NIS2 Quality Mark

NIS2-QM30 HIGH

Versie 3.0
16 oktober 2024

NIS2
QUALITY MARK

Inhoud

Dit is de norm NIS2-QM30 High, behorende bij het NIS2 Quality Mark, integraal onderdeel van het Compliance en Certificeringsschema van NIS2 Quality Mark en de Stichting Kwaliteitsinnovatie
Versie 3.0 © 2024

Er zijn meer normen gericht op het vergroten van de cyberweerbaarheid. Om daarin de weg te wijzen en mogelijk dubbel werk te voorkomen, wordt bij elke norm een mapping indication meegegeven, zodat de lezer ziet hoe elk onderdeel van de norm zich mogelijk verhoudt tot andere gezagvolle normen in Europa, in het bijzonder de ISO-norm 27001.

***Mapping indication:** De maatregel toont gelijkenis met een andere norm, maar kan niet als volledig identiek worden beschouwd. Het dient als hulpmiddel bij het identificeren van overlappende gebieden, zonder de unieke kenmerken van de normen te verliezen.*

Voor wat betreft de maatregelen uit de ISO-norm 27001: de 'A' waarnaar wordt verwezen betreft de nummering uit bijlage A van de 27001 norm. Deze is leidend voor 27001.

1. Organisatorische maatregelen

1.2 Informatiebeveiligingsbeleid en bestuurlijke goedkeuring

Het management van de organisatie dient een beleid te formuleren waarin strategische doelstellingen zijn geformuleerd inzake de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tegen cyberdreigingen. Het beleid is akkoord bevonden door het hogere management en gedeeld met medewerkers en andere betrokkenen.

De organisatie dient specifieke beleidsregels te formuleren die gebaseerd zijn op het cyberbeleid en die ondersteuning moeten bieden aan proactieve paraatheid en beveiliging tegen incidenten en cyberdreigingen. De beleidsregels geven duidelijkheid over standaardpraktijken zoals toegangsbeveiliging, applicatiebeheer, IT-beheer, netwerkbeheer en back-up-beheer. De beleidsregels zijn goedgekeurd door geschikt management en gecommuniceerd aan relevante medewerkers.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat medewerkers te weinig urgentie voelen en kaders meekrijgen voor het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tegen cyberdreigingen.

Focuspunten

- Ontwikkel een gedetailleerd informatiebeveiligingsbeleid dat standaardpraktijken en procedures omvat. Dit beleid moet formeel goedgekeurd worden door het management en gedeeld worden met alle betrokkenen.
- Zorg voor regelmatige updates, wachtwoordwijzigingen, installatiebeheer, toegangsbeperkingen en data-back-ups. Deze praktijken ondersteunen de proactieve beveiliging tegen incidenten en dreigingen.
- Definieer duidelijk wie verantwoordelijk is voor het initiëren en beslissen over cybersecuritymaatregelen. Formele bestuurlijke goedkeuring van het beleid is essentieel voor de naleving en implementatie.
- Het beleid moet regelmatig gecontroleerd en bijgesteld worden, vooral bij belangrijke veranderingen in de organisatie of de externe dreigingsomgeving. Dit garandeert voortdurende effectiviteit en relevantie.

Mapping indication

ISO 27001: A.5.1 – Beleidsregels voor informatiebeveiliging.
IEC 62443-2-1: 2010, Clause 4.2.2, 4.2.3.6
NIST SP 800-53: PL-1 - Policy and procedures

1.3 Toewijzing wie verantwoordelijk is voor cybersecurity

De organisatie dient taken en verantwoordelijkheden bij cybersecurity te definiëren en toe te wijzen. De verantwoordelijkheden voor het initiëren en beslissen over cybersecuritymaatregelen zijn bekend bij de verantwoordelijken. Er is minstens één persoon aangesteld die verantwoordelijk is voor de cybersecurity van de organisatie.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat noodzakelijke acties niet, niet goed, of niet op tijd worden uitgevoerd, door onduidelijkheden over verantwoordelijkheden.

Focuspunten

- Definieer en wijs duidelijke rollen en verantwoordelijkheden toe voor informatiebeveiliging aan alle medewerkers. Dit helpt bij het waarborgen van een gecoördineerde en consistente aanpak van beveiligingspraktijken binnen de organisatie. Er moet een specifieke persoon zijn die verantwoordelijk is voor de algehele informatiebeveiliging.
- Documenteer en communiceer de rollen en verantwoordelijkheden voor informatiebeveiliging naar alle medewerkers. Dit zorgt voor duidelijkheid en helpt medewerkers hun taken en verantwoordelijkheden beter te begrijpen. Training en ondersteuning moeten beschikbaar zijn om ervoor te zorgen dat medewerkers effectief kunnen bijdragen aan de informatiebeveiliging.
- Evalueer en herzie regelmatig de toegewezen rollen en verantwoordelijkheden om ervoor te zorgen dat deze blijven aansluiten bij de veranderende behoeften en risico's van de organisatie. Dit omvat het aanpassen van verantwoordelijkheden bij veranderingen in de organisatie of technologie en het continu informeren van medewerkers over hun rol in de informatiebeveiliging.

Mapping indication

ISO 27001: A.5.2 - Rollen en verantwoordelijkheden
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.2.3.3
NIST SP 800-53: PM-1 - Information security program plan

1.4 Aansturing door het management

Het management van de organisatie dient expliciet van alle medewerkers, inclusief alle nieuwe medewerkers, te eisen dat ze werken volgens de informatiebeveiligingsregels en informatiebeveiligingsprocedures van de organisatie.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat het management de gecommuniceerde regels en procedures met betrekking tot informatiebeveiliging onvoldoende (zichtbaar) ondersteunt.

Focuspunten

- Betrek het management actief bij de controle en naleving van informatiebeveiligingsmaatregelen. Het management moet regelmatig rapportages ontvangen en ervoor zorgen dat alle medewerkers bekend zijn met de vereisten en betrokken zijn bij de uitvoering ervan.
- Communiceer duidelijk naar alle medewerkers het belang van informatiebeveiliging en de specifieke beleidsregels en procedures die moeten worden gevolgd. Zorg ervoor dat voldoende middelen, zoals tijd, geld en training, beschikbaar worden gesteld om de naleving van het informatiebeveiligingsbeleid te waarborgen.

Mapping indication

ISO 27001 A.5.4 – Managementverantwoordelijkheden.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

1.5 Beoordeling van en inzicht in beveiligingsdreigingen

De organisatie dient regelmatig geschikte bronnen te raadplegen om op de hoogte te blijven van dreigingen die relevant kunnen zijn voor de informatiebeveiliging. Indien nodig worden extra maatregelen getroffen als bescherming tegen nieuwe of veranderende dreigingen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat de organisatie informatie over dreigingen heeft gemist die wel beschikbaar was.

Focuspunten

- Zorg ervoor dat de organisatie actief informatie verzamelt over potentiële informatiebeveiligingsdreigingen, zowel door menselijke analisten als door geautomatiseerde systemen. Dit helpt om een breed overzicht te krijgen van mogelijke risico's.
- Voer grondige analyses uit op de verzamelde dreigingsinformatie om de betekenis en impact van de dreigingen te begrijpen. Zorg ervoor dat medewerkers voldoende zijn getraind om deze analyses uit te voeren en relevante signalen te herkennen.
- Gebruik de geanalyseerde dreigingsinformatie om eigen dreigingsprofielen te ontwikkelen en deze in te zetten voor het versterken van de informatiebeveiliging. Documenteer de genomen maatregelen om aan te tonen dat de dreigingsinformatie effectief wordt gebruikt.
- Evalueer regelmatig het proces van dreigingsbeoordeling en -analyse om ervoor te zorgen dat het up-to-date blijft en aansluit bij de veranderende dreigingsomgeving. Dit bevordert een proactieve benadering van informatiebeveiliging binnen de organisatie.

Mapping indication

ISO 27001: A.5.7 - Informatie en analyses over dreigingen.
NIST SP 800-53: RA-5 - Vulnerability monitoring and scanning.

1.6.1 Overzicht van informatie

De organisatie dient een overzicht met categorieën van bedrijfsinformatie op te stellen en te onderhouden. Per categorie is een eigenaar (beheerder) benoemd die verantwoordelijk is voor de bescherming van de informatie in die categorie.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat informatie niet is geïdentificeerd en geen eigenaar heeft, en daardoor onvoldoende wordt beschermd.

Focuspunten

- Zorg voor een volledig en betrouwbaar overzicht van alle informatie, activa en assets van de organisatie, inclusief klantgegevens, contracten, personeel, machines, apparatuur en gebouwen. Dit overzicht helpt bij het effectief beheren en beveiligen van deze middelen.
- Stel een informatieregister op waarin alle informatiegegevens zijn gedocumenteerd, inclusief waar de informatie is opgeslagen, in welke vorm, wie ermee werkt, en hoelang het bewaard moet blijven. Dit zorgt voor een gestructureerd beheer van informatie.
- Wijs duidelijke eigenaren of beheerders toe voor elk onderdeel binnen het informatieregister. Deze personen zijn verantwoordelijk voor het juiste beheer en de beveiliging van hun toegewezen informatie en activa.
- Controleer en actualiseer het beleid en het informatieregister regelmatig om ervoor te zorgen dat het altijd compleet, correct en actueel is. Dit garandeert dat de beveiligingsmaatregelen up-to-date blijven en effectief zijn.

Mapping indication

ISO 27001: A.5.9 – Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

1.6.2 Overzicht van ICT-bedrijfsmiddelen

De organisatie dient een overzicht van ICT-bedrijfsmiddelen op te stellen en te onderhouden, met inbegrip van servers, dataopslagsystemen en firewalls. Per bedrijfsmiddel (of groep van bedrijfsmiddelen) is een eigenaar (beheerder) benoemd die verantwoordelijk is voor de bescherming ervan.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat bepaalde ICT-bedrijfsmiddelen niet geïdentificeerd zijn en geen eigenaar hebben, en daardoor onvoldoende worden beschermd.

Focuspunten

- Inventariseer alle ICT-bedrijfsmiddelen binnen de organisatie, zoals computers, servers, dataopslagsystemen en firewalls. Dit overzicht helpt bij het effectief beheren en beveiligen van alle ICT-middelen.
- Stel een inventarislijst op waarin alle ICT-bedrijfsmiddelen, inclusief hun locaties, omschrijvingen en datum van aanschaf, zijn opgenomen. Zorg ervoor dat deze lijst volledig, correct en actueel is.
- Wijs eigenaren/beheerders aan voor elk ICT-bedrijfsmiddel op de inventarislijst. Deze personen zijn verantwoordelijk voor het beheer, de beveiliging en het onderhoud van hun toegewezen ICT-middelen.
- Controleer en actualiseer de inventarislijst regelmatig om ervoor te zorgen dat deze altijd up-to-date is. Dit garandeert een betrouwbare basis voor het beheer en het veilig houden van ICT-bedrijfsmiddelen.

Mapping indication

ISO 27001: A.5.9 – Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2
IEC 62443-2-1:2010, Clause 4.2.3.4 IEC 62443-3-3:2013 SR 7.8

1.7 Informatie en aanverwante bedrijfsmiddelen acceptabel gebruiken

De organisatie moet richtlijnen opstellen en delen over het veilig gebruiken van informatie en daaraan gerelateerde bedrijfsmiddelen zoals computers, laptops, telefoons, opslagmedia en bedrijfsapplicaties.

Doel

De kans te verlagen dat medewerkers informatiebeveiligingsincidenten veroorzaken als gevolg van onwetendheid, onervarenheid, achteloosheid, onnauwkeurigheid of onverschilligheid bij het omgaan met bedrijfsinformatie.

Focuspunten

- Stel duidelijke regels en procedures op voor gebruiken van informatie en aanverwante bedrijfsmiddelen, zoals netwerkapparatuur en clouddiensten. Dit helpt om misbruik te voorkomen en de integriteit van de informatie te waarborgen.
- Communiceer deze regels en procedures effectief naar alle medewerkers, zodat iedereen op de hoogte is van hoe informatie en bedrijfsmiddelen op een veilige manier gebruikt moeten worden. Dit bevordert naleving en bewustwording binnen de organisatie.
- Monitor en handhaaf de naleving van de vastgestelde regels en procedures. Zorg ervoor dat er mechanismen zijn om overtredingen te detecteren en passende maatregelen te nemen wanneer nodig.
- Evalueer en actualiseer regelmatig de regels en procedures zodat ze blijven aansluiten bij de nieuwste beveiligingsnormen en de veranderende behoeften van de organisatie. Dit garandeert dat de maatregelen effectief blijven en up-to-date zijn.

Mapping indication

ISO 27001: A.5.10 - Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3
IEC 62443-3-3:2013, SR 3.4, SR 4.1
NIST SP 800-53: AC-2 - Accountmanagement.

1.8 Het inleveren van bedrijfsmiddelen na gebruik

De organisatie dient, met behulp van een procedure en een checklist, te zorgen dat medewerkers en inhuurkrachten bedrijfsmiddelen (zoals laptops, telefoons, keycards en sleutels) inleveren na het aflopen of aanpassen van hun arbeidsovereenkomst.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een bedrijfsmiddel na na het aflopen of aanpassen van een arbeidsovereenkomst in verkeerde handen valt of onveilig wordt gebruikt.

Focuspunten

- Inventariseer alle bedrijfsmiddelen die medewerkers gebruiken, zoals computers, smartphones en andere apparatuur. Dit helpt bij het beheren en terugvorderen van bedrijfsmiddelen wanneer een medewerker de organisatie verlaat.
- Stel een duidelijke procedure en checklist op voor het inleveren van bedrijfsmiddelen bij vertrek van een medewerker. Deze procedure moet stapsgewijs beschrijven wat er moet gebeuren om ervoor te zorgen dat alle middelen correct worden teruggegeven.
- Wijs een verantwoordelijke persoon of afdeling aan die toeziet op het inleverproces. Deze persoon of afdeling zorgt ervoor dat de procedure wordt gevolgd en dat alle bedrijfsmiddelen daadwerkelijk worden ingeleverd.
- Controleer en actualiseer de procedure en checklist regelmatig om ervoor te zorgen dat deze up-to-date blijft en aansluit bij de huidige bedrijfspraktijken en technologieën. Dit garandeert een effectief inleverproces en helpt bij het waarborgen van de informatiebeveiliging.

Mapping indication

ISO 27001: A.5.11 - Retourneren van bedrijfsmiddelen.

1.9 Informatie indelen

De organisatie dient een overzicht bij te houden van verschillende categorieën van bedrijfsinformatie die hetzelfde niveau van vertrouwelijkheid hebben. Per categorie is vastgesteld hoe de betreffende bedrijfsinformatie behandeld en beschermd moet worden om de vertrouwelijkheid ervan te waarborgen. Per categorie is ook vastgesteld of de betreffende bedrijfsinformatie gelabeld moet worden om beter herkenbaar te zijn voor medewerkers.

Doel

Een informatieclassificatieschema biedt ondersteuning bij het opstellen van regels voor het behandelen en beschermen van bepaalde soorten informatie. Labelen kan de kans verkleinen dat er een informatiebeveiligingsincident optreedt doordat een werknemer niet weet hoe een bepaald soort informatie behandeld moet worden.

Focuspunten

- Stel een classificatieschema op waarin verschillende categorieën voor informatie zijn gedefinieerd, zoals "openbaar", "intern" en "zeer vertrouwelijk". Dit helpt om informatie systematisch te labelen en te beheren op basis van de gevoeligheid en beveiligingsbehoeften.
- Label alle informatie binnen de organisatie volgens het opgestelde classificatieschema. Dit zorgt ervoor dat medewerkers in één oogopslag kunnen zien hoe ze met verschillende soorten informatie moeten omgaan en welke beschermingsmaatregelen nodig zijn.
- Communiceer het classificatieschema en de bijbehorende procedures duidelijk naar alle medewerkers. Dit bevordert bewustwording en naleving van de beveiligingsrichtlijnen voor informatiebehandeling.
- Evalueer en actualiseer regelmatig het classificatieschema en de procedures om ervoor te zorgen dat ze blijven aansluiten bij de veranderende behoeften van de organisatie en de nieuwste beveiligingsnormen. Dit garandeert dat de classificatie en bescherming van informatie up-to-date en effectief blijven.

Mapping indication

ISO 27001 A.5.12 - Classificeren van informatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
NIST SP 800-53: RA-2 - Security categorization

1.11 Het intern en extern overbrengen van informatie

De organisatie moet richtlijnen opstellen die duidelijk aangeven welke middelen en externe partijen gebruikt mogen worden voor de veilige overdracht van vertrouwelijke informatie, zowel intern als met externe partijen. Daarnaast zorgt de organisatie ervoor dat alle medewerkers op de hoogte zijn van deze richtlijnen voor het veilig overdragen van informatie.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een onveilige, onjuiste of onbetrouwbare overdracht van informatie.

Focuspunten

- Stel duidelijke regels en procedures op voor het veilig overbrengen van informatie, zowel intern binnen de organisatie als extern naar derden. Dit zorgt ervoor dat de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tijdens de overdracht wordt gewaarborgd.
- Communiceer de vastgestelde regels en procedures naar alle medewerkers en, indien nodig, naar externe partijen zoals klanten en leveranciers. Dit bevordert naleving en zorgt ervoor dat iedereen op de hoogte is van de juiste manieren om informatie veilig over te dragen.
- Maak onderscheid tussen verschillende soorten informatieoverdracht, zoals elektronische (e-mail, sociale netwerken), fysieke (papieren documenten, USB-sticks) en mondelinge overdracht (telefoongesprekken, persoonlijke gesprekken). Dit helpt bij het specificeren van veiligheidsmaatregelen voor elke overdrachtsmethode.
- Controleer regelmatig of de regels en procedures effectief worden nageleefd en of ze up-to-date zijn. Dit garandeert dat de informatieoverdracht consistent veilig blijft, zelfs wanneer er nieuwe communicatiemiddelen of dreigingen ontstaan.

Mapping indication

ISO 27001 A.5.14 - Overdragen van informatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 12
IEC 62443-2-1:2010, Clause 4.2.3.4
NIST SP 800-53: SC-8 - Transmission confidentiality and integrity.

1.13 Registratie en uitschrijving gebruikers

De organisatie dient een procedure op te stellen en in gebruik te nemen voor het aanmaken, aanpassen en tijdig verwijderen van alle soorten accounts waar geregistreerde medewerkers en inhuurkrachten gebruik van maken.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een persoon of systeem onjuist of onterecht geregistreerd staat en daardoor niet de juiste toegangsrechten heeft.

Focuspunten

- Leg beleid en procedures vast voor het beheren van identiteitsgegevens, inclusief het registreren, aanpassen en verwijderen van deze gegevens. Dit waarborgt een gestructureerd beheer van de identiteit van personeel gedurende de gehele levenscyclus.
- Definieer en wijs duidelijke rollen en verantwoordelijkheden toe voor het beheer van het authenticatieproces en de levenscyclus van identiteiten. Dit zorgt ervoor dat het proces goed wordt beheerd en dat elke stap nauwkeurig wordt uitgevoerd.
- Zorg ervoor dat het beleid en de procedures betrekking hebben op alle aspecten van identiteitsbeheer, zoals gebruikersnamen, e-mailadressen en personeelsnummers. Dit draagt bij aan een veilige en consistente authenticatie binnen de organisatie.
- Communiceer het beleid en de procedures naar alle relevante medewerkers om ervoor te zorgen dat iedereen op de hoogte is van de juiste processen en verantwoordelijkheden. Dit bevordert naleving en helpt om identiteitsgegevens effectief te beheren.

Mapping indication

ISO 27001: A.5.16 – Identiteitsbeheer.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 5, 12, 13
IEC 62443-2-1:2010, Clause 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
NIST SP 800-53: IA-2 - Identification and authentication (organizational users).

1.14 Beheer van toegangsrechten

De organisatie dient een procedure te implementeren die ervoor moet zorgen dat toegangsrechten op de juiste wijze worden verstrekt, aangepast en verwijderd. Er wordt een registratie bijhouden waaruit blijkt wie er logische en fysieke toegangsrechten hebben ontvangen en op welke datum deze weer zijn ingetrokken.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat toegangsrechten onterecht of onjuist zijn toegewezen aan het account van een gebruiker.

Focuspunten

- Registreer wie toegang heeft tot welke informatie en bedrijfsmiddelen, en definieer zowel logische als fysieke toegangsrechten. Dit helpt bij het beheersen en controleren van toegangsrechten binnen de organisatie.
- Stel een procedure en checklist op voor het toekennen, wijzigen en intrekken van toegangsrechten. Dit zorgt ervoor dat toegangsrechten op een gestructureerde en consistente manier worden beheerd.
- Controleer bij beëindiging van een dienstverband of alle accounts correct worden afgesloten en alle toegangsrechten worden ingetrokken. Dit voorkomt ongeoorloofde toegang na vertrek van een medewerker.
- Evalueer en actualiseer regelmatig de autorisatiematrix om ervoor te zorgen dat deze up-to-date blijft en aansluit bij de huidige rollen en verantwoordelijkheden binnen de organisatie. Dit garandeert dat de toegangsrechten altijd correct en relevant zijn.

Mapping indication

ISO 27001: A.5.18 – Toegangsrechten.
NIST SP 800-53: AC-2 - Account Management.

1.15 Bescherming van informatie in samenwerking met leveranciers

De organisatie dient processen en procedures te definiëren die de organisatie in staat stellen om te bepalen of diensten en producten van leveranciers in voldoende mate aansluiten bij de informatiebeveiligingseisen van de organisatie. Indien nodig worden passende maatregelen getroffen om de risico's te beheersen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van het gebruik van een ondeugdelijke diensten of producten van een leveranciers.

Focuspunten

- Inventariseer de informatiebeveiligingsrisico's die gepaard gaan met het afnemen van producten en diensten van leveranciers. Dit helpt om mogelijke bedreigingen en zwakke punten te identificeren.
- Beoordeel de geïdentificeerde risico's en stel prioriteiten vast op basis van de ernst en impact van de risico's. Dit zorgt ervoor dat de meest kritieke risico's als eerste worden aangepakt.
- Neem passende maatregelen om de geïdentificeerde risico's te beperken, zoals het implementeren van beveiligingsprotocollen, het bijwerken van contractuele afspraken en het samenwerken met leveranciers om hun beveiligingsstandaarden te verbeteren.
- Communiceer de vastgestelde procedures en beveiligingsmaatregelen duidelijk naar alle relevante medewerkers en leveranciers. Dit bevordert de naleving en zorgt ervoor dat iedereen op de hoogte is van de verwachtingen en vereisten voor informatiebeveiliging in de samenwerking met leveranciers.

Mapping indication

ISO 27001: A.5.19 - Informatiebeveiliging in leveranciersrelaties.
IEC 62443-2-1:2010, Clause 4.3.4.2

1.16 Borgen van informatieveiligheid in overeenkomsten met leveranciers

De organisatie dient processen en procedures te definiëren die de organisatie in staat stellen om te bepalen of waarborgen die leveranciers bieden in voldoende mate aansluiten bij de informatiebeveiligingseisen van de organisatie. Indien nodig worden aanvullende afspraken overeengekomen.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden als gevolg van het onduidelijke afspraken over informatiebeveiliging met leveranciers.

Focuspunten

- Leg duidelijke beveiligingseisen en verantwoordelijkheden vast in overeenkomsten met leveranciers. Dit zorgt ervoor dat beide partijen precies weten wat er nodig is om de informatieveiligheid te waarborgen en wie verantwoordelijk is voor de uitvoering daarvan.
- Maak concrete afspraken met leveranciers over de maatregelen die gezamenlijk genomen worden om cyberrisico's te mitigeren. Dit helpt om bestaande beveiligingsrisico's effectief aan te pakken en de veiligheid van gedeelde informatie te garanderen.
- Zorg ervoor dat de medewerkers die overeenkomsten met leveranciers opstellen, voldoende kennis hebben van informatiebeveiliging en de relevante wetgeving. Dit voorkomt dat er belangrijke beveiligingsaspecten over het hoofd worden gezien bij het afsluiten van contracten.
- Gebruik een checklist om te controleren of alle benodigde beveiligingsmaatregelen in de overeenkomsten zijn opgenomen en of de logische toegangsrechten goed zijn vastgelegd. Dit helpt bij het systematisch vastleggen van afspraken en voorkomt dat leveranciers te veel vrijheid krijgen in het kiezen van beveiligingsmaatregelen.

Mapping indication

ISO 27001: A.5.20 - Adresseren van informatiebeveiliging in leveranciersovereenkomsten.
IEC 62443-2-1:2010, Clause 4.3.2.6.4, 4.3.2.6.7.

1.18 Toezicht, evaluatie en wijzigingsbeheer van leveranciersdiensten

De organisatie dient op basis van een risicobeoordeling vast te stellen welke leveranciers van diensten in aanmerking komen om extra gemonitord te worden. Van de geselecteerde leveranciers wordt regelmatig op basis van onderzoek beoordeeld of de betrouwbaarheid en veiligheid van de dienstverlening in voldoende mate aansluit bij de daarover gemaakte afspraken en de actuele eisen van de organisatie.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt door een onverwachte verandering in de aanpak van informatiebeveiliging of dienstverlening van een leverancier.

Focuspunten

- Voer regelmatige controles en evaluaties uit op de informatiebeveiligingspraktijken en dienstverlening van leveranciers. Dit kan door middel van interne controles of externe audits, om ervoor te zorgen dat de contractuele beveiligingseisen worden nageleefd.
- Stel een duidelijk proces in voor het monitoren en beheren van veranderingen in de diensten van leveranciers. Dit helpt om ervoor te zorgen dat elke wijziging in hun bedrijfsactiviteiten of beveiligingsmaatregelen geen negatieve impact heeft op de informatiebeveiliging.
- Leg de informatiebeveiligingspraktijken en dienstverleningsnormen vast in overeenkomsten met leveranciers. Dit maakt het eenvoudiger om deze te controleren en biedt een duidelijke basis voor evaluaties.
- Evalueer systematisch de resultaten van leveranciersbeoordelingen en onderneem actie bij tekortkomingen. Dit kan variëren van het voeren van corrigerende gesprekken tot het beëindigen van contracten, indien noodzakelijk, om het beveiligingsniveau van de organisatie te waarborgen.

Mapping indication

ISO 27001: A.5.22 - Monitoren, beoordelen en beheren van wijzigingen van leveranciersdiensten.
IEC 62443-2-1:2010, Clause 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.

1.19 Informatie veilig houden bij het gebruik van cloudservices

De organisatie dient processen te definiëren die de organisatie in staat stellen om te bepalen of waarborgen die leveranciers van clouddiensten bieden in voldoende mate aansluiten bij het cybersecuritybeleid van de organisatie.

Doel

Voorkomen dat het afnemen van een clouddienst tot informatiebeveiligingsincidenten leidt, of tot het niet naleven van contractuele of wettelijke verplichtingen.

Focuspunten

- Stel duidelijke processen op voor gebruik van clouddiensten, van aanschaf tot opzegging. Dit zorgt ervoor dat alle aspecten van cloudgebruik binnen de organisatie gestructureerd en veilig verlopen.
- Bepaal en documenteer de verantwoordelijkheden van zowel de organisatie als de Cloud Service Providers (CSP's). Dit helpt om misverstanden te voorkomen en zorgt ervoor dat beveiligingsmaatregelen consistent worden toegepast.
- Voer regelmatige evaluaties uit van de prestaties en veiligheid van de CSP's, zodat je zeker weet dat ze blijven voldoen aan de informatiebeveiligingseisen van de organisatie. Dit kan bijvoorbeeld door geplande check-ins en beoordelingen vanuit verschillende afdelingen zoals IT en inkoop.
- Ontwikkel een specifiek proces voor het veilig beëindigen van clouddiensten, inclusief ondersteuning bij het overstappen van de ene CSP naar de andere. Dit proces moet rekening houden met de uitdagingen van dataoverdracht en systeemaanpassing, zodat de continuïteit van de bedrijfsvoering gewaarborgd blijft.

Mapping indication

ISO 27001: 5.23 - Informatiebeveiliging voor het gebruik van clouddiensten.

1.20 Richtlijnen voor de aanpak van informatiebeveiligingsincidenten (cybersecurityincidenten)

Er dient een plan te worden opgesteld dat duidelijk maakt hoe de organisatie omgaat met een vermoede of vastgestelde inbreuk op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. In het plan wordt duidelijk aangegeven wie verantwoordelijk is voor welke taken.

Doel

Voorkomen dat de afhandeling van informatiebeveiligingsincidenten niet efficiënt verloopt, waardoor de gevolgen van incidenten onnodig groot worden.

Focuspunten

- Stel een Incident Response Plan (IRP) op waarin duidelijk wordt beschreven hoe de organisatie omgaat met informatiebeveiligingsincidenten. Dit plan moet gedetailleerde stappen bevatten voor het identificeren, melden, en oplossen van incidenten.
- Definieer en wijs duidelijke taken en bevoegdheden toe voor het beheer van cybersecurty incidenten. Zorg ervoor dat iedereen binnen de organisatie weet wie verantwoordelijk is voor welke taken bij een incident.
- Communiceer de processen en verantwoordelijkheden uit het IRP naar alle medewerkers. Dit zorgt ervoor dat iedereen op de hoogte is van de procedures en weet wat er van hen wordt verwacht bij een incident.
- Test en evalueer regelmatig de effectiviteit van het Incident Response Plan. Dit helpt om eventuele zwakke punten in de aanpak te identificeren en zorgt ervoor dat de organisatie voorbereid blijft op nieuwe en opkomende dreigingen.

Mapping indication

ISO 27001: 5.24 - Plannen en voorbereiden van beheer van informatiebeveiligingsincidenten.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.2.5.7, 4.3.4.5.11
NIST SP 800-53: IR-8 - Incident response plan

1.21 Registratie, beoordeling en afhandeling van informatiebeveiligingsincidenten

De organisatie dient gebeurtenissen met betrekking tot informatiebeveiliging te beoordelen om vast te stellen of het incidenten betreffen. Incidenten worden geregistreerd en afgehandeld in overeenstemming met gedocumenteerde procedures.

Doel

Voorkomen dat de afhandeling van informatiebeveiligingsincidenten niet efficiënt verloopt, waardoor de gevolgen van incidenten onnodig groot worden.

Focuspunten

- Registreer elke informatiebeveiligingsgebeurtenis en bepaal of het een afwijking, gebeurtenis of incident is. Dit helpt bij het correct categoriseren en prioriteren van beveiligingsproblemen en draagt bij aan een effectieve beveiligingsstrategie.
- Beoordeel elke ongewone gebeurtenis zorgvuldig om te bepalen of er actie nodig is. Dit zorgt ervoor dat niet elke gebeurtenis onnodig als incident wordt behandeld, maar dat er wel aandacht is voor potentiële risico's.
- Handel incidenten volgens vastgestelde procedures af en zorg ervoor dat alle stappen, van registratie tot afhandeling, goed worden gedocumenteerd. Dit garandeert een gestructureerde en consistente aanpak van beveiligingsincidenten.
- Rapporteer alle incidenten en afwijkingen aan het management, zodat er inzicht is in de beveiligingssituatie en er indien nodig op strategisch niveau bijgestuurd kan worden. Dit zorgt voor een goede communicatie en betrokkenheid.

Mapping indication

ISO 27001: 5.25 - Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 13
NIST SP 800-53: IR-4 - Incident handling.

1.22 Indicenten melden aan externen

De organisatie heeft en gebruikt een gedocumenteerde procedure om informatiebeveiligingsincidenten in overeenstemming met wettelijke en contractuele eisen te melden aan externen.

Doel

Voorkomen dat er reputatieschade of financiële schade ontstaat doordat het omgaan met informatiebeveiligingsincidenten onvoldoende aansluit bij de voor de organisatie relevante wettelijke en contractuele verplichtingen.

Focuspunten

- Leg duidelijke procedures vast voor het melden en handelen bij informatieveiligheidsincidenten, inclusief stappen voor zowel binnen als buiten reguliere werktijden. Dit helpt de organisatie om snel en effectief te reageren op incidenten, waardoor de impact geminimaliseerd wordt.
- Zorg ervoor dat incidenten met aanzienlijke gevolgen, zoals zware operationele verstoringen of financiële schade, tijdig worden gemeld bij het CSIRT en de bevoegde autoriteiten. Dit draagt bij aan een gecoördineerde en wettelijk conforme aanpak van ernstige incidenten.
- Communiceer de vastgestelde procedures duidelijk naar alle medewerkers, zodat iedereen weet hoe te handelen bij een cyberincident. Dit verhoogt de paraatheid en zorgt ervoor dat incidenten adequaat worden aangepakt, ongeacht wanneer ze zich voordoen.
- Voorzie nieuwe medewerkers van gerichte training over de procedures voor het omgaan met informatieveiligheidsincidenten. Dit garandeert dat ook zij goed voorbereid zijn om te reageren op beveiligingsincidenten en bijdragen aan de algehele veiligheid van de organisatie.

Mapping indication

ISO 27001: 5.26 - Beoordelen van en besluiten over informatiebeveiligingsincidenten.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 17
IEC 62443-2-1:2010, Clause 4.3.4.5.1
NIST SP 800-53: IR-4 - Incident handling.

1.23 Voorbereiding ICT ten behoeve van bedrijfscontinuïteit

De organisatie moet een plan opstellen dat ICT-continuïteitseisen bevat, waaronder doelstellingen voor de maximale hersteltijd van essentiële informatiesystemen. Er zijn technische en organisatorische maatregelen geïmplementeerd om bij een verstoring aan de ICT-continuïteitseisen te kunnen voldoen.

Doel

Voorkomen dat bij een verstoring de hersteltijden en het dataverlies van essentiële informatiesystemen onvoldoende aansluiten bij bedrijfscontinuïteitsdoelstellingen van de organisatie.

Focuspunten

- Stel doelstellingen en continuïteitseisen op voor bedrijfscontinuïteit bij onverwachte gebeurtenissen, zoals cyberaanvallen. Dit helpt om snel weer operationeel te zijn en de impact op de bedrijfsvoering te minimaliseren.
- Ontwikkel een gedetailleerd plan voor bedrijfscontinuïteit dat onder andere back-upbeheer, noodvoorzieningen en crisisbeheer omvat. Dit plan moet duidelijk beschrijven hoe de organisatie haar activiteiten kan voortzetten tijdens en na een incident.
- Implementeer en onderhoud de ICT-gereedheid op basis van de vastgestelde doelstellingen en continuïteitseisen. Dit zorgt ervoor dat de technische infrastructuur klaar is om te reageren op verstoringen.
- Test de ICT-gereedheid regelmatig om ervoor te zorgen dat alle systemen en procedures effectief werken tijdens een incident. Dit garandeert dat de organisatie snel en efficiënt kan herstellen van onvoorziene gebeurtenissen.

Mapping indication

ISO 27001: A.5.30 - ICT-gereedheid voor bedrijfscontinuïteit.
NIST SP 800-53: CP-2 - Contingency Plan.

1.24 Objectieve toetsing van de aanpak van informatiebeveiliging

De organisatie moet op geplande momenten een onafhankelijke beoordeling laten uitvoeren om te bepalen of de informatiebeveiligingsaanpak voldoende bijdraagt aan het behalen van de doelstellingen uit het informatiebeveiligingsbeleid. Als blijkt dat de aanpak tekortschiet, neemt het management corrigerende maatregelen.

Doel

Zorgen dat de organisatie voortdurend een passende en effectieve aanpak voor informatiebeveiligingsbeheer toepast.

Focuspunten

- Plan regelmatig onafhankelijke beoordelingen, zoals externe audits, om te controleren of de organisatie voldoet aan de eisen op het gebied van informatiebeveiliging. Dit helpt om een objectieve evaluatie te krijgen van de huidige maatregelen en processen.
- Stel duidelijke auditcriteria vast die auditoren kunnen gebruiken om de effectiviteit van de informatiebeveiligingsmaatregelen en bedrijfscontinuïteit te beoordelen. Dit zorgt voor een gestructureerde en consistente beoordeling.
- Zorg ervoor dat de auditors beschikken over de juiste competenties en kennis van de sector waarin de organisatie actief is. Dit garandeert dat de beoordeling grondig en relevant is, en dat de aanbevelingen waardevol zijn voor de organisatie.
- Implementeer verbeteringen op basis van de resultaten van de audits. Dit zorgt ervoor dat de organisatie continu haar informatiebeveiligingspraktijken en bedrijfscontinuïteitsplannen verbetert en aanpast aan nieuwe uitdagingen en bedreigingen.

Mapping indication

ISO 27001: 5.35 - Onafhankelijke beoordeling van informatiebeveiliging.
NIST SP 800-53: CA-2 - Control assessments.

1.25 Handhaven van voorschriften, regelgeving en standaarden voor informatiebeveiliging

De organisatie dient met geplande tussenpozen een onafhankelijke beoordeling te laten uitvoeren om vast te stellen of de organisatie werkt volgens de eisen van de NIS2 Quality Mark norm en volgens de eigen informatiebeveiligingseisen van de organisatie in de vorm van interne regels, afspraken, processen en procedures.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat regels, afspraken, processen en procedures onvoldoende worden nageleefd of toegepast.

Focuspunten

- Stel een duidelijk informatiebeveiligingsbeleid op, inclusief meldingsprocedures voor kwetsbaarheden, en zorg ervoor dat deze regelmatig worden getest op actualiteit en naleving. Dit helpt om een consistent en effectief beveiligingsniveau binnen de organisatie te handhaven.
- Controleer op vaste momenten of alle afspraken en regels uit het informatiebeveiligingsbeleid strikt worden nageleefd. Dit zorgt ervoor dat de informatie binnen de organisatie veilig blijft en dat potentiële zwakke punten tijdig worden geïdentificeerd.
- Rapporteer de resultaten van deze controles en toetsen aan het management. Dit bevordert de betrokkenheid van het management en zorgt ervoor dat noodzakelijke acties snel kunnen worden ondernomen om de informatiebeveiliging te versterken.
- Beoordeel regelmatig de effectiviteit van de beheersmaatregelen die zijn vastgelegd in het informatiebeveiligingsbeleid. Dit garandeert dat de maatregelen blijven voldoen aan de veranderende eisen en dreigingen in de digitale omgeving.

Mapping indication

ISO 27001: 5.36 - Naleving van beleid, regels en normen voor informatiebeveiliging.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 2, 4, 5, 16, 18

1.26 Samen de toeleveringsketen beveiligen

De organisatie moet de informatiebeveiligingsrisico's vaststellen gerelateerd aan de afname van ICT-producten en -diensten van leveranciers, of van leveranciers dieper in de toeleveringsketen. Relevante afspraken met betrekking tot informatiebeveiliging in de ICT-toeleveringsketen zijn overeengekomen met leveranciers van de organisatie.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van het gebruik van een ondeugdelijke dienst of product van leveranciers, of van leveranciers dieper in de toeleveringsketen.

Focuspunten

- Inventariseer de risico's bij je belangrijkste leveranciers om te begrijpen welke bedreigingen er zijn voor jouw organisatie. Dit helpt bij het identificeren van zwakke punten in de toeleveringsketen.
- Maak gezamenlijke afspraken met leveranciers over digitale beveiliging. Dit zorgt ervoor dat alle partijen dezelfde normen en procedures volgen om cyberdreigingen te minimaliseren.
- Informeer ontvangers (personen of organisaties) tijdig over de beheersmaatregelen die ze kunnen nemen bij een significante cyberdreiging in de organisatie. Dit zorgt voor een gecoördineerde en effectieve reactie op mogelijke bedreigingen.
- Evalueer en actualiseer regelmatig de risico-inventarisatie en de gemaakte afspraken met leveranciers. Dit garandeert dat de beveiligingsmaatregelen up-to-date blijven en effectief zijn tegen nieuwe dreigingen.

Mapping indication

ISO 27001: A.5.21 – Beheren van informatiebeveiliging in de ICT-toeleveringsketen.

1.27 Verzamelen bewijsmateriaal

De organisatie dient vast te stellen bij welk type incidenten welk bewijsmateriaal verzameld en veilig gesteld moet worden voor het kunnen achterhalen van de oorzaak, of voor het kunnen leveren van bewijs aan derden.

Doel

Voorkomen dat de organisatie schade lijdt omdat er na een informatiebeveiligingsincident geen informatie meer beschikbaar is voor achterhalen van de oorzaak, of voor het kunnen leveren van (juridisch) bewijs aan derden.

Focuspunten

- Stel procedures op voor het identificeren, verzamelen en bewaren van bewijsmateriaal bij informatiebeveiligingsincidenten. Dit zorgt ervoor dat er een gestandaardiseerde aanpak is die medewerkers kunnen volgen bij een incident.
- Communiceer deze procedures duidelijk naar alle medewerkers, zodat iedereen weet hoe en wanneer bewijsmateriaal verzameld moet worden. Dit garandeert een uniforme aanpak binnen de organisatie en draagt bij aan een effectieve respons op incidenten.
- Bepaal en implementeer concrete maatregelen om tijdens een incident een passend niveau van informatiebeveiliging te waarborgen. Dit omvat maatregelen voor beschikbaarheid, integriteit en vertrouwelijkheid van informatie.
- Evalueer en actualiseer regelmatig de procedures en maatregelen om ervoor te zorgen dat ze up-to-date blijven en aansluiten bij de nieuwste beveiligingsnormen en dreigingen. Dit garandeert dat de organisatie effectief kan reageren op incidenten en de integriteit van bewijsmateriaal behouden blijft.

Mapping indication

ISO 27001: A.5.28 - Verzamelen van bewijsmateriaal.
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 27001: 5.29 - Informatiebeveiliging tijdens een verstoring.
NIST SP 800-53: CP-2 - Contingency Plan.

2. Mensgerichte maatregelen

2.1 Geheimhoudingsplicht in arbeidsovereenkomsten

In alle vormen van arbeidsovereenkomsten dient een geheimhoudingsplicht te zijn opgenomen.

Doel

Voorkomen dat een medewerker vertrouwelijke informatie deelt met onbevoegden en daarmee een informatiebeveiligingsincident veroorzaakt.

Focuspunten

- Neem in alle arbeidsovereenkomsten expliciet de verantwoordelijkheden van medewerkers op het gebied van informatiebeveiliging op. Dit zorgt ervoor dat alle medewerkers zich bewust zijn van hun verplichtingen en wat er van hen verwacht wordt om de veiligheid van informatie te waarborgen.
- Verwijs in de arbeidsovereenkomsten naar een gedragscode waarin de specifieke richtlijnen voor informatiebeveiliging zijn opgenomen. Dit maakt de overeenkomst overzichtelijker en biedt gedetailleerde instructies voor het naleven van beveiligingsprotocollen.
- Zorg ervoor dat de verantwoordelijkheden voor informatiebeveiliging duidelijk worden gecommuniceerd aan alle medewerkers, inclusief tijdelijke medewerkers, contractanten en vrijwilligers. Dit helpt om een uniforme standaard voor informatiebeveiliging binnen de hele organisatie te handhaven.
- Controleer regelmatig of de bepalingen in de arbeidsovereenkomsten up-to-date zijn en aansluiten bij de huidige informatiebeveiligingseisen en -normen. Dit garandeert dat de afspraken relevant blijven en effectief bijdragen aan de veiligheid van de organisatie.

Mapping indication

ISO 27001: A.6.2 - Arbeidsovereenkomst.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 6
IEC 62443-2-1:2010, Clause 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

2.2 Educatie van bestuurders en medewerkers over digitale veiligheid

De directie en bestuurders van de organisatie dienen een opleiding of een cursus te volgen zodat ze cyberbeveiligingsrisico's kunnen identificeren en beoordelen. Medewerkers van de organisatie krijgen een opleiding en training over digitale veiligheid die past bij hun functie en ze worden getest op hun kennis van regels en procedures van de organisatie.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden door een gebrek aan bewustzijn van informatiebeveiligingsrisico's, of door een gebrek aan kennis over regels en procedures van de organisatie.

Focuspunten

- Zorg dat directie en bestuurders een opleiding of cursus volgen om cyberbeveiligingsrisico's te kunnen identificeren en beoordelen. Dit versterkt hun vermogen om passende beveiligingsmaatregelen te nemen en een veilige informatieomgeving te waarborgen.
- Implementeer video-trainingsmodules en andere vormen van educatie voor medewerkers over digitale veiligheid. Dit zorgt ervoor dat alle medewerkers zich bewust zijn van de risico's van informatieverwerking en weten hoe ze deze kunnen minimaliseren.
- Organiseer opleidingen die zijn afgestemd op de specifieke functies binnen de organisatie. Hierdoor krijgt elke medewerker de juiste kennis en vaardigheden die nodig zijn voor hun rol in het beschermen van informatie.
- Test regelmatig de kennis van medewerkers en hun naleving van het beleid. Dit helpt om de opgedane kennis effectief toe te passen en dat medewerkers zich houden aan de vastgestelde beveiligingsrichtlijnen.

Mapping indication

ISO 27001: A.6.3 - Bewustwording van, opleiding en training in informatiebeveiliging.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2
NIST SP 800-53: AT-3 – Role based training

2.4 Blijvende verantwoordelijkheden na vertrek of wijziging in de arbeidsrelatie

Met medewerkers en inhuurkrachten dient te worden overeengekomen dat er een geheimhoudingsplicht blijft gelden na het aflopen of aanpassen van hun arbeidsovereenkomst.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat iemand zich vrij voelt om gevoelige bedrijfsinformatie te delen na het aflopen of aanpassen van hun arbeidsovereenkomst.

Focuspunten

- Leg in de arbeidsovereenkomst vast welke taken en bevoegdheden op het gebied van informatiebeveiliging blijven gelden na het vertrek of de functiewijziging van een medewerker. Dit helpt om de veiligheid van gevoelige informatie te garanderen, zelfs nadat iemand de organisatie verlaat.
- Communiceer duidelijk met vertrekkende of intern doorstromende medewerkers over hun blijvende verantwoordelijkheden, zoals geheimhouding en het correct omgaan met vertrouwelijke gegevens. Dit zorgt ervoor dat zij zich bewust zijn van hun verplichtingen, ook na het beëindigen of wijzigen van hun dienstverband.
- Zorg ervoor dat er procedures zijn om deze blijvende verantwoordelijkheden te handhaven, bijvoorbeeld door een geheimhoudingsovereenkomst op te nemen in het exitgesprek of door het verstrekken van schriftelijke bevestigingen. Dit biedt een juridisch kader dat de organisatie beschermt tegen mogelijke datalekken of misbruik van informatie.
- Toets regelmatig of de afspraken rondom blijvende verantwoordelijkheden nog actueel en effectief zijn, en pas deze zo nodig aan. Dit garandeert dat de organisatie steeds beschermd blijft, ongeacht veranderingen in personeelssamenstelling.

Mapping indication

ISO 27001: A.6.5 - Verantwoordelijkheden na beëindiging of wijziging van het dienstverband.
NIST SP 800-53: PS-4 - Personnel Termination.

2.5 Overeenkomsten voor geheimhouding

De organisatie dient ervoor te zorgen dat medewerkers en inhuurkrachten een geheimhoudingsovereenkomst ondertekenen, waarin wordt vastgelegd dat vertrouwelijke informatie die tijdens de samenwerking wordt uitgewisseld, niet openbaar mag worden gemaakt aan derden.

Doel

Voorkomen dat een medewerker of een inhuurkracht vertrouwelijke informatie deelt met onbevoegden en daarmee een informatiebeveiligingsincident veroorzaakt.

Focuspunten

- Formuleer duidelijke overeenkomsten voor gegevensbescherming die specifiek aangeven hoe informatie moet worden behandeld en welke verplichtingen medewerkers en andere betrokkenen hebben. Zorg ervoor dat deze overeenkomsten zowel vertrouwelijkheids- als geheimhoudingsaspecten bevatten, afhankelijk van de gevoeligheid van de informatie.
- Zorg dat alle medewerkers en relevante belanghebbenden deze overeenkomsten ondertekenen voordat ze toegang krijgen tot gevoelige informatie. Dit biedt juridische zekerheid en benadrukt de verantwoordelijkheid van alle partijen om zorgvuldig om te gaan met informatie.
- Implementeer een procedure om de gegevensbeschermingsovereenkomsten regelmatig te evalueren en bij te werken. Dit kan door jaarlijkse controles of interne audits om ervoor te zorgen dat de afspraken actueel blijven en aansluiten bij de veranderende eisen en omstandigheden.
- Gebruik een digitaal systeem om herinneringen te sturen voor periodieke evaluaties en updates van de overeenkomsten. Dit helpt om consistent te blijven in het waarborgen van de gegevensbescherming binnen de organisatie.

Mapping indication

ISO 27001: A.6.6 - Vertrouwelijkheids- of geheimhoudingsovereenkomsten.

2.6 Thuis- of hybride werken op een veilige manier

De organisatie dient regels te formuleren en te communiceren voor een veilige informatieverwerking op externe locaties. De organisatie zorgt ervoor dat alle medewerkers de regels voor het werken op externe locaties kennen.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat medewerkers informatie op een onveilige manier openen, verwerken of opslaan tijdens werken op externe locaties.

Focuspunten

- Stel duidelijke regels op voor veilige informatieverwerking buiten de fysieke bedrijfslocatie, zoals thuis of op externe locaties. Dit helpt om gevoelige gegevens te beschermen tegen cyberincidenten.
- Implementeer beveiligingsmaatregelen specifiek gericht op thuis- en hybride werken, zoals het gebruik van VPN's, encryptie en sterke wachtwoorden. Dit zorgt ervoor dat gegevens veilig blijven, ongeacht waar medewerkers zich bevinden.
- Zorg ervoor dat alle medewerkers op de hoogte zijn van de regels en beveiligingsmaatregelen voor werken op afstand. Dit kan door middel van trainingen en regelmatige communicatie over de laatste veiligheidsrichtlijnen.
- Controleer en actualiseer regelmatig de beveiligingsmaatregelen en richtlijnen voor thuis- en hybride werken. Dit garandeert dat de maatregelen effectief blijven en inspelen op nieuwe cyberdreigingen.

Mapping indication

ISO 27001: A.6.7 - Werken op afstand.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: AC-17 - Remote Access.

2.7 Melding van gebeurtenissen met betrekking tot informatiebeveiliging

De organisatie dient alle medewerkers duidelijk te maken hoe waargenomen of mogelijke incidenten met betrekking tot informatiebeveiliging snel en via de juiste communicatiekanalen kunnen worden gemeld.

Doel

Voorkomen dat potentiële informatiebeveiligingsincidenten niet tijdig opgepakt of voorkomen kunnen worden doordat medewerkers waargenomen of vermoede informatiebeveiligingsgebeurtenissen niet of te laat melden.

Focuspunten

- Incidenten of kwetsbaarheden die de informatiebeveiliging bedreigen, moeten snel kunnen worden gedetecteerd en gecommuniceerd, vooral tijdens de ontwikkeling en het onderhoud van netwerk- en informatiesystemen.
- Zorg ervoor dat meldingen van cyberincidenten eenvoudig en snel gedaan kunnen worden via interne communicatiekanalen zoals e-mail, WhatsApp, en telefoon voor een directe respons.
- Overweeg de implementatie van een digitaal meldsysteem of app om gedetailleerde rapportage van bedreigingen voor de informatiebeveiliging mogelijk te maken en snel te kunnen reageren.
- Zorg dat alle medewerkers duidelijke instructies hebben over hoe zij beveiligingsproblemen moeten melden, en dat deze meldingen worden opgevangen en afgehandeld door een aangewezen meldpunt binnen de organisatie.

Mapping indication

ISO 27001: A.6.8 - Melden van informatiebeveiligingsgebeurtenissen.
IEC 62443-2-1:2010, Clause 4.3.4.5.9 IEC 62443-3-3:2013, SR 6.1
NIST SP 800-53: IR-6 - Incident Reporting.

2.8 Achtergrondcontroles bij kandidaten voor een dienstverband

De organisatie moet richtlijnen vaststellen en uitvoeren voor het screenen van kandidaten voordat zij in dienst treden. De breedte en diepgang van de screenings staan in verhouding tot de informatiebeveiligingsrisico's die gepaard gaan met de beoogde functies.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat medewerkers onvoldoende competent, betrouwbaar of gemotiveerd blijken te zijn.

Focuspunten

- Zorg ervoor dat er een grondige achtergrondcontrole wordt uitgevoerd voordat nieuwe medewerkers worden aangenomen of bestaande medewerkers worden belast met vertrouwelijke taken. Dit helpt om bedrijfsrisico's te minimaliseren en zorgt ervoor dat alleen geschikte personen toegang krijgen tot gevoelige informatie.
- Formuleer gedetailleerde regels en procedures voor het uitvoeren van achtergrondcontroles. Leg duidelijk vast welke specifieke controles nodig zijn voor verschillende functies of verantwoordelijkheden, zoals het controleren van diploma's, werkverleden, en het aanvragen van een Verklaring Omtrent Gedrag (VOG).
- Neem screeningsvereisten voor gevoelige functies expliciet op in het beveiligingsbeleid. Dit beleid moet regelmatig worden herzien en aangepast om te blijven voldoen aan de veranderende eisen van de organisatie en de wetgeving.
- Wijs één of twee personen aan die gemachtigd en bekwaam zijn om deze achtergrondcontroles uit te voeren. Zorg ervoor dat deze personen goed op de hoogte zijn van de wet- en regelgeving met betrekking tot privacy en arbeidsrecht, en dat ze ethische overwegingen in acht nemen bij het uitvoeren van de controles.

Mapping indication

ISO 27001: A.6.1 - Screening.
NIST SP 800-53: PS-3 - Personnel Screening.

3. Fysieke maatregelen

3.1 Fysieke toegangsbeveiliging

De organisatie dient op basis van een risicobeoordeling een passende fysieke beveiliging te ontwerpen en te implementeren voor terreinen, gebouwen, kantoren en ruimten. Het ontwerp houdt rekening met de behoefte van de organisatie om binnen een omgeving specifieke toegang te kunnen verlenen of te voorkomen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een onbevoegde persoon zich toegang verschaft tot een terrein, gebouw, kantoor of ruimte.

Focuspunten

- Zorg dat alle beveiligingszones binnen de organisatie duidelijk gedefinieerd zijn, zodat belangrijke informatie en bedrijfsmiddelen optimaal beschermd worden. Beveiligingszones kunnen zowel fysiek zijn, zoals beveiligde kamers, als digitaal, zoals afgeschermde netwerksegmenten.
- Zorg voor strikte fysieke toegangsbeveiliging door processen en middelen in te zetten die gecontroleerde toegang tot terreinen en gebouwen garanderen. Beperk de toegang tot bepaalde zones enkel tot personen met de juiste bevoegdheden.
- Voer een uitgebreide risico-inventarisatie uit om de specifieke informatiebeveiligingsrisico's binnen de organisatie in kaart te brengen. Gebruik de resultaten om toegangsbeveiligingsmaatregelen op maat in te stellen die effectief inspelen op deze risico's.

Mapping indication

ISO 27001: A.7.1 - Fysieke beveiligingszones.
IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
NIST SP 800-53: PE-2 - Physical access authorizations.

ISO 27001: A.7.2 - Fysieke toegangsbeveiliging.
IEC 62443-2-1:2010, Clause 4.3.3.3.2, 4.3.3.3.8
NIST SP 800-53: PE-3 - Physical access control.

3.5 Regelgeving voor vertrouwelijke informatie achterlaten op bureau en scherm

De organisatie dient regels te formuleren en te communiceren voor het vergrendelen van actieve computerschermen en voor het verwijderen van papier en opslagmedia met vertrouwelijke informatie op onbemande werkplekken. De organisatie zorgt ervoor dat alle medewerkers de regels voor onbemande werkplekken kennen en naleven..

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat iemand misbruik maakt van gemakkelijk toegankelijke informatie of een niet-vergrendeld scherm op een onbewaakte werkplek.

Focuspunten

- Stel duidelijke regels op voor een "Clear Desk" beleid, waarbij werknemers verplicht zijn om alle papieren documenten en verwijderbare opslagmedia veilig op te bergen wanneer ze hun werkplek verlaten. Dit voorkomt dat gevoelige informatie onbeheerd en toegankelijk blijft.
- Implementeer een "Clear Screen" beleid dat voorschrijft dat computerschermen vergrendeld moeten worden wanneer ze onbeheerd worden achtergelaten. Dit omvat het instellen van automatische schermvergrendeling na een bepaalde periode van inactiviteit.
- Communiceer het "Clear Desk" en "Clear Screen" beleid duidelijk naar alle medewerkers en zorg voor regelmatige herhaling van het belang ervan. Dit verhoogt het bewustzijn en zorgt ervoor dat iedereen zich aan de regels houdt.
- Monitor en handhaaf naleving van het "Clear Desk" en "Clear Screen" beleid door middel van regelmatige controles en audits. Dit helpt om ervoor te zorgen dat de regels consistent worden gevolgd en dat vertrouwelijke informatie beschermd blijft.

Mapping indication

ISO 27001: A.7.7 - 'Clear Desk' en 'Clear Screen'.

3.8 Bedrijfsapparatuur veilig verwijderen of hergebruiken

De organisatie dient een procedure op te stellen en in gebruik te nemen voor het veilig verwijderen of hergebruiken van bedrijfsapparatuur die ingebouwde opslagmedia bevat. De richtlijnen specificeren dat gevoelige gegevens en software moeten worden gewist of overschreven voordat een apparaat mag worden afgevoerd of hergebruikt.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt door het verwijderen of hergebruiken van een apparaat waarop nog informatie en/of in licentie gegeven software bleek te staan.

Focuspunten

- Stel een checklist op voor het veilig verwijderen of overschrijven van gevoelige informatie en software van apparaten met opslagmedia. Deze checklist helpt te controleren of alle gevoelige gegevens volledig zijn verwijderd voordat de apparatuur wordt vervangen of hergebruikt.
- Definieer duidelijke regels en procedures voor het veilig wissen van gegevens van apparaten zoals computers, tablets en telefoons. Dit voorkomt dat gevoelige informatie per ongeluk achterblijft en in verkeerde handen valt.
- Communiceer deze regels en procedures naar alle medewerkers en zorg voor regelmatige training over het veilig verwijderen van gegevens. Dit bevordert naleving en zorgt ervoor dat iedereen op de hoogte is van de juiste stappen.
- Implementeer en gebruik betrouwbare softwaretools voor het veilig wissen of overschrijven van gegevens. Zorg ervoor dat deze tools regelmatig worden bijgewerkt en voldoen aan de nieuwste beveiligingsnormen.

Mapping indication

ISO 27001: A.7.14 - Veilig verwijderen of hergebruiken van apparatuur.
IEC 62443-2-1:2010, Clause 4.3.4.4.4 IEC 62443-3-3:2013, SR 4.2
NIST SP 800-53: MP-6 - Media Sanitization.

3.9 Toegangsbeveiliging definiëren

De organisatie moet per functie of rol toegangsrechten definiëren, afgestemd op de behoeften van elke functie of rol en beperkt tot wat noodzakelijk is.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat personen onnodig toegang hebben tot bepaalde informatie of andere bedrijfsmiddelen.

Focuspunten

- Stel duidelijke toegangsregels op die bepalen wie toegang heeft tot welke gevoelige informatie en bedrijfsmiddelen. Dit helpt om ongeautoriseerde toegang te voorkomen en de beveiliging te waarborgen.
- Implementeer strikte fysieke beveiligingsmaatregelen voor cruciale bedrijfsmiddelen, zoals servers en patchkasten. Dit kan onder andere door middel van toegangscontroles tot gebouwen, camerabewaking en beveiligde serverruimtes.
- Registreer en monitor de toegang tot gevoelige bedrijfsmiddelen, zodat je weet wie wanneer toegang heeft gehad. Dit zorgt voor een gedetailleerd overzicht en helpt bij het opsporen van ongeautoriseerde toegang.
- Evalueer en actualiseer regelmatig de toegangsregels en beveiligingsmaatregelen om ervoor te zorgen dat ze effectief blijven en aansluiten bij de veranderende bedrijfsbehoeften en dreigingslandschap.

Mapping indication

ISO 27001: A.5.15 – Toegangsbeveiliging.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
NIST SP 800-53: AC-3 – Access enforcement.

4. Technologische maatregelen

4.1 Beveiliging en beheer gebruikersapparaten

Bedrijfsapparaten die medewerkers en inhuurkrachten gebruiken (zoals PC's, laptops, telefoons en tablets) dienen te worden beveiligd tegen onbevoegd gebruik, het onbevoegd installeren van software en het onbevoegd wijzigen van beveiligingsinstellingen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een gebruikersapparaat onvoldoende beveiligd is, of doordat het bedrijfsnetwerk onvoldoende beveiligd is tegen onveilige gebruikersapparaten.

Focuspunten

- Stel een actuele lijst op van alle gebruikersapparaten binnen de organisatie en zorg voor continu toezicht op de beveiligingsconfiguraties. Dit helpt om altijd een stap voor te blijven op potentiële dreigingen en ervoor te zorgen dat de apparaten zo veilig mogelijk zijn.
- Implementeer maatregelen zoals laptopversleuteling, beperking van adminrechten en verplichting van sterke wachtwoorden en pincodes. Dit zorgt ervoor dat medewerkersapparaten goed beveiligd zijn tegen cyberincidenten.
- Communiceer duidelijke regels en beveiligingseisen voor het gebruik van gebruikersapparaten naar alle medewerkers. Zorg dat iedereen op de hoogte is van de procedures voor het beschermen van hun apparaten en de risico's van ongeautoriseerde toegang.
- Beheer en update regelmatig de beveiligingsinstellingen van alle apparaten, inclusief het installeren van software-updates en handhaven van beveiligingsprotocollen. Dit garandeert dat de apparaten altijd goed beschermd zijn tegen nieuwe dreigingen.

Mapping indication

ISO 27001: A.8.1 - User Endpoint Devices.

4.2 Bijzondere toegangsbevoegdheden

De organisatie dient een procedure te implementeren die ervoor moet zorgen dat bijzondere toegangsrechten, zoals van systeem- en applicatiebeheerders, op de juiste wijze worden verstrekt, aangepast en verwijderd. Er wordt een registratie bijhouden waaruit blijkt wie er bijzondere toegangsrechten hebben ontvangen en op welke datum deze weer zijn ingetrokken.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat bijzondere toegangsrechten onterecht of onjuist zijn toegewezen aan het account van een gebruiker.

Focuspunten

- Documenteer zorgvuldig welke personen of groepen binnen de organisatie bijzondere toegangsbevoegdheden hebben, zodat altijd duidelijk is wie toegang heeft tot specifieke onderdelen van systemen of platformen.
- Implementeer een procedure voor het toewijzen en gebruik van bijzondere toegangsbevoegdheden, waarbij restricties worden gehanteerd om te waarborgen dat alleen de juiste personen of processen deze rechten verkrijgen en gebruiken.
- Zorg voor een actueel overzicht van alle 'privileged accounts' en communiceer de regels rondom het gebruik hiervan duidelijk naar de betrokken medewerkers, zodat iedereen op de hoogte is van de verantwoordelijkheden die deze accounts met zich meebrengen.
- Stel procedures in voor het tijdig deactiveren van 'privileged accounts' en het regelmatig aanpassen van wachtwoorden, met speciale aandacht voor accounts die aan externe leveranciers zijn toegewezen, om zo de veiligheid van gevoelige informatie te waarborgen.

Mapping indication

ISO 27001: A.8.2 - Speciale toegangsrechten.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1

4.4 Bestrijding en preventie van malware

De organisatie dient maatregelen tegen malware te implementeren, waaronder technische maatregelen voor het tijdig detecteren en onschadelijk maken van malware.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat malware leidt tot een aantasting van de beschikbaarheid, integriteit of vertrouwelijkheid van informatie.

Focuspunten

- Installeer en onderhoud betrouwbare anti-malware software, virusscanners en spamfilters op alle systemen binnen de organisatie. Dit helpt om de digitale omgeving te beschermen tegen kwaadaardige software en ongewenste e-mails.
- Overweeg het gebruik van encryptie voor belangrijke documenten en gevoelige informatie. Dit zorgt ervoor dat zelfs bij ongeautoriseerde toegang, de informatie niet gelezen kan worden zonder de juiste encryptiesleutels.
- Train medewerkers regelmatig op het herkennen en voorkomen van malware-aanvallen. Dit verhoogt het bewustzijn van de risico's en zorgt ervoor dat iedereen binnen de organisatie weet hoe ze veilig moeten omgaan met digitale dreigingen.
- Zorg voor een beleid en procedure voor het bestrijden van malware, inclusief het regelmatig updaten van beveiligingssoftware en het uitvoeren van systeemscans. Dit garandeert dat de bescherming tegen malware up-to-date blijft en effectief is tegen nieuwe bedreigingen.

Mapping indication

ISO 27001: A.8.7 - Bescherming tegen malware.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10, 13
IEC 62443-2-1:2010, Clause 4.3.4.3.8
IEC 62443-3-3:2013, SR 3.2
NIST SP 800-53: SI-3 - Malicious code protection.

4.5 Back-up en herstel

Back-ups van gegevens en systemen moeten worden uitgevoerd volgens een vastgesteld back-upplan. Back-ups worden getest om te controleren dat ze deugdelijk zijn op het moment dat ze moeten worden gebruikt.

Doel

Voorkomen dat essentiële informatie permanent niet meer beschikbaar is als gevolg van een kwaadaardige aanval, een menselijke fout, een ramp of een andere oorzaak.

Focuspunten

- Stel een uitgebreid back-up beleid op volgens de 3-2-1 systematiek, waarbij je drie kopieën van de data bewaart op twee verschillende media, waarvan één kopie offsite. Dit garandeert dat de gegevens veilig en toegankelijk blijven bij een calamiteit.
- Maak regelmatig back-ups van alle belangrijke data en systemen, zoals klantgegevens, financiële administratie en databases. Dit zorgt ervoor dat er altijd een recente kopie beschikbaar is in geval van dataverlies.
- Test de back-ups periodiek op betrouwbaarheid om er zeker van te zijn dat ze correct werken en dat de data teruggezet kan worden indien nodig. Dit voorkomt verrassingen op het moment dat een herstel noodzakelijk is.
- Communiceer duidelijk de verantwoordelijkheden binnen het back-up proces, inclusief wie verantwoordelijk is voor het uitvoeren, monitoren en testen van de back-ups. Dit zorgt voor een gestructureerde aanpak en voorkomt dataverlies door menselijke fouten.

Mapping indication

ISO 27001: A.8.13 - Back-up van informatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 11
IEC 62443-2-1:2010, Clause 4.3.4.3.9
IEC 62443-3-3:2013, SR 7.3, SR 7.4
NIST SP 800-53: CP-9 – System backup

4.6 Redundantie van infrastructuur

De organisatie dient op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitsdoelstellingen (zie 1.23) vast te stellen welke onderdelen van de ICT-infrastructuur meervoudig moeten worden uitgevoerd. De meervoudige uitvoering (redundantie) is geïmplementeerd en getest om de doelstellingen te kunnen realiseren.

Doel

Voorkomen dat bij een verstoring de hersteltijden van essentiële informatiesystemen onvoldoende aansluiten bij de bedrijfscontinuïteitsdoelstellingen van de organisatie.

Focuspunten

- Bepaal de minimaal vereiste beschikbaarheid voor de informatieverwerkende faciliteiten binnen de organisatie en zorg ervoor dat deze duidelijk is vastgesteld, zodat je weet aan welke eisen de systemen moeten voldoen.
- Zorg ervoor dat alle informatieverwerkende faciliteiten voldoende redundantie hebben, zodat ze blijven functioneren, zelfs als een onderdeel uitvalt, en voldoen aan de gestelde beschikbaarheidseisen.
- Implementeer redundantiemethoden zoals dataopslag op meerdere locaties of automatische overschakeling naar een reservesysteem, om te garanderen dat belangrijke systemen en diensten operationeel blijven bij storingen.
- Houd regelmatig toezicht op de redundantiemechanismen en test deze om te controleren of ze effectief zijn en daadwerkelijk zorgen voor de continuïteit van de informatieverwerkende faciliteiten.

Mapping indication

ISO 27001: A.8.14 - Redundantie van informatieverwerkende faciliteiten.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 2
IEC 62443-2-1:2010, Clause 4.3.3.3.9, 4.3.4.4.1
IEC 62443-3-3:2013, SR 4.2, SR 7.1, SR 7.2

4.7 Software op bedrijfsmiddelen up-to-date houden

De organisatie moet een beleid opstellen en toepassen voor van het voortdurend up-to-date en veilig houden van software op alle bedrijfsmiddelen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een niet gerepareerde kwetsbaarheid in software.

Focuspunten

- Implementeer procedures voor het automatisch updaten van software op alle computers en apparaten. Dit zorgt ervoor dat updates zo snel mogelijk worden geïnstalleerd zonder dat medewerkers handmatig actie hoeven te ondernemen.
- Stel richtlijnen op voor het veilig updaten van software, inclusief de frequentie en methoden voor het installeren van updates. Dit helpt om systemen te beschermen tegen nieuwe bedreigingen en kwetsbaarheden.
- Communiceer het belang van regelmatige software-updates aan alle medewerkers en zorg ervoor dat zij op de hoogte zijn van de procedures. Dit bevordert naleving en zorgt ervoor dat alle apparaten up-to-date blijven.
- Werk samen met externe leveranciers voor het updaten van operationele systemen indien nodig, en zorg ervoor dat de integriteit en werking van de systemen gewaarborgd blijft. Dit kan de efficiëntie verbeteren en ervoor zorgen dat updates correct en tijdig worden uitgevoerd.

Mapping indication

ISO 27001: A.8.19 - Installeren van software op operationele systemen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 7, 4, 12
IEC 62443-2-1:2010, Clause 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6

4.8 Netwerken beheren en beveiligen

De organisatie moet taken en plichten vastleggen en toewijzen voor het beheer en de configuratie van netwerken en netwerkapparatuur. Alle netwerkapparaten zijn opgenomen in een inventaris en hebben een eigenaar (beheerder). De inventaris wordt onderhouden en bevat relevante informatie over de netwerkapparaten.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat netwerken of netwerkapparaten onvoldoende worden beheerd of onjuist worden geconfigureerd.

Focuspunten

- Zorg ervoor dat netwerkcomponenten en -apparaten goed beveiligd zijn, zodat informatie binnen je netwerken beschermd blijft tegen ongewenste toegang en aanvallen. Dit omvat het implementeren van sterke beveiligingsmaatregelen zoals firewalls, encryptie en toegangscontrole.
- Monitor continu het gedrag van je netwerken om verdachte activiteiten en mogelijke beveiligingsincidenten snel te detecteren. Analyseer deze incidenten grondig om de oorzaak te achterhalen en passende maatregelen te nemen om toekomstige problemen te voorkomen.
- Documenteer en werk netwerkconfiguraties nauwkeurig bij wanneer er wijzigingen worden doorgevoerd. Dit helpt om altijd een actueel overzicht te behouden van de netwerkinfrastructuur en maakt het gemakkelijker om problemen op te sporen en op te lossen.
- Overweeg netwerkautomatisering om routinetaken zoals het bijwerken van configuraties en het controleren van de netwerkstatus te stroomlijnen. Dit vermindert de kans op menselijke fouten en zorgt voor een efficiënter en veiliger netwerkbeheer.

Mapping indication

ISO 27001: A.8.20 - Beveiliging netwerkcomponenten.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 7, 12, 16
IEC 62443-2-1:2010, Clause 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8

4.9 Netwerksegmentatie

De organisatie dient regels vast te stellen en toe te passen voor het segmenteren van groepen gebruikers, informatiesystemen en informatiediensten in de netwerken van de organisatie.

Doel

Netwerksegmentatie verbetert informatiebeveiliging door gevoelige gegevens en kritieke systemen te isoleren, ongeautoriseerde toegang te beperken en de impact van cyberaanvallen te minimaliseren. Dit voorkomt dat dreigingen zich door het hele netwerk verspreiden en helpt bij een gerichte bescherming van specifieke netwerkdelen.

Focuspunten

- Splits het netwerk op in specifieke segmenten, zoals aparte Wifi-segmenten, VLAN's, Firewalls of Subnets. Dit helpt om problemen in één deel van het netwerk te isoleren en voorkomt dat ze het hele netwerk treffen.
- Stel duidelijke regels en procedures op voor netwerksegmentatie, waarbij wordt bepaald hoe en waarom segmenten worden gecreëerd. Dit zorgt voor een gestructureerde en doelgerichte aanpak van netwerkbeheer.
- Werk samen met je IT-leverancier om de netwerksegmentatie te implementeren. Dit zorgt ervoor dat de segmentatie op de juiste manier wordt uitgevoerd en voldoet aan de nieuwste beveiligingsnormen.
- Evalueer en actualiseer regelmatig de netwerksegmentatie om ervoor te zorgen dat deze blijft aansluiten bij de veranderende behoeften van de organisatie en nieuwe beveiligingsuitdagingen. Dit garandeert dat het netwerk effectief en veilig blijft.

Mapping indication

ISO 27001: A.8.22 – Netwerksegmentatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 7, 12, 16
IEC 62443-2-1:2010, Clause 4.3.3.4
IEC 62443-3-3:2013, SR 3.1, SR 3.8

4.10 Authenticatiemethoden toepassen

De organisatie dient te zorgen dat toegepaste authenticatiemethoden in lijn zijn met de gevoeligheid van de informatie die men probeert te benaderen. MFA moet in ieder geval worden toegepast voor accounts met beheerdersrechten, bij toegang tot systemen met gevoelige informatie en voor alle gebruikers die via het internet inloggen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat er bij het inloggen gebruik wordt gemaakt van een onveilige authenticatiemethode.

Focuspunten

- Implementeer multifactor-authenticatie (MFA) voor alle accounts met beheerdersrechten en toegang tot systemen met bedrijfsgevoelige informatie. Dit zorgt voor een extra beveiligingslaag die ongeautoriseerde toegang moeilijker maakt.
- Gebruik authenticatiemethoden die passen bij de gevoeligheid van de informatie en systemen die worden benaderd. Voorzie cruciale systemen altijd van MFA of continue-authenticatieoplossingen om de beveiliging te versterken.
- Zorg dat gebruikers die via het internet inloggen ook MFA gebruiken. Dit beschermt de systemen tegen aanvallen waarbij wachtwoorden mogelijk zijn gecompromitteerd.
- Beveilig communicatiekanalen zoals spraak-, video- en tekstcommunicatie met veilige protocollen. Zorg ervoor dat noodcommunicatiesystemen ook goed beveiligd zijn om betrouwbare communicatie tijdens incidenten te garanderen.

Mapping indication

ISO 27001: A.8.5 - Beveiligde authenticatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 5, 6, 13
IEC 62443-2-1:2010, Clause 4.3.3.6.6, 4.3.3.7.4
IEC 62443-3-3:2013, SR 1.1, SR 1.13, SR 2.6
NIST SP 800-53: IA-2 - Identification and authentication (organizational users).

4.11 Logbestanden

De organisatie dient logbestanden van relevante gebeurtenissen te registreren en te analyseren. Op basis van een risicobeoordeling is door de organisatie bepaald wat relevante gebeurtenissen zijn en op welke wijze de geregistreerde logbestanden dienen te worden geanalyseerd.

Doel

Voorkomen dat belangrijke informatiebeveiligingsgebeurtenissen te laat worden gedetecteerd, of niet kunnen worden gedetecteerd omdat de benodigde logbestanden niet beschikbaar zijn.

Focuspunten

- Stel regels op voor het creëren, opslaan en beschermen van logbestanden. Dit zorgt ervoor dat alle activiteiten, uitzonderingen en fouten zorgvuldig worden geregistreerd en beschermd tegen ongeautoriseerde toegang en wijzigingen.
- Implementeer een centrale bewaarplaats voor logbestanden waar deze veilig kunnen worden opgeslagen en gemakkelijk toegankelijk zijn voor analyse. Dit bevordert de efficiëntie bij het onderzoeken van onregelmatigheden en het nemen van corrigerende maatregelen.
- Analyseer regelmatig de logbestanden om afwijkend gedrag in netwerken, systemen en applicaties vroegtijdig op te sporen. Dit helpt om potentiële bedreigingen en beveiligingsincidenten proactief te identificeren en aan te pakken.
- Synchroniseer de systeemtijd van alle systemen die logboeken bijhouden met de UTC-tijd. Dit zorgt voor consistentie in de tijdregistratie en vergemakkelijkt de analyse van logboeken.
- Bewaak en beperk de toegang tot logboeken om te voorkomen dat onbevoegde personen wijzigingen kunnen aanbrengen. Zorg ervoor dat logboeken minstens 30 dagen worden bewaard, zodat er voldoende historische gegevens beschikbaar zijn voor grondige analyses.

Mapping indication

ISO 27001: A.8.15 – Logging.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 1, 3, 4, 8
IEC 62443-2-1:2010, Clause 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
NIST SP 800-53: AU-2 – Event logging.

4.12 Cryptografie en encryptie

De organisatie dient op basis van een risicobeoordeling regels op te stellen en toe te passen die duidelijk maken in welke gevallen opgeslagen en verzonden informatie beveiligd moet worden met een specifieke vorm van cryptografie. Deze regels maken ook duidelijk hoe cryptografische sleutels veilig moeten worden bewaard.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt doordat een onbevoegde persoon toegang krijgt tot leesbare informatie die opgeslagen is of verzonden wordt.

Focuspunten

- Stel beleid op over cryptografie en encryptie om te zorgen voor een veilige digitale omgeving en communicatie, waarin duidelijke procedures worden beschreven voor het gebruik en de controle van encryptieprotocollen zoals TLS en HTTPS. Zorg ervoor dat dit beleid regelmatig wordt getoetst op effectiviteit.
- Implementeer TLS en HTTPS om de beveiliging van gegevensoverdracht via het internet te waarborgen, waarbij alle gevoelige informatie tijdens online communicatie wordt versleuteld en beschermd tegen ongeautoriseerde toegang. Controleer of de organisatie beleid heeft opgesteld voor cryptografie en encryptie dat voldoet aan de vastgestelde beveiligingsnormen
- Zorg ervoor dat alle TLS-certificaten in overeenstemming zijn met de vastgestelde beveiligingsnormen, waaronder een minimale sleutellengte van 2048 bits. Houd streng toezicht op de geldigheidsduur van certificaten en zorg dat ze tijdig worden vernieuwd om veiligheidsrisico's te voorkomen.
- Controleer periodiek alle e-maildomeinen op de juiste beveiligingsmaatregelen zoals DNSSEC, DKIM, DMARC en SPF, en los kritieke problemen snel op om te waarborgen dat e-mailcommunicatie veilig blijft.

Mapping indication

ISO 27001: A.8.24 – Cryptografische maatregelen.
NIST SP 800-53: SC-13 - Cryptographic protection

4.14 Technische kwetsbaarheden tijdig vinden en repareren

De organisatie moet verantwoordelijkheden vaststellen en toewijzen voor het op tijd opsporen, registreren en repareren van technische kwetsbaarheden in netwerken en informatiesystemen die onder het beheer van de organisatie vallen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een niet ontdekte technische kwetsbaarheid.

Focuspunten

- Identificeer en documenteer regelmatig technische kwetsbaarheden in de informatiesystemen, zoals softwarefouten of onjuiste configuraties. Zorg dat er een duidelijk proces is voor het opsporen van deze kwetsbaarheden, inclusief wie hiervoor verantwoordelijk is en welke tools of methoden worden gebruikt.
- Evalueer zorgvuldig de blootstelling en het risico van elke geïdentificeerde kwetsbaarheid door te bepalen hoe groot de kans is dat deze wordt misbruikt en wat de impact zou zijn op de organisatie. Prioriteer kwetsbaarheden op basis van deze evaluatie om te beslissen welke maatregelen het eerst moeten worden genomen.
- Implementeer snel en effectief de juiste maatregelen om de kwetsbaarheden te verhelpen, zoals het toepassen van software-updates of patches. Zorg ervoor dat deze maatregelen worden getest voordat ze in productie worden genomen om onverwachte problemen te voorkomen.
- Zorg voor een continu proces om nieuwe kwetsbaarheden op te sporen en aan te pakken, inclusief regelmatige monitoring van externe bronnen zoals beveiligingsbulletins. Houd het proces actueel door periodieke beoordelingen en updates van de procedures, zodat nieuwe bedreigingen effectief kunnen worden aangepakt.

Mapping indication

ISO 27001: A.8.8 - Beheer van technische kwetsbaarheden.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 7, 10
NIST SP 800-53: RA-5 - Vulnerability monitoring and scanning.

4.15 Gecontroleerd doorvoeren van wijzigingen

De organisatie dient een proces op te stellen en in te voeren voor het gecontroleerd doorvoeren van wijzigingen in netwerken en informatiesystemen die onder het beheer van de organisatie vallen. Het proces bevat een verplichte analyse van de mogelijke impact op de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een onvoldoende voorbereide wijziging in door de organisatie beheerde netwerken en informatiesystemen.

Focuspunten

- Stel procedures op om informatieveiligheid te waarborgen bij het doorvoeren van wijzigingen in systemen die informatie verwerken, zoals computers, maar ook voor het beheren van netwerken en informatiesystemen in hun hele levenscyclus. Zorg ervoor dat deze procedures worden gevolgd om de veiligheid en integriteit van de systemen te waarborgen, vooral bij niet-standaard wijzigingen.
- Leg vast hoe wijzigingen in systemen moeten worden uitgevoerd, en ontwikkel een beleid dat de volledige levenscyclus van netwerk- en informatiesystemen dekt, van ontwikkeling tot vernietiging. Dit beleid moet zorgen voor consistente beveiligingsmaatregelen gedurende de gehele levensduur van de systemen.
- Zorg ervoor dat alle personen die wijzigingen moeten beheren voldoende getraind zijn in het waarborgen van informatiebeveiliging. Dit is cruciaal, vooral wanneer er spoedwijzigingen of niet-standaard wijzigingen plaatsvinden die mogelijk onverwachte risico's met zich meebrengen.
- Documenteer en evalueer alle wijzigingen, inclusief de impact op de informatiebeveiliging. Zorg ervoor dat spoedwijzigingen goed worden beheerd en dat er na afloop van de spoedprocedure altijd een evaluatie plaatsvindt om de effecten op de veiligheid te beoordelen en de nodige aanpassingen te maken.

Mapping indication

ISO 27001: A.8.32 - Wijzigingsbeheer.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 4, 5, 12
IEC 62443-2-1:2010, Clause 4.3.4.3.2, 4.3.4.3.3
IEC 62443-3-3:2013, SR 7.6
NIST SP 800-53: CM-3 - Configuration change control.

5. OT maatregelen

5.1 Register van alle OT-bedrijfsmiddelen

De organisatie dienst een overzicht van OT-bedrijfsmiddelen op te stellen en te onderhouden, met inbegrip van relevante configuratiegegevens, zoals softwareversies en patchniveaus. Per bedrijfsmiddel is een eigenaar (beheerder) benoemd.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden doordat OT-bedrijfsmiddelen niet geïdentificeerd zijn en geen eigenaar hebben, en daardoor niet veilig worden beheerd.

Focuspunten

- Stel een gedetailleerd register op van alle OT-bedrijfsmiddelen binnen de organisatie, inclusief zowel hardware- als softwarecomponenten. Dit zorgt voor een compleet overzicht van alle operationele technologieën die worden gebruikt.
- Documenteer in het register ook de specifieke softwareversies en de huidige patchniveaus van elke OT-component. Dit helpt bij het identificeren van mogelijke beveiligingsrisico's en zorgt ervoor dat alle systemen up-to-date zijn.
- Maak een overzicht van alle netwerkverbindingen en externe koppelingen met het bedrijfsnetwerk. Dit geeft inzicht in de volledige OT-infrastructuur en helpt bij het beheren van zowel interne als externe beveiligingsrisico's.
- Controleer en actualiseer het register regelmatig zodat alle informatie accuraat en up-to-date blijft. Dit is essentieel voor het tijdig identificeren van nieuwe risico's en het effectief beheren van OT-bedrijfsmiddelen.

Mapping indication

BIACS:
121, 124: 2.8.2.1 Maatregelen gecontroleerd wijzigen.
50: 2.4.2.1 Maatregelen netwerkkoppelingen.
132: 2.9.2.1 Maatregelen beheer en onderhoud.

5.2 Bepaal de afhankelijkheid van OT-systemen

De organisatie dient per OT-systeem in kaart te brengen hoe afhankelijk de organisatie hiervan is, wat de kans op uitval is, en wat de impact bij uitval is.

Doel

Het vaststellen van risico's in verband met het uitvallen van OT-systemen om deze risico's met passende beheersmaatregelen en passende prioriteit te kunnen beheersen.

Focuspunten

- Identificeer per OT-bedrijfsmiddel hoe cruciaal het is voor de operationele processen van de organisatie. Dit helpt om prioriteiten te stellen bij het beheer en de beveiliging van deze systemen.
- Voer een risicoanalyse uit voor elk OT-bedrijfsmiddel, waarbij je de kans op uitval en de mogelijke impact op de organisatie beoordeelt. Gebruik de formule kans x impact om de risico's te kwantificeren en te prioriteren.
- Documenteer de bevindingen van de risicoanalyse in een overzicht dat duidelijk aangeeft welke OT-bedrijfsmiddelen het meest kritisch zijn voor de organisatie. Dit overzicht ondersteunt bij het maken van strategische beslissingen over onderhoud en investeringen.
- Houd het overzicht van afhankelijkheden en risico's up-to-date door regelmatig de risicoanalyse te herzien. Dit zorgt ervoor dat de organisatie voorbereid blijft op veranderingen in de technologie of bedrijfsomgeving die de afhankelijkheid van bepaalde OT-bedrijfsmiddelen kunnen beïnvloeden.

Mapping indication

BIACS:
130: 2.9.2.1 Maatregelen beheer en onderhoud.
139: 2.10.2 Maatregelen back-ups.

5.4 Back-ups van OT-systemen

Back-ups van OT-systemen dienen te worden gemaakt volgens een gedefinieerd back-up-plan. Back-ups worden getest om te controleren dat ze deugdelijk zijn op het moment dat ze moeten worden gebruikt.

Doel

Voorkomen dat OT-systemen niet meer beschikbaar zijn als gevolg van een kwaadaardige aanval, een menselijke fout, een ramp of een andere oorzaak.

Focuspunten

- Maak regelmatig back-ups van de configuratie-instellingen en operationele parameters van alle OT-systemen. Dit zorgt ervoor dat de systemen snel en effectief hersteld kunnen worden na technische problemen of een cyberaanval.
- Test de gemaakte back-ups periodiek om te verifiëren dat ze correct functioneren en daadwerkelijk kunnen worden hersteld. Dit garandeert dat de back-ups betrouwbaar zijn en kunnen worden gebruikt in geval van een incident.
- Zorg ervoor dat de back-ups regelmatig worden bijgewerkt om de meest recente configuraties en operationele parameters te reflecteren. Dit voorkomt dat verouderde informatie wordt hersteld, wat tot verdere problemen kan leiden.
- Bewaar de back-ups op een veilige locatie, gescheiden van de operationele systemen, om het risico van dataverlies door fysieke schade of cyberaanvallen te minimaliseren. Dit draagt bij aan de continuïteit en veiligheid van de organisatie.

Mapping indication

BIACS:
143, 144, 145: 2.10.2 Maatregelen back-ups

5.5 Recovery plan OT-systemen

De organisatie moet een bedrijfscontinuïteitsplan opstellen dat de continuïteitseisen beschrijft voor mogelijke verstoringen, inclusief de geaccepteerde hersteltijd voor essentiële OT-systemen. Technische en organisatorische maatregelen zijn geïmplementeerd om bij verstoringen te voldoen aan de OT-continuïteitseisen, en de effectiviteit van deze maatregelen is getest.

Doel

Voorkomen dat bij een verstoring de hersteltijden van essentiële OT-systemen onvoldoende aansluiten bij continuïteitsdoelstellingen van de organisatie.

Focuspunten

- Stel een gedetailleerd herstelplan op dat de stappen beschrijft voor het snel en effectief herstellen van systemen na een storing of cyberaanval. Dit plan moet ook de rollen en verantwoordelijkheden van alle betrokkenen, inclusief externe partijen, duidelijk vastleggen.
- Voer periodieke tests uit van het herstelplan om te verifiëren dat het proces effectief is en dat alle benodigde middelen, zoals configuraties, documentatie en reserveonderdelen, beschikbaar zijn. Indien het uitvoeren van daadwerkelijke tests te risicovol is, voer dan een dry-run of simulatie uit om het herstelproces te testen zonder de systemen daadwerkelijk te beïnvloeden.
- Documenteer en communiceer het herstelplan naar alle relevante medewerkers en externe partijen. Dit zorgt ervoor dat iedereen precies weet wat er moet gebeuren tijdens een incident en dat de continuïteit van de bedrijfsprocessen gewaarborgd blijft.
- Evalueer en actualiseer het herstelplan regelmatig, vooral na belangrijke systeemupdates of -upgrades. Dit garandeert dat het plan up-to-date blijft en effectief kan worden toegepast bij eventuele toekomstige storingen of aanvallen.

Mapping indication

BIACS:
40, 41: 2.3.2 Maatregelen beveiligingsincidenten en incident response plan.

5.6 Segmentatie van OT-netwerken

De organisatie dient regels vast te stellen en toe te passen voor het segmenteren van OT-netwerken van de organisatie.

Doel

Netwerksegmentatie verbetert informatiebeveiliging door gevoelige gegevens en kritieke systemen te isoleren, ongeautoriseerde toegang te beperken en de impact van cyberaanvallen te minimaliseren. Dit voorkomt dat dreigingen zich door het hele netwerk verspreiden en helpt bij een gerichte bescherming van specifieke netwerkdelen.

Focuspunten

- Zorg ervoor dat het netwerk binnen de organisatie is opgedeeld in afzonderlijke segmenten, waarbij elk segment specifiek wordt toegerust met de juiste toegangsrechten. Dit beperkt de toegang tot gevoelige informatie en voorkomt dat een mogelijke bedreiging zich ongecontroleerd over het hele netwerk verspreidt.
- Werk met gescheiden netwerk segmenten binnen het netwerk om de bescherming van gevoelige informatie te waarborgen en de cyberweerbaarheid te vergroten. Dit draagt bij aan het opbouwen van een gelaagde verdedigingsstrategie, waardoor het voor kwaadwillenden moeilijker wordt om het volledige netwerk aan te vallen.
- Controleer regelmatig of de netwerken binnen de organisatie zijn opgedeeld in afzonderlijke segmenten met specifieke toegangsrechten, vooral in kritieke onderdelen van het netwerk. Dit zorgt ervoor dat de segmentatie effectief blijft en dat gevoelige informatie altijd adequaat beschermd wordt.
- Zorg ervoor dat de segmentatie van het netwerk goed gedocumenteerd is, zodat alle betrokkenen precies weten hoe de segmenten zijn ingericht en welke toegangsrechten van toepassing zijn. Dit bevordert een consistent beheer en voorkomt ongeautoriseerde toegang tot gevoelige segmenten van het netwerk.

Mapping indication

BIACS:
29, 31, 51: 2.4.2.1 Maatregelen netwerkkoppelingen

5.8 Remote toegang tot kritieke OT-systemen

De organisatie dient een server gebruiker die als beveiligd toegangspunt fungeert bij remote toegang tot kritieke OT-systemen die onder het beheer van de organisatie vallen. De betreffende server heeft een eigenaar (beheerder) die verantwoordelijk is voor de beveiliging ervan.

Doel

Het gebruik van een beveiligd toegangspunt verkleint het risico op ongeautoriseerde toegang tot interne OT-systemen door externe toegang te centraliseren en te beperken. Dit vermindert het aanvalsoppervlak, verbetert controle en monitoring van toegangspogingen, en verhoogt de algehele beveiliging van het OT-netwerk.

Focuspunten

- Zorg ervoor dat remote toegang tot kritieke systemen zoals ICS en SCADA uitsluitend mogelijk is via een centraal access point, een zogenaamde Jump Host, om de risico's van onbevoegde toegang te minimaliseren.
- Implementeer strikte procedures en controles, zoals tweefactorauthenticatie en encryptie, om de veiligheid van remote toegang te waarborgen. Deze maatregelen zorgen ervoor dat alleen geautoriseerde gebruikers via de Jump Host toegang krijgen tot het netwerk.
- Monitor en log alle activiteiten die via de Jump Host plaatsvinden. Dit maakt het mogelijk om verdachte activiteiten vroegtijdig te detecteren en erop te reageren, wat bijdraagt aan de algehele beveiliging van het netwerk.
- Zorg ervoor dat de Jump Host zelf goed beveiligd is, met regelmatige updates en controles, om te voorkomen dat deze zwakke schakel wordt in de beveiligingsketen.

Mapping indication

BIACS:
22, 28, 33: 2.2.2.2 Technische maatregelen voor logische toegang

5.9 OT-patches installeren

De organisatie dient verantwoordelijkheden vast te stellen en toe te wijzen voor het tijdig toepassen van essentiële patches op de systemen binnen OT-netwerken die onder het beheer van de organisatie vallen.

Doel

Patching in OT-netwerken is cruciaal om kwetsbaarheden te dichten die systemen blootstellen aan cyberaanvallen. OT-netwerken, die vaak industriële processen en kritieke infrastructuur aansturen, hebben doorgaans verouderde systemen met beperkte beveiliging. Ongepatchte systemen kunnen leiden tot verstoringen, productie-uitval en gevaarlijke situaties. Omdat OT-systemen vaak 24/7 operationeel zijn, is patchmanagement complex, maar noodzakelijk om zowel beveiliging als bedrijfscontinuïteit te waarborgen.

Focuspunten

- Zorg ervoor dat er een gedetailleerd overzicht is van alle software en systemen die binnen de organisatie worden gebruikt, zodat duidelijk is wanneer patches moeten worden toegepast om beveiligingslekken te dichten.
- Voer periodieke scans uit op alle systemen binnen de OT-infrastructuur om potentiële beveiligingsrisico's vroegtijdig te identificeren en te beheersen.
- Analyseer de resultaten van deze scans zorgvuldig en volg deze op door de vereiste patches zo snel mogelijk te installeren op alle relevante systemen.
- Zorg ervoor dat de verantwoordelijkheid voor patch- en scanbeheer duidelijk is toegewezen, bijvoorbeeld via leveranciersovereenkomsten, zodat de beveiliging van de OT-systemen altijd op peil blijft.

Mapping indication

BIACS:
73, 74, 75, 76, 77: 2.5.2.3 Maatregelen patching

5.11 Overzicht van OT-systemen en aanvullende informatie

De organisatie dienst een overzicht van alle OT-systemen op te stellen en te onderhouden, met inbegrip van informatie over hardware, software, firmware, configuraties, beveiligingsinstellingen, leveranciers en onderhoud. Per OT-systeem is een eigenaar (beheerder) benoemd.

Doel

Voor een organisatie is een overzicht van OT-systemen en hun specifieke informatie belangrijk voor informatiebeveiliging, omdat het inzicht biedt in mogelijke kwetsbaarheden. Dit vergemakkelijkt risicobeheer, incidentrespons en de bescherming van vitale infrastructuur tegen cyberaanvallen of technische storingen.

Focuspunten

- Houd nauwkeurig de versies en revisies van alle gebruikte OT-apparatuur en -componenten bij. Dit is essentieel om snel en effectief te kunnen reageren op beveiligingsproblemen en om ervoor te zorgen dat updates efficiënt worden uitgevoerd.
- Documenteer de leveranciersinformatie van elke OT-apparatuur, inclusief fabrikant en contactgegevens. Dit stelt de organisatie in staat om snel ondersteuning te krijgen, updates te ontvangen en informatie over bekende problemen of kwetsbaarheden te verkrijgen.
- Werk het overzicht van versies, revisies en leveranciersinformatie regelmatig bij, vooral na systeemupdates of wanneer nieuwe apparatuur wordt geïnstalleerd. Dit garandeert dat de organisatie altijd beschikt over de meest actuele informatie.
- Gebruik deze informatie om onderhoudsplanning te optimaliseren en om te anticiperen op mogelijke problemen. Dit draagt bij aan het minimaliseren van risico's en het waarborgen van de continuïteit van de operationele processen.

Mapping indication

BIACS:
121, 124: 2.8.2.1 Maatregelen gecontroleerd wijzigen.
132: 2.9.2.1 Maatregelen beheer en onderhoud.

6. IT maatregelen

6.1 Toegang tot de broncode

De organisatie dient de toegang tot broncode en software libraries te beschermen tegen onbevoegde toegang en ongewenste wijzigingen.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt door ongeautoriseerde of niet passend geconfigureerde toegang tot broncode of software libraries.

Focuspunten

- Implementeer strikt versiebeheer voor de broncode, zodat alle wijzigingen nauwkeurig worden bijgehouden. Dit zorgt ervoor dat ontwikkelaars altijd kunnen terugvallen op eerdere versies en dat de volledige geschiedenis van aanpassingen inzichtelijk is.
- Stel gedegen toegangscontrolemechanismen in voor de broncode, waarbij alleen geautoriseerde personen toegang hebben tot specifieke delen van de code. Dit voorkomt ongeautoriseerde toegang en beschermt de integriteit van de software.
- Gebruik een betrouwbaar versiebeheersysteem zoals Git, SVN of BitBucket, en maak gebruik van functionaliteiten zoals branching en CI/CD-pipelines om de kwaliteit en veiligheid van de broncode te waarborgen.
- Monitor en evalueer regelmatig de effectiviteit van het versiebeheer en de toegangscontrole. Zorg ervoor dat deze mechanismen up-to-date blijven en voldoen aan de nieuwste beveiligingsnormen, zodat de integriteit en veiligheid van de software continu gewaarborgd blijft.

Mapping indication

ISO 27001: 8.4 - Toegangsbeveiliging op broncode.

6.2 Actueel houden van de programmacode en externe componenten

Organisaties die applicaties ontwikkelen dienen ervoor te zorgen dat programmacode, inclusief externe componenten zoals libraries en frameworks, regelmatig wordt bijgewerkt met de laatste beveiligingsupdates. Dit is vastgelegd in een formeel proces, waarbij updates binnen een vastgestelde termijn worden uitgevoerd en gedocumenteerd. Het proces wordt periodiek geëvalueerd en gecontroleerd op naleving.

Doel

Het up-to-date houden van programmacode en externe onderdelen met de laatste beveiligingsupdates helpt om beveiligingslekken te dichten en nieuwe bedreigingen te voorkomen. Door dit consequent te doen, wordt het risico verkleind op datalekken, ongeautoriseerde toegang en andere beveiligingsincidenten.

Focuspunten

- Zorg ervoor dat de programmacode, inclusief third party components, regelmatig wordt geüpdatet om bekende kwetsbaarheden te verhelpen en de informatiebeveiliging te waarborgen.
- Implementeer een systeem, zoals Dependabot van Github, om continu te monitoren op security updates en patches voor zowel eigen geschreven code als externe componenten.
- Beoordeel periodiek de integratie van third party components om te verzekeren dat deze geen onnodige beveiligingsrisico's met zich meebrengen.
- Documenteer en volg alle updates en patches zorgvuldig zodat de programmacode altijd actueel en veilig blijft.

Mapping indication

Geen Mapping indication aanwezig.

6.3 Veilige applicaties ontwikkelen

Organisaties die applicaties ontwikkelen dienen ‘best practices’ vast te stellen voor het ontwikkelen van veilige software. De naleving van deze ‘best practices’ wordt gecontroleerd. Er worden principes voor veilig coderen toegepast.

Doel

Voorkomen dat er een bug, kwetsbaarheid of logische fout aanwezig is in door de organisatie gemaakte applicatie, en dat dit tot een informatiebeveiligingsincident leidt wanneer de applicatie wordt gebruikt.

Focuspunten

- Zorg ervoor dat architectuurrichtlijnen consistent worden toegepast tijdens het ontwikkelproces. Dit garandeert dat de software schaalbaar, onderhoudbaar en van hoge kwaliteit is.
- Volg de OWASP-richtlijnen, met name de OWASP Top 10, bij de ontwikkeling van webapplicaties. Dit helpt om de grootste beveiligingsrisico's te identificeren en te mitigeren, waardoor de software veiliger wordt tegen cyberdreigingen.
- Integreer de architectuurrichtlijnen en OWASP-richtlijnen in het ontwikkelproces door middel van design patterns en best practices. Dit bevordert niet alleen de veiligheid, maar ook de efficiëntie en kwaliteit van de softwareontwikkeling.
- Monitor en evalueer regelmatig de naleving van deze richtlijnen en aanbevelingen. Zorg ervoor dat ontwikkelaars op de hoogte blijven van de nieuwste architectuurrichtlijnen en OWASP-updates, zodat de software voortdurend voldoet aan de hoogste beveiligingsnormen.

Mapping indication

ISO 27001: A.8.27 - Veilige systeemarchitectuur en technische uitdagingen.

6.4 Bewustwording van informatiebeveiliging bij de ontwikkeling van applicaties

Organisaties die applicaties ontwikkelen dienen ervoor te zorgen dat ontwikkelaars zich bewust zijn van de informatiebeveiligingsrisico's die samenhangen met het ontwikkelen van applicaties en het gebruiken van die applicaties bij het verwerken van informatie.

Doel

Voorkomen dat er een bug, kwetsbaarheid of logische fout aanwezig is in door de organisatie gemaakte applicatie, en dat dit tot een informatiebeveiligingsincident leidt wanneer de applicatie wordt gebruikt.

Focuspunten

- Zorg ervoor dat iedereen binnen de organisatie regelmatig training en bewustwordingssessies krijgt over informatiebeveiliging, zodat ze goed op de hoogte zijn van de risico's en het belang van veilige handelingen.
- Bevorder kennis van en het gebruik van security standaarden zoals OWASP, CIS Controls of SANS Top 20 Critical Security Controls onder medewerkers om de beveiligingspraktijken binnen de organisatie te versterken.
- Stimuleer actief de betrokkenheid van medewerkers bij het toepassen van beveiligingsstandaarden, zodat ze begrijpen hoe hun acties bijdragen aan de algehele veiligheid van de organisatie.
- Evalueer en actualiseer regelmatig de security awareness programma's zodat ze relevant blijven en aansluiten bij de huidige beveiligingsrisico's en -standaarden.

Mapping indication

ISO 27001: A.6.3 - Bewustwording van, opleiding en training in informatiebeveiliging.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 14, 16
IEC 62443-2-1:2010, Clause 4.3.2.4.2
NIST SP 800-53: AT-2 - Literacy training and awareness.

6.5 Testen van de beveiliging van applicaties

Organisaties die applicaties (laten) ontwikkelen dienen vooraf eisen te stellen aan de beveiliging van de applicaties met het oog op het gebruik ervan in de praktijk. Bij het testen van een ontwikkelde applicatie worden niet alleen de gebruikersaspecten getest, maar ook de beveiligingsaspecten van de applicatie.

Doel

Voorkomen dat er een bug, kwetsbaarheid of logische fout aanwezig is in door de organisatie gemaakte applicatie, en dat dit tot een informatiebeveiligingsincident leidt wanneer de applicatie wordt gebruikt.

Focuspunten

- Zorg ervoor dat de organisatie regelmatig onafhankelijke kwaliteitstoetsen en externe audits uitvoert, zoals PEN-testen, om de veiligheid van systemen en data te waarborgen. Dit helpt om de integriteit en veiligheid van nieuwe functionaliteiten te controleren en potentiële kwetsbaarheden tijdig aan te pakken.
- Leg de bevindingen van deze toetsen en audits vast op een gestandaardiseerde manier, bijvoorbeeld door ze te rangschikken volgens het Common Vulnerability Scoring System (CVSS), zodat kwetsbaarheden op prioriteit kunnen worden aangepakt.
- Neem proactief actie op basis van de resultaten van de toetsen en audits om de geïdentificeerde kwetsbaarheden te verhelpen en de algehele beveiliging te versterken.
- Gebruik de inzichten verkregen uit deze toetsen en audits om toekomstige ontwikkelingen te verbeteren en de continuïteit van de beveiliging binnen de organisatie te waarborgen.

Mapping indication

ISO 27001: A.8.29 - Testen van de beveiliging tijdens ontwikkeling en acceptatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 8, 10
IEC 62443-2-1:2010, Clause 4.2.3.1, 4.2.3.7
NIST SP 800-53: SA-11 - Developer security testing and evaluation.

6.6 Uitbestede softwareontwikkeling

Wanneer het ontwikkelen van maatwerksoftware (deels) is uitbesteed aan een externe partij bewaakt de organisatie actief de ontwikkelactiviteiten en stelt de organisatie vast of de opgeleverde software voldoet aan de informatiebeveiligingseisen.

Doel

Voorkomen dat er een bug, kwetsbaarheid of logische fout aanwezig is in door de organisatie gemaakte applicatie, en dat dit tot een informatiebeveiligingsincident leidt wanneer de applicatie wordt gebruikt.

Focuspunten

- Zorg ervoor dat je, wanneer je softwareontwikkeling uitbesteedt, goed in kaart brengt welke informatiebeveiligingsmaatregelen je partners nemen. Het is cruciaal om te weten welke stappen de externe softwareontwikkelaars zetten om de beveiliging van je gegevens en systemen te waarborgen.
- Stel duidelijke beveiligingsvereisten op en communiceer deze naar je externe softwareontwikkelaars. Dit helpt om ervoor te zorgen dat de ontwikkelde software voldoet aan de vastgestelde beveiligingsstandaarden, zoals OWASP, CIS Controls of de SANS Top 20.
- Voer regelmatig beoordelingen uit op de beveiligingsmaatregelen van de externe ontwikkelaars. Dit kan door middel van audits en andere controles om te verifiëren dat de beveiligingsvereisten worden nageleefd en dat er geen tekortkomingen zijn in de opgeleverde software.
- Houd er rekening mee dat bij offshoring de prioriteit die aan beveiliging wordt gegeven, kan verschillen. Het is belangrijk om deze risico's goed te managen en ervoor te zorgen dat alle betrokken partijen dezelfde beveiligingsnormen hanteren.

Mapping indication

ISO 27001: A.8.3 - Beperking toegang tot informatie.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 3, 4, 6, 7, 12, 13, 16
IEC 62443-2-1:2010, Clause 4.3.3.7.3
IEC 62443-3-3:2013, SR 2.1
NIST SP 800-53: AC-3 - Access enforcement

6.7 Scheiden van ontwikkel, test, acceptatie en productie

Organisaties die applicaties (laten) ontwikkelen, dienen ervoor te zorgen dat ontwikkel- en testomgevingen gescheiden blijven van productieomgevingen, bijvoorbeeld door gebruik te maken van gescheiden virtuele of fysieke omgevingen, in combinatie met gescheiden toegangsrechten.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van een onbevoegde of onbedoelde verandering aan een productieomgeving door een ontwikkelaar of tester.

Focuspunten

- Zorg ervoor dat de ontwikkel-, test-, acceptatie- en productieomgevingen duidelijk van elkaar gescheiden zijn om risico's te minimaliseren en de veiligheid te waarborgen. Dit betekent dat elke omgeving geïsoleerd moet blijven, zodat wijzigingen of tests in de ene omgeving geen invloed kunnen hebben op de andere.
- Voer strikte controles en procedures in om ongeautoriseerde toegang tussen de verschillende omgevingen te voorkomen. Door toegang zorgvuldig te beheren, voorkom je dat fouten of ongewenste wijzigingen in de productieomgeving plaatsvinden, wat essentieel is voor de continuïteit en veiligheid van je systemen.
- Gebruik een aparte acceptatieomgeving waarin testscenario's worden uitgevoerd die de productieomgeving nauwkeurig nabootsen. Dit zorgt ervoor dat eventuele problemen vroegtijdig worden ontdekt en opgelost voordat nieuwe functies of wijzigingen in de productie worden doorgevoerd.
- Regelmatige evaluaties van de scheiding tussen deze omgevingen en de bijbehorende controles helpen om de integriteit van het gehele systeem te waarborgen zodat de juiste maatregelen nog steeds effectief zijn.

Mapping indication

ISO 27001: A.8.31 - Scheiding van ontwikkel-, test- en productieomgevingen.
CIS Controls V8 (ETSI TR 103 305 1 V4.1.1), Critical Security Control 16

6.8 Procedures en maatregelen voor het deployen van software

Organisaties die software op hun operationele systemen (laten) installeren, dienen procedures en maatregelen te implementeren om dit op een veilige en gecontroleerde wijze uit te voeren.

Doel

Voorkomen dat er een informatiebeveiligingsincident optreedt als gevolg van het ongecontroleerd installeren van software op een operationeel systeem, met gevolgen voor zowel de bedrijfscontinuïteit als de veiligheid van de operationele systemen.

Focuspunten

- Zorg ervoor dat er gedocumenteerde procedures en methoden zijn voor het deployen van software, waarbij Infrastructure as Code (IAC) een belangrijke rol kan spelen. Dit zorgt voor een gestandaardiseerde en gecontroleerde implementatie, waardoor de consistentie en veiligheid van de softwareinstallaties worden gewaarborgd.
- Pas Infrastructure as Code (IAC) toe om het deployment proces te automatiseren en herhaalbaar te maken. Dit helpt niet alleen bij het handhaven van informatiebeveiliging, maar zorgt ook voor een efficiënte en foutloze installatie van softwareoplossingen.
- Implementeer regelmatige evaluaties en bijwerkingen van de deployment procedures zodat ze blijven voldoen aan de nieuwste beveiligingsnormen en technologieën. Dit draagt bij aan de continue verbetering van de kwaliteit en veiligheid van softwareinstallaties.
- Waarborg dat iedereen binnen het team bekend is met de procedures en methoden voor softwaredeployment, en zorg voor training indien nodig. Dit versterkt de naleving en effectiviteit van de gestandaardiseerde deployment processen binnen de organisatie.

Mapping indication

Geen Mapping indication aanwezig.

6.9 Overzicht van geleverde software

De organisatie dient een overzicht van alle klanten op te stellen en te onderhouden die gebruik maken van software die door de organisatie is gemaakt. Dit overzicht moet duidelijk aangeven welke klant momenteel welke versie van welke software gebruikt.

Doel

Een actueel overzicht van klanten en hun softwareversies helpt de organisatie bij het snel identificeren van kwetsbare of verouderde software, het efficiënt toepassen van beveiligingspatches en het beheren van incidenten. Dit minimaliseert beveiligingsrisico's en zorgt voor betere bescherming tegen potentiële dreigingen bij klanten.

Focuspunten

- Stel een gedetailleerde klantendatabase op waarin je vastlegt welke software en versies door elke klant worden gebruikt. Dit helpt bij het nauwkeurig plannen van onderhoud, updates en licentiebeheer.
- Koppel klantinformatie aan specifieke softwareversies en licenties, zodat je effectief kunt monitoren welke klanten toegang hebben tot welke software. Dit is cruciaal voor het beheren van licenties en het naleven van contractuele afspraken.
- Gebruik de verzamelde gegevens om de impact van nieuwe versies, patches of updates te analyseren. Dit stelt je in staat om de omvang van wijzigingen te begrijpen en om gerichte ondersteuning te bieden aan klanten die mogelijk getroffen worden.
- Actualiseer en controleer regelmatig de klantendatabase om ervoor te zorgen dat alle informatie up-to-date blijft. Dit zorgt voor een efficiënt onderhoudsproces en helpt bij het minimaliseren van fouten in licentiebeheer en software-updates.

Mapping indication

Geen Mapping indication aanwezig.

6.10 Overzicht houden over geleverde apparatuur en programmatuur

De organisatie dient alle aan klanten geleverde apparatuur en programmatuur nauwkeurig te inventariseren en vast te leggen in een actueel en gedocumenteerd overzicht van het IT-landschap. Dit overzicht dient periodiek te worden bijgewerkt en gecontroleerd. Het proces moet waarborgen dat proactief onderhoud wordt uitgevoerd en dat beveiligingsupdates tijdig bij klanten worden toegepast.

Doel

Een nauwkeurige inventarisatie van apparatuur en programmatuur helpt bij het identificeren van kwetsbaarheden, het effectief beheren van risico's, en het waarborgen van tijdige beveiligingsupdates. Dit vermindert de kans op beveiligingsincidenten en versterkt de algehele veiligheid van het IT-landschap.

Focuspunten

- Zorg voor een nauwkeurige inventarisatie van alle geleverde apparatuur en programmatuur, inclusief versies, om een volledig overzicht van het IT-landschap van de klanten te hebben. Dit overzicht is cruciaal voor effectief beheer, proactief onderhoud en het tijdig toepassen van beveiligingsupdates.
- Stel een gedetailleerde inventarislijst op die precies bijhoudt welke apparatuur en programmatuur bij welke klant in gebruik is, inclusief de versies. Dit vergemakkelijkt het plannen van onderhoud en het doorvoeren van updates, waardoor de kans op beveiligingsproblemen en ongeautoriseerd gebruik wordt verkleind.
- Zorg ervoor dat de inventarislijst altijd up-to-date is, door deze direct bij te werken zodra er wijzigingen worden doorgevoerd. Dit vermindert het risico op fouten en helpt bij het handhaven van de betrouwbaarheid en veiligheid van de IT-infrastructuur.
- Implementeer een systeem voor automatisch bijwerken van de inventarislijst, zodat veranderingen in apparatuur en programmatuur onmiddellijk worden geregistreerd. Dit zorgt ervoor dat de inventarislijst accuraat blijft en helpt bij het proactief beheren van beveiligingsrisico's.

Mapping indication

Geen Mapping indication aanwezig.

6.12 Afstemming met klanten over nieuwe software en updates

De organisatie dient een proces op te stellen en in te voeren voor het in overleg met klanten installeren van nieuwe versies van software of van patches.

Doel

Voorkomen dat er informatiebeveiligingsincidenten optreden door onvoldoende afstemming met klanten over het installeren van nieuwe software of patches.

Focuspunten

- Identificeer de doelgroep van klanten die de nieuwe versie of patch nodig hebben, en stel een tijdschema op voor de uitrol. Dit helpt om de impact op de klanten te minimaliseren en zorgt voor een gestructureerde aanpak bij het uitrollen van updates.
- Informeer klanten proactief over de beschikbaarheid, inhoud en voordelen van de nieuwe versie of patch. Geef indien nodig duidelijke instructies voor de implementatie, zodat klanten goed voorbereid zijn op de veranderingen.
- Automatiseer zoveel mogelijk het proces van het distribueren en installeren van nieuwe versies en patches. Dit verkort de tijd die nodig is om verbeteringen door te voeren en vermindert het risico op fouten tijdens de installatie.
- Zorg voor een gestandaardiseerd stappenplan voor het releasen en patchen, dat de fasen van identificatie, communicatie en distributie omvat. Dit waarborgt een consistent proces dat efficiënt en effectief is in het uitrollen van verbeteringen bij klanten.

Mapping indication

Geen Mapping indication aanwezig.

Copyright

Toelichting op Mapping indication

Onze norm voor cybersecurity is het resultaat van een uitgebreide samenwerking tussen een divers team van experts op het gebied van cyberbeveiliging. Dit multidisciplinaire team bestond uit vertegenwoordigers van NIS2 organisaties, mkb bedrijven, onafhankelijke cybersecurityspecialisten en auditoren. Door deze gevarieerde samenstelling hebben we ervoor gezorgd dat onze norm een breed scala aan perspectieven en expertise omvat, wat heeft geleid tot een unieke en uiterst waardevolle benadering van cybersecurity. Hoewel onze norm mogelijk enige overlap vertoont met andere cybersecuritynormen op bepaalde punten, moeten gebruikers begrijpen dat onze norm een op zichzelf staand product is, dat is ontwikkeld met het oog op de specifieke behoeften en uitdagingen van moderne bedrijven. De inhoud en aanpak van onze norm kunnen daarom verschillen van die van andere normen, zelfs als er enige gelijkenis bestaat. Het is belangrijk om te benadrukken dat onze norm is ontworpen om de best practices op het gebied van cybersecurity te omvatten, gebaseerd op de inzichten en ervaringen van onze diverse teamleden. Daarom moeten gebruikers onze norm beschouwen als een uniek instrument dat is ontwikkeld met het oog op maximale toegevoegde waarde en effectiviteit voor organisaties die streven naar verbeterde cybersecurity.

Disclaimer