Auteur | Marit Swart
Uitgifte | juni 2025

NIS2 en het ECD: 10 praktische stappen voor zorginstellingen*

Van beleid tot praktijk: NIS2 toepassen op het ECD van jouw zorginstelling

01

Risicoanalyse

Beleid gericht op het identificeren en classificeren van cyberrisico's rondom het ECD, waarop passende maatregelen worden gebaseerd.

02

Incidentenbehandeling

Beleid met richtlijnen voor het snel herkennen, aanpakken en herstellen van cyberincidenten om schade aan het ECD te minimaliseren.

03

Bedrijfscontinuïteit

Beleid gericht op het waarborgen van de continuïteit of het snel herstel van kritieke bedrijfsprocessen en middelen, zoals het ECD, bij verstoringen.

04

Beveiliging van de toeleveringsketen

Beleid gericht op het beheersen van cyberrisico's door maatregelen en bewustwording van digitale afhankelijkheid, om verstoring door aanvallen op de ECD-leverancier te voorkomen.

05

Beleid voor veilige aanschaf en beheer van het ECD

Beleid gericht op veilig verwerven, onderhouden en beveiligen van het ECD tegen kwetsbaarheden.

06

Cyberhygiëne basispraktijken

Beleid gericht op het stimuleren van veilig en verantwoord gebruik van het ECD door medewerkers ter vermindering van cyberrisico's.

07

Cryptografie

Beleid gericht op het toepassen van cryptografie om de vertrouwelijkheid, integriteit, authenticiteit, authenticatie van data te waarborgen.

08

Personeel, toegangsbeleid en activa

Beleid gericht op het beveiligen van personeel, toegangsbeheer en ECD-assets.

09

Toets de effectiviteit van maatregelen

Beleid gericht op het periodiek toetsen of cyberbeveiligingsmaatregelen bij het ECD het beoogde effect hebben.

10

Registratie in het entiteitenregister

Registreer uw zorginstelling in het entiteitenregister van het NCSC door een bestuurder of een medewerker met cyberbeveiligingskennis.

** Met de toelichtingen op de volgende pagina's kan gericht invulling worden gegeven aan het beleid.*

Toelichting bij het stappenplan*

01

Beleid inzake risicoanalyse en beveiliging van netwerk- en informatiesystemen, artikel 21 lid 2 sub a NIS2-richtlijn

Het uitvoeren van een risicoanalyse vormt de basis voor alle beleidsvorming die de NIS2-richtlijn vereist. Deze analyse richt zich niet alleen op het ECD, maar kan breder worden toegepast op andere kritieke onderdelen van de organisatie, zoals digitale systemen, reputatie, financiële gegevens, medewerkersgegevens en vertrouwelijke kennisproducten.

Bij het ECD kunnen risico's zich onder andere uiten in systeemuitval of ongeautoriseerde toegang. Elk risico wordt beoordeeld op de kans van optreden en de impact van een verstoring. Daarbij wordt gebruikgemaakt van de BIV-classificatie, die focust op beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

De resultaten van de risicoanalyse worden zorgvuldig gedocumenteerd en opgeslagen op een beveiligde locatie, uitsluitend toegankelijk voor geautoriseerde personen. Voor onaanvaardbare risico's worden passende beheersmaatregelen vastgesteld, waarmee de organisatie risico's actief kan mitigeren en beheersen. Voor de risicoanalyse kan tevens gebruik worden gemaakt van standaarden als ISO 31000.

02

Incidentenbehandeling, artikel 21 lid 2 sub b NIS2-richtlijn

Incidentenbehandeling omvat alle acties en procedures die gericht zijn op het voorkomen, opsporen, analyseren en indammen van of het reageren op en het herstellen van een cyberincident (artikel 6 onder 8 NIS2-richtlijn).

Voor een effectieve incidentbehandeling is goede voorbereiding cruciaal. Op basis van de risicoanalyse worden scenario's opgesteld voor veelvoorkomende cyberincidenten. Na melding is het belangrijk vast te stellen of het om een incident gaat en wat de aard en ernst ervan is. Detectie kan onder andere via ECD-logbestanden.

Een meldpunt voor cyberincidenten is verplicht, zodat meldingen centraal en gestructureerd worden afgehandeld. Voor medewerkers is het essentieel te weten wanneer, hoe en bij wie zij een (mogelijk) cyberincident moeten melden. Een CISO of een functionaris met kennis van informatiebeveiliging is daarbij een logische contactpersoon. Het ligt voor de hand dat de verantwoordelijke de melding ook rapporteert aan Z-CERT voor verdere opvolging. Documentatie van alle verrichte stappen is nodig om achteraf te leren en incidentrespons, training en bewustwording continu te verbeteren.

03

Bedrijfscontinuïteit, artikel 21 lid 2 sub c NIS2-richtlijn

Bedrijfscontinuïteitsplannen zijn erop gericht dat de zorgverlening zoveel mogelijk doorgaat tijdens een verstoring. Denk hierbij aan het tijdelijk overschakelen van digitale processen, zoals medicatielijsten in het ECD, naar papieren alternatieven. Daarnaast moeten duidelijke hersteldoelstellingen worden vastgelegd, bijvoorbeeld dat het ECD binnen een bepaald aantal uur weer operationeel is.

Ook de organisatie van crisiscommunicatie is cruciaal. Belangrijke contactpersonen, zoals Z-CERT (CSIRT), IGJ, leverancier van het ECD, bestuurders en de CISO (of andere eindverantwoordelijke voor cyberbeveiliging), moeten vooraf zijn vastgelegd. Eveneens moeten de communicatiekanalen bekend en beschikbaar zijn. Voor interne communicatie kunnen portofoons of groepsapps worden ingezet, terwijl voor externe communicatie – bijvoorbeeld met naasten of leveranciers – telefoon en e-mail geschikt zijn.

Belangrijk is dat noodcommunicatie losstaat van de reguliere ICT-systemen van de organisatie. Denk hierbij aan geprinte draaiboeken en alternatieve communicatiemiddelen die blijven functioneren bij ICT-uitval.

04

Beveiliging van de toeleveringsketen, artikel 21 lid 2 sub d NIS2-richtlijn

Om de continuïteit en veiligheid van essentiële applicaties zoals het ECD te waarborgen en het risico op cyberincidenten met impact op de zorgverlening te beperken, is het belangrijk om in een Service Level Agreement (SLA) duidelijke afspraken vast te leggen over de minimale beschikbaarheid. Denk hierbij aan het garanderen van een bepaald uptimepercentage per maand, bijvoorbeeld 99,8%.

Daarnaast mogen van leveranciers van netwerk- en informatiesystemen aantoonbare beveiligingsmaatregelen worden verwacht. Dit betekent dat zij moeten voldoen aan erkende normen zoals NEN 7510 of ISO 27001. Deze normen bieden waarborgen voor de beveiliging, betrouwbaarheid en integriteit van systemen en gegevens, en dragen bij aan naleving van de NIS2-richtlijn.

05

Beveiliging bij de aanschaf en het onderhoud van het ECD, artikel 21 lid 2 sub e NIS2-richtlijn

In het kader van NIS2 is het belangrijk dat organisaties hun netwerk- en informatiesystemen goed beveiligen. Dit begint met sterke maatregelen zoals firewalls en netwerksegmentatie om het netwerk te beschermen. Daarnaast is het cruciaal dat systemen zorgvuldig worden geconfigureerd en dat wijzigingen aan software en hardware volgens vaste procedures verlopen, met een goede registratie van deze aanpassingen.

Beveiligingsupdates moeten snel worden doorgevoerd en kwetsbaarheden actief worden opgespoord en opgelost. Ook tijdens de ontwikkeling van software moet beveiliging vanaf het begin worden ingebouwd. Tot slot speelt het inkoopproces een belangrijke rol: alleen systemen die aan strenge cybersecurity-eisen voldoen, mogen worden aangeschaft. Samen zorgen deze stappen ervoor dat de organisatie beter bestand is tegen digitale bedreigingen en voldoet aan de NIS2-eisen.

** Disclaimer:*
Dit stappenplan en de begeleidende toelichting kunnen ook worden gebruikt om te voldoen aan de NIS2-richtlijn voor andere netwerk- en informatiesystemen binnen uw organisatie.

Vervolg toelichting

06

Cyberhygiëne basispraktijken (artikel 21 lid 2 sub g NIS2-richtlijn)

Cyberhygiëne omvat eenvoudige, dagelijkse handelingen die digitale veiligheid bevorderen. Een onderdeel van cyberhygiëne is bewustwording. Dit wordt vormgegeven via o.a. e-learnings, intranet en campagnes en is afgestemd op rollen, actuele dreigingen en beleidsmaatregelen. Opleiding is verplicht voor medewerkers en bestuurders (aanvulling op NEN 7510). Het programma moet regelmatig worden herhaald, aansluiten op het beveiligingsbeleid en opgenomen zijn in beleid en planning.

Voor zorgpersoneel kan dit bijvoorbeeld gaan over het correct afvoeren van medicijnzakjes met persoonsgegevens, terwijl voor de salarisadministratie de focus ligt op het herkennen van verzoeken tot ongeoorloofde wijzigingen in bankgegevens.

07

Cryptografie (artikel 21 lid 2 sub h NIS2-richtlijn)

Gebruik uitsluitend goedgekeurde encryptiestandaarden, met passende sleutellengte. Overweeg sleutelgeneratie als aanvullende maatregel voor systemen zoals het ECD.

Voor sleutelmanagement zijn duidelijke procedures nodig voor het aanmaken, bewaren, archiveren, terugvinden, back-uppen en loggen van sleutelgebruik. Leg deze aspecten vast in het beleid.

08

Beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en activabeheer (artikel 21 lid 2 sub i NIS2-richtlijn)

Screening helpt risico's van onbetrouwbare medewerkers te beperken. Dit omvat het verifiëren van referenties, diploma's en identiteit. Het revalidatiecentrum vraagt standaard een Verklaring Omtrent het Gedrag (VOG) aan bij indiensttreding, zeker voor functies met kwetsbare personen. Daarnaast moet uw instelling zorgdragen dat medewerkers hun verantwoordelijkheden op het gebied van informatiebeveiliging begrijpen en accepteren. Nieuwe medewerkers krijgen bijvoorbeeld instructies over het veilige gebruik van het ECD en hun rol hierin.

Binnen NIS2 is het tevens essentieel dat toegang tot netwerk- en informatiesystemen, zoals het ECD of strikt wordt geregeld. Alleen geautoriseerde medewerkers krijgen toegang, afgestemd op hun functie en taken. Dit voorkomt ongeoorloofde toegang en beperkt de impact van mogelijke beveiligingsincidenten. Autorisaties worden periodiek geëvalueerd en aangepast bij functiewijzigingen of vertrek van medewerkers.

09

Toetsing van maatregelen (artikel 21 lid 2 sub f NIS2-richtlijn)

De NIS2 vraagt om continue verbetering van cyberbeveiliging en de bijbehorende maatregelen. Aangezien de aandacht van de NIS2-richtlijn gefocust is op continue verbetering kan hierin de PDCA-cyclus worden herkend.

Het toetsingsbeleid omvat doorgaans het doel, de reikwijdte en de toetsfrequentie. Het doel is vaststellen of uw zorginstelling passende beheersmaatregelen heeft getroffen en voldoet aan wet- en regelgeving. In lijn met NEN 7510 wordt aanbevolen ten minste jaarlijks te toetsen, tenzij contractuele afspraken een hogere frequentie vereisen.

Leg de wijze van toetsing vast in beleid. Toetsing kan plaatsvinden via een pentest of securityscan. Overleg met de CISO helpt bij het bepalen van de meest passende toetsvorm voor de organisatie. De toetsing kan intern of extern worden uitgevoerd (bijv. door een CISO) en wordt gerapporteerd aan het bestuur. Ook het toetsingsbeleid zelf wordt periodiek herzien, met oog voor organisatieveranderingen en nieuwe risico's. Verbeterpunten worden opgenomen in het beleidsplan voor effectiviteitstoetsing.

10

Registratieplicht (artikel 27 NIS2-richtlijn en artikel 43 Cyberbeveiligingswet)

De registratieplicht geldt zodra de Cyberbeveiligingswet in werking treedt. De verwachting is dat dit medio 2025 zal gebeuren. Vanaf dat moment dienen organisaties zich in te schrijven in het entiteitenregister van het NCSC.

Organisaties moeten dan o.a. KvK-nummer, adres, sector, type entiteit (essentieel/belangrijk), EU-lidstaten en contactgegevens aanleveren. Ook is één assettype verplicht (IP-adres, domeinnaam of ASN).

Registratie wordt bij voorkeur uitgevoerd door een cybersecuritydeskundige, zoals een CISO of informatiemanager. De registratie kan tevens worden uitgevoerd door een bestuurder.

Let op!
Is uw zorginstelling NEN 7510-gecertificeerd? Dan hoeft u alleen nog een meldpunt voor cyberbeveiligingsincidenten in te richten en bestuurders op te leiden!