dat persoonlijke en administratieve accounts moeten worden gescheiden.
- Gebruik voor gastaccounts minimale privileges (bijvoorbeeld alleen internettoegang) die nodig zijn voor de zakelijke behoeften.
- Documenteer het beheer van vergunningen in een procedure en werk die zo nodig bij.
- Gebruik waar nodig "Single Sign On" (SSO).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.2

SUB-SUBCATEGORIE: Waar mogelijk worden geautomatiseerde mechanismen toegepast ter ondersteuning van het beheer van gebruikersaccounts op de kritieke systemen van de organisatie, met inbegrip van het uitschakelen, controleren, rapporteren en verwijderen van gebruikersaccounts.

RICHTLIJNEN: Overweeg elke persoon met toegang tot de kritieke systemen van de organisatie afzonderlijk te identificeren met een gebruikersnaam om generieke en anonieme accounts en toegang te verwijderen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.3

SUB-SUBCATEGORIE: In het toegangscontrolebeleid van de organisatie moeten beperkingen van het accountgebruik voor specifieke tijdsperioden en locaties in aanmerking worden genomen en dienovereenkomstig worden toegepast.

RICHTLIJNEN: Specifieke beperkingen kunnen bijvoorbeeld bestaan uit het beperken van het gebruik tot bepaalde dagen van de week, tijdstippen van de dag of specifieke tijdsperioden.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control  
SUBCAT ID CYFUN: PR.AC-4  
Maatregel: PR.AC-4.4  
SUB-SUBCATEGORIE: Er moet worden vastgesteld wie toegang moet hebben tot de bedrijfskritische informatie n technologie van de organisatie, en de middelen om die toegang te krijgen.  
RICHTLIJNEN: Middelen om toegang te krijgen kunnen zijn: een sleutel, wachtwoord, code of administratief privilege.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.5

SUB-SUBCATEGORIE: De toegang van werknemers tot gegevens en informatie moet worden beperkt tot de systemen en specifieke informatie die zij nodig hebben om hun werk te doen (het beginsel van "least privilege").

RICHTLIJNEN: Het beginsel van "Least Privilege" moet worden opgevat als het beginsel dat een beveiligingsarchitectuur zo moet worden ontworpen dat elke werknemer de minimale systeembronnen en machtigingen krijgt die de werknemer nodig heeft om zijn functie uit te oefenen. Overweeg:

- Niet toe te staan dat een werknemer toegang heeft tot alle bedrijfsinformatie.
- Het aantal internettoegangen en interconnecties met partnernetwerken te beperken tot het strikt noodzakelijke om het toezicht op de uitwisselingen gemakkelijker te kunnen centraliseren en homogeniseren.
- Ervoor te zorgen dat wanneer een werknemer het bedrijf verlaat, alle toegang tot de informatie of systemen van het bedrijf onmiddellijk wordt geblokkeerd.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.6

SUB-SUBCATEGORIE: Bij het beheer van de toegangsrechten wordt het principe van functiesplitsing gehanteerd (Separation of Duties - SoD).

RICHTLIJNEN: Richtlijnen

Functiesplitsing (Separation of Duties - SoD) omvat bijvoorbeeld:

- Het verdelen van operationele functies en systeemondersteunende functies over verschillende rollen.
- Het uitvoeren van systeemondersteunende functies met verschillende personen.
- Niet toestaan dat een enkele persoon zowel een (financiële of andere) transactie initieert als goedkeurt.
- Ervoor zorgen dat beveiligingspersoneel dat toegangscontrole functies beheert, niet ook auditfuncties beheert.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.7

SUB-SUBCATEGORIE: Niemand heeft beheerdersrechten voor dagelijkse taken.

RICHTLIJNEN: Overweeg het volgende:

- Scheid beheerdersaccounts van gebruikersaccounts.
- Geef gebruikersaccounts geen rechten om beheertaken uit te voeren.
- Maak unieke lokale beheerderswachtwoorden en schakel ongebruikte accounts uit.
- Verbied het surfen op internet vanuit administratieve accounts.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-4

Maatregel: PR.AC-4.8

SUB-SUBCATEGORIE: Geprivilegieerde gebruikers moeten worden beheerd, gemonitord en geaudit.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### Entry

FUNCTIONS:

CATEGORY NAME CYFUN:

SUBCAT ID CYFUN:

Maatregel: PR.AC-4.9

SUB-SUBCATEGORIE: Privileged users shall be managed, monitored and audited.

RICHTLIJNEN:

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Access Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.1

SUB-SUBCATEGORIE: Op alle netwerken van de organisatie moeten firewalls worden geïnstalleerd en geactiveerd.

RICHTLIJNEN: Overweeg het volgende:

- Installeer en gebruik een firewall tussen het interne netwerk en het internet. Dit kan een functie zijn van een (draadloos) toegangspunt/router, of het kan een functie zijn van een door de Internet Service Provider (ISP) geleverde router.
- Zorg ervoor dat er antivirussoftware is geïnstalleerd op gekochte firewalloplossingen en dat het inlog\_x0002\_en beheerderswachtwoord van de beheerder bij de installatie en daarna regelmatig wordt gewijzigd.
- Op elk computersysteem (inclusief smartphones en andere netwerkapparaten) een softwarefirewall installeren, gebruiken en bijwerken.
- Zorg voor firewalls op al uw computers en netwerken, zelfs als u gebruik maakt van een cloud service provider of een virtueel privénetwerk (VPN). Zorg ervoor dat op het thuisnetwerk en de systemen voor telewerken firewalls voor hardware en software zijn geïnstalleerd, operationeel zijn en regelmatig worden bijgewerkt.
- Overweeg de installatie van een Intrusion Detection / Prevention System (IDPS). Deze systemen analyseren het netwerkverkeer op een gedetailleerder niveau en kunnen een hoger beschermingsniveau bieden.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Access Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.2

SUB-SUBCATEGORIE: Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door netwerksegmentatie en -scheiding.

RICHTLIJNEN: • Overweeg verschillende beveiligingszones in het netwerk te creëren (bijvoorbeeld basisnetwerksegmentatie via VLAN's of andere mechanismen voor netwerktoegangscontrole) en het verkeer tussen deze zones te controleren/bewaken.

- Wanneer het netwerk "vlak" is, kan de compromittering van een vitale netwerkcomponent leiden tot de compromittering van het gehele netwerk.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Access Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.3

SUB-SUBCATEGORIE: Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door:

- (1) Identificeren, documenteren en controleren van verbindingen tussen systeemcomponenten.

(2) Externe verbindingen met de kritieke systemen van de organisatie te beperken.

RICHTLIJNEN: Mechanismen voor grensbeveiliging zijn bijvoorbeeld routers, gateways, uni directionele gateways, datadiodes en firewalls die systeemcomponenten scheiden in logisch gescheiden netwerken of subnetwerken.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.4

SUB-SUBCATEGORIE: De organisatie moet, waar mogelijk, geauthentiseerde proxyservers implementeren voor gedefinieerd communicatieverkeer tussen de kritieke systemen van de organisatie en externe netwerken.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.5

SUB-SUBCATEGORIE: De organisatie moet verbindingen en communicatie aan de buitengrenzen en aan belangrijke interne grenzen binnen de kritieke systemen van de organisatie bewaken en controleren door waar nodig grensbeschermingsvoorzieningen te implementeren.

RICHTLIJNEN: Overweeg de uitvoering van de volgende aanbevelingen:

- Scheid uw openbare WIFI-netwerk van uw bedrijfsnetwerk.
- Bescherm uw zakelijke WIFI met geavanceerde encryptie.
- Een oplossing voor netwerktoegangscontrole (Network Access Control - NAC) implementeren.
- Versleutel verbindingen met uw bedrijfsnetwerk.
- Verdeel uw netwerk volgens beveiligingsniveaus en pas firewallregels toe. Isoleer uw netwerken voor serverbeheer.
- Forceer VPN op openbare netwerken.
- Implementeer een gesloten beleid voor beveiligingsgateways ("deny all policy": alleen verbindingen toestaan/openen die vooraf expliciet zijn geautoriseerd).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-5

Maatregel: PR.AC-5.6

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat de kritieke systemen van de organisatie veilig uitvallen wanneer een grensbeschermingsvoorziening operationeel faalt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-6

Maatregel: PR.AC-6.1

SUB-SUBCATEGORIE: De organisatie moet gedocumenteerde procedures implementeren om de identiteit van personen te verifiëren alvorens referenties ("credentials") af te geven die toegang geven tot de systemen van de organisatie.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Acces Control

SUBCAT ID CYFUN: PR.AC-6

Maatregel: PR.AC-6.2

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat unieke referenties worden gebruikt voor elke geverifieerde gebruiker, elk apparaat en elk proces dat interageert met de kritieke systemen van de organisatie; zij moet ervoor zorgen dat deze worden geverifieerd en dat unieke identificatiecodes worden vastgelegd bij het uitvoeren van systeeminteracties.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Identity Management and Access Control

SUBCAT ID CYFUN: PR.AC-7

Maatregel: PR.AC-7.1

SUB-SUBCATEGORIE: De organisatie moet een gedocumenteerde risicobeoordeling uitvoeren op de kritieke systeemtransacties van de organisatie en gebruikers, apparaten en andere middelen authenticiseren (bv. single-factor, multifactor) in verhouding tot het risico van de transactie (bv. de veiligheids- en privacy risico's van personen en andere organisatorische risico's).

RICHTLIJNEN: Overweeg voor nieuwe systemen een op beveiliging gebaseerde ontwerp ("security-by-design"); voor bestaande systemen zou een afzonderlijke risicobeoordeling moeten worden gebruikt.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-1

Maatregel: PR.AT-1.1

SUB-SUBCATEGORIE: De werknemers moeten de nodige opleiding krijgen.

RICHTLIJNEN: • Tot de werknemers behoren alle gebruikers en beheerders van de ICT/OT-systemen; zij zouden onmiddellijk bij indiensttreding en daarna regelmatig moeten worden opgeleid over het informatiebeveiligingsbeleid van de onderneming en over wat er van hen wordt verwacht om de bedrijfsinformatie en -technologie te beschermen.

• De opleiding zou voortdurend moeten worden bijgewerkt en versterkt door bewustmakingscampagnes.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-1

Maatregel: PR.AT-1.2

SUB-SUBCATEGORIE: De organisatie moet het herkennen en rapporteren van bedreigingen van binnenuit opnemen in de beveiligingsbewustmakingsopleiding.

RICHTLIJNEN: Overweeg het volgende:

- Communiceer en bespreek regelmatig om ervoor te zorgen dat iedereen zich bewust is van zijn verantwoordelijkheden.
- Ontwikkel een "outreach"-programma door in een document de boodschappen te verzamelen die u aan uw personeel wil overbrengen (onderwerpen, doelgroepen, doelstellingen, enz.) en plan uw communicatieritme in een kalender (wekelijks, maandelijks, eenmalig, enz.). Communiceer voortdurend en op een boeiende manier, waarbij u het management, IT-collega's, de ICT-dienstverlener en HR- en communicatiemanagers betreft.
- Behandel onderwerpen als: herkenning van fraudepogingen, phishing, beheer van gevoelige informatie, incidenten, enz. Het doel is dat alle werknemers begrijpen hoe ze bedrijfsinformatie kunnen beschermen.
- Bespreek met uw management, uw ICT-collega's of uw ICT-dienstverlener enkele oefenscenario's (bv. wat te doen bij een virusalarm, als een storm de stroom afsnijdt, als gegevens worden geblokkeerd, als een account wordt gehackt enz.). Het centrale contactpunt in geval van een incident moet bij iedereen bekend zijn.
- Organiseer een simulatie van een scenario om uw kennis te testen. Overweeg de oefening bijvoorbeeld ten minste eenmaal per jaar uit te voeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-1

Maatregel: PR.AT-1.3

SUB-SUBCATEGORIE: De organisatie moet een evaluatiemethode toepassen om de doeltreffendheid van de bewustmakingsopleidingen te meten.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-2

Maatregel: PR.AT-2.1

SUB-SUBCATEGORIE: Geprivilegieerde gebruikers moeten gekwalificeerd zijn voordat rechten worden verleend, en deze gebruikers moeten kunnen aantonen dat zij hun taken, verantwoordelijkheden en bevoegdheden begrijpen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-3

Maatregel: PR.AT-3-1

SUB-SUBCATEGORIE: De organisatie moet beveiligingseisen vaststellen en handhaven voor bedrijfskritische derde partijen ("third-party providers") en gebruikers.

RICHTLIJNEN: De handhaving zou moeten inhouden dat "derde belanghebbenden" (bv. leveranciers, klanten, partners) kunnen aantonen dat zij hun rol en verantwoordelijkheden begrijpen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-3

Maatregel: PR.AT-3-2

SUB-SUBCATEGORIE: Derde partijen moeten elke overplaatsing, beëindiging of overgang van personeel met fysieke of logische toegang tot bedrijfskritische systeemonderdelen van de organisatie melden.

RICHTLIJNEN: Derde partijen zijn bijvoorbeeld dienstverleners, contractanten en andere organisaties die systeemontwikkeling, technologische diensten, uitbestede toepassingen of netwerk- en beveiligingsbeheer leveren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-3

Maatregel: PR.AT-3-3

SUB-SUBCATEGORIE: De organisatie monitort leveranciers en gebruikers van bedrijfskritische diensten op naleving van de beveiligingsvoorschriften.

RICHTLIJNEN: Auditresultaten van derden kunnen als auditbewijs worden gebruikt.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-3

Maatregel: PR.AT-3-4

SUB-SUBCATEGORIE: De organisatie auditeert bedrijfskritische externe dienstverleners op naleving van de beveiligingsvoorschriften.

RICHTLIJNEN: Auditresultaten van derden kunnen als auditbewijs worden gebruikt.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-4

Maatregel: PR.AT-4.1

SUB-SUBCATEGORIE: Hogere leidinggevendenden moeten kunnen aantonen dat hun taken, verantwoordelijkheden en bevoegdheden begrijpen.

RICHTLIJNEN: Richtsnoeren voor rolprofielen en de daarbij behorende titels, opdrachten, taken, vaardigheden, kennis en competenties zijn te vinden in de "European Cybersecurity Skills Framework Role Profiles" van ENISA.  
(<https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles>)

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Awareness and Training

SUBCAT ID CYFUN: PR.AT-5

Maatregel: PR.AT-5.1

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat het personeel dat verantwoordelijk is voor de fysieke bescherming en beveiliging van de kritieke systemen en faciliteiten van de organisatie via opleiding gekwalificeerd is, voordat privileges worden verleend, en dat het zijn verantwoordelijkheden begrijpt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-1

Maatregel: PR.DS-1.1

SUB-SUBCATEGORIE: De organisatie moet haar kritieke systeeminformatie die als kritisch/gevoelig is aangemerkt, beschermen wanneer deze in rust is.

RICHTLIJNEN: De onderstaande maatregelen kunnen worden overwogen:

- Overweeg het gebruik van encryptietechnieken voor gegevensopslag, gegevensoverdracht of gegevenstransport (bijv. laptop, USB).
- Overweeg encryptie van eindgebruikersapparaten en verwijderbare media die gevoelige gegevens bevatten (bv. harde schijven, laptops, mobiele apparaten, USB-opslagapparaten, ...). Dit kan bijvoorbeeld gebeuren met Windows BitLocker®, VeraCrypt, Apple FileVault®, Linux® dm-crypt, ...
- Overweeg encryptie van gevoelige gegevens die in de cloud zijn opgeslagen.
- Speciale beveiligingen kunnen worden geïmplementeerd om ongeoorloofde toegang tot, vervorming of wijziging van systeemgegevens en auditgegevens te voorkomen (bijvoorbeeld beperkte toegangsrechten, dagelijkse back-ups, gegevensversleuteling, installatie van een firewall).
- Versleutel harde schijven, externe media, opgeslagen bestanden, configuratiebestanden en gegevens die in de cloud zijn opgeslagen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-2

Maatregel: PR.DS-2.1

SUB-SUBCATEGORIE: De organisatie moet haar kritieke systeeminformatie die als kritisch/gevoelig is aangemerkt, beschermen wanneer deze in transit is.

RICHTLIJNEN: De onderstaande maatregelen kunnen worden overwogen:

- Wanneer de organisatie vaak gevoelige documenten of e-mails verzendt, kan worden overwogen om die documenten en/of e-mails te versleutelen met geschikte, ondersteunde en toegestane softwaretools.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-3

Maatregel: PR.DS-3.1

SUB-SUBCATEGORIE: Activa en media moeten veilig worden verwijderd.

RICHTLIJNEN: • Zorg er bij het verwijderen van materiële activa zoals bedrijfscomputers/laptops, servers, harde schijf(sen) en andere opslagmedia

(USB-stations, papier...) voor dat alle gevoelige bedrijfs- of persoonsgegevens veilig worden gewist (incl. elektronisch "gewist") voordat ze worden verwijderd en vervolgens fysiek worden vernietigd (of opnieuw in gebruik worden genomen). Dit wordt ook wel "opschonen" genoemd en houdt dus verband met de eis en de richtsnoeren in PR.IP-6.

- Overweeg een toepassing voor wissen op afstand te installeren op laptops, tablets, mobiele telefoons en andere mobiele apparaten van het bedrijf.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-3

Maatregel: PR.DS-3.2

SUB-SUBCATEGORIE: De organisatie moet de aansprakelijkheid voor alle bedrijfskritische bedrijfsmiddelen gedurende de gehele levenscyclus van het systeem afdwingen, met inbegrip van verwijdering, overdracht en vervreemding.

RICHTLIJNEN: Aansprakelijkheid kan het volgende omvatten:

- De toestemming om bedrijfskritische activa de faciliteit te laten betreden of te verlaten.
- Toezicht houden op en bijhouden van documentatie over de verplaatsingen van bedrijfskritische activa.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-3

Maatregel: PR.DS-3.3

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat verwijderingsacties worden goedgekeurd, gevolgd, gedocumenteerd en geverifieerd.

RICHTLIJNEN: Verwijderingsacties omvatten sanering van de media (zie PR.IP-6).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-3

Maatregel: PR.DS-3.4

SUB-SUBCATEGORIE: De organisatie zorgt ervoor dat de nodige maatregelen worden genomen om verlies, misbruik, beschadiging of diefstal van activa tegen te gaan.

RICHTLIJNEN: Dit kan gebeuren door beleid, processen & procedures (rapportage), technische & organisatorische middelen (encryptie, toegangscontrole (AC), Mobile Device Management (MDM), monitoring, veilig wissen, bewustmaking, ondertekende gebruikersovereenkomst, richtlijnen & handleidingen, back-ups, bijwerken van inventaris ...).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-4

Maatregel: PR.DS-4.1

SUB-SUBCATEGORIE: De capaciteitsplanning moet ervoor zorgen dat er voldoende middelen zijn voor de kritische systeeminformatieverwerking, netwerken, telecommunicatie en gegevensopslag van de organisatie.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-4

Maatregel: PR.DS-4.2



SUB-SUBCATEGORIE: De kritische systemen van de organisatie moeten worden beschermd tegen denial-of-service aanvallen of het effect van dergelijke aanvallen moet ten minste worden beperkt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-4

Maatregel: PR.DS-4.3

SUB-SUBCATEGORIE: Auditgegevens met betrekking tot de kritieke systemen van de organisatie moeten naar een alternatief systeem worden overgebracht.

RICHTLIJNEN: Wees ervan bewust dat logdiensten een knelpunt kunnen worden en de goede werking van de bronsystemen kunnen belemmeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-5

Maatregel: PR.DS-5.1

SUB-SUBCATEGORIE: De organisatie neemt passende maatregelen die leiden tot de bewaking van haar kritische systemen aan de buitengrenzen en kritische interne punten wanneer ongeoorloofde toegang en activiteiten, met inbegrip van het lekken van gegevens, worden ontdekt.

RICHTLIJNEN: • Overweeg specifieke beschermingsmaatregelen (beperkte toegangsrechten, dagelijkse back-ups, gegevensversleuteling, installatie van firewalls, enz.).

• Overweeg een frequente audit van de configuratie van de centrale directory (Active Directory in een Windows-omgeving), met specifieke aandacht voor de toegang tot gegevens van belangrijke personen in het bedrijf.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-6

Maatregel: PR.DS-6.1

SUB-SUBCATEGORIE: De organisatie moet software-, firmware- en informatie-integriteitscontroles uitvoeren om ongeoorloofde wijzigingen in haar kritieke systeemcomponenten tijdens opslag, vervoer, opstarten en wanneer dit nodig is op te sporen.

RICHTLIJNEN: Met de modernste mechanismen voor integriteitscontrole (bv. pariteitscontroles, cyclische redundantiecontroles, cryptografische hashes) en de bijbehorende instrumenten kan de integriteit van informatiesystemen en gehoste toepassingen automatisch worden bewaakt.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-6

Maatregel: PR.DS-6.2

SUB-SUBCATEGORIE: De organisatie moet waar mogelijk geautomatiseerde instrumenten toepassen om een melding te geven wanneer tijdens de integriteitscontrole discrepanties worden ontdekt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Data Security

SUBCAT ID CYFUN: PR.DS-6

Maatregel: PR.DS-6.3

SUB-SUBCATEGORIE: De organisatie moet automatische reacties met vooraf gedefinieerde veiligheidswaarborgen implementeren wanneer integriteitsschendingen worden ontdekt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Data Security  
SUBCAT ID CYFUN: PR.DS-7  
Maatregel: PR.DS-7.1  
SUB-SUBCATEGORIE: De ontwikkelings- en testomgeving(en) moet(en) worden geïsoleerd van de productieomgeving.  
RICHTLIJNEN: • Elke verandering die men wil aanbrengen in de ICT/OT-omgeving moet eerst worden getest in een omgeving die verschilt en gescheiden is van de productieomgeving (operationele omgeving) voordat die verandering daadwerkelijk wordt doorgevoerd. Op die manier kan het effect van die veranderingen worden geanalyseerd en kunnen aanpassingen worden gedaan zonder de operationele activiteiten te verstoren.  
• Overweeg het toevoegen en testen van cyberbeveiligingsfuncties al tijdens de ontwikkeling ("secure development lifecycle" principes).

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Data Security  
SUBCAT ID CYFUN: PR.DS-8  
Maatregel: PR.DS-8.1  
SUB-SUBCATEGORIE: De organisatie moet hardware-integriteitscontroles uitvoeren om ongeoorloofde sabotage van de hardware van haar kritieke systemen op te sporen.  
RICHTLIJNEN: Met de modernste ("state-of-the-practice") mechanismen voor integriteitscontrole (bv. pariteitscontroles, cyclische redundantiecontroles, cryptografische hashes) en de bijbehorende instrumenten kan de integriteit van informatiesystemen en gehoste toepassingen automatisch worden bewaakt.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Data Security  
SUBCAT ID CYFUN: PR.DS-8  
Maatregel: PR.DS-8.2  
SUB-SUBCATEGORIE: De organisatie moet de detectie van ongeoorloofde sabotage van de hardware van haar kritieke systemen opnemen in de incidentenbestrijdingscapaciteit van de organisatie.  
RICHTLIJNEN:

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-1  
Maatregel: PR.IP-1.1  
SUB-SUBCATEGORIE: De organisatie moet een basisconfiguratie voor haar bedrijfskritische systemen ontwikkelen, documenteren en bijhouden.  
RICHTLIJNEN: • Baseline-configuraties omvatten bijvoorbeeld informatie over de bedrijfskritische systemen van de organisatie, de huidige versienummers en patchinformatie van besturingssystemen en toepassingen, configuratie-instellingen/parameters, netwerktopologie en de logische plaatsing van die componenten binnen de systeemarchitectuur.  
• De netwerktopologie moet de zenuwpunten van de IT/OT-omgeving omvatten (externe verbindingen, servers die gegevens en/of gevoelige functies hosten, beveiliging van DNS-diensten, enz.).

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-1  
Maatregel: PR.IP-1.2  
SUB-SUBCATEGORIE: De organisatie moet haar bedrijfskritische systemen zodanig configureren dat zij alleen essentiële mogelijkheden bieden. Daarom moet de

basisconfiguratie worden herzien en moeten onnodige mogelijkheden worden uitgeschakeld.

RICHTLIJNEN: • De configuratie van een systeem om alleen de door de organisatie gedefinieerde essentiële functies te leveren, staat bekend als het "concept van de minste functionaliteit ("concept of least functionality")".

- Mogelijkheden omvatten functies, poorten, protocollen, software en/of diensten.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-2

Maatregel: PR.IP-2.1

SUB-SUBCATEGORIE: De levenscyclus van de ontwikkeling ("System Development Life Cycle") van systemen en toepassingen moet beveiligingsoverwegingen omvatten.

RICHTLIJNEN: • De levenscyclus voor systeem- en applicatieontwikkeling zou het aankoopproces van de bedrijfskritische systemen van de organisatie en de onderdelen daarvan moeten omvatten.

- Er zou moeten worden overwogen om (webapplicatie) ontwikkelaars bewust te maken van kwetsbaarheden, preventietraining te geven, en geavanceerde training in "social engineering" voor belangrijke functies.

- Bij het hosten van op internet gerichte toepassingen zou de implementatie van een Web Application Firewall (WAF) moeten worden overwogen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-2

Maatregel: PR.IP-2.2

SUB-SUBCATEGORIE: Het ontwikkelingsproces voor kritieke systemen en systeemcomponenten moet de volledige ontwerpcyclus omvatten en voorziet in een beschrijving van de functionele eigenschappen van veiligheidscontroles, en in ontwerp- en uitvoeringsinformatie voor veiligheidsrelevante systeeminterfaces.

RICHTLIJNEN: De ontwikkelingscyclus omvat ondermeer:

- Alle ontwikkelingsfasen: specificatie, ontwerp, ontwikkeling, uitvoering.
- Configuratiebeheer voor geplande en ongeplande wijzigingen en wijzigingsbeheer tijdens de ontwikkeling.
- Fouten opsporen en oplossen.
- Veiligheidstesten.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-3

Maatregel: PR.IP-3.1

SUB-SUBCATEGORIE: Wijzigingen moeten worden getest en gevalideerd vóórdat zij in operationele systemen worden doorgevoerd.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-3

Maatregel: PR.IP-3.2

SUB-SUBCATEGORIE: Voor geplande wijzigingen in de kritieke systemen van de organisatie moet een veiligheidsimpactanalyse worden uitgevoerd in een afzonderlijke testomgeving alvorens deze in een operationele omgeving worden geïmplementeerd.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-4  
Maatregel: PR.IP-4.1  
SUB-SUBCATEGORIE: Back-ups voor bedrijfskritische gegevens van de organisatie moeten worden uitgevoerd en opgeslagen op een ander systeem dan het apparaat waarop de oorspronkelijke gegevens zich bevinden.  
RICHTLIJNEN: De bedrijfskritische systeemgegevens van de organisatie omvatten bijvoorbeeld software, configuraties en instellingen, documentatie, systeemconfiguratiegegevens waaronder back-ups van computerconfiguratie, back-ups van applicatieconfiguratie, enz.  
• Overweeg een regelmatige back-up en zet deze periodiek offline.  
• Doelstellingen inzake hersteltijd ("recovery time") en herstelpunt ("recovery point") moeten worden overwogen.  
• Overweeg de gegevensback-up van de organisatie niet op hetzelfde netwerk op te slaan als het netwerk waarop de oorspronkelijke gegevens staan en zorg voor een offline kopie. Dit voorkomt onder meer bestandsversleuteling door hackers (risico op ransomware).

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-4  
Maatregel: PR.IP-4.2  
SUB-SUBCATEGORIE: De betrouwbaarheid en integriteit van de back-ups moet regelmatig worden geverifieerd en getest.  
RICHTLIJNEN: Dit houdt in dat de procedures voor het herstellen van de back-up regelmatig moeten worden getest.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-4  
Maatregel: PR.IP-4.3  
SUB-SUBCATEGORIE: Verificatie van back-ups moet worden gecoördineerd met de functies in de organisatie die verantwoordelijk zijn voor gerelateerde plannen.  
RICHTLIJNEN: • Gerelateerde plannen zijn bijvoorbeeld bedrijfscontinuïteitsplannen, rampherstelplannen, bedrijfscontinuïteitsplannen, crisiscommunicatieplannen, plannen voor kritieke infrastructuur en reactieplannen voor cyberincidenten.  
• Tijdens het testen van het rampenplan moeten de back-upgegevens worden hersteld.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-4  
Maatregel: PR.IP-4.4  
SUB-SUBCATEGORIE: Er moet een afzonderlijke alternatieve opslaglocatie voor systeemback-ups worden uitgebaat waar dezelfde veiligheidswaarborgen worden gebruikt als de primaire opslaglocatie.  
RICHTLIJNEN: Een offline back-up van uw gegevens wordt idealiter opgeslagen op een andere fysieke locatie dan de oorspronkelijke gegevensbron en waar mogelijk off site voor extra bescherming en beveiliging.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Information Protection Processes & Procedures  
SUBCAT ID CYFUN: PR.IP-4  
Maatregel: PR.IP-4.5  
SUB-SUBCATEGORIE: De back-up van kritieke systemen wordt gescheiden van de back-up van kritieke informatie.

RICHTLIJNEN: De scheiding tussen de back-up van kritieke systemen en de back-up van kritieke informatie zal normaal leiden tot een kortere hersteltijd.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-5

Maatregel: PR.IP-5.1

SUB-SUBCATEGORIE: De organisatie moet beleid en procedures vaststellen, uitvoeren en handhaven met betrekking tot nood- en veiligheidssystemen, brandbeveiligingssystemen en omgevingscontroles voor haar kritische systemen.

RICHTLIJNEN: De onderstaande maatregelen kunnen worden overwogen:

- Beveiliging van onbeheerde computerapparatuur met hangsloten of een locker-en sleutelsysteem.
- Brandbestrijdingsmechanismen die rekening houden met de kritische systeemomgeving van de organisatie (zo kunnen watersprinklersystemen gevaarlijk zijn in specifieke omgevingen).

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-5

Maatregel: PR.IP-5.2

SUB-SUBCATEGORIE: De organisatie moet branddetectieapparatuur implementeren die in geval van brand automatisch wordt geactiveerd en sleutelpersoneel verwittigt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-6

Maatregel: PR.IP-6.1

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat de gegevens van haar kritieke systemen overeenkomstig het beleid worden vernietigd.

RICHTLIJNEN: • Verwijderingsacties omvatten sanering van de media (zie PR.DS-3).

- Er zijn twee hoofdtypen media in gebruik:
  - o Hard copy media (fysieke representaties van informatie)
  - o Elektronische of soft copy media (de bits en bytes in harde schijven, random access memory (RAM), read-only memory (ROM), schijven, geheugenapparaten, telefoons, mobiele computers, netwerkkapparatuur...)

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-6

Maatregel: PR.IP-6.2

SUB-SUBCATEGORIE: De vernietigingsprocessen moeten worden gedocumenteerd en getest.

RICHTLIJNEN: • Vernietigingsprocessen omvatten procedures en apparatuur.

- Overweeg niet-destructieve reinigingstechnieken toe te passen op draagbare opslagapparatuur.
- Overweeg vernietigingsprocedures proportioneel tot de vertrouwelijkheidseisen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-7

Maatregel: PR.IP-7.1

SUB-SUBCATEGORIE: De organisatie moet verbeteringen die voortvloeien uit de monitoring, metingen, beoordelingen en geleerde lessen verwerken in de actualisering van het beschermingsproces (continue verbetering).  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-7

Maatregel: PR.IP-7.2

SUB-SUBCATEGORIE: De organisatie moet onafhankelijke teams voorzien om de beschermingsprocedure(s) te beoordelen.

RICHTLIJNEN: • Onafhankelijke teams kunnen bestaan uit intern of extern onpartijdig personeel.

• Onpartijdigheid houdt in dat de beoordelaars vrij zijn van elke vermeende of werkelijke

belangenverstrengeling met betrekking tot de ontwikkeling, de exploitatie of het beheer van het te beoordelen kritieke systeem van de organisatie of met betrekking tot de bepaling van de doeltreffendheid van de veiligheidscontrole.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-7

Maatregel: PR.IP-7.3

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat het beveiligingsplan voor haar kritieke systemen de toetsing, het testen en de voortdurende verbetering van de beveiligingsprocessen faciliteert.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-8

Maatregel: PR.IP-8.1

SUB-SUBCATEGORIE: De organisatie moet met aangeduide partners samenwerken en informatie delen over haar kritieke systeem gerelateerde beveiligingsincidenten en risicobeperkende (mitigatie) maatregelen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-8

Maatregel: PR.IP-8.2

SUB-SUBCATEGORIE: De doeltreffendheid van de toegepaste beschermingstechnologieën moet worden gecommuniceerd aan de toepasselijke partijen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-8

Maatregel: PR.IP-8.3

SUB-SUBCATEGORIE: De organisatie moet, waar mogelijk, geautomatiseerde mechanismen toepassen om te helpen bij informatiedeling.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-9

Maatregel: PR.IP-9.1

SUB-SUBCATEGORIE: Incidentresponsplannen (Incident Response en Business Continuity) en herstelplannen (Incident Recovery en Disaster Recovery) moeten worden opgesteld, bijgehouden, goedgekeurd en getest om de doeltreffendheid ervan en de gereedheid voor de uitvoering te bepalen.

RICHTLIJNEN: • Het incident response plan is de documentatie van een vooraf bepaalde reeks instructies of procedures om een kwaadaardige cyberaanval op te sporen, erop te reageren en de gevolgen ervan te beperken.

• De plannen zouden hersteldoelstellingen, herstellprioriteiten, metingen (statistieken), rollen m.b.t. bedrijfscontinuïteit, personeelstaken en contactinformatie moeten bevatten.

• De instandhouding van essentiële functies ondanks systeemverstoring en het uiteindelijke herstel van de systemen van de organisatie zou moeten worden geadresseerd.

• Er zou moeten worden overwogen het type incidenten, middelen en managementondersteuning te definiëren om de capaciteit voor incidentenbestrijding en noodsituaties doeltreffend te handhaven en verder te verbeteren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-9

Maatregel: PR.IP-9.2

SUB-SUBCATEGORIE: De organisatie moet de ontwikkeling en het testen van incidentbestrijdingsplannen en herstelplannen coördineren met de belanghebbenden die verantwoordelijk zijn voor de desbetreffende plannen.

RICHTLIJNEN: Verwante plannen zijn bijvoorbeeld bedrijfscontinuïteitsplannen, ramherstelplannen, bedrijfscontinuïteitsplannen, crisiscommunicatieplannen, plannen voor kritieke infrastructuur, reactieplannen voor cyberincidenten en noodplannen voor omwonenden.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-11

Maatregel: PR.IP-11.1

SUB-SUBCATEGORIE: Het personeel dat toegang heeft tot de meest kritieke informatie of technologie van de organisatie moet worden geverifieerd.

RICHTLIJNEN: • De toegang tot kritieke informatie of technologie moet in overweging worden genomen bij de aanwerving, tijdens het dienstverband en bij de beëindiging van het dienstverband.

• Bij achtergrondcontroles moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethiek in verhouding tot de bedrijfsvereisten, de classificatie van de te raadplegen informatie en de gepercipieerde risico's.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-11

Maatregel: PR.IP-11.2

SUB-SUBCATEGORIE: Er moet een proces voor informatie- en cyberbeveiliging worden ontwikkeld en gehandhaafd dat van toepassing is bij de aanwerving, tijdens het dienstverband en bij de beëindiging van het dienstverband.

RICHTLIJNEN: Het proces voor informatie- en cyberbeveiliging van het personeel zou de toegang tot kritieke informatie of technologie moeten omvatten; controles van de achtergrond; gedragscode; rollen, bevoegdheden en verantwoordelijkheden...

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Information Protection Processes & Procedures

SUBCAT ID CYFUN: PR.IP-12

Maatregel: PR.IP-12.1

SUB-SUBCATEGORIE: De organisatie moet een gedocumenteerd proces vaststellen en bijhouden dat een voortdurende evaluatie mogelijk maakt van de kwetsbaarheden en de strategieën om deze te verminderen.

RICHTLIJNEN: • Er zou moeten worden nagegaan welke bronnen kwetsbaarheden in de geïdentificeerde componenten kunnen melden en updates kunnen verspreiden (websites van software-uitgevers, website van het CERT, website van het ENISA).

• De organisatie moet nagaan waar haar kritieke systemen kwetsbaar zijn voor tegenstanders.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.1

SUB-SUBCATEGORIE: Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.

RICHTLIJNEN: Het volgende kan in overweging worden genomen:

- Beperk u tot het installeren van alleen die toepassingen (besturingssystemen, firmware of plug-ins) die u nodig hebt om uw bedrijf te runnen en werk ze regelmatig bij.
- U mag alleen een actuele en door de leverancier ondersteunde versie van de software installeren die u wilt gebruiken. Het kan nuttig zijn om elke maand een dag vast te leggen om op patches te controleren.
- Er zijn producten die uw systeem kunnen scannen en u verwittigen wanneer er een update is voor een toepassing die u hebt geïnstalleerd. Als u een van deze producten gebruikt, zorg er dan voor dat het op updates controleert voor elke toepassing die u gebruikt.
- Installeer patches en beveiligingsupdates tijdig.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.2

SUB-SUBCATEGORIE: De organisatie moet preventief onderhoud en reparaties aan haar kritische systeemcomponenten plannen, uitvoeren en documenteren volgens goedgekeurde processen en instrumenten.

RICHTLIJNEN: De volgende maatregelen kunnen worden overwogen:

- Voer tijdig beveiligingsupdates uit voor alle software.
- Automatiseer het updateproces en controleer de doeltreffendheid ervan.
- Voer een interne patchingcultuur in voor desktops, mobiele apparaten, servers, netwerkcomponenten, enz. om ervoor te zorgen dat updates worden bijgehouden.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.3

SUB-SUBCATEGORIE: De organisatie moet voorkomen dat onderhoudsapparatuur die kritieke systeeminformatie van de organisatie bevat, door onbevoegden wordt verwijderd.

RICHTLIJNEN: Deze controle is voornamelijk gericht op OT/ICS-omgevingen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.4



SUB-SUBCATEGORIE: De organisatie moet voorafgaandelijke goedkeuring, controle en toezicht op onderhoudsinstrumenten voor gebruik op haar kritieke systemen afdwingen.

RICHTLIJNEN: Onderhoudsinstrumenten kunnen hardware/software diagnostische testapparatuur, hardware/software packet sniffers en laptops omvatten.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.5

SUB-SUBCATEGORIE: Onderhoudsinstrumenten en draagbare opslagapparaten moeten worden geïnspecteerd wanneer zij de faciliteit worden binnengebracht en moeten worden beschermd door anti\_x0002\_malwareoplossingen, zodat zij worden gescand op kwaadaardige code voordat zij op de systemen van de organisatie worden gebruikt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.6

SUB-SUBCATEGORIE: De organisatie moet na onderhoud of reparatie/patching van hardware en software de beveiligingscontroles nazien en de nodige maatregelen nemen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-1

Maatregel: PR.MA-1.7

SUB-SUBCATEGORIE: The organization shall verify security controls following hardware and software maintenance or repairs/patching and take action as appropriate.

RICHTLIJNEN:

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-2

Maatregel: PR.MA-2.1

SUB-SUBCATEGORIE: Onderhoud op afstand mag alleen plaatsvinden na voorafgaande goedkeuring, toezicht om ongeoorloofde toegang te voorkomen, en goedkeuring van het resultaat van de onderhoudsactiviteiten zoals beschreven in goedgekeurde processen of procedures.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-2

Maatregel: PR.MA-2.2

SUB-SUBCATEGORIE: De organisatie moet eisen dat diagnostische diensten met betrekking tot onderhoud op afstand worden uitgevoerd vanaf een systeem met een beveiliging die vergelijkbaar is met de beveiliging die op het gelijkwaardige kritieke systeem van de organisatie is geïmplementeerd.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Maintenance

SUBCAT ID CYFUN: PR.MA-2

Maatregel: PR.MA-2.3

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat sterke authenticatie, registratie en sessiebeëindiging voor onderhoud op afstand worden toegepast.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-1

Maatregel: PR.PT-1.1

SUB-SUBCATEGORIE: Logs worden bijgehouden, gedocumenteerd en geëvalueerd.

RICHTLIJNEN: • Zorg ervoor dat de activiteitenregistratiefunctie ("activity logging functionality ") van beschermings-

/detectiehardware of -software (bv. firewalls, antivirus) is ingeschakeld.

• Logs moeten worden geback-up't en opgeslagen voor een vooraf bepaalde periode (zie ook PR.DS-4).

• De logs moeten worden nagezien op ongebruikelijke of ongewenste trends, zoals een groot gebruik van sociale media websites of een ongebruikelijk aantal virussen dat consequent op een bepaalde computer wordt aangetroffen. Deze trends kunnen wijzen op een ernstiger probleem of op de noodzaak van strengere bescherming op een bepaald gebied.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-1

Maatregel: PR.PT-1.2

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat de logs een referentie tijdsbron of interne klok tijdstempel bevatten die wordt vergeleken en gesynchroniseerd met een referentie tijdsbron.

RICHTLIJNEN: Referentie tijdsbronnen zijn bijvoorbeeld een interne NTP-server (Network Time Protocol), een radioklok, een atoomklok en een GPS-tijdsbron.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-1

Maatregel: PR.PT-1.3

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat storingen in de verwerking van audits op de systemen van de organisatie waarschuwingen genereren en bepaalde reacties teweegbrengen.

RICHTLIJNEN: Het gebruik van System Logging Protocol (Syslog) servers kan worden overwogen.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-1

Maatregel: PR.PT-1.4

SUB-SUBCATEGORIE: De organisatie moet bevoegde personen in staat stellen de auditmogelijkheden uit te breiden wanneer gebeurtenissen dat vereisen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-2

Maatregel: PR.PT-2.1

SUB-SUBCATEGORIE: De beperking van het gebruik van draagbare opslagapparatuur moet worden gewaarborgd door een passend gedocumenteerd beleid en ondersteunende beveiligingen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect

FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-2  
Maatregel: PR.PT-2.2  
SUB-SUBCATEGORIE: Draagbare opslagapparatuur die systeemgegevens bevat, moet tijdens transit en wanneer in opslag worden gecontroleerd en beschermd.  
RICHTLIJNEN: Bescherming en controle kan het scannen van alle draagbare opslagapparaten op kwaadaardige code omvatten voordat zij op de systemen van de organisatie worden gebruikt.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-2  
Maatregel: PR.PT-2.3  
SUB-SUBCATEGORIE: De organisatie moet het aansluiten van verwijderbare media technisch verbieden, tenzij strikt noodzakelijk; in andere gevallen moet het uitvoeren van autoruns vanaf dergelijke media worden uitgeschakeld.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-3  
Maatregel: PR.PT-3.1  
SUB-SUBCATEGORIE: De organisatie moet de bedrijfskritische systemen zo configureren dat zij alleen essentiële mogelijkheden bieden.  
RICHTLIJNEN: Overweeg de toepassing van het beginsel van de minste functionaliteit ("least functionality") op toegangssystemen en -middelen (zie ook PR.AC-4).

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-3  
Maatregel: PR.PT-3.2  
SUB-SUBCATEGORIE: De organisatie moet binnen haar kritische systemen vooraf gedefinieerde functies, poorten, protocollen en diensten uitschakelen die zij onnodig acht.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-3  
Maatregel: PR.PT-3.3  
SUB-SUBCATEGORIE: De organisatie moet technische beveiligingen implementeren om een beleid van "alles weigeren" ("deny-all") en "toestemming per uitzondering" ("permit-by-exception") af te dwingen, zodat alleen geautoriseerde softwareprogramma's kunnen worden uitgevoerd.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Protect  
FUNCTIONS: Protect  
CATEGORY NAME CYFUN: Protective technology  
SUBCAT ID CYFUN: PR.PT-4  
Maatregel: PR.PT-4.1  
SUB-SUBCATEGORIE: Web- en e-mailfilters moeten worden geïnstalleerd en gebruikt.  
RICHTLIJNEN: • E-mailfilters zouden kwaadaardige e-mails moeten kunnen detecteren, en het filteren zou moeten worden geconfigureerd op basis van het type berichtbijlagen, zodat bestanden van de gespecificeerde types automatisch worden verwerkt (bv. verwijderd).

- Webfilters zouden de gebruiker moeten waarschuwen wanneer een website mogelijk malware bevat en mogelijk voorkomen dat gebruikers die website bezoeken.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-4

Maatregel: PR.PT-4.2

SUB-SUBCATEGORIE: De organisatie moet de informatiestromen/gegevensstromen binnen haar kritieke systemen en tussen onderling verbonden systemen beheersen.

RICHTLIJNEN: Overweeg het volgende:

- De informatiestroom kan bijvoorbeeld worden ondersteund door het labelen of kleuren van fysieke connectoren als hulpmiddel bij het handmatig aansluiten.
- Door inspectie van de inhoud van berichten kan een informatiestroombeleid worden afgedwongen. Een bericht met een commando aan een actuator mag bijvoorbeeld niet tussen het besturingsnetwerk en een ander netwerk worden doorgegeven.
- Fysieke adressen (bv. een seriële poort) kunnen impliciet of expliciet geassocieerd worden met labels of attributen (bv. hardware I/O-adres). Handmatige methoden zijn typisch statisch. Beleidsmechanismen voor labels of attributen kunnen worden geïmplementeerd in hardware, firmware en software die de toegang tot apparaten controleert of heeft, zoals stuurprogramma's en communicatiecontrollers.

### FUNCTIONS: Protect

FUNCTIONS: Protect

CATEGORY NAME CYFUN: Protective technology

SUBCAT ID CYFUN: PR.PT-4

Maatregel: PR.PT-4.3

SUB-SUBCATEGORIE: De organisatie moet de interface voor externe communicatie beheren door een verkeersstroombeleid ("traffic flow") vast te stellen, dat de vertrouwelijkheid en integriteit van de verzonden informatie beschermt.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Anomalies and Events

SUBCAT ID CYFUN: DE.AE-1

Maatregel: DE.AE-1.1

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat een baseline van netwerkoperaties en verwachte gegevensstromen voor haar kritieke systemen wordt vastgesteld, gedocumenteerd en bijgehouden om gebeurtenissen te volgen.

RICHTLIJNEN: • Overweeg lokale logging op al uw systemen en netwerkapparaten in te schakelen en deze gedurende een bepaalde periode te bewaren, bijvoorbeeld tot 6 maanden.

- Zorg ervoor dat uw logs voldoende informatie bevatten (bron, datum, gebruiker, tijdstempel, enz.) en dat u voldoende opslagruimte hebt voor het genereren ervan.
- Overweeg uw logs te centraliseren.
- Overweeg de inzet van een Security Information and Event Management tool (SIEM) die de correlatie en analyse van uw gegevens vergemakkelijkt.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Anomalies and Events

SUBCAT ID CYFUN: DE.AE-2

Maatregel: DE.AE-2.1

SUB-SUBCATEGORIE: De organisatie moet gedetecteerde events evalueren en analyseren om inzicht te krijgen in aanvalsdoelen en -methoden.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-2  
Maatregel: DE.AE-2.2  
SUB-SUBCATEGORIE: De organisatie moet waar mogelijk geautomatiseerde mechanismen toepassen om gedetecteerde events te beoordelen en te analyseren.  
RICHTLIJNEN: Overweeg uw logs regelmatig te bekijken om anomalieën of abnormale gebeurtenissen te identificeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-3  
Maatregel: DE.AE-3.1  
SUB-SUBCATEGORIE: De functionaliteit voor activiteitenregistratie ("activity logging") van beschermings-/detectieapparatuur of -software (bv. firewalls, antivirus) moet worden ingeschakeld, er moet een back-up van worden gemaakt en deze moet worden nagezien.  
RICHTLIJNEN: • Logs moeten worden geback-upt en opgeslagen voor een vooraf bepaalde periode.  
• De logs moeten worden bekeken op ongebruikelijke of ongewenste trends, zoals een groot gebruik van sociale media websites of een ongebruikelijk aantal virussen dat consequent op een bepaalde computer wordt aangetroffen. Deze trends kunnen wijzen op een ernstiger probleem of op de noodzaak van strengere bescherming op een bepaald gebied. Zie ook PR.PT-1.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-3  
Maatregel: DE.AE-3.2  
SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat gegevens over events worden verzameld en gecorreleerd voor alle kritieke systemen, waarbij gebruik wordt gemaakt van verschillende bronnen, zoals verslagen over events, monitoring d.m.v. audits, netwerkmonitoring, monitoring op fysieke toegang en verslagen van gebruikers/beheerders.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-3  
Maatregel: DE.AE-3.3  
SUB-SUBCATEGORIE: De organisatie moet de analyse van incidenten waar mogelijk integreren met de analyse van informatie over het scannen van kwetsbaarheden, prestatiegegevens, de bewaking van haar kritieke systemen en de bewaking van faciliteiten om nog beter in staat te zijn ongewenste of ongewone activiteiten op te sporen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-4  
Maatregel: DE.AE-4.1  
SUB-SUBCATEGORIE: De negatieve gevolgen van gedetecteerde gebeurtenissen voor de activiteiten, activa en personen van de organisatie moeten worden bepaald en gecorreleerd met de resultaten van de risicobeoordeling.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect

CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-5  
Maatregel: DE.AE-5.1  
SUB-SUBCATEGORIE: De organisatie moet geautomatiseerde mechanismen en door het systeem gegenereerde waarschuwingen toepassen ter ondersteuning van de detectie van events en ter ondersteuning van de vaststelling van drempelwaarden voor beveiligingswaarschuwingen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Anomalies and Events  
SUBCAT ID CYFUN: DE.AE-5  
Maatregel: DE.AE-5.2  
SUB-SUBCATEGORIE: De organisatie moet alarmdrempels voor incidenten vaststellen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-1  
Maatregel: DE.CM-1.1  
SUB-SUBCATEGORIE: Firewalls moeten worden geïnstalleerd en gebruikt op de netwerkgrenzen en aangevuld met firewallbescherming op de eindpunten.  
RICHTLIJNEN: • Eindpunten omvatten desktops, laptops, servers...  
• Overweeg, waar mogelijk, smart phones en andere netwerkapparaten op te nemen bij de installatie en het gebruik van firewalls.  
• Overweeg het aantal interconnectiepoorten naar het internet te beperken.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-1  
Maatregel: DE.CM-1.2  
SUB-SUBCATEGORIE: De organisatie moet ongeoorloofd gebruik van haar bedrijfskritische systemen bewaken en identificeren door het opsporen van ongeoorloofde lokale verbindingen, netwerkverbindingen en verbindingen op afstand.  
RICHTLIJNEN: • Monitoring van netwerkcommunicatie zou plaats moeten vinden aan de buitengrens van de bedrijfskritische systemen van de organisatie en aan belangrijke interne grenzen binnen de systemen.  
• Bij het hosten van op internet gerichte toepassingen zou de implementatie van een Web Application Firewall (WAF) kunnen worden overwogen.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-1  
Maatregel: DE.CM-1.3  
SUB-SUBCATEGORIE: De organisatie moet voortdurend toezicht houden op de beveiligingsstatus van haar netwerk om gedefinieerde informatie-/cyberbeveiligingsevents en indicatoren van potentiële informatie-/cyberbeveiligingsevents op te sporen  
RICHTLIJNEN: Het toezicht op de beveiligingsstatus kan het volgende omvatten:  
• Het genereren van systeemwaarschuwingen wanneer er aanwijzingen zijn van een (mogelijke) compromittering.  
• Detectie en rapportage van atypisch gebruik van kritieke systemen van de organisatie.  
• Het aanleggen van auditregistraties voor bepaalde informatie-/cyberbeveiligingsevents.  
• Versterking van de systeembewaking wanneer er een indicatie is van een verhoogd risico.  
Dit zou de fysieke omgeving, personeel en dienstverlener moeten omvatten.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-1  
Maatregel: DE.CM-1.4  
SUB-SUBCATEGORIE: De fysieke omgeving van de faciliteit wordt bewaakt op potentiële informatie-/cyberbeveiligingsincidenten  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-2  
Maatregel: DE.CM-2.1  
SUB-SUBCATEGORIE: De fysieke toegang tot kritieke systemen en apparaten van de organisatie moet, bovenop de fysieke toegangscontrole tot de faciliteit, worden verhoogd door middel van fysieke inbraakalarmen, bewakingsapparatuur, onafhankelijke bewakingsteams.  
RICHTLIJNEN: Het is aanbevolen om alle bezoekers te loggen.

### Entry  
FUNCTIONS:  
CATEGORY NAME CYFUN:  
SUBCAT ID CYFUN:  
Maatregel: DE.CM-2.2  
SUB-SUBCATEGORIE:  
RICHTLIJNEN:

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-3  
Maatregel: DE.CM-3.1  
SUB-SUBCATEGORIE: Er moeten instrumenten voor eindpunt- en netwerkbescherming worden toegepast om het gedrag van de eindgebruiker te monitoren op gevaarlijke activiteiten  
RICHTLIJNEN: Overweeg de inzet van een Intrusion Detection/Prevention systeem (IDS/IPS)

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-3  
Maatregel: DE.CM-3.2  
SUB-SUBCATEGORIE: Eindpunt- en netwerkbeschermingsinstrumenten die het gedrag van eindgebruikers monitoren op gevaarlijke activiteiten, moeten worden beheerd.  
RICHTLIJNEN: • Overweeg het gebruik van een gecentraliseerd logplatform voor de consolidatie en exploitatie van logbestanden.  
• Overweeg om de waarschuwingen die worden gegenereerd vanwege verdachte activiteiten actief te onderzoeken en passende maatregelen te nemen om de bedreiging te verhelpen, bijvoorbeeld door de inzet van een Security Operations Center (SOC)

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-3  
Maatregel: DE.CM-3.3  
SUB-SUBCATEGORIE: Er moet worden toegezien op het gebruik en de installatie van software.  
RICHTLIJNEN: Alleen geautoriseerde software zou mogen worden gebruikt, en de toegangsrechten van gebruikers zou beperkt moeten worden tot de specifieke

gegevens, middelen en toepassingen die nodig zijn om een vereiste taak uit te voeren ("least privilege principle").

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Continuous Monitoring

SUBCAT ID CYFUN: DE.CM-4

Maatregel: DE.CM-4.1

SUB-SUBCATEGORIE: Anti-virus, -spyware en andere -malware programma's moeten worden geïnstalleerd en bijgewerkt.

RICHTLIJNEN: • Malware omvat virussen, spyware en ransomware en zou moeten worden bestreden door anti-virus en anti-spyware software te installeren, te gebruiken en regelmatig bij te werken op elk apparaat dat in het bedrijf wordt gebruikt (waaronder computers, smartphones, tablets en servers).

• Anti-virus- en anti-spywaresoftware zou automatisch moeten controleren op updates in "real-time" of ten minste dagelijks, eventueel gevolgd door een systeemscan.

• Er zou overwogen moeten worden om dezelfde beschermingsmechanismen tegen kwaadaardige code te bieden voor thuiscomputers (bv. telewerken) of persoonlijke apparaten die voor beroepsmatig werk worden gebruikt ("Bring Your Own Device" - BYOD).

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Continuous Monitoring

SUBCAT ID CYFUN: DE.CM-4

Maatregel: DE.CM-4.2

SUB-SUBCATEGORIE: De organisatie moet een systeem opzetten om valse incidenten ("false positives") te detecteren bij het opsporen en uitroeien van kwaadaardige code.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Continuous Monitoring

SUBCAT ID CYFUN: DE.CM-5

Maatregel: DE.CM-5.1

SUB-SUBCATEGORIE: De organisatie dient aanvaardbare en onaanvaardbare mobiele code en mobiele code technologieën te definiëren; en het gebruik van mobiele code binnen het systeem toe te staan, te bewaken en te monitoren.

RICHTLIJNEN: • Mobiele code omvat elk programma, toepassing of inhoud die over een netwerk kan worden verzonden (bv. ingesloten in een e-mail, document of website) en op een systeem op afstand kan worden uitgevoerd. Technologieën voor mobiele code zijn bijvoorbeeld Java-applets, JavaScript, HTML5, WebGL en VBScript.

• Beslissingen over het gebruik van mobiele code in organisatiesystemen zouden gebaseerd moeten zijn op de mogelijkheid dat de code bij kwaadwillig gebruik schade aan de systemen toebrengt. Voor de selectie en het gebruik van geïnstalleerde mobiele code zouden gebruiksbependingen en uitvoeringsrichtsnoeren moeten gelden.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Continuous Monitoring

SUBCAT ID CYFUN: DE.CM-6

Maatregel: DE.CM-6.1

SUB-SUBCATEGORIE: Alle externe verbindingen door verkopers die IT/OT-toepassingen of infrastructuur ondersteunen, moeten worden beveiligd en actief gemonitord om ervoor te zorgen dat tijdens de verbinding alleen toegestane handelingen plaatsvinden.

RICHTLIJNEN: Dit toezicht omvat toegang door onbevoegd personeel, verbindingen, apparaten en software.

### FUNCTIONS: Detect



FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-6  
Maatregel: DE.CM-6.2  
SUB-SUBCATEGORIE: Op de naleving door externe dienstverleners van het beleid en de procedures inzake personeelsbeveiliging en de contractbeveiligingseisen moet toezicht worden gehouden in verhouding tot hun cyberbeveiligingsrisico's.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-7  
Maatregel: DE.CM-7.1  
SUB-SUBCATEGORIE: De bedrijfskritische systemen van de organisatie moeten worden gemonitord op ongeoorloofde toegang van personeel, verbindingen, apparaten, toegangspunten en software.  
RICHTLIJNEN: • Toegang door onbevoegd personeel omvat ook toegang door externe dienstverleners.  
• Discrepanties in de systeeminventaris zouden in het toezicht moeten worden opgenomen.  
• Ongeoorloofde configuratiewijzigingen aan kritieke systemen van de organisatie zouden in de monitoring moeten worden opgenomen.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-7  
Maatregel: DE.CM-7.2  
SUB-SUBCATEGORIE: Ongeoorloofde wijzigingen in de configuratie van de systemen van de organisatie moeten worden gecontroleerd en aangepakt met passende risicobeperkende (mitigatie) maatregelen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-8  
Maatregel: DE.CM-8.1  
SUB-SUBCATEGORIE: De organisatie moet op kwetsbaarheden in haar kritieke systemen en gehoste toepassingen monitoren en ervoor zorgen dat het scannen geen negatieve gevolgen heeft voor de systeemfuncties.  
RICHTLIJNEN: Overweeg de uitvoering van een permanent programma voor het scannen van kwetsbaarheden; met inbegrip van plannen voor rapportage en beperking.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Continuous Monitoring  
SUBCAT ID CYFUN: DE.CM-8  
Maatregel: DE.CM-8.2  
SUB-SUBCATEGORIE: Het scannen van kwetsbaarheden moet analyse, herstel en het delen van informatieomvatten.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect  
FUNCTIONS: Detect  
CATEGORY NAME CYFUN: Detection processes  
SUBCAT ID CYFUN: DE.DP-2  
Maatregel: DE.DP-2.1  
SUB-SUBCATEGORIE: De organisatie moet detectie van abnormale events uitvoeren in overeenstemming met de toepasselijke federale en regionale wetten,

industriële voorschriften en normen, beleidslijnen en andere toepasselijke vereisten.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Detection processes

SUBCAT ID CYFUN: DE.DP-3

Maatregel: DE.DP-3.1

SUB-SUBCATEGORIE: De organisatie moet valideren dat de processen gebruikt voor het detecteren van abnormale events werken zoals bedoeld.

RICHTLIJNEN: • Validatie omvat testen.

• Validatie zou aantoonbaar moeten zijn.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Detection processes

SUBCAT ID CYFUN: DE.DP-4

Maatregel: DE.DP-4.1

SUB-SUBCATEGORIE: De organisatie moet informatie over gedetecteerde events doorgeven aan vooraf bepaalde partijen.

RICHTLIJNEN: Informatie over gedetecteerde events omvat bijvoorbeeld waarschuwingen over atypisch accountgebruik, ongeoorloofde toegang op afstand, draadloze connectiviteit, verbinding met mobiele apparatuur, gewijzigde configuratie-instellingen, contrasterende inventaris van systeemonderdelen, gebruik van onderhoudsmiddelen en niet-lokaal onderhoud, fysieke toegang, temperatuur en vochtigheid, levering en verwijdering van apparatuur, communicatie aan de grenzen van het informatiesysteem, gebruik van mobiele code, gebruik van Voice over Internet Protocol (VoIP) en openbaarmaking van malware.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Detection processes

SUBCAT ID CYFUN: DE.DP-5

Maatregel: DE.DP-5.1

SUB-SUBCATEGORIE: Verbeteringen die voortvloeien uit monitoring, metingen, beoordelingen, tests, evaluatie en de getrokken lessen ("lessons learned") moeten worden opgenomen in de herzieningen van het detectieproces.

RICHTLIJNEN: • Dit resulteert in een voortdurende verbetering van de opsporingsprocessen.

• Het gebruik van onafhankelijke teams om het opsporingsproces te beoordelen zou kunnen worden overwogen.

### FUNCTIONS: Detect

FUNCTIONS: Detect

CATEGORY NAME CYFUN: Detection processes

SUBCAT ID CYFUN: DE.DP-5

Maatregel: DE.DP-5.2

SUB-SUBCATEGORIE: De organisatie moet gespecialiseerde beoordelingen uitvoeren, waaronder grondige ("in depth") monitoring, het scannen van kwetsbaarheden, het testen op kwaadwillende gebruikers, beoordeling van bedreigingen van binnenuit, prestatie-/belastingstests en verificatie- en validatietests op de kritieke systemen van de organisatie.

RICHTLIJNEN: Deze activiteiten kunnen worden uitbesteed, bij voorkeur aan erkende organisaties.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Response Planning

SUBCAT ID CYFUN: RS.RP-1

Maatregel: RS.RP-1.1

SUB-SUBCATEGORIE: Tijdens of na een informatie-/cyberbeveiligingsincident op de kritieke systemen van de organisatie moet een incidentresponsproces, met inbegrip van rollen, verantwoordelijkheden en bevoegdheden, worden uitgevoerd.

RICHTLIJNEN: • Het incidentresponsplan zou een vooraf bepaalde reeks instructies of procedures moeten omvatten om een kwaadaardige cyberaanval op te sporen, erop te reageren en de gevolgen ervan te beperken.

• De rollen, verantwoordelijkheden en bevoegdheden in het incidentresponsplan zouden specifiek betrekking moeten hebben op de betrokken personen, de contactgegevens, de verschillende rollen en verantwoordelijkheden, en wie de beslissing neemt om responsprocedures in gang te zetten, alsook wie het contact zal zijn met de betrokken externe belanghebbenden.

• Er zou moeten worden overwogen de oorzaken van een gebeurtenis op het gebied van informatie-/cyberbeveiliging vast te stellen en een corrigerende maatregel uit te voeren om te voorkomen dat de gebeurtenis zich herhaalt of zich elders voordoet (een infectie met kwaadaardige code op één machine heeft zich niet elders in het netwerk verspreid). De doeltreffendheid van de genomen corrigerende maatregelen moet worden geëvalueerd. De corrigerende maatregelen moeten afgestemd zijn op de gevolgen van het voorval op het gebied van informatie-/cyberbeveiliging.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RS.CO-1

Maatregel: RS.CO-1.1

SUB-SUBCATEGORIE: De organisatie moet ervoor zorgen dat het personeel zijn rol, doelstellingen, herstellprioriteiten, taakvolgorde en toegewezen verantwoordelijkheden voor de reactie op een evenement begrijpt.

RICHTLIJNEN: Overweeg het gebruik van de CCB Incident Management Guide als leidraad bij deze oefening en overweeg zo nodig externe deskundigen in te schakelen. Test uw plan regelmatig en pas het na elk incident aan.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RS.CO-2

Maatregel: RS.CO-2.1

SUB-SUBCATEGORIE: De organisatie moet de rapportage implementeren over informatie-/cyberbeveiligingsincidenten op haar kritieke systemen binnen een door de organisatie bepaald tijdsbestek aan door de organisatie bepaald personeel of bepaalde rollen.

RICHTLIJNEN: Alle gebruikers zouden één contactpunt moeten hebben om elk incident te melden en moeten worden aangemoedigd om dat te doen.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RS.CO-2

Maatregel: RS.CO-2.2

SUB-SUBCATEGORIE: Gebeurtenissen worden gerapporteerd volgens vastgestelde criteria.

RICHTLIJNEN: De criteria voor rapportage zouden moeten worden opgenomen in het incidentresponseplan.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RS.CO-3

Maatregel: RS.CO-3.1

SUB-SUBCATEGORIE: Informatie m.b.t. informatie-/cyberbeveiligingsincidenten moet worden gecommuniceerd aan de werknemers van de organisatie op een manier die zij kunnen begrijpen.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Communications  
SUBCAT ID CYFUN: RS.CO-3  
Maatregel: RS.CO-3.2  
SUB-SUBCATEGORIE: De organisatie deelt informatie over informatie/cyberbeveiligingsincidenten met relevante belanghebbenden zoals voorzien in het responsplan voor incidenten.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Communications  
SUBCAT ID CYFUN: RS.CO-4  
Maatregel: RS.CO-4.1  
SUB-SUBCATEGORIE: De organisatie moet de acties ter bestrijding van informatie-/cyberbeveiligingsincidenten met alle vooraf bepaalde belanghebbenden coördineren.  
RICHTLIJNEN: • Stakeholders voor incident response zijn bijvoorbeeld eigenaren van missies/bedrijven, eigenaren van kritieke systemen van de organisatie, integrators, verkopers, personeelskantoren, fysieke en personeelsbeveiligingskantoren, juridische afdelingen, operationeel personeel en inkoopkantoren.  
• De coördinatie met belanghebbenden zou plaats moeten vinden in overeenstemming met de incidentbestrijdingsplannen.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Communications  
SUBCAT ID CYFUN: RS.CO-5  
Maatregel: RS.CO-5.1  
SUB-SUBCATEGORIE: De organisatie moet, waar toepasselijk, vrijwillig informatie over informatie/cyberbeveiligingsincidenten delen met externe belanghebbenden, beveiligingsgroepen uit de sector... om een breder situationeel bewustzijn te bereiken m.b.t. informatie/cyberbeveiliging.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Analysis  
SUBCAT ID CYFUN: RS.AN-1  
Maatregel: RS.AN-1.1  
SUB-SUBCATEGORIE: De organisatie moet informatie-/cyberbeveiligingsgerelateerde meldingen van detectiesystemen onderzoeken.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Analysis  
SUBCAT ID CYFUN: RS.AN-1  
Maatregel: RS.AN-1.2  
SUB-SUBCATEGORIE: De organisatie moet geautomatiseerde mechanismen invoeren ter ondersteuning van het onderzoek en de analyse van informatie-/cyberbeveiligingsmeldingen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Analysis  
SUBCAT ID CYFUN: RS.AN-2  
Maatregel: RS.AN-2.1

SUB-SUBCATEGORIE: Grondig onderzoek en analyse van de resultaten moeten de basis vormen voor een volledig begrip van de gevolgen van het informatie-/cyberbeveiligingsincident.

RICHTLIJNEN: • Resultaatanalyse kan voortkomen uit de correlatie tussen de informatie van de gedetecteerde gebeurtenis en de uitkomst van risicobeoordelingen. Op die manier wordt inzicht verkregen in de impact van de gebeurtenis in de hele organisatie.  
• Er zou overwogen moeten worden de detectie van ongeoorloofde wijzigingen in zijn kritieke systemen op te nemen in de mogelijkheden om op incidenten te reageren.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Analysis

SUBCAT ID CYFUN: RS.AN-2

Maatregel: RS.AN-2.2

SUB-SUBCATEGORIE: De organisatie moet geautomatiseerde mechanismen invoeren ter ondersteuning van de impactanalyse van incidenten.

RICHTLIJNEN: De implementatie kan variëren van een ticketingsysteem tot een Security Information and Event Management (SIEM).

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Analysis

SUBCAT ID CYFUN: RS.AN-3

Maatregel: RS.AN-3.1

SUB-SUBCATEGORIE: De organisatie moet op verzoek auditcontrole, analyse en rapportage verstrekken voor onderzoeken na de feiten van informatie-/cyberbeveiligingsincidenten.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Analysis

SUBCAT ID CYFUN: RS.AN-3

Maatregel: RS.AN-3.2

SUB-SUBCATEGORIE: De organisatie moet forensische analyses uitvoeren op verzamelde informatie van informatie/cyberincidenten om de hoofdoorzaak ("root cause") vast te stellen.

RICHTLIJNEN: Overweeg zo nodig forensische analyse op verzamelde informatie van informatie/cyberincidenten te gebruiken om de hoofdoorzaak ("root cause") vast te kunnen stellen.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Analysis

SUBCAT ID CYFUN: RS.AN-4

Maatregel: RS.AN-4.1

SUB-SUBCATEGORIE: Informatie-/cyberbeveiligingsincidenten moeten worden ingedeeld naar ernst en impact overeenkomstig de evaluatiecriteria in het incidentbestrijdingsplan.

RICHTLIJNEN: • Er zou overwogen moeten worden de oorzaken van een incident op het gebied van informatie-/cyberbeveiliging vast te stellen, en een corrigerende maatregel uit te voeren, zodat het incident niet meer voorkomt of zich elders voordoet.

• De doeltreffendheid van eventuele corrigerende maatregelen zou geëvalueerd moeten worden.

• De corrigerende maatregelen zouden proportioneel moeten zijn met de gevolgen van het informatie-/cyberbeveiligingsincident.

### FUNCTIONS: Respond

FUNCTIONS: Respond

CATEGORY NAME CYFUN: Analysis

SUBCAT ID CYFUN: RS.AN-5

Maatregel: RS.AN-5.1  
SUB-SUBCATEGORIE: De organisatie moet processen en procedures voor het beheer van kwetsbaarheden toepassen die het verwerken, analyseren en verhelpen van kwetsbaarheden uit interne en externe bronnen omvatten.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Analysis  
SUBCAT ID CYFUN: RS.AN-5  
Maatregel: RS.AN-5.2  
SUB-SUBCATEGORIE: De organisatie moet geautomatiseerde mechanismen invoeren voor het verspreiden en opvolgen aan de belangrijkste belanghebbenden van mitigatiewerkzaamheden in antwoord op informatie over kwetsbaarheden afkomstig uit interne en externe bronnen.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Mitigation  
SUBCAT ID CYFUN: RS.MI-1  
Maatregel: RS.MI-1.1  
SUB-SUBCATEGORIE: De organisatie moet een capaciteit voor het afhandelen van informatie-/cyberbeveiligingsincidenten op haar bedrijfskritische systemen implementeren die de voorbereiding, detectie, analyse, insluiting ("containment"), uitroeiing, herstel en gedocumenteerde risicoaanvaarding omvat.  
RICHTLIJNEN: Een gedocumenteerde risicoaanvaarding heeft betrekking op risico's die volgens de organisatie niet gevaarlijk zijn voor de bedrijfskritische systemen van de organisatie en waarbij de eigenaar van het risico het risico formeel aanvaardt (gerelateerd aan de risicobereidheid, "risk appetite", van de organisatie).

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Improvements  
SUBCAT ID CYFUN: RS.IM-1  
Maatregel: RS.IM-1.1  
SUB-SUBCATEGORIE: De organisatie moet evaluaties uitvoeren na een incident om lessen te trekken uit de reactie op en het herstel van incidenten, en verbetert vervolgens de processen / procedures / technologieën om haar cyberweerbaarheid te vergroten.  
RICHTLIJNEN: Overweeg na elk incident de betrokkenen samen te brengen en samen na te denken over manieren om te verbeteren wat er is gebeurd, hoe het is gebeurd, hoe er is gereageerd, hoe het beter had kunnen gaan, wat er moet gebeuren om herhaling te voorkomen, enz.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Improvements  
SUBCAT ID CYFUN: RS.IM-1  
Maatregel: RS.IM-1.2  
SUB-SUBCATEGORIE: De uit de afhandeling van incidenten geleerde lessen moeten worden vertaald in bijgewerkte of nieuwe procedures voor de afhandeling van incidenten, die op hun beurt moeten worden getest, goedgekeurd en getraind.  
RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Respond  
FUNCTIONS: Respond  
CATEGORY NAME CYFUN: Improvements  
SUBCAT ID CYFUN: RS.IM-2  
Maatregel: RS.IM-2.1

SUB-SUBCATEGORIE: De organisatie moet de reactie- en herstelplannen aanpassen aan veranderingen in haar context.

RICHTLIJNEN: De context van de organisatie heeft betrekking op de organisatiestructuur, haar kritieke systemen, aanvalsvectoren, nieuwe bedreigingen, verbeterde technologie, de bedrijfsomgeving, problemen die zich hebben voorgedaan tijdens de implementatie/uitvoering/testen van het plan en de lessen die zijn geleerd.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Recovery Planning

SUBCAT ID CYFUN: RC.RP-1

Maatregel: RC.RP-1.1

SUB-SUBCATEGORIE: Er moet een herstelproces voor rampen en informatie-/cyberbeveiligingsincidenten worden ontwikkeld en zo nodig uitgevoerd.

RICHTLIJNEN: • Er zou een proces moeten worden ontwikkeld voor de onmiddellijke acties in geval van brand, medisch noodgeval, inbraak, natuurramp of een incident op het gebied van informatie-/cyberbeveiliging.

• Dit proces zou rekening moeten houden met:

o Taken en verantwoordelijkheden, waaronder de vraag wie de beslissing neemt om

herstelprocedures in te leiden en wie het contact zal zijn met de betrokken externe

belanghebbenden.

o Wat te doen met de informatie en informatiesystemen van het bedrijf in geval van een

incident. Dit omvat het afsluiten of vergrendelen van computers, het verhuizen naar een back\_x0002\_up site, het fysiek verwijderen van belangrijke documenten, enz.

o Wie te bellen in geval van een incident.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Recovery Planning

SUBCAT ID CYFUN: RC.RP-1

Maatregel: RC.RP-1.2

SUB-SUBCATEGORIE: De essentiële functies en diensten van de organisatie moeten worden voortgezet met weinig of geen verlies van operationele continuïteit en de continuïteit moet worden gehandhaafd totdat het systeem volledig is hersteld.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Improvements

SUBCAT ID CYFUN: RC.IM-1

Maatregel: RC.IM - 1.1

SUB-SUBCATEGORIE: De organisatie moet de lessen die zijn getrokken uit herstelactiviteiten bij incidenten verwerken in bijgewerkte of nieuwe herstelprocedures voor systemen en dit, na het testen, borgen met een passende opleiding.

RICHTLIJNEN: Er zijn geen aanvullende richtsnoeren.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RC.CO-1

Maatregel: RC.CO-1.1

SUB-SUBCATEGORIE: De organisatie moet de wijze waarop informatie wordt verspreid centraliseren en coördineren, en beheert de wijze waarop de organisatie aan het publiek wordt gepresenteerd.

RICHTLIJNEN: De organisatie moet de wijze waarop informatie wordt verspreid centraliseren en coördineren, en beheert de wijze waarop de organisatie aan het publiek wordt gepresenteerd.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RC.CO-1

Maatregel: RC.CO-1.2

SUB-SUBCATEGORIE: Er moet een Public Relations Officer worden aangesteld.

RICHTLIJNEN: De Public Relations Officer zou moeten overwegen gebruik te maken van vooraf bepaalde externe contacten (bijv. pers, regelgevers, belangengroepen).

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RC.CO-2

Maatregel: RC.CO-2.1

SUB-SUBCATEGORIE: Er moet een crisisbestrijdingsstrategie worden toegepast om de organisatie te beschermen tegen de negatieve gevolgen van een crisis en te helpen haar reputatie te herstellen.

RICHTLIJNEN: Crisisbestrijdingsstrategieën omvatten bijvoorbeeld maatregelen om de beeldvorming over de crisis vorm te geven, de perceptie van de organisatie in crisis te veranderen, en het negatieve effect dat de crisis teweegbrengt te verminderen.

### FUNCTIONS: Recover

FUNCTIONS: Recover

CATEGORY NAME CYFUN: Communications

SUBCAT ID CYFUN: RC.CO-3

Maatregel: RC.CO-3.1

SUB-SUBCATEGORIE: De organisatie moet de herstelactiviteiten meedelen aan vooraf bepaalde belanghebbenden, directie- en managementteams.

RICHTLIJNEN: Communicatie van herstelactiviteiten aan belanghebbenden geldt alleen voor entiteiten die onder de NIS\_x0002\_wetgeving vallen.