Safeonweb
@Work

EEN INITIATIEF VAN

CENTRE FOR CYBER SECURITY BELGIUM

CYBER FUNDAMENTALS

ESSENTIEEL

Versie 2023-03-01

Centrum voor Cybersecurity België
Wetstraat 18
1000 Brussel
België

info@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

Inhoudsopgave

Inleiding

Het **CCB Cyberfundamentals Framework is** een reeks concrete maatregelen om:

- gegevens te beschermen,
- het risico van de meest voorkomende cyberaanvallen aanzienlijk verminderen,
- de cyberweerbaarheid van een organisatie vergroten.

De eisen en richtsnoeren worden aangevuld met de relevante inzichten die zijn opgenomen in het NIST/CSF-raamwerk, ISO 27001/ISO 27002, IEC 62443 en de CIS Critical security Controls (ETSI TR 103 305-1).

De codering van de eisen komt overeen met de in het NIST/CSF-raamwerk gebruikte codes. Aangezien niet alle NIST CSF-eisen van toepassing zijn, kunnen sommige codes die wel in het NIST CSF-raamwerk voorkomen, ontbreken.

Het raamwerk en de proportionele benadering van de zekerheidsniveaus zijn gevalideerd door praktijkmensen in het veld en met behulp van geanonimiseerde informatie over cyberaanvallen in de echte wereld, verstrekt door het federale Cyber Emergency Response Team (CERT.be - de operationele dienst van het Centrum voor Cyberveiligheid België).

Het **CCB Cyberfundamentals Framework is** opgebouwd rond vijf kernfuncties: identificeren, beschermen, detecteren, reageren en herstellen. Deze functies maken het mogelijk om, ongeacht de organisatie en de bedrijfstak, de communicatie rond cyberbeveiliging te bevorderen tussen zowel technische vakmensen als belanghebbenden, zodat cybergerelateerde risico's kunnen worden opgenomen in de algemene risicobeheerstrategie van de organisatie.

- **Identificeren (Identify)**
  Ken belangrijke cyberdreigingen voor uw meest waardevolle activa. In wezen kunt u niet beschermen wat u niet weet dat het bestaat. Deze functie helpt een organisatorisch begrip te ontwikkelen van hoe cyberbeveiligingsrisico's met betrekking tot systemen, mensen, activa, gegevens en capaciteiten moeten worden beheerd.
- **Beschermen (“Protect”)**
  De protect-functie richt zich op het ontwikkelen en uitvoeren van de waarborgen die nodig zijn om een cyberrisico te beperken of in te dammen.
- **Detecteren (“Detect”)**
  Het doel van de functie Detect is te zorgen voor de tijdige detectie van cyberbeveiligingsgebeurtenissen.
- **Reageren (“Respond”)**
  Bij de functie Reageren gaat het om de Controlees die helpen reageren op cyberbeveiligingsincidenten. De Respond-functie ondersteunt het vermogen om de impact van een potentieel cyberbeveiligingsincident in te dammen.

- **Herstellen (“Recover”)**
  De functie Herstellen richt zich op de beveiligingen die helpen de veerkracht te behouden en diensten te herstellen die door een cyberbeveiligingsincident zijn getroffen.

Om in te spelen op de ernst van de bedreiging waaraan een organisatie is blootgesteld, worden naast het niveau **Starter** (Small) 3 betrouwbaarheidsniveaus geboden: **Basis, Belangrijk en Essentieel** (“Basic”, “Important” en “Essential”**)**.

Met het **startniveau Small** kan een organisatie een eerste beoordeling maken. Het is bedoeld voor micro-organisaties of organisaties met beperkte technische kennis.

Het **zekerheidsniveau Basis** bevat de standaard informatiebeveiligingsmaatregelen voor alle ondernemingen. Deze bieden een effectieve beveiligingswaarde met technologie en processen die over het algemeen al beschikbaar zijn. Waar nodig worden de maatregelen aangepast en verfijnd. Voortbouwend op het basisniveau worden beveiligingsmaatregelen aangevuld om organisaties te beschermen tegen verhoogde cyberrisico's om een hoger niveau van zekerheid te bereiken.

Het **zekerheidsniveau Belangrijk is** bedoeld om de risico's van gerichte cyberaanvallen door actoren met gemeenschappelijke vaardigheden en middelen, naast de bekende cyberbeveiligingsrisico's, tot een minimum te beperken.

Het **zekerheidsniveau Essentieel** gaat een stap verder om ook in te spelen op het risico van geavanceerde cyberaanvallen door actoren met uitgebreide vaardigheden en middelen.

Verschillende controles vereisen bijzondere aandacht; deze maatregelen worden aangeduid als **- kernmaatregel -**.

Het raamwerk is een levend document en zal voortdurend worden bijgewerkt en verbeterd, rekening houdend met de feedback van belanghebbenden, het evoluerende risico van specifieke cyberbeveiligingsdreigingen, de beschikbaarheid van technische oplossingen en voortschrijdend inzicht.

De gegevens, het personeel, de apparaten, de systemen en de faciliteiten die de organisatie in staat stellen bedrijfsdoeleinden te bereiken, worden geïdentificeerd en beheerd in overeenstemming met hun relatieve belang voor de doelstellingen en de risicostrategie van de organisatie.

ID.AM-1: Inventarisatie van de binnen de organisatie gebruikte fysieke apparaten en systemen.

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.

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.

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-geautoriseerd.
- Niet-toegestane hardware kan worden opgespoord tijdens inventarisaties, verzoeken om ondersteuning door de gebruiker of op andere manieren.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1
IEC 62443-2-1:2010, clausule 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.9, 5.11, 7.9, 8.1

ID.AM-2: Inventarisatie van de binnen de organisatie gebruikte softwareplatforms en -toepassingen.

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-geautoriseerde software.
- Het gebruik van een hulpmiddel voor IT-activabeheer kan worden overwogen.

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.

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 2.
IEC 62443-2-1:2010, clausule 4.2.3.4
IEC 62443-3-3:2013, SR 7.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.9

ID.AM-3: De organisatorische communicatie- en gegevensstromen worden in kaart gebracht.

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).

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...).

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

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 12.
IEC 62443-2-1:2010, clausule 4.2.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.14

ID.AM-4: Externe informatiesystemen worden gecatalogiseerd.

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-geauthentiseerde verbinding met externe systemen.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 12.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.12, 7.9

ID.AM-5: Middelen worden geprioriteerd op basis van hun classificatie, kriticiteit en bedrijfswaarde.

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

Richtlijnen

- Bepaal de middelen van de organisatie (bijv. hardware, apparaten, gegevens, tijd, personeel, informatie en software) op basis van volgende vragen:
  - Wat zou er met mijn bedrijf gebeuren als deze middelen openbaar worden gemaakt, beschadigd worden, verloren gaan...?
  - Wat gebeurt er met mijn bedrijf als de integriteit van de middelen niet langer gegarandeerd is?
  - 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, kriticiteit en bedrijfswaarde.
- De middelen moeten bedrijfsactiva omvatten.
- Er zou een classificatie voor gevoelige informatie moeten worden gemaakt door eerst categorieën te bepalen, bijv.
  - Openbaar - vrij toegankelijk voor iedereen, zelfs extern
  - Intern - alleen toegankelijk voor leden van de organisatie
  - 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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3.
IEC 62443-2-1:2010, clausule 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.12, 7.9

ID.AM-6: Rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging worden vastgesteld voor het gehele personeel en belanghebbenden van derden.

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.
- kernmaatregel -

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.

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

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.2.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 5.4, 5.23, 5.24, 6.2, 6.5, 8.24

De missie, doelstellingen, belanghebbenden en activiteiten van de organisatie worden begrepen en geprioriteerd; die informatie wordt gebruikt voor het bepalen van cyberbeveiligingsrollen en verantwoordelijkheden, en het ondersteunen van beslissingen met betrekking tot risicobeheer.

ID.BE-1: De rol van de organisatie in de toeleveringsketen wordt vastgesteld en gecommuniceerd.

De rol van de organisatie in de toeleveringsketen moet worden vastgesteld, gedocumenteerd 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.

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.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.19, 5.20, 5.21, 5.22

ID.BE-2: De plaats van de organisatie in de kritieke infrastructuur en haar bedrijfstak wordt vastgesteld en gecommuniceerd.

De plaats van de organisatie in de kritieke infrastructuur en haar bedrijfstak moet worden vastgesteld en meegedeeld.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.2.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1

ID.BE-3: Prioriteiten met betrekking tot de missie, doelstellingen en activiteiten van de organisatie worden vastgesteld en gecommuniceerd.

Prioriteiten met betrekking tot de missie, doelstellingen en activiteiten van de organisatie moeten worden vastgesteld en gecommuniceerd.

Richtlijnen

De behoefte aan informatiebescherming moet worden vastgesteld en de desbetreffende processen moeten zo nodig worden herzien.

Referenties

IEC 62443-2-1:2010, clausule 4.2.2, 4.2.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.2, 6.1, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.1

ID.BE-4: Afhankelijkheden en kritieke functies voor de levering van kritieke diensten zijn vastgesteld.

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 kriticiteit.

Richtlijnen

Afhankelijkheden en bedrijfskritische functies moeten ondersteunende diensten omvatten.

Referenties

IEC 62443-2-1:2010, clausule 4.2.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.1, 8, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 7.11, 7.12, 8.6

ID.BE-5: Voor alle operationele staten (bv. onder dwang/aanval, tijdens herstel, normale operaties) worden vereisten vastgesteld met betrekking tot weerbaarheid ter ondersteuning van de levering van kritieke diensten.

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 de toepassing van veerkrachtmechanismen ter ondersteuning van normale en ongunstige operationele situaties (bijvoorbeeld failsafe, load balancing, hot swap).
- Overweeg rekening te houden met aspecten van bedrijfscontinuïteitsbeheer in bijvoorbeeld Business Impact Analyse (BIA), Disaster Recovery Plan (DRP) en Business Continuity Plan (BCP).

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 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...).

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.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.29, 7.5, 8.14

Het beleid, de procedures en de processen voor het beheer en de controle van de regelgevende, juridische, risico-, milieu- en operationele vereisten van de organisatie worden begrepen, en vormen de basis voor het beheer van het cyberbeveiligingsrisico.

ID.GV-1: Het cyberbeveiligingsbeleid van de organisatie wordt vastgesteld en gecommuniceerd.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14.
IEC 62443-2-1:2010, clausule 4.3.2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4, 5, 7.5, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.1

ID.GV-3: Wettelijke en regelgevende voorschriften inzake cyberbeveiliging, met inbegrip van verplichtingen inzake privacy en burgerlijke vrijheden, worden begrepen en beheerd.

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 4.2, 7.4, 7.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.31, 5.32, 5.33, 5.34

ID.GV-4: Governance- en risicobeheerprocessen adresseren risico's met betrekking tot cyberbeveiliging.

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.

Informatie- en cyberbeveiligingsrisico’s moeten worden gedocumenteerd, formeel goedgekeurd, en bij wijzigingen bijgewerkt.

Richtlijnen

Overweeg het gebruik van instrumenten voor risicobeheer.

Referenties

IEC 62443-2-1:2010, clausule 4.2.3, 4.4.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6

De organisatie begrijpt het cyberbeveiligingsrisico voor de operaties, activa en betrokken individuen van de organisatie (inclusief missie, functies, imago of reputatie).

ID.RA-1: Kwetsbaarheden van activa worden vastgesteld en gedocumenteerd.

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 7.
IEC 62443-2-1:2010, clausule 4.2.3, 4.2.3.9, 4.2.3.12.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 7, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.36, 8.8

ID.RA-2: Informatie over cyberdreigingen wordt ontvangen van fora en bronnen voor informatie-uitwisseling.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14.
IEC 62443-2-1:2010, clausule 4.2.3, 4.2.3.9, 4.2.3.12.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.2, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6

ID.RA-5: Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden gebruikt om het risico te bepalen.

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.

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.

De resultaten van risicobeoordelingen moeten aan de belanghebbenden worden gecommuniceerd.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 7, 10.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 6.1, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.8

ID.RA-6: Respons op risico's worden vastgesteld en geprioriteerd.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 7, 10.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 6.1.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.8

De prioriteiten, beperkingen, risicotoleranties en aannames van de organisatie worden vastgesteld en gebruikt ter ondersteuning van operationele risicobeslissingen.

ID.RM-1: Risicobeheerprocessen worden vastgesteld, beheerd en goedgekeurd door belanghebbenden in de organisatie.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1) Kritische beveiliging Controle 7, 10
IEC 62443-2-1:2010, 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.2, 6.1.3, 8.3, 9.3.

ID.RM-2: De risicotolerantie van de organisatie wordt bepaald en duidelijk uitgedrukt.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.2.6.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.2, 6.1.3, 7.4, 8.3, 9.3.

ID.RM-3: De organisatie bepaalt haar risicotolerantie op basis van haar rol in de analyse van kritieke infrastructuur en sectorspecifieke risico's.

De risicotolerantie van de organisatie wordt bepaald door haar rol in de kritische infrastructuur en sectorspecifieke risicoanalyses.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.2, 6.1.3, 8.3, 9.3.

De prioriteiten, beperkingen, risicotoleranties en aannames van de organisatie worden vastgesteld en gebruikt ter ondersteuning van risicobeslissingen in verband met het beheer van risico's in de toeleveringsketen. De organisatie heeft de processen voor het identificeren, beoordelen en beheren van risico's in de toeleveringsketen vastgesteld en geïmplementeerd.

ID.SC-1: **De processen voor het beheer van cyberrisico's in de toeleveringsketen worden geïdentificeerd, vastgesteld, beoordeeld, beheerd en goedgekeurd door de belanghebbenden van de organisatie.**

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.3, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.19, 5.20, 5.21, 5.22

ID.SC-2: Leveranciers en externe partners van informatiesystemen, componenten en diensten worden geïdentificeerd, geprioriteerd en beoordeeld met behulp van een risicobeoordelingsproces voor de cybertoeleveringsketen.

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.

Een 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.

Referenties

IEC 62443-2-1:2010, clausule 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.1, 5.3, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.19, 5.20, 5.21, 5.22

ID.SC-3: Contracten met leveranciers en externe partners worden gebruikt om passende maatregelen te implementeren, die dermate zijn ontworpen opdat wordt beantwoord aan de doelstellingen van het cyberbeveiligingsprogramma van de organisatie en haar cyber risicobeheersplan voor de toeleveringsketen.

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.

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.
- kernmaatregel -

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.

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.
- kernmaatregel -

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

IEC 62443-2-1:2010, clausule 4.3.2.6.4, 4.3.2.6.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.19, 5.20, 5.21, 5.22

ID.SC-4: Leveranciers en externe partners worden routinematig beoordeeld aan de hand van audits, testresultaten of andere vormen van evaluaties om te bevestigen dat zij aan hun contractuele verplichtingen voldoen.

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 evaluaties

Richtlijnen

Entiteiten die niet onder de NIS-wetgeving vallen, zouden zich kunnen beperken tot bedrijfskritische leveranciers en partners.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.2.6.7
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 9.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.22

ID.SC-5: Respons- en herstelplanning en tests worden uitgevoerd met leveranciers en derde partijen.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 18.
IEC 62443-2-1:2010, clausule 4.3.2.5.7, 4.3.4.5.**11**
IEC 62443-3-3:2013, SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6.1.3, 8.1, 8.3, bijlage A (zie ISO 27002).

De toegang tot fysieke en logische activa en bijbehorende faciliteiten is beperkt tot bevoegde gebruikers, processen en apparaten, en wordt beheerd in overeenstemming met het ingeschatte risico van ongeoorloofde toegang tot toegelaten activiteiten en transacties.

PR.AC-1: Identiteiten en referenties ("credentials") worden afgegeven, beheerd, geverifieerd, ingetrokken en gecontroleerd voor geautoriseerde apparaten, gebruikers en processen.

Identiteiten en referenties ("credentials") voor geautoriseerde apparaten en gebruikers moeten worden beheerd.

-kernmaatregel-

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.

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.

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

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 3, 4, 5, 12, 13.
IEC 62443-2-1:2010, clausule 4.3.3.5.1, 4.3.3.7.4.
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.16, 5.17, 5.18, 8.2, 8.5

PR.AC-2: De fysieke toegang tot activa wordt beheerd en beschermd.

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:
  - Haal altijd de sleutels of badges van een werknemer terug wanneer deze het bedrijf definitief verlaat.
  - Verander de alarmcodes van het bedrijf regelmatig.
  - 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.

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:
  - Voer een pasjessysteem in en creëer verschillende veiligheidszones.
  - De fysieke toegang tot servers en netwerkcomponenten kan worden beperkt tot bevoegd personeel.
  - Alle toegang tot servers en netwerkcomponenten kan worden vastgelegd.
- Toegangsregisters voor bezoekers zouden moeten worden bijgehouden, geëvalueerd en zo nodig worden uitgebaat.

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...)

Activa gerelateerd met kritieke zones moeten fysiek worden beschermd.

Richtlijnen

- Overweeg om stroomapparatuur, stroombekabeling, netwerkbekabeling en netwerkinterfaces te beschermen tegen toevallige schade, verstoring en fysiek geknoei.
- Overweeg redundante en fysiek gescheiden stroomsystemen te implementeren voor de kritische activiteiten van de organisatie.

Referenties

IEC 62443-2-1:2010, clausule 4.3.3.3.2, 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 7.1, 7.2, 7.3, 7.5, 7.6, 7.8, 7.9, 7.10, 7.12, 7.14, 8.1

PR.AC-3: De toegang op afstand wordt beheerd.

De draadloze toegangspunten van de organisatie moeten worden beveiligd.

Richtlijnen

Denk aan het volgende wanneer een draadloos netwerk wordt gebruikt:

- 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.

Gebruiksbeperkingen, verbindingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot de kritieke systeemomgeving van de organisatie moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.
- kernmaatregel –

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.

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.

De netwerken van de organisatie die op afstand toegankelijk zijn, moeten worden beveiligd, onder meer door middel van multifactorauthenticatie (MFA).
- kernmaatregel –

Richtlijnen

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

De beveiliging van verbindingen met externe systemen moet worden geverifieerd en gekaderd door gedocumenteerde overeenkomsten.

Richtlijnen

Toegang vanaf vooraf bepaalde IP-adressen kan worden overwogen.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 5, 6, 13.
IEC 62443-2-1:2010, clausule 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.14, 6.7, 7.9, 8.1, 8.5, 8.20.

PR.AC-4: De toegangsrechten en machtigingen worden beheerd, met inachtneming van de beginselen van "least privilege" en scheiding van taken.

De toegangsrechten voor gebruikers tot de systemen van de organisatie moeten worden gedefinieerd en beheerd.
- kernmaatregel –

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).

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.

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.

Er moet worden vastgesteld wie toegang moet hebben tot de bedrijfskritische informatie en technologie van de organisatie, en de middelen om die toegang te krijgen.
- kernmaatregel -

Richtlijnen

Middelen om toegang te krijgen kunnen zijn: een sleutel, wachtwoord, code of administratief privilege.

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").

- kernmaatregel -

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.

Bij het beheer van de toegangsrechten wordt het principe van functiesplitsing gehanteerd (Separation of Duties – SoD).

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.

Niemand heeft beheerdersrechten voor dagelijkse taken.

- kernmaatregel -

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.

Geprivilegieerde gebruikers moeten worden beheerd, gemonitord en geaudit.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 4, 6, 7, 12, 13, 16.
IEC 62443-2-1:2010, clausule 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.3, 5.15, 8.2, 8.3, 8.4, 8.18.

PR.AC-5: Netwerkintegriteit (netwerksegregatie, netwerksegmentatie...) wordt beschermd.

Op alle netwerken van de organisatie moeten firewalls worden geïnstalleerd en geactiveerd.
- kernmaatregel -

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- 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.

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

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.

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.
- kernmaatregel -

Richtlijnen

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

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.

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.
- kernmaatregel -

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).

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 4, 7, 12, 16.
IEC 62443-2-1:2010, clausule 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.14, 8.20, 8.22, 8.26

PR.AC-6: Identiteiten worden aangetoond en verbonden aan referenties ("credentials") en bevestigd in interacties.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 4, 5, 6.
IEC 62443-2-1:2010, clausule 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4.
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.3, 5.15, 8.2, 8.3, 8.18.

PR.AC-7: Identiteiten worden aangetoond en verbonden aan referenties ("credentials") en bevestigd in interacties.

De organisatie moet een gedocumenteerde risicobeoordeling uitvoeren op de kritieke systeemtransacties van de organisatie en gebruikers, apparaten en andere middelen authentiseren (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).
- kernmaatregel -

Richtlijnen

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

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 4, 5, 6, 9, 12 en 13.
IEC 62443-2-1:2010, clausule 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9.
IEC 62443-3-3:2013 SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.**10**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6.1, 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.16, 5.17, 5.34, 8.5

Het personeel en de partners van de organisatie krijgen voorlichting over cyberbeveiligingsbewustzijn en worden opgeleid om hun taken en verantwoordelijkheden op het gebied van cyberbeveiliging overeenkomstig de desbetreffende beleidsmaatregelen, procedures en overeenkomsten uit te voeren.

PR.AT-1: Alle gebruikers worden geïnformeerd en opgeleid.

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.

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 betrekt.
- 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.

De organisatie moet een evaluatiemethode toepassen om de doeltreffendheid van de bewustmakingsopleidingen te meten.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14, 16
IEC 62443-2-1:2010, clausule 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.2, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 6.3, 8.7

PR.AT-2: Geprivilegieerde gebruikers begrijpen hun rollen en verantwoordelijkheden.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 4, 14, 16
IEC 62443-2-1:2010, Clausule 4.3.2.4.2, 4.3.2.4.3.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.3, 7.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 6.3

PR.AT-3: Belanghebbenden van derden (bijv. leveranciers, klanten, partners) begrijpen hun rol en verantwoordelijkheden.

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.

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.

De organisatie monitort leveranciers en gebruikers van bedrijfskritische diensten op naleving van de beveiligingsvoorschriften.

Richtlijnen

Auditresultaten van derden kunnen als auditbewijs worden gebruikt.

De organisatie auditeert bedrijfskritische externe dienstverleners op naleving van de beveiligingsvoorschriften.

Richtlijnen

Auditresultaten van derden kunnen als auditbewijs worden gebruikt.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14.
IEC 62443-2-1:2010, Clausule 4.3.2.4.2, 4.3.2.4.3.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.3, 8.1, 9.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 5.4, 5.12, 6.3

PR.AT-4: Hogere leidinggevenden begrijpen hun taken en verantwoordelijkheden.

Hogere leidinggevenden 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)

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14, 17
IEC 62443-2-1:2010, clausule 4.3.2.4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 4.2, 5.3, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 5.4, 5.12, 6.3

PR.AT-5: Fysiek en cyberbeveiligingspersoneel begrijpt hun rollen en verantwoordelijkheden.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 14.
IEC 62443-2-1:2010, Clausule 4.3.2.4.2, 4.3.2.4.3.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5.3, 7.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 6.3

Informatie en registraties (gegevens) worden beheerd in overeenstemming met de risicostrategie van de organisatie om de vertrouwelijkheid, integriteit en beschikbaarheid van informatie te beschermen.

PR.DS-1: Data in rust is beschermd.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3.
IEC 62443-3-3:2013, SR 3.4, SR 4.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.10

PR.DS-2: Data-in-transitie is beschermd.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3.
IEC 62443-3-3:2013, SR 3.1, SR 3.8, SR 4.1, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.10, 5.14, 8.20, 8.26

PR.DS-3: Activa worden formeel beheerd gedurende de verhuizing, overdracht en verwijdering.

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.

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.

De organisatie moet ervoor zorgen dat verwijderingsacties worden goedgekeurd, gevolgd, gedocumenteerd en geverifieerd.

Richtlijnen

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

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 ...).

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1
IEC 62443-2-1:2010, Clausule 4.3.3.3.9, 4.3.4.4.1.
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.10, 7.10, 7.14

PR.DS-4: Voldoende capaciteit om de beschikbaarheid te waarborgen.

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 2
IEC 62443-2-1:2010, Clausule 4.3.3.3.9, 4.3.4.4.1.
IEC 62443-3-3:2013, SR 4.2, SR 7.1, SR 7.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.14, 8.32

PR.DS-5: Beveiligingen tegen datalekken worden geïmplementeerd.

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.
- kernmaatregel -

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3.
IEC 62443-3-3:2013 SR 5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.3, 5.10, 5.13, 5.14, 5.15, 6.1, 6.2, 6.5, 6.6, 7.5, 7.6, 7.8, 8.2, 8.3, 8.4, 8.18, 8.20, 8.22, 8.24, 8.26

PR.DS-6: Integriteitscontrolemechanismen worden gebruikt om de integriteit van software, firmware en informatie te controleren.

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.

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.

De organisatie moet automatische reacties met vooraf gedefinieerde veiligheidswaarborgen implementeren wanneer integriteitsschendingen worden ontdekt.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 2, 7
IEC 62443-3-3:2013, SR 3.1, SR 3.3, SR 3.4, SR 3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.7, 8.19, 8.26, 8.32

PR.DS-7: De ontwikkelings- en testomgeving(en) zijn gescheiden van de productieomgeving.

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).

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 16,
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.31

PR.DS-8: Integriteitscontrolemechanismen worden gebruikt om de integriteit van de hardware te verifiëren.

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.

De organisatie moet de detectie van ongeoorloofde sabotage van de hardware van haar kritieke systemen opnemen in de incidentenbestrijdingscapaciteit van de organisatie.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

IEC 62443-2-1:2010, clausule 4.3.4.4.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 7.13

Er wordt een beveiligingsbeleid (dat betrekking heeft op het doel, het toepassingsgebied, de rollen, de verantwoordelijkheden, de inzet van het management en de coördinatie tussen organisatorische eenheden), processen en procedures gehandhaafd en gebruikt om de bescherming van informatiesystemen en -middelen te beheren.

PR.IP-1: Er wordt een basisconfiguratie van informatietechnologie/industriële controlesystemen gecreëerd en onderhouden, waarin de beveiligingsbeginselen zijn verwerkt .

De organisatie moet een basisconfiguratie voor haar bedrijfskritische systemen ontwikkelen, documenteren en bijhouden.
- kernmaatregel –

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.).

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 7, 4, 12.
IEC 62443-2-1:2010, Clausule 4.3.4.3.2, 4.3.4.3.3.
IEC 62443-3-3:2013, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.19, 8.32

PR.IP-2: Een levenscyclus voor systeemontwikkeling om systemen te beheren wordt geïmplementeerd.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 16.
IEC 62443-2-1:2010, clausule 4.3.4.3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.8, 8.25, 8.27

PR.IP-3: Er zijn processen voor het beheer van configuratiewijzigingen aanwezig.

Wijzigingen moeten worden getest en gevalideerd vóórdat zij in operationele systemen worden doorgevoerd.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 4, 5, 12
IEC 62443-2-1:2010, Clausule 4.3.4.3.2, 4.3.4.3.3.
IEC 62443-3-3:2013, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.19, 8.32

PR.IP-4: Er worden back-ups van informatie gemaakt, onderhouden en getest.

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.
- kernmaatregel -

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).

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.

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 11.
IEC 62443-2-1:2010, clausule 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.29, 5.33, 8.13

PR.IP-5: Beleid en voorschriften met betrekking tot de fysieke bedrijfsomgeving voor bedrijfsmiddelen van de organisatie worden nageleefd .

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).

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

IEC 62443-2-1:2010, clausule 4.3.3.3.1, 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 6.1, 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 7.5, 7.8, 7.11, 7.12

PR.IP-6: Gegevens worden vernietigd overeenkomstig beleid.

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:
  - Hard copy media (fysieke representaties van informatie)
  - 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, netwerkapparatuur...)

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.4.4.4
IEC 62443-3-3:2013, SR 4.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.10, 7.10, 7.14

PR.IP-7: De beschermingsprocessen worden verbeterd.

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.

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.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.4.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 9, 10.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.27

PR.IP-8: De doeltreffendheid van beschermingstechnologieën wordt gedeeld.

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.

De doeltreffendheid van de toegepaste beschermingstechnologieën moet worden gecommuniceerd aan de toepasselijke partijen.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

De organisatie moet, waar mogelijk, geautomatiseerde mechanismen toepassen om te helpen bij informatiedeling.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.4, bijlage A (zie ISO 27002**).**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.27

PR.IP-9: Responsplannen (Incident Response en Business Continuity) en herstelplannen (Incident Recovery en Disaster Recovery) zijn aanwezig en worden beheerd .

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, herstelprioriteiten, 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.

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, rampherstelplannen, bedrijfscontinuïteitsplannen, crisiscommunicatieplannen, plannen voor kritieke infrastructuur, reactieplannen voor cyberincidenten en noodplannen voor omwonenden.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.2.5.7, 4.3.4.5.11
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 4.2, 6, 8, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.24, 5.29

PR.IP-11: Cyberbeveiliging is opgenomen in de personeelsbeheer (afbouwen, personeelsscreening...).

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.

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...

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 4, 6
IEC 62443-2-1:2010, Clausule 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), 4.1, 4.2, 7.1, 7.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.4, 5.11, 6.1, 6.2, 6.3, 6.4, 6.5.

PR.IP-12: Een plan voor het beheer van kwetsbaarheden wordt ontwikkeld en uitgevoerd.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 2, 4, 5, 16, 18.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 8, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.36, 6.8, 8.8, 8.32

Onderhoud en reparatie van industriële besturings- en informatiesystemen worden uitgevoerd in overeenstemming met beleid en procedures.

PR.MA-1: Onderhoud en reparatie van bedrijfsmiddelen van de organisatie worden uitgevoerd en geregistreerd, met goedgekeurde en gecontroleerde gereedschappen.

Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.
- kernmaatregel –

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.

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.

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

Richtlijnen

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

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.

Onderhoudsinstrumenten en draagbare opslagapparaten moeten worden geïnspecteerd wanneer zij de faciliteit worden binnengebracht en moeten worden beschermd door anti-malwareoplossingen, zodat zij worden gescand op kwaadaardige code voordat zij op de systemen van de organisatie worden gebruikt.
- kernmaatregel -

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

IEC 62443-2-1:2010, clausule 4.3.3.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.2, 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 7.2, 7.9, 7.10, 7.13

PR.MA-2: Onderhoud op afstand van bedrijfsmiddelen van de organisatie moet worden goedgekeurd, geregistreerd en uitgevoerd op een wijze die ongeoorloofde toegang voorkomt.

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.

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.

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 4, 7
IEC 62443-2-1:2010, clausule 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.4.4.6.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.2, 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.19, 5.22, 7.13

Technische beveiligingsoplossingen worden beheerd om de beveiliging en veerkracht van systemen en activa te waarborgen, in overeenstemming met de desbetreffende beleidslijnen, procedures en overeenkomsten.

PR.PT-1: Registraties van audits/logs worden vastgesteld, gedocumenteerd, uitgevoerd en herzien overeenkomstig beleid.

Logs worden bijgehouden, gedocumenteerd en geëvalueerd.
- kernmaatregel -

Richtlijnen

- Zorg ervoor dat de activiteitenregistratiefunctie (“activity logging functionality “) van beschermings-/detectiehardware of -software (bv. firewalls, antivirus) is ingeschakeld.
- Logs moeten worden geback-upt 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.

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-tijdbron.

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.

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 3, 4, 8.
IEC 62443-2-1:2010, clausule 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.4
IEC 62443-3-3:2013 SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 9.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.15, 8.17, 8.34

PR.PT-2: Verwisselbare media worden beschermd en het gebruik ervan wordt beperkt overeenkomstig het beleid.

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.

Draagbare opslagapparatuur die systeemgegevens bevat, moet tijdens transit en wanneer in opslag worden gecontroleerd en beschermd.
- kernmaatregel -

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 10
IEC 62443-3-3:2013, SR 2.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.10, 5.12, 5.13, 7.7, 7.10.

PR.PT-3: Het beginsel van minimale functionaliteit wordt toegepast door systemen zo te configureren dat ze alleen essentiële mogelijkheden bieden.

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).

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 4 en 7.
IEC 62443-2-1:2010, Clausule 4.3.3.5, 4.3.3.6, 4.3.3.7.
IEC 62443-3-3:2013, SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.15

PR.PT-4: Communicatie- en besturingsnetwerken zijn beveiligd.

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 4, 10, 12, 13.
IEC 62443-3-3:2013, SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.14, 8.20, 8.26

Afwijkende activiteiten worden gedetecteerd en de potentiële impact van events wordt begrepen.

DE.AE-1: Een baseline van netwerkoperaties en verwachte gegevensstromen voor gebruikers en systemen wordt vastgesteld en beheerd.

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.
- kernmaatregel -

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.

Referenties

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 8, 13
IEC 62443-2-1:2010, clausule 4.4.3.3
ISO/IEC 27001:2012, clausule 8.1, 9.1, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.37, 8.20, 8.21, 8.32

DE.AE-2: Gedetecteerde events worden geanalyseerd om inzicht te krijgen in aanvalsdoelen en -methoden.

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 8, 13, 15.
IEC 62443-2-1:2010, artikel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8.
IEC 62443-3-3:2013, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 9.1, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.24, 5.25, 8.15

DE.AE-3: Gegevens m.b.t. events worden verzameld en gecorreleerd uit meerdere bronnen en sensoren.

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.
- kernmaatregel -

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.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 3, 8, 10, 13, 15.
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 9.1, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.28, 8.15

DE.AE-4: De impact van events wordt bepaald.

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.

Referenties

CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 13
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 9.1, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.25

DE.AE-5: Er worden alarmdrempels voor incidenten vastgesteld.

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.

De organisatie moet alarmdrempels voor incidenten vaststellen.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 8, 13
IEC 62443-2-1:2010, clausule 4.2.3.10
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 9.1, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.25

Het informatiesysteem en de activa worden gecontroleerd om cyberbeveiligingsgebeurtenissen vast te stellen en de doeltreffendheid van de beschermende maatregelen te verifiëren.

DE.CM-1: Het netwerk wordt gemonitord om potentiële cyberbeveiligingsevents op te sporen.

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.

De organisatie moet ongeoorloofd gebruik van haar bedrijfskritische systemen bewaken en identificeren door het opsporen van ongeoorloofde lokale verbindingen, netwerkverbindingen en verbindingen op afstand.

- kernmaatregel –

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.

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.

De fysieke omgeving van de faciliteit wordt bewaakt op potentiële informatie-/cyberbeveiligingsincidenten.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 8, 10, 13.
IEC 62443-2-1:2010, clausule 4.3.3.3.8
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.22, 8.15, 8.30

DE.CM-2: De fysieke omgeving wordt bewaakt om potentiële cyberbeveiligingsgebeurtenissen op te sporen.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002**).**
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.22, 7.1, 7.2, 8.15, 8.30

DE.CM-3: Personeelsactiviteiten worden gemonitord om potentiële cyberbeveiligingsgebeurtenissen op te sporen.

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).

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).

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").

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 3, 8, 13, 15.
IEC 62443-3-3:2013, SR 6.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.15

DE.CM-4: Kwaadaardige code wordt gedetecteerd.

Anti-virus, -spyware en andere -malware programma's moeten worden geïnstalleerd en bijgewerkt.
- kernmaatregel –

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).

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 8, 10, 13
IEC 62443-2-1:2010, clausule 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.7

DE.CM-5: Ongeoorloofde mobiele code is gedetecteerd.

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 gebruiksbeperkingen en uitvoeringsrichtsnoeren moeten gelden.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 8, 10
IEC 62443-3-3:2013 SR 2.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.19

DE.CM-6: De activiteit van externe dienstverleners wordt gemonitord om potentiële cyberbeveiligingsgebeurtenissen op te sporen.

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.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.3.3.8
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.22, 8.15, 8.30

DE.CM-7: Monitoring op onbevoegd personeel, verbindingen, apparatuur en software wordt uitgevoerd.

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.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 1, 2, 8, 13, 15.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.1, 7.5, 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.22, 8.15, 8.30

DE.CM-8: Kwetsbaarheidsscans worden uitgevoerd.

De organisatie moet op kwetsbaarheden in haar kritieke systemen en gehoste toepassingen monitoren en scannen 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.

Het scannen van kwetsbaarheden moet analyse, herstel en het delen van informatie omvatten.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 8, 10
IEC 62443-2-1:2010, clausule 4.2.3.1, 4.2.3.7
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8, 9.1, 9.2, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.8, 8.29

Detectieprocessen en -procedures worden onderhouden en getest om ervoor te zorgen dat men zich bewust is van abnormale events.

DE.DP-2: Detectie moet gebeuren conform alle toepasselijke eisen.

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.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.34, 5.36, 8.8

DE.DP-3: Detectieprocessen worden getest.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.4.3.2
IEC 62443-3-3:2013, SR 3.3
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.29

DE.DP-4: Informatie over gedetecteerde events wordt gecommuniceerd.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.4.5.9
IEC 62443-3-3:2013, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 6.8

DE.DP-5: De processen voor het detecteren van abnormale events worden voortdurend verbeterd.

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.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, 9, 10.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.27

Responsprocessen en -procedures worden uitgevoerd en gehandhaafd, om te zorgen voor een reactie op gededecteerde cyberbeveiligingsincidenten.

RS.RP-1: Het responsplan wordt uitgevoerd tijdens of na een incident.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.4.5.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8.1, 8.3, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.26

De responsactiviteiten worden gecoördineerd met interne en externe belanghebbenden (bijvoorbeeld externe steun van wetshandhavingsinstanties).

RS.CO-1: Het personeel kent zijn rol en volgorde van handelen wanneer een reactie nodig is.

De organisatie moet ervoor zorgen dat het personeel zijn rol, doelstellingen, herstelprioriteiten, 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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, artikel 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5, 7.3, 7.4, 8.1, 8.3, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.2, 5.24, 6.3

RS.CO-2: Incidenten worden gemeld overeenkomstig de vastgestelde criteria.

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.

Gebeurtenissen worden gerapporteerd volgens vastgestelde criteria.

Richtlijnen

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

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.4.5.**5**
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5, 7.3, 7.4, 8.1, 8.3, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.5, 6.8

RS.CO-3: Informatie wordt gedeeld in overeenstemming met de responsplannen.

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.

De organisatie deelt informatie over informatie/cyberbeveiligingsincidenten met relevante belanghebbenden zoals voorzien in het responsplan voor incidenten.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010 Clausule 4.3.4.5.2
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, 8.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 6.8

RS.CO-4: Coördinatie met belanghebbenden vindt plaats in overeenstemming met de responsplannen.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.4.5.5
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, 8.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6, 5.26

RS.CO-5: Er vindt vrijwillige informatie-uitwisseling plaats met externe belanghebbenden om een breder situationeel bewustzijn over cyberbeveiliging te bereiken.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.3, 7.4, 8.1, 8.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6

Er worden analyses uitgevoerd om een doeltreffende reactie te waarborgen en herstelactiviteiten te ondersteunen.

RS.AN-1: Meldingen van detectiesystemen worden onderzocht.

De organisatie moet informatie-/cyberbeveiligingsgerelateerde meldingen van detectiesystemen onderzoeken.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

De organisatie moet geautomatiseerde mechanismen invoeren ter ondersteuning van het onderzoek en de analyse van informatie-/cyberbeveiligingsmeldingen.

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, artikel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8.
IEC 62443-3-3:2013 SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 9.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.26, 8.15

RS.AN-2: De gevolgen van het incident worden begrepen.

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.

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).

Referenties

IEC 62443-2-1:2010, artikel 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 4.2, 9.1, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.25, 5.27

RS.AN-3: Forensisch onderzoek wordt uitgevoerd .

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

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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.

Referenties

IEC 62443-3-3:2013, SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 4.1, 4.2, 9, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), Controle 5.28

RS.AN-4: Incidenten worden in categorieën ingedeeld overeenkomstig de responsplannen.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.4.5.6
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 8.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.25

RS.AN-5: Er zijn processen vastgesteld voor het ontvangen, analyseren en reageren op kwetsbaarheden die uit interne en externe bronnen (bv. interne tests, beveiligingsbulletins of beveiligingsonderzoekers) aan de organisatie bekend zijn gemaakt.

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.
- kernmaatregel -

Richtlijnen

Er zijn geen aanvullende richtsnoeren.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 7.5, 8.3, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 8.8

Er worden activiteiten uitgevoerd om uitbreiding van een gebeurtenis te voorkomen, de gevolgen ervan te beperken en het incident op te lossen.

RS.MI-1: Incidenten worden beheerst.

RS.MI-2: Incidenten worden gemitigeerd.

RS.MI-3: Nieuw vastgestelde kwetsbaarheden worden gemitigeerd of gedocumenteerd als aanvaarde risico's.

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).

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 17.
IEC 62443-2-1:2010, clausule 4.3.4.5.6
IEC 62443-3-3:2013 SR 5.1, SR 5.2, SR 5.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6, 7.5, 8.3, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.26, 8.7, 8.8

.

De responsactiviteiten van de organisatie worden verbeterd door lessen te trekken uit huidige en eerdere opsporings- en responsactiviteiten.

RS.IM-1: In de responsplannen zijn de geleerde lessen verwerkt.

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.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.3.4.5.10, 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6.1, 8.3, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.26, 5.27

RS.IM-2: Reactie- en herstelstrategieën worden bijgewerkt.

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.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 6.1, 8.3, 10, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.27

Herstelprocessen en -procedures worden uitgevoerd en gehandhaafd om te zorgen voor herstel van systemen of activa die zijn getroffen door cyberbeveiligingsincidenten.

RC.RP-1: Het herstelplan wordt uitgevoerd tijdens of na een cyberbeveiligingsincident.

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:
  - 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.
  - 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-up site, het fysiek verwijderen van belangrijke documenten, enz.
  - Wie te bellen in geval van een incident.

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.

Referenties

CIS Controles V8 (ETSI TR 103 305 1 V4.1.1), Kritische Beveiliging Controle 11.
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 8, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.26

De herstelplanning en -processen worden verbeterd door in toekomstige activiteiten rekening te houden met de opgedane ervaring.

RC.IM-1: In de herstelplannen zijn de geleerde lessen verwerkt.

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.

Referenties

IEC 62443-2-1:2010, clausule 4.4.3.4
ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 7.5, 8, 10.2, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.27

Herstelactiviteiten worden gecoördineerd met interne en externe partijen (bv. coördinatiecentra, internetproviders, eigenaars van aanvallende systemen, slachtoffers, andere CSIRT's en verkopers).

RC.CO-1: De public relations worden beheerd.

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.

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).

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6

RC.CO-2: Reputatie wordt hersteld na een incident.

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.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6

RC.CO-3: De herstelactiviteiten worden gecommuniceerd aan interne en externe belanghebbenden en aan directie- en managementteams.

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-wetgeving vallen.

Referenties

ISO/IEC 27001:2022 (NBN ISO/IEC 27001:2023), clausule 5, 7.4, bijlage A (zie ISO 27002).
ISO/IEC 27002:2022 (NBN EN ISO/IEC 27002:2022), controle 5.6

Bijlage A: Lijst van kernmaatregelen voor het zekerheidsniveau 'Basis'

BESCHERMEN (PROTECT)

PR.AC-1: Identiteiten en referenties worden afgegeven, beheerd, geverifieerd, ingetrokken en gecontroleerd voor geautoriseerde apparaten, gebruikers en processen.

(1) Identiteiten en referenties voor geautoriseerde apparaten en gebruikers moeten worden beheerd.

PR.AC-3: De toegang op afstand wordt beheerd.

(2) De netwerken van de organisatie die op afstand toegankelijk zijn, moeten worden beveiligd, onder meer door middel van multifactor authenticatie (MFA).

PR.AC-4: De toegangsrechten en machtigingen worden beheerd, met inachtneming van de beginselen van "least privilege" en scheiding van taken.

(3) De toegangsrechten voor gebruikers tot de systemen van de organisatie moeten worden gedefinieerd en beheerd.

(4) Er moet worden vastgesteld wie toegang moet hebben tot de bedrijfskritische informatie en technologie van de organisatie, en de middelen om die toegang te krijgen.

(5) 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").

(6) Niemand heeft beheerdersrechten voor dagelijkse taken.

PR.AC-5: Netwerkintegriteit (netwerksegregatie, netwerksegmentatie...) wordt beschermd.

(7) Op alle netwerken van de organisatie moeten firewalls worden geïnstalleerd en geactiveerd.

(8) Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door netwerksegmentatie en -scheiding.

PR.IP-4: Er worden back-ups van informatie gemaakt, onderhouden en getest.

(9) 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.

PR.MA-1: Onderhoud en reparatie van bedrijfsmiddelen van de organisatie worden uitgevoerd en geregistreerd, met goedgekeurde en gecontroleerde gereedschappen.

(10) Patches en beveiligingsupdates voor besturingssystemen en kritieke systeemcomponenten moeten worden geïnstalleerd.

PR.PT-1:	Registraties van audits/logs worden vastgesteld, gedocumenteerd, uitgevoerd en herzien overeenkomstig beleid.

(11) Logs worden bijgehouden, gedocumenteerd en geëvalueerd.

DETECTEREN (DETECT)

DE.AE-3:	Gegevens m.b.t. gebeurtenissen worden verzameld en gecorreleerd uit meerdere bronnen en sensoren.

(12) 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.

DE.CM-4:	Kwaadaardige code wordt gedetecteerd.

(13) Anti-virus, -spyware en andere -malware programma's moeten worden geïnstalleerd en bijgewerkt.

Bijlage B: Lijst van aanvullende kernmaatregelen voor het zekerheidsniveau "Belangrijk" en "Essentieel"

De onderstaande lijst vormt **een aanvulling** op de kernmaatregelen voor het zekerheidsniveau "Basis".

IDENTIFICEREN (IDENTIFY)

ID.AM-6:	Rollen, verantwoordelijkheden en bevoegdheden op het gebied van informatie- en cyberbeveiliging worden vastgesteld voor het gehele personeel en belanghebbenden van derden.

(1) 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.

BESCHERMEN (PROTECT)

PR.AC-3:	De toegang op afstand wordt beheerd.

(2) Gebruiksbeperkingen, verbindingsvereisten, implementatierichtlijnen en autorisaties voor toegang op afstand tot de kritieke systeemomgeving van de organisatie moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.

PR.AC-5:	Netwerkintegriteit (netwerksegregatie, netwerksegmentatie...) wordt beschermd.

(3) Waar nodig moet de netwerkintegriteit van de kritieke systemen van de organisatie worden beschermd door (1) het identificeren, documenteren en controleren van verbindingen tussen systeemcomponenten en (2) het beperken van externe verbindingen met de kritieke systemen van de organisatie.

(4) 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.

PR.DS-5:	Beveiligingen tegen datalekken worden geïmplementeerd.

(5) 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.

PR.IP-1:	Er wordt een basisconfiguratie van informatietechnologie/industriële controlesystemen gecreëerd en onderhouden, waarin de beveiligingsbeginselen zijn verwerkt.

(6) De organisatie moet voor haar bedrijfskritische systemen een basisconfiguratie ontwikkelen, documenteren en bijhouden.

DETECTEREN (DETECT)

DE.CM-1: Het netwerk wordt bewaakt om potentiële cyberbeveiligingsgebeurtenissen op te sporen.

(7) De organisatie moet ongeoorloofd gebruik van haar bedrijfskritische systemen bewaken en vaststellen door het opsporen van ongeoorloofde lokale verbindingen, netwerkverbindingen en verbindingen op afstand.

REAGEREN (RESPOND)

RS.AN-5: Er zijn processen vastgesteld voor het ontvangen, analyseren en reageren op aan de organisatie bekendgemaakte kwetsbaarheden uit interne en externe bronnen.

(8) 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.

Bijlage C: Lijst van aanvullende kernmaatregelen voor het zekerheidsniveau “Essentieel”

De onderstaande lijst vormt **een aanvulling** op de kernmaatregelen voor het zekerheidsniveaus "Basis" en “Belangrijk”.

IDENTIFICEREN (IDENTIFY)

ID.SC-3: Contracten met leveranciers en externe partners worden gebruikt om passende maatregelen te implementeren, die dermate zijn ontworpen opdat wordt beantwoord aan de doelstellingen van het cyberbeveiligingsprogramma van de organisatie en haar cyber risicobeheersplan voor de toeleveringsketen.

(1) 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.

(2) 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.

BESCHERMEN (PROTECT)

PR.AC-7: Identiteiten worden aangetoond en verbonden aan referenties (“credentials”) en bevestigd in interacties.

(3) De organisatie moet een gedocumenteerde risicobeoordeling uitvoeren op de kritieke systeemtransacties van de organisatie en gebruikers, apparaten en andere middelen authentiseren (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).

PR.MA-1: Onderhoud en reparatie van bedrijfsmiddelen van de organisatie worden uitgevoerd en geregistreerd, met goedgekeurde en gecontroleerde gereedschappen.

(4) De organisatie moet voorkomen dat onderhoudsapparatuur die kritieke systeeminformatie van de organisatie bevat, door onbevoegden wordt verwijderd.

(5) Onderhoudsinstrumenten en draagbare opslagapparaten moeten worden geïnspecteerd wanneer zij de faciliteit worden binnengebracht en moeten worden beschermd door anti-malwareoplossingen, zodat zij worden gescand op kwaadaardige code voordat zij op de systemen van de organisatie worden gebruikt.

(6) De organisatie moet na onderhoud of reparatie/patching van hardware en software de beveiligingscontroles nazien en de nodige maatregelen nemen.

PR.PT-2: Verwisselbare media worden beschermd en het gebruik ervan wordt beperkt overeenkomstig het beleid.

(7) Draagbare opslagapparatuur die systeemgegevens bevat, moet tijdens transit en wanneer in opslag worden gecontroleerd en beschermd.

DETECTEREN (DETECT)

DE.AE-1: Een baseline van netwerkoperaties en verwachte gegevensstromen voor gebruikers en systemen wordt vastgesteld en beheerd.

(8) 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.

Disclaimer

Dit document en zijn bijlagen zijn opgesteld door het Centrum voor Cyberveiligheid België (CCB), een federale administratie opgericht bij koninklijk besluit van 10 oktober 2014 en onder het gezag van de eerste minister.

Dit document bevat technische informatie die oorspronkelijk in het Engels is geschreven. Deze informatie heeft betrekking op de beveiliging van netwerken en informatiesystemen is gericht tot IT-diensten die de Engelse termen van computertaal gebruiken. Een vertaling in het Nederlands, Frans of Duits van deze technische informatie is niettemin beschikbaar bij het CCB.

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

- Is uitsluitend van algemene aard en zijn niet bedoeld om rekening te houden met alle bijzondere situaties.
- Is niet noodzakelijkerwijs volledig, nauwkeurig of op alle punten actueel.

Verantwoordelijke redacteur

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

Juridisch depot

D/2023/14828/001