NIS2 Quality Mark

NIS2-QM20 SUBSTANTIAL

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

1.6.1 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

- Inventariseer alle informatiegegevens binnen de organisatie, zoals klantgegevens, contracten en financiële administratie. Dit overzicht helpt bij het identificeren en effectief beveiligen van alle informatie.
- Stel een informatieregister op dat alle soorten informatie, inclusief opslaglocaties, vormen (digitaal of op papier) en bewaartermijnen, bevat. Dit register moet compleet, correct en actueel zijn.
- Wijs eigenaren/beheerders aan voor specifieke informatiecategorieën in het register. Deze personen zijn verantwoordelijk voor het beheer en de beveiliging van hun toegewezen informatie.
- Controleer en actualiseer het informatieregister regelmatig om ervoor te zorgen dat het volledig en up-to-date blijft. Dit garandeert dat de informatie correct beheerd en beschermd wordt.

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

1.13 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

- Stel een procedure op voor het registreren, aanpassen en verwijderen van gebruikersaccounts van personeel. Dit zorgt ervoor dat de levenscyclus van identiteiten goed beheerd en gedocumenteerd wordt.
- Definieer en wijs duidelijke rollen en verantwoordelijkheden toe voor het beheer van gebruikersaccounts. Dit helpt om te waarborgen dat elke stap in de levenscyclus van een identiteit correct wordt uitgevoerd en gecontroleerd.
- Zorg ervoor dat identiteitsgegevens, zoals gebruikersnamen, e-mailadressen en personeelsnummers, uniek en goed beveiligd zijn. Dit is essentieel voor de authenticatie en autorisatie binnen de organisatie en helpt om ongeautoriseerde toegang te voorkomen.
- Communiceer de procedures en verantwoordelijkheden rondom het beheer van identiteitsgegevens naar alle medewerkers. Dit bevordert naleving en bewustwording van het belang van een goed beheer van identiteiten binnen de organisatie.

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.
- Stel een autorisatiematrix op die duidelijk maakt welke toegangsrechten bij welke rol horen. 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

1.20 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

1.23 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.

1.26 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.

2.2 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

2.6 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

- Zorg voor een duidelijke en eenvoudige procedure voor het melden van cyberincidenten, zodat medewerkers snel en effectief bedreigingen voor de informatieveiligheid kunnen rapporteren.
- Maak afspraken over de kanalen die gebruikt moeten worden voor meldingen, zoals e-mail, WhatsApp en telefonie, om een snelle en betrouwbare respons te garanderen.
- Overweeg het gebruik van een digitaal meldsysteem of een specifieke app voor uitgebreidere en gedetailleerde rapportage van cyberincidenten. Dit kan helpen bij het systematisch vastleggen en opvolgen van meldingen.
- Zorg ervoor dat er een centraal meldpunt is binnen de organisatie, zoals de servicedesk of het IT-team, dat verantwoordelijk is voor het ontvangen en behandelen van meldingen over informatiebeveiligingsincidenten.

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.

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.
- Stel een autorisatiematrix op die duidelijk maakt welke toegangsrechten bij welke rol horen. 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.
- 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: Clausule 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.

4.4 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

4.7 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

4.9 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 logbestanden 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.

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-bedrijfsmiddelen

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-systeem 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-systeem, 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-systemen 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-systemen 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.

5.11 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 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.

6.3 Veilige software ontwikkelen

De organisatie dient ‘best practices’ vast te stellen voor het ontwikkelen van veilige software. De naleving van deze ‘best practices’ wordt gecontroleerd.

Doel

Voorkomen dat een bug, logische fout of andere kwetsbaarheid aanwezig is in door de organisatie gemaakte software, en dat dit tot een informatiebeveiligingsincident leidt wanneer de software 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.

6.9 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.

6.12 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 van 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