Hoe bereid ik mij voor op NIS2?

Is NIS2 op jouw bedrijf van toepassing? En welke stappen moet je zetten om aan de richtlijn te voldoen?

In dit whitepaper lees je alles wat je moet weten over NIS2, de Europese security-richtlijn. Een helder stappenplan helpt je op weg om NIS2-proof te worden.

it local
Happy with it

Wat is NIS2?

NIS staat voor Network and Information Security (of in het Nederlands: 'NIB' voor Netwerk- en Informatie Beveiliging). Het is een set regels van de EU om de cyberbeveiliging in de EU te versterken en de regels op dat gebied op één lijn te brengen. NIS2 is de tweede versie van de Europese NIS-richtlijn.

In tegenstelling tot de AVG, die voor de hele EU geldt, werkt NIS2 via nationale regels. Dit betekent dat elke lidstaat zijn eigen wetten zal hebben die gebaseerd zijn op NIS2. Die wetgeving is in ons land nu in de maak. Dit betekent ook dat we nog niet helemaal zeker weten wat er precies van ons wordt verwacht. Maar we weten wel dat het verstandig is om je goed in te lezen en voor te bereiden. Daarom hebben we **alle belangrijke info voor je samengevat in dit whitepaper**. Zo weet jij wat je minimaal moet weten en heb je een basis in handen om nu alvast aan de slag te gaan.

Invoering: 1 juli 2026

De tekst van de NIS2-richtlijn is eind 2022 gepubliceerd door de EU. Het was de bedoeling om de richtlijn omgezet te hebben in Nederlandse wetgeving op 18 oktober 2024. Dat is niet gehaald. Maar de inwerkingtreding van de **Cyberbeveiligingswet** (Cbw), zoals de NIS2-implementatiewet gaat heten, lijkt nu snel te gaan gebeuren. De Tweede Kamer behandelt de stukken eind maart 2026 en stemt daarna erover. Naar verwachting geeft aansluitend de Eerste Kamer ook snel haar akkoord. Omdat de meeste wetten ingaan op 1 januari of 1 juli lijkt **1 juli 2026** de logische invoeringsdatum te worden.

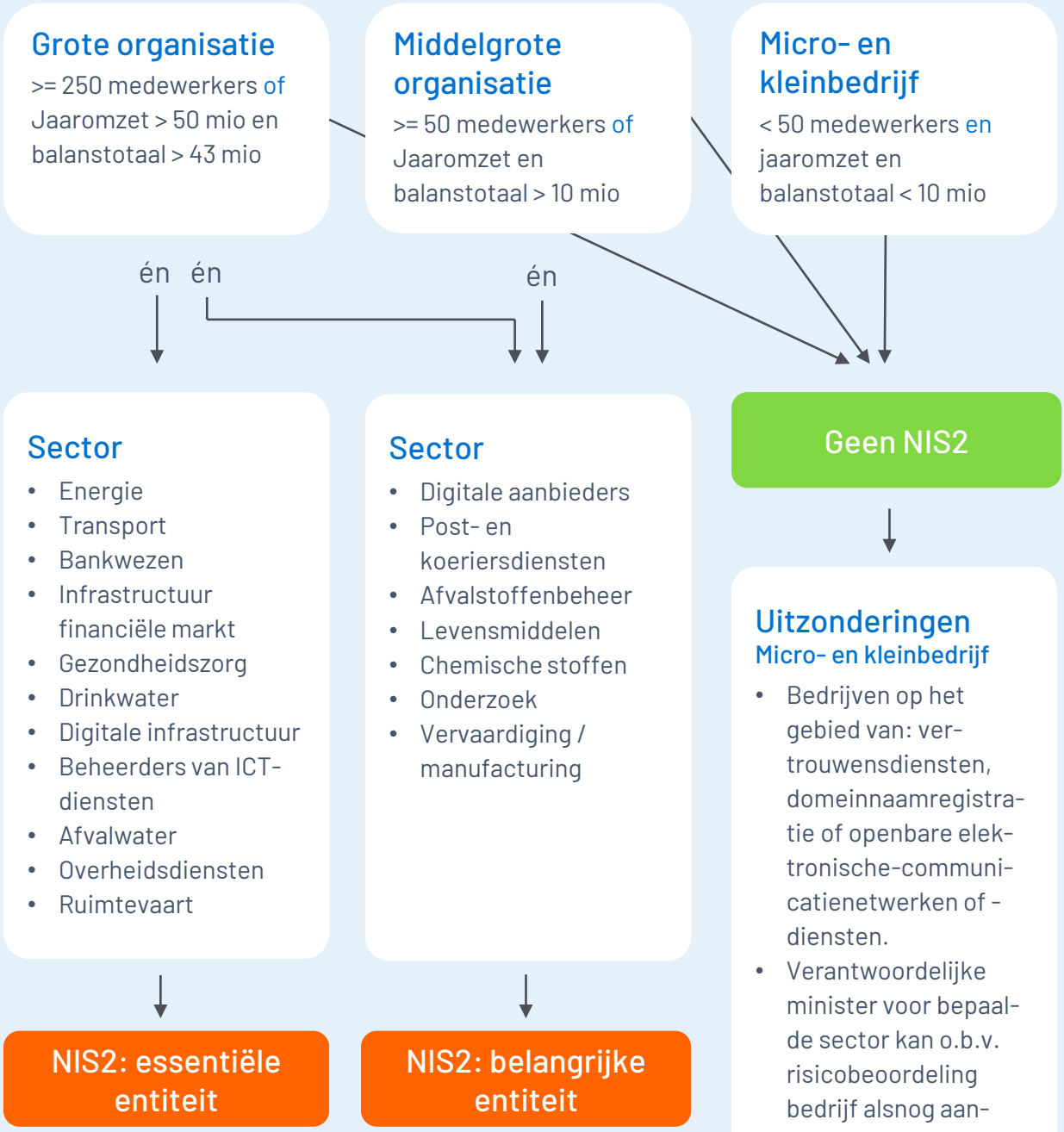
Val ik onder de NIS 2-richtlijn?

De NIS2-richtlijn is van toepassing op organisaties die behoren tot wat de richtlijn *essentiële* en *belangrijke* sectoren noemt. Waar een verstoring als gevolg van een cyberaanval problemen kan veroorzaken voor de samenleving. De organisaties die onder de richtlijn vallen worden aangeduid als *entiteiten*.

Het schema op de volgende pagina biedt je in een notendop helderheid en laat je zien of de richtlijn ook op jouw organisatie van toepassing is.

Is NIS2 van toepassing op mijn organisatie?

Doe de snelle check en weet of jouw organisatie een essentiële of belangrijke entiteit is. En daarmee onder de NIS2-richtlijn valt:



Wil je een gedetailleerde check doen of NIS2 van toepassing is op jouw organisatie? Doe dan de zelfevaluatie van de Rijksoverheid.

Essentieel of belangrijk... maakt dat nog verschil?
Essentiële en belangrijke entiteiten moeten aan dezelfde eisen voldoen. De EU beschouwt ze als onderdeel van de kritieke infrastructuur waarvan de werking van cruciaal belang is voor de samenleving. Doordat essentiële entiteiten de ruggengraat van onze samenleving vormen en belangrijke entiteiten wat meer ondersteunend zijn, zijn er wel verschillen in het niveau van toezicht. De *Rijksinspectie Digitale Infrastructuur (RDI)*, die in Nederland straks verantwoordelijk is voor het toezicht, controleert essentiële entiteiten proactief. Dat wil zeggen dat de RDI deze entiteiten regelmatig monitort om naleving van de richtlijn te waarborgen. Belangrijke entiteiten worden alleen gecontroleerd als er meldingen van niet-naleving zijn.

Niet essentieel of belangrijk, toch NIS2 van toepassing

Is jouw organisatie geen essentiële of belangrijke entiteit? Dan kan NIS2 toch (indirect) van toepassing zijn als je in de keten zit van een NIS2-plichtige organisatie.

Wat zijn de verplichtingen van NIS2?

Het doel van NIS2 is om de eisen voor cyberbeveiliging voor organisaties te versterken en te stroomlijnen. Als je onder de richtlijn valt **moet je daarom voldoen aan een set van minimale vereisten** op deze 10 gebieden:

1. Beleid met betrekking tot risicoanalyse en beveiliging van informatiesystemen.
2. Afhandeling van incidenten.
3. Bedrijfscontinuïteit, zoals het beheer van back-ups, rampenherstel en crisismanagement.
4. Beveiliging van de toeleveringsketen, inclusief beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar directe leveranciers of dienstverleners.
5. Beveiliging in verwerving, ontwikkeling en onderhoud van netwerk- en informatiesystemen, inclusief omgang met kwetsbaarheden en openbaarmaking.
6. Beleid en procedures om de effectiviteit van cybersecurity-risicobeheersings-maatregelen te beoordelen.

7. Basismaatregelen voor cybersecurity en cybersecurity-training. Dit betreft onder andere zero trust-beginselen, software-updates, configuratie van apparaten, netwerksegmentatie, identiteits- en toegangsbeheer, gebruikersbewustzijn en trainingen voor zowel personeel als management.
8. Beleid en procedures voor het gebruik van cryptografie en versleuteling.
9. Beveiliging van menselijke hulpbronnen, toegangsbeheerbeleid en activabeheer.
10. Het gebruik van multifactorauthenticatie of continue authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatie-systemen.

Melden van incidenten

NIS2 omvat ook een meerstappen-benadering voor het melden van *significante incidenten**, waarbij binnen de regeling een evenwicht wordt gezocht tussen snelle rapportage om de verspreiding van incidenten te voorkomen en grondige rapportage om waardevolle lessen te leren. Als organisatie heb je bij een significant incident 24 uur de tijd om een vroegtijdige waarschuwing in te dienen, 72 uur om een incidentmelding in te dienen en één maand om een definitief rapport in te dienen.

Significant incident

* Een *significant incident* is een serieuze operationele verstoring van de dienstverlening of financiële gevolgen voor de betrokken entiteit waardoor natuurlijke of rechtspersonen worden of kunnen worden geraakt door aanzienlijke materiële of immateriële schade.

Training voor leidinggevenden

Ten slotte moeten leidinggevenden training krijgen waarmee ze risico's kunnen beoordelen en verminderen en de verplichtingen van de organisatie kunnen begrijpen.

Niet alleen verplichtingen, ook hulp

NIS2 zadelt organisaties niet alleen op met eisen en verplichtingen. De richtlijn schrijft ook ondersteuning voor. Dat betekent onder meer dat straks één of meerdere *Computer Security Incident Response Teams* (CSIRT's) essentiële en belangrijke entiteiten tijdig informeren over dreigingen en bijstand verlenen. En komt er op Europees niveau een kwetsbaarheidsdatabase.

Voldoen aan NIS2: wat betekent dit concreet voor mij?

Om aan de NIS2-richtlijn te gaan voldoen moet je met jouw organisatie flink aan de bak. Dit zijn kort samengevat de concrete acties die je moet ondernemen, onderverdeeld in 6 categorieën:

1. Governance

- Voer een context- en gap-analyse uit om duidelijkheid te krijgen over de verplichtingen, waar jouw organisatie staat ten opzichte van de richtlijn en het ideale implementatieplan. Stel een jaarlijkse cyclus op, die je integreert met de jaarlijkse cyclus van de AVG (Algemene Verordening Gegevensbescherming) en de jaarlijkse cyclus voor IT-beveiliging.

2. Beleid en procedures

- Ontwikkel beleidsregels en procedures voor werkzaamheden met betrekking tot NIS2.
- Stel algemene IT-beveiligingsbeleidsregels op.
- Veranker de beleidsregels bij het management, in de jaarlijkse cyclus en in lopende taken.

3. Risicomanagement

- Breng je activa in kaart.
- Herken bedreigingen en kwetsbaarheden en voer hierop een risicobeoordeling uit.
- Verminder risico's door de juiste maatregelen te implementeren.

4. Leveranciers
- Identificeer je belangrijke leveranciers en leg overeenkomsten vast.
- Voer risicobeoordelingen uit en leg veiligheidsmaatregelen vast.
- Stel een audit en een plan op voor voortdurende beoordeling in jaarlijkse cycli.

5. Training
- Train jouw management over hun eigen NIS2-verplichtingen en de verplichtingen van je organisatie.
- Verzorg als organisatorische beveiligingsmaatregel bewustwordingstrainingen voor alle relevante medewerkers.

6. Incidentmanagement
- Stel een procedure en een methode op voor de juiste registratie en afhandeling van incidenten.

Wat gebeurt er als ik niet voldoe aan NIS2?

Val je als organisatie onder de NIS2-richtlijn, maar leef je de richtlijn niet goed na? Dan liggen sancties op de loer. En die kunnen serieuze vormen aannemen.

NIS2 kent een uitgebreid kader voor toezichts- en handhavingsactiviteiten in de lidstaten. Bevoegde autoriteiten (zoals onder meer de RDI in Nederland) zijn verantwoordelijk voor toezicht op de naleving van de richtlijn. Zij maken gebruik van toezichtsmaatregelen als audits, controles, verzoeken om informatie en toegang tot documenten.

De richtlijn bevat een consistente structuur van sancties, waaronder bindende instructies, implementatie van aanbevelingen voor beveiligingsaudits, afstemming met NIS-vereisten en administratieve boetes. De hoogte van deze administratieve boetes varieert. Ben je een essentiële entiteit, dan kun je een boete krijgen tot maximaal € 10.000.000,- of 2% van de jaaromzet. Als belangrijke entiteit bedraagt een boete maximaal € 7.000.000,- of 1,4% van de jaaromzet. De toezichthouder houdt rekening met de aard en ernst van de inbreuk en eventuele schade of verlies.

Let op: persoonlijke aansprakelijkheid

In tegenstelling tot de GDPR kunnen natuurlijke personen in het management binnen bedrijven ook persoonlijk (en potentieel zelfs strafrechtelijk) aansprakelijk worden gesteld.

Hoe kan IT Local mij ontzorgen?

Wij helpen je graag om je voor te bereiden op de NIS2-richtlijn. Dat doen we aan de hand van een stappenplan dat gebaseerd is op de eerder genoemde 6 categorieën met uit te voeren acties. Bij iedere stap geven we aan wat je moet doen en hoe wij je kunnen helpen.

STAP 1 Governance: voer een nulmeting uit

Als eerste stap breng je in kaart waar je op dit moment staat met jouw organisatie op het gebied van cybersecurity. Hoe staat je IT-omgeving ervoor? En hoe staat het met de securityprocessen en -procedures van jouw organisatie? Een **nulmeting via een assessment** kan dit inzicht geven. En is de basis voor de rest van het stappenplan. Door het assessment ieder jaar te **herhalen** heb je een periodieke check van waar je staat en wat je eventueel verder moet verbeteren. En maak je het zoals de richtlijn voorschrijft cyclisch.

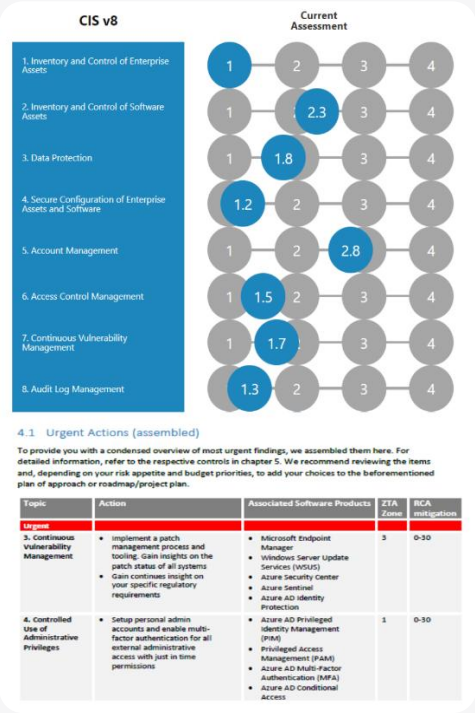
Hoe kunnen wij je hierbij helpen?

Uitvoeren van een CSAT-scan
Met een scan via onze Cyber Security Assessment Tool (CSAT) ontvang je een analyse van jouw volledige IT-infrastructuur. De tool verzamelt relevante beveiligings-gegevens via jouw Microsoft-omgeving. Via een aanvullende vragenlijst, onderdeel van de tool, polsen wij naar beleidsregels, controles en andere belangrijke indicatoren.

De tool is gebaseerd op het *CIS 18-framework*, een internationale standaard, en analyseert ook vanuit de uitgangspunten van NIS2.

De CSAT geeft na de scan in een helder **rapport** aan welke acties en verbetermaatregelen je zou moeten nemen om je beveiliging op orde te brengen. Deze verbetermaatregelen zijn verdeeld in acties die binnen 30 dagen zouden moeten worden uitgevoerd (de urgente acties), binnen 30 tot 90 dagen en na 90 dagen. Met de acties die uit de scan rollen, helpen we je als IT-partij met een uitgebreid palet aan security-oplossingen natuurlijk ook graag. We nemen de acties op in een IT-Roadmap en geven daarbij een indicatie van de bijbehorende planning en een investerings-indicatie.

Omdat je IT-omgeving altijd aan veranderingen onderhevig is en nieuwe cyberdreigingen aan de orde van de dag zijn herhalen wij de CSAT-scan jaarlijks.



STAP 2 Beleid en procedures

In deze stap ga je aan de slag met het opstellen van beveiligingsbeleid en een continuïteitsplan. NIS2 vereist dat je een gedocumenteerd beveiligingsbeleid opstelt en onderhoudt. Dit beleid bevat de beveiligingsmaatregelen en -procedures van jouw organisatie en communiceer je naar alle betrokken medewerkers. Daarnaast vereist NIS2 dat je een continuïteitsplan opstelt en onderhoudt. Dit heeft betrekking op back-upbeheer, plannen voor noodvoorzieningen en crisisbeheer.

Hoe kunnen wij je hierbij helpen?

Beleid en procedures opstellen is niet onze core business. Maar we kunnen je zeker op weg helpen. Zo kunnen onze security-specialisten je inzicht geven in hoe we dit voor onszelf hebben gedaan in het kader van onze ISO 27001- en NEN 7510-certificering. Want de ISO-/NEN-normen hebben veel raakvlakken met NIS2 en bieden een goede basis om een passend cybersecuritykader op te stellen. Wat ook kan is dat we je in contact brengen met een van onze partners uit ons netwerk.

Op het gebied van back-upbeheer ontzorgen we je graag via deze twee diensten:

Managed 365-back-up
Microsoft biedt met haar Microsoft 365-back-up een retentietijd van je data van 7 dagen. Met onze aanvullende dienst *Managed 365-back-up* kun je langer teruggaan in de tijd, tot wel 90 dagen. Jouw waardevolle data in Microsoft 365 zijn veilig opgeslagen in ons datacenter. En bij dataverlies kun je er snel weer over beschikken. We controleren en testen het back-up-proces doorlopend. Bij calamiteiten herstellen we de verloren data en zorgen we dat alles snel weer werkt.

Managed server back-up
Met *Managed server-back-up* ben je er altijd van verzekerd dat waardevolle serverdata veilig zijn opgeslagen: lokaal én in ons datacenter. We controleren en testen het back-up-proces doorlopend. Bij calamiteiten herstellen we de verloren data en zorgen we dat alles weer werkt.

STAP 3 Risicomanagement

Risicomanagement is een belangrijk onderdeel van de NIS2-richtlijn. Om aan deze eis te voldoen, moet je de volgende stappen doorlopen:

Inventariseren en vastleggen activa
Maak een overzicht van alle relevante netwerk- en informatiesystemen die je organisatie gebruikt of beheert. Inclusief de gegevens die daarop worden verwerkt, opgeslagen of uitgewisseld. Deze activa moet je classificeren naar belangrijkheid, kwetsbaarheid en afhankelijkheid van andere systemen.

Identificeren bedreigingen
Breng de mogelijke bronnen, methoden en doelen van cyberaanvallen op je netwerk- en informatiesystemen in kaart. Zowel de interne als de externe bedreigingen. Denk bij bedreigingen bijvoorbeeld aan hackers, malware, natuurrampen, menselijke fouten of sabotage.

Risicobeoordeling bedreigingen
Analyseer en prioriteer de kans en de impact van elke geïdentificeerde bedreiging. Dit houdt in dat je rekening houdt met de waarschijnlijkheid dat een bedreiging zich voordoet, de ernst van de schade die kan worden veroorzaakt en de mogelijke gevolgen voor de continuïteit, vertrouwelijkheid, integriteit en beschikbaarheid van je netwerk- en informatiesystemen.

Risicobeperkende maatregelen
Neem passende technische en organisatorische maatregelen om de risico's die je hebt vastgesteld te verminderen of te elimineren. Deze maatregelen kunnen bestaan uit preventie, detectie, reactie en herstel. Je moet hierbij ook rekening houden met de kosten-batenverhouding, de proportionaliteit en de doeltreffendheid van de maatregelen.

Meten van het effect van de maatregelen
Evalueer en controleer regelmatig de doeltreffendheid van je risicobeperkende maatregelen. Dit omvat het testen, monitoren, auditen en rapporteren van je netwerk- en informatiesystemen. Meld eventuele incidenten of inbreuken aan de bevoegde autoriteiten en belanghebbenden en leer van hun ervaringen om jouw risicomanagement te verbeteren.

Hoe kunnen wij je hierbij helpen?

Door jouw organisatie op het juiste securityniveau te brengen (via een afgewogen pakket aan securitydiensten) kunnen we risico's fors verminderen. Daarnaast hebben we in het kader van onze certificeringen een flink aantal risicobeperkende maatregelen voor onszelf in de praktijk gebracht. Zoals screening van medewerkers, een zone-indeling op kantoor met no-go-areas voor bezoekers en schermvergrendeling bij het verlaten van de werkplek. Ook jouw organisatie kunnen we hiermee helpen.

Lock Computer (WIN-L)

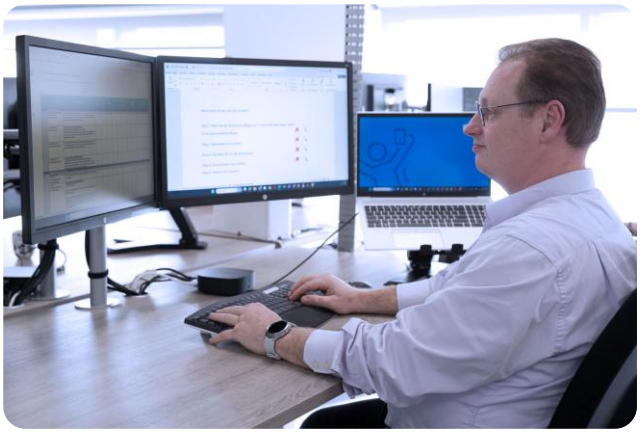
Drie concrete diensten lichten we er graag even uit:

XDR
Met onze XDR-dienst (eXtended Detection and Response) verzeker je je van 24/7-monitoring, meer inzicht, snellere detectie van dreigingen en het automatisch stoppen van aanvallen. Het kijkt over alle lagen heen om verbanden te leggen die je anders zou missen. Voor deze dienst werken we samen met onze gerenommeerde securitypartner *Masero*.

Wachtwoordbeheer via Keeper

Een laagdrempelige en veilige wachtwoordtool die we zelf gebruiken en ook voor jouw organisatie kunnen instellen is Keeper. *Keeper Security* biedt een robuust platform voor wachtwoord- en geheimenbeheer, zowel voor bedrijven als voor persoonlijk gebruik. Met Keeper:

- Bescherm, beheer en deel je wachtwoorden, aanmeldingsgegevens, metadata en bestanden veilig binnen jouw organisatie.
- Maak je gedeelde teammappen en beheer je gebruikersrechten voor het toevoegen, verwijderen, aanpassen en delen van deze records.
- Gebruik je de op rollen gebaseerde toegangscontrole (RBAC) om gemakkelijke toegang te ondersteunen.
- Volg je alle gebruikersactiviteiten op elke locatie en elk apparaat.



Asset management-app

Met de door onszelf ontwikkelde Asset management-app hebben onze klanten altijd een volledig overzicht van alle bedrijfsmiddelen van hun medewerkers en kunnen ze deze gemakkelijk en veilig beheren. De app:

- Managet het proces van aanvragen, uitgifte en inname van bedrijfsmiddelen (denk aan laptops, telefoons, toegangspassen en auto's).
- Faciliteert het samenvoegen, tekenen en opslaan van bruikleenovereenkomsten per bedrijfsmiddel (direct vanuit de app).
- Is geïntegreerd met Microsoft Active Directory en Intune (MDM) voor de rolgebaseerde inrichting en het beheer van alle devices.
- Biedt je dashboards voor inzicht in afschrijvings- en investeringsmomenten.

Wij verzorgen aanvullend het innemen, wipen, rolgebaseerd inrichten en het uitgeven van de devices.

STAP 4 Leveranciers

Een ander belangrijk aspect van NIS2 is het beheren van de relaties met jouw leveranciers die essentiële diensten of functies leveren. Stel een proces op waarin je deze leveranciers in kaart brengt en leg de overeenkomsten die je met hen hebt vast. Inclusief jullie verwachtingen, verantwoordelijkheden en aansprakelijkheden op het gebied van cyberbeveiliging. Voer regelmatig risicobeoordelingen uit om de potentiële impact van een cyberincident op je leveranciers en jezelf te bepalen. Op basis van deze beoordelingen moet je passende veiligheidsmaatregelen invoeren en vastleggen om de risico's te verminderen of te beheersen. Dit kunnen technische, organisatorische of contractuele middelen zijn.

Ten slotte moet je een audit- en beoordelingsplan opstellen waarmee je de naleving en prestaties van je leveranciers op het gebied van cyberbeveiliging controleert. In dit plan neem je jaarlijkse cycli van audits, rapportages en verbeteracties op. Zo kun je de kwaliteit en veiligheid van je leveranciersrelaties waarborgen en verbeteren.

Hoe kunnen wij je hierbij helpen?

Ook in het beheren van relaties met jouw leveranciers kunnen we je hulp bieden. Zo kunnen we je inzicht geven in hoe we dit voor onszelf hebben gedaan in het kader van onze certificeringen. Of we brengen je in contact met een van onze partners uit ons netwerk.

STAP 5 Training

Het vergroten van de cyberweerbaarheid van je organisatie is ook een NIS2-eis. Om dit te bereiken train je jouw medewerkers en het management op het gebied van cybersecurity.

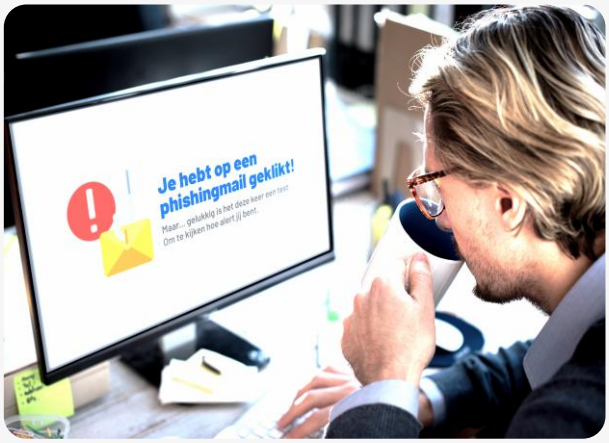
Dit houdt het volgende in:

- Maak je organisatie bewust van de risico's, bedreigingen en maatregelen die samenhangen met NIS2 en de rol die elke medewerker daarin speelt.
- Train jouw management op het gebied van strategisch leiderschap, governance, risicomanagement en incidentrespons in relatie tot NIS2.
- Verzorg periodieke awareness-trainingen voor al je medewerkers om hun kennis en vaardigheden op peil te houden en te toetsen. Hoe gaan ze bijvoorbeeld om met verdachte mail? Weten ze hoe ze een bestand veilig kunnen delen? En weten ze hoe ze zonder risico kunnen inloggen op een externe locatie?

Hoe kunnen wij je hierbij helpen?

Wij trainen via ons security awareness-programma het veiligheidsbewustzijn van je medewerkers. Dat doen we door ze onaangekondigd en op regelmatige basis ‘phishingmail’ te sturen. Na openen van of klikken op zo’n mail geven we de medewerkers direct feedback. We monitoren voortdurend wat er gebeurt en aan de hand van heldere overzichten rapporteren we jullie managers hoe het ervoor staat met de alertheid van jouw organisatie.

Voor medewerkers die dit onderwerp lastig vinden verzorgen wij automatisch meerdere trainingsmomenten, zodat zij deze belangrijke materie gaan beheersen en bedreigingen herkennen.



Is er nog geen *security-beleid*? Dan helpen we je graag met het opzetten hiervan. We nemen jullie medewerkers mee in de uitgangspunten van het beleid en zorgen ervoor dat ze de spelregels kennen.

Voor het *trainen van jouw management* helpen we je graag bij het selecteren van een geschikte partner die dit voor je kan verzorgen.

STAP 6 Incidentmanagement

Twee dingen die je in relatie tot NIS2 moet doen op het gebied van incident-management:

Stel een incidentenprocedure op
Stel een duidelijke en effectieve procedure op voor het melden, analyseren, beoordelen en afhandelen van incidenten die een aanzienlijke impact kunnen hebben op de continuïteit van je dienstverlening of op de openbare veiligheid. Deze procedure moet ook voorzien in de communicatie met relevante belanghebbenden, zoals toezicht-houders, klanten, en leveranciers.

Doorlopend incidentmanagement
Zorg ervoor dat je niet alleen reageert op incidenten, maar ook proactief maatregelen neemt om incidenten te voorkomen, te detecteren en te beperken. Dit omvat het regelmatig testen en evalueren van je netwerk- en informatiesystemen, het bijhouden van een incidentenregister, het uitvoeren van risicoanalyses en het implementeren van verbeteracties op basis van lessen die je hebt geleerd.

Hoe kunnen wij je hierbij helpen?

We kunnen je inzicht geven in hoe we dit voor onze eigen organisatie hebben opgepakt. En je daarbij ook inzicht geven in onze incidentenprocedure. Of we brengen je in contact met een van onze partners uit ons netwerk.

EN TOT SLOT Maak het officieel!

Heb je alle 6 stappen doorlopen en denk je dat je de zaken op orde hebt? Dan wil je natuurlijk nog het stempel 'NIS-proof'. Zodat je het ook officieel kunt aantonen en juridisch geborgd hebt. Daarvoor moet je een aanvullende audit door een accountant of certificeringsbedrijf laten uitvoeren.

Hoe kunnen wij je hierbij helpen

We brengen je voor de aanvullende audit graag in contact met een van onze partners uit ons netwerk.

Aan de slag met NIS2? Wij helpen je graag!

We hopen dat dit whitepaper je duidelijk heeft gemaakt of NIS2 op jouw organisatie van toepassing is, wat de regeling inhoudt en wat je als essentiële of belangrijke entiteit moet doen om NIS2-proof te worden.

We helpen je graag bij de verschillende stappen als je aan de slag gaat. Interesse? Meld je dan aan voor een gratis en vrijblijvend adviesgesprek waarin we in een half uur jouw NIS2-uitdaging onder de loep nemen, je wat meer vertellen over ons stappenplan en jouw vragen beantwoorden.

We helpen je natuurlijk ook graag als je niet onder de richtlijn valt, maar jouw security wel wilt verbeteren. Sowieso een goed idee, want je moet de digitale veiligheid van jouw organisatie niet laten afhangen van de invoering van NIS2. Dat doen hackers ook niet 😉

Goed om over ons te weten als securitypartner: we bieden met onze security journey een aanpak in 3 stappen om digitaal veilig te worden en te blijven en we zijn ISO 27001- en NEN 7510-gecertificeerd.

it local
Happy with it

itlocal.nl | info@itlocal.nl | (088) 40 43 400 | Westervoortsedijk 73-LB, 6827 AV Arnhem