Inhoudsopgave

Inleiding 4
IDENTIFICEREN (IDENTIFY)
ID.AM-1: Inventarisatie van de binnen de organisatie gebruikte fysieke apparaten en systemen. 6
ID.AM-2: Inventarisatie van de binnen de organisatie gebruikte softwareplatforms en -toepassingen. 6
ID.AM-3: De organisatorische communicatie- en gegevensstromen worden in kaart gebracht. 7
ID.AM-4: Externe informatiesystemen worden gecatalogiseerd. 7
ID.AM-5: Middelen worden geprioriteerd op basis van hun classificatie, kriticiteit en bedrijfswaarde. 7
ID.GV-1: Het cyberbeveiligingsbeleid van de organisatie wordt vastgesteld en gecommuniceerd. 8
ID.GV-3: Wettelijke en regelgevende voorschriften inzake cyberbeveiliging, met inbegrip van verplichtingen inzake privacy en burgerlijke vrijheden, worden begrepen en beheerd 8
ID.GV-4: Governance- en risicobeheerprocessen adresseren risico's met betrekking tot cyberbeveiliging. 9
ID.RA-1: Kwetsbaarheden van activa worden vastgesteld en gedocumenteerd. 10
ID.RA-5: Bedreigingen, kwetsbaarheden, waarschijnlijkheden en gevolgen worden gebruikt om het risico te bepalen. 10
BESCHERMEN (PROTECT)
PR.AC-1: Identiteiten en referenties worden afgegeven, beheerd, geverifieerd, ingetrokken en gecontroleerd voor geautoriseerde apparaten, gebruikers en processen. 11
PR.AC-2: De fysieke toegang tot activa wordt beheerd en beschermd. 12
PR.AC-3: De toegang op afstand wordt beheerd. 12
PR.AC-4: De toegangsrechten en machtigingen worden beheerd, met inachtneming van de beginselen van "least privilege" en scheiding van taken. 13
PR.AC-5: Netwerkintegriteit (netwerksegregatie, netwerksegmentatie...) wordt beschermd. 14
PR.AT-1: Alle gebruikers worden geïnformeerd en opgeleid. 15
PR.DS-1: Data in rust is beschermd. 16
PR.DS-2: Data-in-transitie is beschermd. 16
PR.DS-3: Activa worden formeel beheerd gedurende de verhuizing, overdracht en verwijdering. 17
PR.DS-7: De ontwikkelings- en testomgeving(en) zijn gescheiden van de productieomgeving. 17
PR.IP-4: Er worden back-ups van informatie gemaakt, onderhouden en getest. 18
PR.IP-11: Cyberbeveiliging is opgenomen in de personeelsbeheer (deprovisionering, personeelsscreening...). 18
PR.MA-1: Onderhoud en reparatie van bedrijfsmiddelen van de organisatie worden uitgevoerd en geregistreerd, met goedgekeurde en gecontroleerde gereedschappen. 19
PR.PT-1: Registraties van audits/logs worden vastgesteld, gedocumenteerd, uitgevoerd en herzien overeenkomstig beleid. 20
PR.PT-4: Communicatie- en besturingsnetwerken zijn beveiligd. 20
DETECT
DE.AE-3: Gegevens m.b.t. events worden verzameld en gecorreleerd uit meerdere bronnen en sensoren. . 21
DE.CM-1: Het netwerk wordt bewaakt om potentiële cyberbeveiligingsevents op te sporen. 22
DE.CM-3: Personeelsactiviteiten worden gemonitord om potentiële cyberbeveiligingsgebeurtenissen op te sporen. 22
DE.CM-4: Kwaadaardige code wordt gedetecteerd. 23
RESPOND
RS.RP-1: Het responsplan wordt uitgevoerd tijdens of na een incident 24
RS.CO-3: Informatie wordt gedeeld in overeenstemming met de responsplannen. 25
RS.IM-1: In de responsplannen zijn de geleerde lessen verwerkt. 26
RECOVER
RC.RP-1: Het herstelplan wordt uitgevoerd tijdens of na een cyberbeveiligingsincident. 27

Bijlage A: Lijst van kernmaatregelen voor het zekerheidsniveau 'Basis' 28

Inleiding

Het **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 - de operationele dienst van het Centrum voor Cybersecurity België).

Het **CyberFundamentals Framework is** opgebouwd rond vijf kernfuncties: identificeren, beschermen, detecteren, reageren en herstellen. Deze functies maken het mogelijk om, ongeacht de organisatie en de sector, 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 Controles 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 niveau **Starter** (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.

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.

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.

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).

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.

Voor het zekerheidsniveau "Basis" worden geen eisen gesteld, maar worden richtsnoeren gegeven om de informatiebeveiliging te verbeteren.

Richtlijnen

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

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.

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

Het beleid, de processen en de procedures voor het beheer en de controle van de regelgevende, wettelijke, 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.

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.

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.

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 doorgang 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.

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-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

- Onthoud 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.

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

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 worden afgegeven, beheerd, geverifieerd, ingetrokken en gecontroleerd voor geautoriseerde apparaten, gebruikers en processen.

Identiteiten en referenties 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.

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 zouden in overweging kunnen 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.

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.

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).

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).

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.

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.

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.

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

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.

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

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.

Deze controle is vervat in andere elementen van het raamwerk; er worden geen aanvullende eisen gesteld.

Richtlijnen

- 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.

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.

Deze controle is vervat in andere elementen van het raamwerk; er worden geen aanvullende eisen gesteld.

Richtlijnen

Wanneer de organisatie vaak gevoelige documenten of e-mails verzendt, wordt aanbevolen 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.

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

Voor het zekerheidsniveau "Basis" worden geen eisen gesteld, maar worden richtsnoeren gegeven om de informatiebeveiliging te verbeteren.

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

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-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).

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-11: Cyberbeveiliging is opgenomen in de personeelsbeheer (deprovisionering, 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.

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

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.

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

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.

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-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.

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-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.

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

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 bewaakt 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.

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-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).

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).

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

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.

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-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.

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

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

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

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 moeteen 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.

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

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 multifactorauthenticatie (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.

Disclaimer

Dit document en zijn bijlagen zijn opgesteld door het Centrum voor Cybersecurity 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 Cybersecurity België
De heer De Bruycker, Directeur-generaal
Wetstraat, 18
1000 Brussel

Juridisch depot

D/2023/14828/001