NIS2 Wetgeving

Uw e-book voor NIS2 compliance

BOSSIT

Inhoudstafel

Voorwoord

Digitale systemen zijn steeds meer de essentiële basis van onze samenleving geworden. Belangrijke sectoren zoals gezondheidszorg, logistiek, bankwezen en nutsvoorzieningen kunnen niet langer functioneren zonder een betrouwbare en veilige digitale infrastructuur. Dit maakt hen ook kwetsbaar voor kwaadwillende die streven naar financieel gewin of verstoring van de maatschappelijke orde.

In het huidige landschap zijn de afgelopen jaren de cyberrisico's aanzienlijk toegenomen, voornamelijk als gevolg van technologische, maatschappelijke en geopolitieke ontwikkelingen. Cybercriminaliteit is inmiddels sterk geprofessionaliseerd en heeft zich ontwikkeld tot een goed georganiseerde miljardenindustrie. Nationale overheden hebben digitale wapens stevig geïntegreerd in hun militaire arsenaal. Bovendien brengen ontwikkelingen zoals de groei van hybride werkvormen nieuwe risico's met zich mee. Het is niet langer de vraag óf, maar wanneer organisaties te maken zullen krijgen met een cyberaanval.

Dit vereist niet alleen maatregelen op zich, maar ook wetgeving met betrekking tot beveiligingsvoorzieningen voor alle organisaties die een essentiële rol spelen in de samenleving. Met NIS2 onderneemt de Europese Unie een nieuwe poging om lidstaten hierin te ondersteunen.

NIS2 kan aanzienlijke impact hebben, ook voor jouw organisatie. De nieuwe wetgeving is bindend, en het niet naleven ervan kan niet alleen het risico op ernstige cyberincidenten vergroten, maar ook leiden tot aanzienlijke boetes. Het is nog nooit zo cruciaal geweest om de beveiliging van tevoren goed op orde te hebben.

“Het is niet de vraag of, maar wanneer organisaties te maken krijgen met een cyberaanval.”

Wat dit e-book voor jou in petto heeft

Dit e-book biedt een diepgaande verkenning van NIS2. We verstrekken antwoorden op veelvoorkomende vragen, onthullen de verschillen met NIS, behandelen de juridische aspecten van de richtlijn en bieden praktische begeleiding voor organisaties die zich op NIS2 moeten voorbereiden.

01

NIS en NIS2

NIS naar NIS2

NIS2 staat voor Network Information Security 2, een richtlijn opgesteld door de Europese Unie die als fundament dient voor nationale wetgeving over cybersecurity. Het Europees Parlement beoogt hiermee de beveiligingsstandaarden en cyberweerbaarheid in heel Europa te versterken. NIS2 specificeert de minimale maatregelen die organisaties zouden moeten nemen om hun digitale systemen te beschermen, geeft aan op welke organisaties deze richtlijn van toepassing is, en benoemt de consequenties van non-compliance

Richtlijn vs. wetgeving

NIS2 een richtlijn. Het heeft niet de aard van een strikte verordening, maar omvat wel wat in juridische termen een 'resultaatverplichting' wordt genoemd. Het is aan de individuele lidstaten van de EU om nationale wetgeving te ontwikkelen op basis van NIS2 en zo het beoogde resultaat van NIS2 zo effectief mogelijk te bereiken. Lidstaten hebben hiervoor tot oktober 2024 de tijd.

Opvolger van NIS

NIS2 is geen geheel nieuwe ontwikkeling. Sinds 2016 bestaat de NIS-richtlijn. NIS2 fungeert als directe opvolger van NIS. De richtlijn is op diverse punten herzien, en dit is niet zonder reden: NIS2 sluit beter aan bij de huidige ontwikkelingen en de groeiende dreiging van cyberaanvallen. Zo is NIS2 van toepassing op een breder scala aan organisaties. Naast vitale sectoren richt NIS2 zich ook op bijvoorbeeld ICT-dienstverleners, de maakindustrie en organisaties die een rol spelen in vitale toeleveringsketens (zie 'Voor wie is NIS2 bedoeld?'). Bovendien omvat NIS2 een meldplicht voor cyberincidenten, en lidstaten worden verplicht om de naleving te controleren, met zelfs proactieve controle voor de meest vitale organisaties.

Evolutie

2013: De Europese Commissie publiceert de Europese Unie Cybersecurity Strategie, waarin de behoefte aan een gecoördineerde aanpak van cybersecurity binnen de EU-lidstaten wordt benadrukt.

2016: Het Europees Parlement en de Raad van de Europese Unie keuren de Network and Information Security-richtlijn (NIS-richtlijn) goed.

2018: Deadline voor EU-lidstaten om de NIS-richtlijn om te zetten in hun nationale wetgeving.

2019: EU-lidstaten moeten Computer Security Incident Response Teams (CSIRT's) oprichten om samenwerking en informatie-uitwisseling tussen lidstaten en het Europees Agentschap voor Cybersecurity (ENISA)

2021: EU-lidstaten werken verder aan de implementatie van de NIS-richtlijn en het versterken van hun cybersecurity-capaciteiten in overeenstemming met de vereisten.

2022: 28 november de Europese Raad stelt de NIS2-richtlijn vast. 27 december publicatie van de NIS2- richtlijn in de Official Journal van de Europese Unie.

2023: Januari 2023 start van de Implementatietermijn van 21 maanden. Binnen deze termijn moeten EU-lidstaten de richtlijn omzetten naar wetgeving.

2024

Naar verwachting treedt de wet eind 2024 in werking in België. De organisaties die onder de NIS2-richtlijn vallen, moeten vanaf dat moment aan deze wet voldoen.

02

Juridische context van NIS2

Voor wie is NIS2 van toepassing?

NIS2 is gericht op ondernemingen en instellingen die een cruciale functie vervullen in de samenleving. De richtlijn maakt een onderscheid tussen organisaties die als 'essentieel' en 'belangrijk' worden beschouwd. Uiteindelijk is NIS2 van toepassing op een uitgebreider spectrum van organisaties in vergelijking met de vorige NIS-richtlijn.

Doelgroepen NIS2

- Essentiële organisaties
- Belangrijke organisaties
- Ketenpartners van essentiële of belangrijke organisaties
- Kleine bedrijven die vallen onder de uitzondering (strategische doelwitten)
- Apart aangewezen organisaties

Is NIS2 van toepassing voor uw onderneming?

Essentiële organisaties

Dit betreffen omvangrijke organisaties die een essentiële rol vervullen in de samenleving. Met 'groot' bedoelt NIS2 organisaties met meer dan 250 medewerkers of een netto-omzet van meer dan 50 miljoen euro en een balanstotaal van meer dan 43 miljoen euro.

- Energie
- Transport
- Bankwezen
- Infrastructuur voor de financiële markt
- Drinkwater
- Afvalwater
- Digitale infrastructuur
- Beheer van ICT-diensten
- Gezondheidszorg
- Overheid
- Ruimtevaart

Belangrijke organisaties

Naast essentiële entiteiten maakt NIS2 ook melding van belangrijke entiteiten. Dit zijn middelgrote organisaties binnen de essentiële entiteiten of actief in een van de zes aanvullende sectoren. Met 'middelgroot' doelt de richtlijn op organisaties met minimaal 50 werknemers of een jaaromzet of balanstotaal van meer dan 10 miljoen euro.

- Post- en koeriersdiensten
- Afvalstoffenbeheer
- Levensmiddelen
- Maakindustrie
- Chemische stoffen
- Onderzoek

Ketenpartners

Een extra categorie organisaties die moet voldoen aan NIS2 betreft diegenen die deel uitmaken van het kernproces van de toeleveringsketen van een essentiële of belangrijke organisatie. Het kan dus voorkomen dat jouw toeleveranciers of dienstverlenende partners zelf niet actief zijn in een van de eerdergenoemde sectoren of minder dan 50 medewerkers hebben, en daarom niet worden gelabeld als 'essentieel' of 'belangrijk', maar desondanks dienen te voldoen aan NIS2. De EU heeft deze categorie niet zonder reden toegevoegd. In het verleden zijn namelijk verschillende grootschalige cyberaanvallen op organisaties in vitale sectoren gestart bij een partner in de keten. Het is dus van groot belang dat ook zij hun beveiliging op orde hebben.

Uitgezonderde kleine bedrijven

Een aantal kleine bedrijven past niet binnen de eerdergenoemde categorieën, maar moet desondanks voldoen aan NIS2. Hierbij gaat het om bedrijven die een belangrijke rol spelen in de infrastructuur van het internet en daardoor strategische doelwitten zijn voor cyberaanvallen. Voorbeelden hiervan zijn bedrijven die toplevel-domeinnamen beheren, aanbieders van domeinnaamregistratiediensten, of verstrekkers van openbare communicatienetwerken of -diensten. Ook overheidsinstanties in deze sectoren vallen automatisch onder de NIS2-richtlijn.

Apart aangewezen uitzonderingen

Als je niet binnen een van de eerdergenoemde categorieën valt, bestaat nog steeds de mogelijkheid dat je moet voldoen aan NIS2. De overheid kan namelijk organisaties bij uitzondering aanwijzen die toch aan deze richtlijn moeten voldoen.

Toezicht en handhaving

NIS2 legt verplichtingen op en is geen vrijblijvende richtlijn; het wordt daadwerkelijk omgezet in wetgeving. Alle organisaties die onder een van de categorieën genoemd in 2.1 vallen, dienen hieraan te voldoen. Een significant verschil met de oorspronkelijke NIS-richtlijn is de aanpak van controle op naleving. Organisaties binnen de categorie 'essentieel' kunnen proactieve, willekeurige inspecties verwachten. Dit houdt in dat ze op elk moment zonder specifieke reden moeten kunnen aantonen dat ze aan de wettelijke vereisten voldoen.

Ook organisaties behorend tot de categorie 'belangrijk' moeten zich aan de NIS2-richtlijn houden. Voor hen gelden echter geen proactieve inspecties. Ze dienen pas aan te tonen dat ze aan de wet voldoen wanneer er duidelijke aanleiding is, wat in de praktijk meestal voortkomt uit een (ernstig) cyberincident.

Automatische toepassing

Als jouw organisatie actief is in een van de genoemde categorieën, is het automatisch verplicht te voldoen aan NIS2. Dit vormt een wezenlijk verschil met de initiële versie van NIS, waarbij expliciete aanwijzing door een ministerie vereist was. Deze noodzaak is nu niet langer van toepassing.

Twijfel je of jouw organisatie aan NIS2 moet voldoen?

De officiële documentatie van de richtlijn biedt een gedetailleerde beschrijving van de soorten organisaties en bedrijfsactiviteiten binnen elke genoemde sector. Hierdoor ontstaat geen twijfel over de verplichting van jouw organisatie om al dan niet aan NIS2 te voldoen.

Boetes

Als een organisatie na controle niet voldoet aan de richtlijn, kan de sectorale toezichthouder een boete opleggen. Lidstaten hebben zelf de bevoegdheid om de hoogte van deze boete te bepalen, in overeenstemming met de aard en ernst van de nalatigheid. De boetes voor de ernstigste gevallen van nalatigheid zijn als volgt (waarbij de minimale boete steeds het hoogste bedrag van de gegeven keuzes is):

- Voor essentiële organisaties: minimaal 10 miljoen euro of 2% van de wereldwijde jaaromzet.
- Voor belangrijke organisaties: minimaal 7 miljoen euro of 1,4% van de wereldwijde jaaromzet.

Hoofdelijke aansprakelijkheid

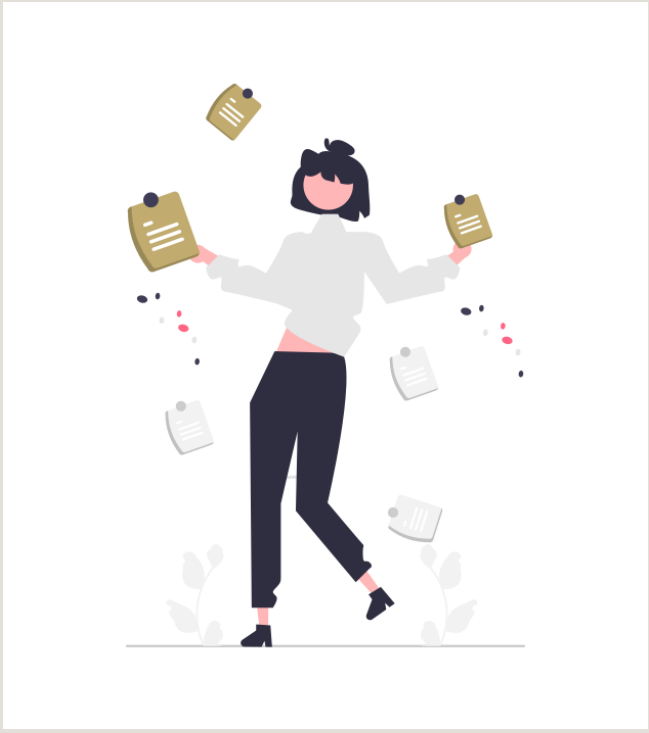
Een opmerkelijke toevoeging in NIS2 is dat alle bestuurders persoonlijk verantwoordelijk en hoofdelijk aansprakelijk zijn voor de naleving van NIS2. Niemand kan zich verschuilen achter de beslissingen of nalatigheid van een ander. NIS2 is daarmee relevant voor de gehele boardroom.

03

Kernprincipes van NIS2

Zorgplicht

De zorgplicht houdt in dat de organisatie passende securitymaatregelen moet nemen om de digitale veiligheid en de continuïteit van de dienstverlening te waarborgen. NIS2 specificeert niet exact welke technologieën of oplossingen organisaties moeten implementeren. De richtlijn benadrukt het belang van 'passende en evenredige technische, operationele en organisatorische maatregelen', rekening houdend met de stand van de techniek. Niettemin geeft NIS2 wel richtlijnen voor aandachtsgebieden die organisaties ten minste moeten behandelen:



- Beleid rondom risicoanalyse: Organisaties dienen beleid te hebben over periodieke analyses van securityrisico's, waaronder regelmatige evaluaties van externe risico's en pentests om kwetsbaarheden in de IT-infrastructuur te identificeren.
- Analyse van de effectiviteit van securitymaatregelen: Het is vereist dat organisaties regelmatig controleren of genomen maatregelen adequaat zijn.
- Beveiliging van de toeleveringsketen: NIS2 brengt de focus op ketenveiligheid met zich mee. Maatregelen dienen niet enkel gericht te zijn op het voorkomen van incidenten binnen de eigen organisatie, maar ook op de bescherming van de gehele keten. Dit houdt in dat organisaties overeenkomsten moeten vaststellen met toeleveranciers en dienstenpartners over de omgang met elkaars data en de beveiliging van communicatie.
- Aandacht voor cyberhygiëne en security-awareness: In tegenstelling tot NIS verplicht NIS2 goede cyberhygiëne. Organisaties moeten ervoor zorgen dat medewerkers zich digitaal veilig gedragen en dienen regelmatig trainingen te geven op het gebied van security-awareness.
- Beleid rondom cryptografie en encryptie: NIS2 is specifiek over deze securitymaatregel en vereist dat organisaties waar mogelijk encryptie toepassen, bijvoorbeeld voor de versleuteling van gevoelige data- en communicatiestromen.
- Beleid voor fysieke beveiliging van personeelstoegang en activa: Aangezien cybercriminelen ook via fysieke toegang aanvallen kunnen plegen, vraagt NIS2 ook om aandacht voor fysieke beveiliging. Organisaties moeten weten wie aanwezig is op de werkvloer en welke toegangsrechten medewerkers hebben.

- Gebruik van multifactorauthenticatie (MFA) en beveiliging van communicatiestromen NIS2 specificeert expliciet het gebruik van multifactorauthenticatie waar dat passend is.
- Beveiliging van informatiesystemen Informatiesystemen moeten afdoende beschermd zijn tegen cyberaanvallen, malware en andere digitale bedreigingen. De keuze voor 'passende en evenredige' securitycontrols varieert per organisatie, maar omvat bijvoorbeeld oplossingen voor identiteits- en toegangsbeheer, endpointsecurity en XDR (Extended Detection and Response). Voor organisaties die intensief gebruikmaken van (multi)cloud, zijn SASE (Secure Access Service Edge) - oplossingen een logische keuze.

- Beveiliging bij het ontwerpen, ontwikkelen en onderhouden van netwerk- en informatiesystemen
  Een effectief netwerkbeheer en adequate beveiliging van het netwerk zijn essentieel. NIS2 benadrukt ook expliciet dat organisaties snel moeten reageren op nieuw ontdekte kwetsbaarheden.
  Vulnerability Management is van belang om tijdig op de hoogte te zijn van nieuwe kwetsbaarheden en te voldoen aan compliance. Daarnaast is een adequaat update- en patchbeleid onmisbaar om geïdentificeerde kwetsbaarheden te verhelpen. Het aansluiten bij een Security Operations Center (SOC) en/of Incident Response-dienstverlening vormt waardevolle aanvullingen voor de detectie en respons op securityincidenten.
- Incidentenafhandeling
  Organisaties dienen een incident-responseplan te hebben, waarin beschreven staat welke stappen de organisatie onderneemt bij een cyberincident en wie welke verantwoordelijkheden draagt.
- Continuïteit van de dienstverlening
  Na een incident moeten organisaties zo snel mogelijk hun dienstverlening kunnen herstellen. Dit vereist onder andere een degelijk back-up- en recoverybeleid, evenals passende noodvoorzieningen zoals reserve-laptops en werkplekken.

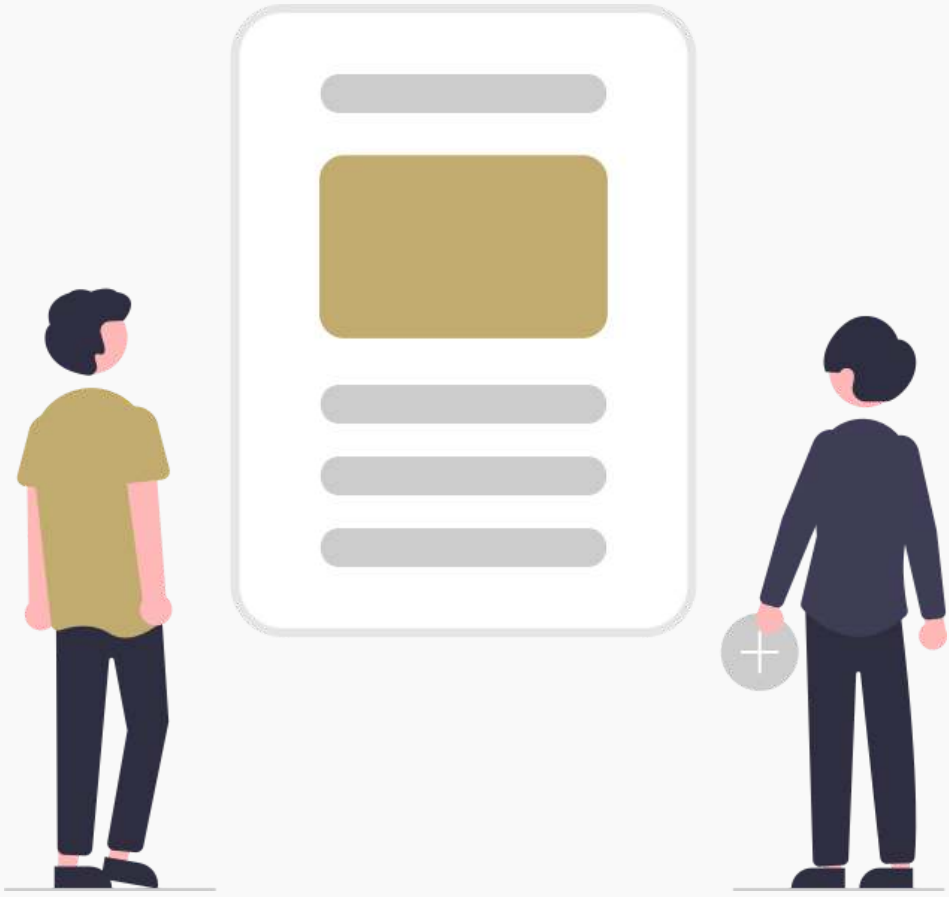
Meldingsplicht

In tegenstelling tot de vorige NIS-richtlijn omvat NIS2 nu ook een meldingsplicht. Wanneer organisaties te maken krijgen met een verstoring in hun digitale dienstverlening, zijn ze verplicht dit te melden bij de relevante autoriteit, een vergelijkbare verplichting als die in de Algemene Verordening Gegevensbescherming (AVG), waarbij organisaties ernstige datalekken moeten rapporteren aan de Autoriteit Persoonsgegevens.

NIS2 stelt de volgende voorwaarden aan een melding:

- De melding moet in alle gevallen zo spoedig mogelijk plaatsvinden.
- Als het incident de dienstverlening heeft verstoord, moet de organisatie het incident binnen 24 uur melden.
- In alle andere gevallen moet de melding binnen 72 uur plaatsvinden.

Na een maand moeten organisaties een eindverslag indienen over alle incidenten. Dit verslag bevat onderzoeksresultaten, de gevolgen van de aanval en de genomen maatregelen om herhaling te voorkomen. De organisaties dienen dit rapport in bij de betreffende autoriteit, op dit moment het Nationaal Cyber Security Centrum (NCSC).



04

Implementatie van NIS2

Voldoen aan NIS2 is geen vanzelfsprekendheid. Voor een sterke en veerkrachtige beveiligingsomgeving is het essentieel om deze kritisch te evalueren en indien nodig verbeteringen door te voeren. Tegelijkertijd is naleving op zichzelf niet het allerbelangrijkste. Cyberincidenten kunnen aanzienlijke gevolgen hebben voor de organisatie, haar klanten en de maatschappij als geheel. Een robuuste beveiliging is dus niet alleen een noodzakelijke voorwaarde voor een stabiele bedrijfsvoering, maar ook een morele en maatschappelijke verantwoordelijkheid. Een intrinsieke motivatie om beveiliging op orde te brengen is van belang om ervoor te zorgen dat dit niet slechts een eenmalige inspanning blijft. Ongeacht de motivatie is het cruciaal om snel aan de slag te gaan met het verbeteren van de beveiligingsomgeving. Op dit moment bestaat er nog ruimte om zaken grondig aan te pakken. Zodra NIS2 is omgezet in wetgeving, kunnen ernstige incidenten niet alleen bedrijfseconomische en maatschappelijke, maar ook juridische gevolgen hebben.

Met het onderstaande stappenplan en de bijbehorende tips bieden we begeleiding op weg naar NIS2-compliance.

Maak waar mogelijk gebruik van bestaande raamwerken

Verschillende bestaande raamwerken kunnen van onschatbare waarde zijn bij het streven naar NIS2-compliance. Deze raamwerken bieden structuur, dienen als inspiratie voor te nemen beveiligingsmaatregelen en leiden je stap voor stap naar een robuuste en veerkrachtige cybersecurityomgeving. Het is van groot belang dat zo'n raamwerk goed aansluit bij je organisatie, zowel in omvang als in organisatiecultuur. Een voorbeeld van een goed en veelgebruikt set maatregelen is de CIS Controls. Dit betreft een lijst van 120 best practices die zijn opgesteld door organisaties die zelf ooit slachtoffer zijn geweest van ernstige cyberaanvallen. Voor deze organisaties dienen de CIS Controls-maatregelen als een soort 'lessons learned'. De maatregelen zijn opgedeeld in drie niveaus, zodat ze een gezonde mix bieden voor organisaties van diverse typen en omvang.

Stappenplan

Mogelijk heeft jouw organisatie recentelijk een ISO 27001- of NEN 7510-traject afgerond. In dat geval kunnen we geruststellen: NIS2 maakt bestaande securitycertificeringen zeker niet overbodig. Dergelijke gerenommeerde certificeringstrajecten vormen een effectieve manier om security op een structurele wijze te integreren binnen de organisatie. Het is echter belangrijk op te merken dat een dergelijke certificering niet automatisch impliceert dat je ook direct NIS2-compliant bent.

Als je ICT-diensten verleent aan 'essentiële' of 'belangrijke' organisaties, kunnen lidstaten zelfs vereisen dat je beschikt over een door de EU erkende certificering.

Stap 1: Risicoanalyse uitvoeren
Identificeer en analyseer mogelijke risico's en bedreigingen voor de informatiebeveiliging binnen de organisatie.
Evalueer de mogelijke impact van deze risico's en bedreigingen op de vertrouwelijkheid, integriteit en beschikbaarheid van informatie.
Prioriteer de risico's op basis van de waarschijnlijkheid van een incident en de mogelijke impact.

Stap 2: Beveiligingsmaatregelen implementeren
Selecteer beveiligingsmaatregelen die geschikt zijn voor jouw organisatie op basis van geïdentificeerde risico's en bedreigingen, en toets deze aan de NIS2-richtlijn.
Implementeer technische en organisatorische maatregelen om de vertrouwelijkheid, integriteit en beschikbaarheid van data en systemen te waarborgen.
Zorg ervoor dat de beveiligingsmaatregelen voldoen aan de vereisten en aanbevelingen van de NIS2-richtlijn.

Stap 3: Incident-responseplannen ontwikkelen
Ontwikkel plannen en procedures om effectief te reageren op beveiligingsincidenten.
Definieer rollen en verantwoordelijkheden van betrokken medewerkers bij het detecteren, rapporteren en reageren op incidenten.
Stel een proces op voor het evalueren en herstellen van systemen en gegevens na een beveiligingsincident. Train medewerkers regelmatig in het volgen van het incident-responseplan.

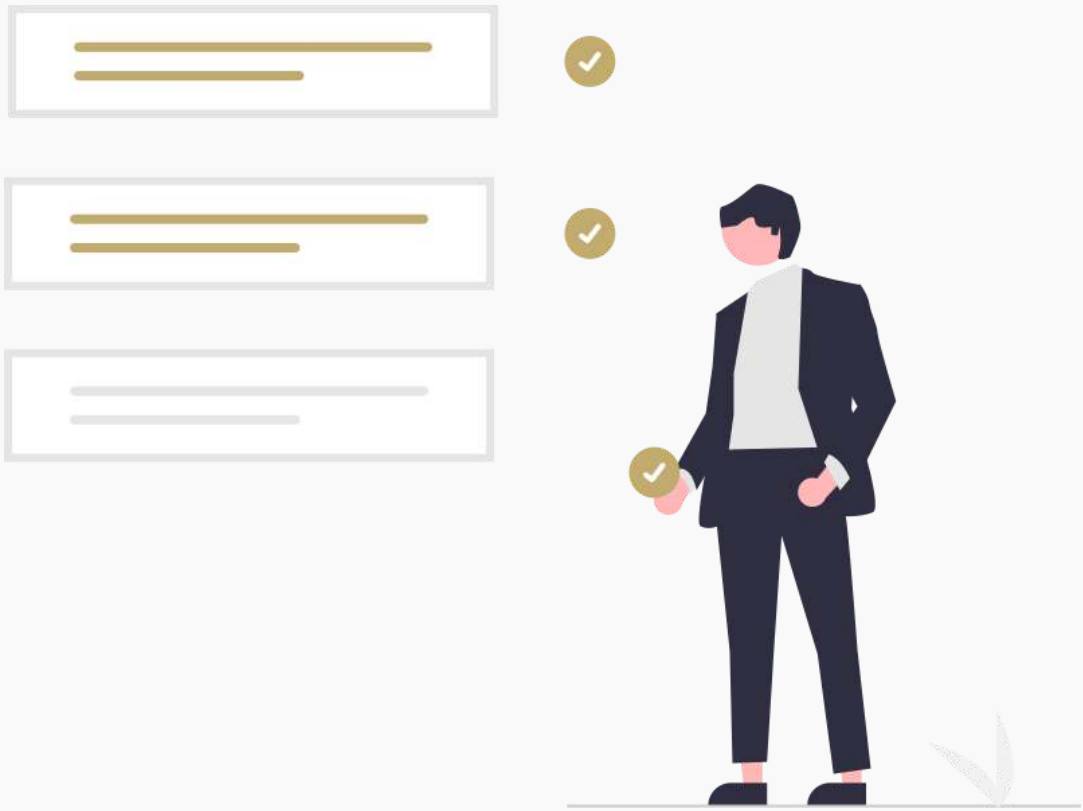
Stap 4: Bewaking en evaluatie

Stel een monitoringprogramma op om afwijkingen en incidenten te detecteren en te rapporteren.

Evalueer regelmatig de effectiviteit van beveiligingsmaatregelen en incident-responseplannen.

Pas maatregelen aan op basis van lessen uit eerdere incidenten of veranderingen in de bedrijfsomgeving.

Zorg ervoor dat je voldoet aan de rapportageverplichtingen van de NIS2-richtlijn.



Samenvatting

NIS2, als EU-richtlijn, heeft als doel de cybersecurity en cyberweerbaarheid in heel Europa te versterken. Het dient als opvolger van de NIS-richtlijn en vormt de basis voor nationale wetgeving in diverse lidstaten. NIS2 is van toepassing op essentiële organisaties, belangrijke organisaties, ketenpartners, uitgezonderde kleine bedrijven, en apart aangewezen organisaties, waaronder kleine bedrijven die een cruciale rol spelen in de internet-infrastructuur en overheidsinstanties.

De richtlijn vereist naleving van beveiligingsmaatregelen en melding van cyberincidenten. Controles op naleving zullen plaatsvinden, met proactieve controles voor essentiële organisaties en controles op aanleiding voor belangrijke organisaties. Niet-naleving kan leiden tot boetes, waarvan de hoogte afhankelijk is van de organisatiecategorie. Bestuurders zijn persoonlijk verantwoordelijk en hoofdelijk aansprakelijk voor NIS2-compliance.

NIS2 heeft twee hoofdpijlers: een zorgplicht, waarbij organisaties passende technische, operationele, en organisatorische maatregelen moeten nemen voor digitale veiligheid en continuïteit, en een meldplicht. Organisaties moeten incidenten binnen 24 uur (bij dienstverstoring) of binnen 72 uur (in andere gevallen) melden aan de betreffende autoriteit.

Voor NIS2-compliance kunnen bestaande raamwerken zoals CIS Controls en certificeringen zoals ISO 27001 of NEN 7510 waardevol zijn.

Slotwoord

Een solide beveiliging was al lang geen vrijblijvende aangelegenheid meer, maar NIS2 heeft elke mogelijke twijfel hierover weggenomen. Desondanks mag het vermijden van boetes nooit de voornaamste drijfveer zijn om de beveiliging op orde te hebben. Hoewel het overkoepelende doel van de EU 'hoog-over' is - het vergroten van de weerbaarheid van de lidstaten - is dit doel niet alleen van belang voor de EU als geheel, maar ook voor elke individuele organisatie.

Een ernstig cyberincident kan namelijk potentieel rampzalige gevolgen hebben. In de eerste plaats voor de organisatie zelf, zoals verstoord dienstverlening, diefstal van bedrijfsgeheimen, ontevreden klanten en (onherstelbare) imagoschade. Zulke gevolgen kunnen uiteindelijk een organisatie definitief ten gronde richten en veel meer schade aanrichten dan welke boete dan ook. Maar ook voor de samenleving als geheel, bijvoorbeeld bij grootschalige datalekken, economische nevenschade en uitval van cruciale voorzieningen.

Een robuuste beveiliging is dan ook niet slechts een kwestie van een 'vinkje' om boetes en juridische problemen te vermijden. Het is een ethische, morele en bedrijfseconomische missie. NIS2 is daarbij niet het einddoel, maar eerder een instrument. Bovendien verwachten we dat NIS2 en de daaruit voortvloeiende wetgeving niet het juridische eindstation zijn op het gebied van beveiliging. Het realiseren van een veerkrachtige organisatie is altijd waardevol, voor de organisatie zelf, de mens en de maatschappij, voor NIS2 en als een stevige basis voor toekomstige wetgeving op het gebied van beveiliging.

Meer informatie nodig? Heb je nog vragen over dit e-book of NIS2?
Wil je vrijblijvend overleggen met onze experts over de impact van NIS2 op jouw organisatie?

Neem dan contact op met BOSSIT via hello@bossit.be

Uw Cyber beveiliging op alles voorbereid

IT of Cyber security is cruciaal, want vroeg of laat krijgt u te maken met hackers of virussen. Het belangrijkste is dus om u daar zo goed mogelijk op voor te bereiden. Als security specialist maakt BOSSIT uw IT-omgeving geschikt om elke dreiging veerkrachtig op te vangen.

Mail naar **hello@bossit.be** of bel
Rob Gielen - Business Security Manager op **+32 484 111 022**
Glenn Bogaerts - Ethical Hacker / Pentester op **+32 474 701 606**

www.bossit.be

BOSSIT

BOSSIT
Meerstraat 2D - 2880 Bornem - België
T +32 474 701 606