

NIS2-wetgeving en security voor een MKB-bedrijf

*Zo blijft jouw organisatie veilig,
compliant en bereikbaar*



Inhoud

1.	Waarom NIS2 en cybersecurity nú topprioriteit zijn	2
1.1	De vijf bouwstenen voor een veilige organisatie	2
2.	Wat is NIS2? De wetgeving in begrijpelijke taal	3
3.	Digitale weerbaarheid: De vijf basisprincipes voor MKB	3
4.	Wat betekent NIS2 concreet voor jouw organisatie?	4
5.	De werkplek als aanvalssector	5
5.1	De Moderne Werkplek zegt veiligheid op 1	5
6.	XDR: Van losse beveiliging naar één slimme verdedigingslinie	6
6.1	XDR tegenover traditionele beveiliging	7
6.2	XDR als onderdeel van een complete securitystrategie	7
7.	Bereikbaarheid& continuïteit als onderdeel van security	7
8.	De mens als cruciale schakel	8
8.1	Security Awareness Training: Versterk je menselijke firewall	8
8.2	Inzicht en aantoonbaarheid	9
9.	Veilig werken in de cloud: Kansen en verantwoordelijkheden	9
9.1	De bouwstenen voor een veilige cloudomgeving	10
10.	Van losse maatregelen naar een samenhangende securitystrategie	11
11.	NIS2 als kans om je organisatie structureel te versterken	12

1. Waarom NIS2 en cybersecurity nú topprioriteit zijn

Cyberdreigingen nemen toe en raken elk bedrijf, groot of klein. Van ransomware en phishing tot ketenrisico's: één fout kan leiden tot flinke schade of zelfs stilstand van je organisatie. De NIS2-wetgeving verandert de spelregels rondom security en raakt hierbij ook het MKB. De wet legt verantwoordelijkheid bij bestuur en directie en stelt eisen aan beveiliging, incidentmelding en continuïteit. Security is geen IT-feestje meer, maar een directieverantwoordelijkheid.

Bij Company Connect helpen we bedrijven deze uitdagingen concreet aan te pakken. Niet als abstracte adviseur of leverancier van losse tools, maar als strategische partner die samen met jou kijkt naar praktische oplossingen die jouw organisatie veilig, compliant en toekomstbestendig maken. In deze whitepaper nemen we je stap voor stap mee: van risico's en wettelijke verplichtingen tot concrete maatregelen die je direct kunt implementeren.

1.1 De vijf bouwstenen voor een veilige organisatie

Om NIS2-compliance te bereiken en je organisatie écht te beveiligen, is het belangrijk te kijken naar alle lagen van de beveiliging. In deze whitepaper gebruiken we daarom een overzichtelijke cirkel van vijf bouwstenen, die samen de basis vormen van een veilige organisatie:

- 1. Menselijke firewall** – medewerkers als eerste verdedigingslinie, bewust en getraind via Security Awareness Training.
- 2. Veilige (moderne) werkplek** – veilige toegang tot systemen, 2FA en moderne werkplekoplossingen.
- 3. Cloud- en databeveiliging** – veilig opslaan en delen van data, zowel lokaal als in de cloud.
- 4. XDR en monitoring** – geavanceerde detectie en respons op dreigingen, zodat incidenten snel worden opgevangen.
- 5. Continuïteit en bereikbaarheid** – operationeel blijven, ook bij storingen of aanvallen, met oplossingen zoals 4G-backup, EVM/EVI en veilige wachtwoordbeheer-tools.



Elke laag versterkt de andere, zodat je organisatie niet alleen compliant is, maar ook daadwerkelijk weerbaar, wendbaar en toekomstbestendig. In de whitepaper leggen we per laag uit wat dit concreet betekent voor jouw bedrijf, waar de grootste risico's liggen en welke praktische stappen je kunt zetten om ze te beperken.

Benieuwd hoe jouw organisatie zich kan voorbereiden op NIS2? Wil je weten waar je grootste risico's zitten en hoe je die direct kunt aanpakken? In deze whitepaper laten we je zien hoe je van losse maatregelen naar een samenhangende securitystrategie komt, met duidelijke voorbeelden en oplossingen die direct toepasbaar zijn in het MKB.

2. Wat is NIS2? De wetgeving in begrijpelijke taal

De NIS2-wetgeving is niet langer een concept voor de toekomst, maar wordt binnenkort werkelijkheid. Deze wetgeving legt strengere regels op voor cybersecurity binnen de EU. Het doel van deze wet is duidelijk: organisaties beschermen tegen digitale dreigingen en de continuïteit van kritieke diensten waarborgen. NIS2 is breder en strenger dan zijn voorganger en richt zich niet alleen op grote bedrijven of IT-dienstverleners, maar raakt ook het MKB — direct of via ketenverantwoordelijkheid.

Onder NIS2 moeten organisaties onder andere voldoen aan:

- Meldplicht incidenten: iedere ernstige cyberincident moet snel worden gemeld bij de bevoegde autoriteit.
- Zorgplicht beveiliging: organisaties moeten passende technische en organisatorische maatregelen nemen om risico's te beperken.
- Aansprakelijkheid van bestuur/directie: bestuurders kunnen verantwoordelijk worden gehouden bij onvoldoende naleving, inclusief boetes of andere sancties.

Bij Company Connect helpen we organisaties om deze wetgeving praktisch toepasbaar te maken. We vertalen de regels naar concrete maatregelen die passen bij jouw bedrijfsvoering en MKB-omgeving, zoals veilige moderne werkplekken, cloudbeveiliging, XDR-oplossingen en awareness-trainingen. Zo wordt compliance niet een theoretische checklist, maar een integraal onderdeel van jouw dagelijkse bedrijfsvoering.

3. Digitale weerbaarheid: De vijf basisprincipes voor MKB

De wetgeving klinkt misschien abstract, maar er zijn concrete handvatten waarmee je jouw organisatie weerbaar kunt maken. Digitale weerbaarheid betekent dat systemen, processen én medewerkers zó zijn ingericht dat risico's worden voorkomen, incidenten snel worden gedetecteerd, schade wordt beperkt en je organisatie snel herstelt. Voor het MKB vormt dit een praktisch kader om te voldoen aan NIS2 en de juiste beveiligingsmaatregelen te nemen.

De vijf basisprincipes van digitale weerbaarheid vormen een soort stappenplan om jou een handje te helpen:

1. Breng je risico's in kaart
2. Bevorder veilig gedrag
3. Bescherm systemen, applicaties en apparaten
4. Beheer toegang tot data en diensten
5. Bereid je voor op incidenten

Digitale weerbaarheid wordt zo weer tastbaar: elke bouwsteen draagt bij aan één of meerdere principes.

Awareness-training versterkt bijvoorbeeld het in kaart brengen van risico's en het bevorderen van veilig gedrag, terwijl XDR helpt bij het voorbereiden op incidenten en het beschermen van systemen, applicaties en apparaten. Nu we weten hoe je de basisprincipes van digitale weerbaarheid toepast, is het tijd om te bekijken wat NIS2 concreet van jouw organisatie vraagt.



4. Wat betekent NIS2 concreet voor jouw organisatie?

De gevolgen van NIS2 voor je dagelijkse bedrijfsvoering zijn heel concreet. NIS2 legt duidelijke verplichtingen op voor organisaties, ongeacht hun grootte en geeft bestuurders en directie een directe verantwoordelijkheid. Niets doen is geen optie: falen kan leiden tot boetes, reputatieschade en operationele verstoringen.

De belangrijkste verplichtingen zijn:

- **Risicoanalyse:** inzicht in je kritieke systemen, processen en data om prioriteiten te stellen.
- **Technische en organisatorische maatregelen:** van veilige werkplekken en toegangsbeheer tot monitoring en XDR-oplossingen.
- **Training van medewerkers:** je menselijke firewall is cruciaal; bewustzijn en security-awareness-training zijn verplicht onderdeel van de zorgplicht.

Echter, veel organisaties lopen tegen dezelfde uitdagingen aan: onvolledige inventarisaties, losse oplossingen zonder overzicht, of onvoldoende aandacht voor medewerkers. Bij Company Connect ondersteunen we MKB-bedrijven van analyse tot implementatie. Eén aanspreekpunt voor security, netwerk, werkplek en awareness zorgt dat compliance praktisch en overzichtelijk wordt.

5. De werkplek als aanvalssector



Veel van de risico's die NIS2 adresseert, ontstaan juist op de werkplek. Bewust werken op de werkplek vormt de eerste laag van bescherming, waarbij je medewerkers de menselijke firewall vormen. Maar ook de technologie waarmee ze werken, speelt een cruciale rol. De moderne werkplek — inclusief laptops, mobiele apparaten, hybride werken en cloudomgevingen — is een populair doelwit voor cyberaanvallen. Onvoldoende beveiligde werkplekken vergroten de kans op datalekken, ransomware en andere incidenten die onder NIS2 gemeld moeten worden.

De Moderne Werkplek is de digitale werkomgeving van jouw bedrijf waarin jij samenwerkt en communiceert met jouw collega's en klanten, via Microsoft 365. De bereikbaarheid en veiligheid van de Moderne Werkplek zijn enorm van belang. Daarom bieden wij oplossingen aangepast op het individu waarin jij je bereikbaarheid kunt afstellen naar jouw gewenste momenten. Daarnaast zorgen wij ervoor dat je bereikbaar bent waar en wanneer jij wil, altijd veilig.

5.1 De Moderne Werkplek zegt veiligheid op 1

Doordat de digitale handelingen plaatsvinden in de online werkomgeving, kunnen wij jou ondersteunen in het optimaliseren van de veiligheid van jouw gegevens. Binnen de Moderne Werkplek kan alles uitgevoerd worden, van mailen tot het openen van een PowerPoint-presentatie. Je bevindt je in een veilige omgeving, waar informatie automatisch wordt opgeslagen in een back-up. Wanneer gegevens verloren zijn, zijn deze terug te vinden, terwijl het de hackers nog moeilijker gemaakt wordt om data te verkrijgen. Maar wat zijn nou concreet de redenen om gebruik te maken van de Moderne Werkplek? Dat is simpel, zet met deze stap de veiligheid op 1:

- **Veiliger te werk gaan.** Doordat de data binnen de online werkplek blijft, kun je veiliger omgaan met de informatie van jouw bedrijf en jouw klanten.
- **Two-factor authentication.** Bij de Moderne Werkplek werk je via een veiligere verbinding, doordat er een dubbele verificatie moet plaatsvinden voordat jij bij de bestanden kunt. Via een app kun je een melding op jouw telefoon ontvangen, waar je toestemming kunt geven om de online omgeving te openen.
- **Maak gebruik van cloudopslag.** Doordat je gebruikmaakt van een cloudopslag, staat de data online. Je kunt verder werken vanaf een ander apparaat wanneer jij verbonden bent met het internet. Het wordt niet allemaal los op jouw apparaat gezet, waardoor er geen problemen ontstaan als iemand anders jouw laptop of mobiel in handen krijgt.

- **Gemakkelijk communiceren en delen.** De communicatie wordt geoptimaliseerd, terwijl het gemak behouden wordt. Door de centrale portal van je Moderne Werkplek, kunnen documenten snel gedeeld worden via bijvoorbeeld SharePoint, terwijl het communiceren kan plaatsvinden met behulp van functionaliteiten zoals Microsoft Teams of Outlook.
- **Afgestemd op het individu.** Doordat de moderne werkplek is afgestemd op de werkzaamheden van de individuele werknemer, kan ieder te werk gaan zoals zij dit zelf willen. Dit zorgt voor optimale prestaties.
- **Tijd en geld besparen.** Jullie kunnen diverse taken uit handen geven, om tijd en geld te besparen. Er is veel expertise nodig voor het migreren, implementeren en beheren van werkplekken. Je krijgt van ons een Microsoft 365 Business gebaseerde werkplek die door ons beheerd wordt. Dit zorgt voor een mindering in tijdrovende taken.

Voor MKB-organisaties betekent dit dat het beschermen van de werkplek direct bijdraagt aan continuïteit en dataveiligheid. Tevens is het een belangrijke stap in richting volledige NIS2-compliance. Bij Company Connect combineren we onze expertise in een omgeving waarin medewerkers veilig kunnen werken.

Medewerkers zijn cruciaal, maar ook technologie moet meewerken. Hier komt XDR om de hoek kijken, dat signalen vroegtijdig opvangt en incidenten detecteert voordat ze schade veroorzaken. Binnen de Moderne Werkplek wordt XDR ingezet als centrale beveiligingslaag die continu meedraait op de achtergrond. Dit betekent dat beveiliging niet langer gefragmenteerd is, maar integraal onderdeel vormt van de werkplek zelf.

6. XDR: Van losse beveiliging naar één slimme verdedigingslinie

XDR (*Extended Detection & Response*) brengt *endpoint*, mail, identiteit en netwerk samen in één platform. Traditionele antivirus is tegenwoordig niet meer voldoende: dreigingen worden complexer en infiltreren vaak via meerdere kanalen. XDR zorgt voor continue beveiliging en detectie, zonder dat je zelf handmatig hoeft in te grijpen. De XDR-toevoeging bij je Moderne Werkplek geeft je snellere detectie, beter overzicht en minder schade, waardoor je risico's effectief beperkt blijven:

Een medewerker ontvangt een phishing-mail → XDR detecteert verdachte activiteit op het endpoint en in de mailserver → het systeem blokkeert automatisch de link en genereert een waarschuwing voor de IT-beheerder.



6.1 XDR tegenover traditionele beveiliging

XDR is te onderscheiden van traditionele beveiliging, doordat de focus op response ligt. Detectie alleen is niet genoeg, dus maakt XDR het mogelijk om direct in te grijpen. Dit laat zien hoe XDR technologie ondersteunt: dreigingen worden automatisch op meerdere lagen gedetecteerd en gestopt. Dit gebeurt bijvoorbeeld door een apparaat te isoleren, een account tijdelijk te blokkeren, verdachte processen te stoppen, of herstelmaatregelen te starten. Hierdoor wordt schade beperkt en continuïteit gewaarborgd.

Voor NIS2 is dit cruciaal. XDR helpt bij:

- Snellere incidentdetectie en -respons, zodat dreigingen vroeg worden opgevangen.
- Aantoonbare beveiligingsmaatregelen, waarmee je kunt laten zien dat je voldoet aan zorgplicht en compliance.

6.2 XDR als onderdeel van een complete securitystrategie

Bij Company Connect zorgen we ervoor dat XDR niet alleen een tool is, maar onderdeel van een complete securitystrategie. Wij helpen MKB-bedrijven niet alleen bij de technische implementatie, maar ook met begeleiding en advies. Zo ontstaat een geïntegreerde verdedigingslinie die werkt vóórdat schade optreedt.

De Moderne Werkplek vraagt om moderne beveiliging. XDR biedt het inzicht en de slagkracht die nodig zijn om cyberdreigingen effectief het hoofd te bieden. Door XDR te integreren binnen de Moderne Werkplek ontstaat een veilige, toekomstbestendige werkomgeving waarin medewerkers onbezorgd kunnen werken en organisaties grip houden op hun security. Zelfs met XDR en training is continuïteit essentieel: een aanval mag je bedrijf niet platleggen. In het volgende hoofdstuk laten we zien hoe bereikbaarheid en continuïteit hand in hand gaan met security.

7. Bereikbaarheid & continuïteit als onderdeel van security



Wat gebeurt er met jouw bedrijf als de verbinding wegvalt?

Security gaat niet alleen over het beschermen van data. Voor een organisatie is het minstens zo belangrijk om bereikbaar en operationeel te blijven, zelfs wanneer er iets misgaat. Eerder hebben wij je een stappenplan gegeven aan de hand van de vijf basisprincipes van digitale weerbaarheid. De vijfde stap is “bereid je voor op incidenten”, maar hoe doe je dat?

Een storing in internet, netwerk of telefonie kan directe impact hebben: medewerkers kunnen niet werken, klanten raken ontevreden en bedrijfsprocessen lopen vertraging op. Daarom maakt bereikbaarheid en continuïteit deel uit van een robuuste securitystrategie. Met oplossingen zoals:

- **EVM (Extra Veilig Mobiel).** Zorgt dat jouw mobiele verkeer wordt afgeschermd van kwaadwillende aanvallen, zodat je zorgeloos kunt werken.
- **EVI (Extra Veilig Internet).** Bescherm je internetverbinding door schadelijke websites te blokkeren, malware en ransomware tegen te houden en privacygevoelige gegevens te beveiligen.
- **4G-backup.** Schakelt automatisch over op het mobiele KPN 4G-LTE netwerk bij uitval, zodat kritische bedrijfsprocessen doorgaan en omzetverlies, gemiste deadlines of boetes voorkomen worden.

Bij Company Connect maken we het je makkelijk: wij regelen EVI en 4G back-up kant-en-klaar, met snelle service en één vast aanspreekpunt als KPN Excellence Business Partner. Zo kunnen bedrijven veilig en zonder zorgen online blijven, 24/7.

8. De mens als cruciale schakel

Technologie ontwikkelt zich razendsnel, maar medewerkers blijven de belangrijkste schakel. Door bewustzijn, training en slimme detecties te combineren, ontstaat een robuuste verdedigingslinie waarin mens en systeem elkaar versterken.

In de praktijk begint 80 tot 90% van de cyberincidenten bij menselijk handelen. Een phishing-mail die wordt geopend, een zwak wachtwoord of het onbewust delen van gegevens is vaak het startpunt van een aanval. Juist daarom vraagt NIS2 niet alleen om technische maatregelen, maar ook om aantoonbare training en bewustwording van medewerkers als onderdeel van de zorgplicht.



8.1 Security Awareness Training: Versterk je menselijke firewall

Met Security Awareness Training (SAT) versterken organisaties hun menselijke firewall op een structurele manier. Geen eenmalige sessie, maar een geautomatiseerd, meertalig en doorlopend trainingsprogramma dat medewerkers actief betreft bij cybersecurity. Maak security begrijpelijk voor je medewerkers – zonder IT-jargon.

De training bestaat uit realistische phishing-simulaties en gerichte online modules, die automatisch op het juiste moment bij de juiste medewerker terechtkomen. Zo leren medewerkers risico's herkennen in hun dagelijkse werk, terwijl de organisatie inzicht krijgt in waar de grootste kwetsbaarheden zitten. De training bevat 3 fases:

1. Testperiode met realistische phishing simulaties. Dit laat zien waar extra aandacht nodig is. (± 2 maanden)
2. Online training & bewustwording. Hierdoor nemen ze betere beslissingen voor ze op links klikken of gegevens delen. (± 5 weken)
3. Tweede testperiode. Pas de geleerde kennis toe en krijg inzicht in een sterkere menselijke firewall. (± 1 maand)



8.2 Inzicht en aantoonbaarheid

Via duidelijke rapportages en dashboards krijgt de organisatie inzicht in zowel risicoscores (per afdeling of individu), betrokkenheid per trainingstype en meetbare verbetering over tijd. Deze rapportages maken securitybewustzijn niet alleen zichtbaar, maar ook aantoonbaar. Dit zorgt voor een verdere ondersteuning binnen NIS2-compliance.

Veiligheid stopt bovendien niet bij bewustwording alleen. Medewerkers werken steeds vaker hybride en in de cloud. Daarom is Security Awareness Training het meest effectief in combinatie met een veilige Moderne Werkplek, XDR-detectie en cloudbeveiliging. In het volgende hoofdstuk laten we zien hoe deze lagen samen zorgen voor bescherming: waar en hoe jouw medewerkers ook werken.

9. Veilig werken in de cloud: Kansen en verantwoordelijkheden

De cloud is niet meer weg te denken uit het dagelijkse werk. Bestanden delen, samenwerken en applicaties gebruiken gebeurt steeds vaker volledig online. Toch bestaan er nog veel misverstanden over cloud security. Een veelgehoorde aanname is dat de cloud “automatisch veilig” is. In werkelijkheid geldt: de cloud is veilig, mits deze goed is ingericht en beheerd.

9.1 De bouwstenen voor een veilige cloudomgeving

Binnen NIS2 ligt de verantwoordelijkheid voor beveiliging nadrukkelijk bij de organisatie zelf. Cloudleveranciers zorgen voor de infrastructuur, maar toegang, identiteit, rechten en gebruik vallen onder jouw eigen verantwoordelijkheid. Juist daar ontstaan risico's wanneer cloudomgevingen niet correct zijn ingericht. Een veilige cloudomgeving rust op een aantal onmisbare bouwstenen:



- **Identity management en 2FA (*Two-Factor Authentication*)**
 - Gebruikers krijgen alleen toegang tot wat zij nodig hebben en altijd met een extra verificatiestap. Zelfs als inloggegevens worden onderschept, voorkomt 2FA ongeautoriseerde toegang.
- **Sterk wachtwoordbeheer met *KPN ÉÉN Password Manager***
 - Unieke, sterke wachtwoorden per applicatie zijn essentieel, maar in de praktijk lastig te beheren. Met een centrale password manager worden wachtwoorden veilig opgeslagen en gedeeld, zonder dat medewerkers ze hoeven te onthouden of hergebruiken. Verder wordt er automatisch gescand of jouw gegevens in een datalek zitten.
- **Duidelijke rechtenstructuur**
 - Medewerkers beschikken over minimale rechten, passend bij hun rol. Zo wordt de impact van een eventueel incident beperkt.
- **Monitoring en logging**
 - Afwijkend gedrag in cloud- en accountgebruik wordt zichtbaar en kan vroegtijdig worden opgepakt, bijvoorbeeld via XDR.

Zonder deze basis kan één gecompromitteerd account voldoende zijn om toegang te krijgen tot gevoelige data, met mogelijke meldplicht, operationele verstoring en reputatieschade als gevolg. Company Connect helpt organisaties bij secure cloud-implementaties die aansluiten op het MKB en voldoen aan wetgeving zoals NIS2. Door cloudomgevingen in te richten (inclusief *identity management*, 2FA en veilig wachtwoordbeheer) maken we veilig werken mogelijk zonder dat dit ten koste gaat van gebruiksgemak.

Al deze onderdelen zijn afzonderlijk waardevol, maar pas in samenhang ontstaat echte digitale weerbaarheid. NIS2 geeft de kaders, de werkplek en cloud vormen de dagelijkse werkomgeving, XDR zorgt voor detectie en respons, awareness versterkt de menselijke firewall en bereikbaarheid borgt continuïteit. Samen zorgen mens, proces en technologie voor een veilige en toekomstbestendige organisatie.

10. Van losse maatregelen naar een samenhangende securitystrategie

Veel organisaties nemen beveiligingsmaatregelen stap voor stap. Een antivirus hier, een training daar, een cloudoplossing of back-up als het nodig is. Los van elkaar zijn dit waardevolle onderdelen, maar op zichzelf bieden ze geen volledige bescherming. Cyberdreiging stopt namelijk niet bij één systeem, één medewerker of één moment.

NIS2 maakt duidelijk dat security vraagt om een integrale aanpak, waarin mens, proces en technologie samenkomen. Alleen dan ontstaat grip: inzicht in risico's, overzicht over maatregelen en zekerheid dat alles op elkaar aansluit. Zonder samenhang ontstaan juist blinde vlekken, versnipperd beheer en onzekerheid over compliance.

In een samenhangende securitystrategie:

- Medewerkers weten hoe zij veilig moeten werken en risico's herkennen.
- Processen liggen vast rondom incidenten, toegang en continuïteit.
- Technologie zoals werkplekbeveiliging, cloud, XDR en bereikbaarheid versterkt elkaar, in plaats van los opereren.

Hierin vervult Company Connect de rol van regisseur van IT en security. Niet als leverancier van losse producten, maar als partner die het totaaloverzicht bewaakt. Door security, connectiviteit, werkplek en awareness onder te brengen bij één partij ontstaat rust, duidelijkheid en snelheid. Er is één aanspreekpunt, één strategie en één samenhangend geheel.

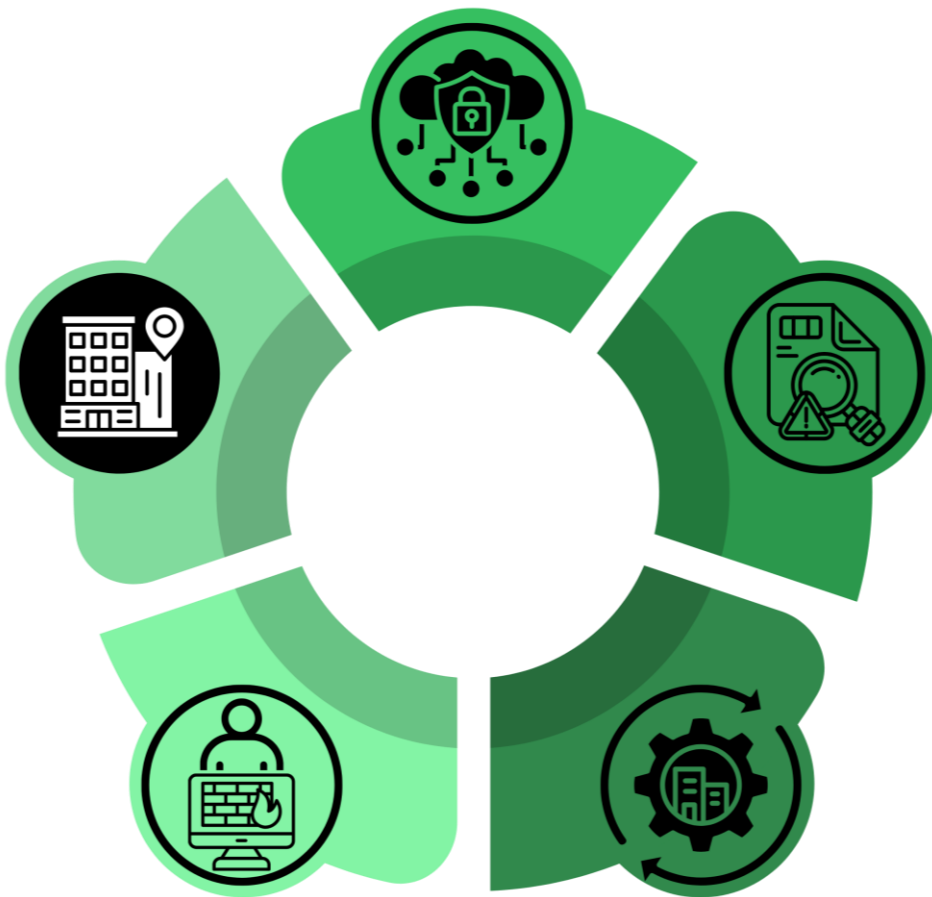
Door deze lagen bewust te combineren, ontstaat een veilig, compliant en MKB-proof ecosysteem. Geen losse oplossingen, maar een samenhangende aanpak die meegroeit met de organisatie en inspeelt op toekomstige dreigingen. Dáár draait moderne cybersecurity om: overzicht houden, risico's beheersen en met vertrouwen blijven ondernemen. Wij zorgen voor het overzicht, jij voor je bedrijf.

11. NIS2 als *kans* om je organisatie structureel te versterken

Hoewel de nieuwe NIS2-wetgeving kan aanvoelen als een last, is het juist een kans om je organisatie structureel te versterken. Organisaties die nú investeren in een samenhangende securitystrategie — waarin mens, proces en technologie samenwerken — zijn niet alleen veiliger, maar ook betrouwbaarder en toekomstbestendig. Ze beperken risico's, voldoen aan wetgeving en bouwen aan continuïteit en vertrouwen bij klanten en partners.

De stappen die we in deze whitepaper hebben besproken — van bewustwording van medewerkers, een veilige werkplek, XDR en cloudbeveiliging, tot bereikbaarheid en geïntegreerd beheer — vormen samen het fundament. Door deze maatregelen te combineren, wordt cybersecurity geen losse puzzelstukjes, maar een samenhangend ecosysteem dat NIS2-proof is én past bij de praktijk van het MKB.

Met de juiste strategie, tools en training transformeer je NIS2 van een verplichting naar een voordeel: een organisatie die veilig, wendbaar en veerkrachtig is voor alle uitdagingen van vandaag en morgen. Wil je weten waar jouw bedrijf staat op het gebied van security en NIS2? Plan een vrijblijvend gesprek: praktisch, duidelijk en zonder verplichtingen.



Wil jij jouw organisatie structureel veiliger maken, NIS2 compliant en tegelijkertijd toekomstbestendig werken? Bij Company Connect staan security, bereikbaarheid en continuïteit centraal, met oog voor duurzaamheid en efficiëntie.

Al onze diensten voldoen niet alleen aan de hoogste veiligheidsnormen, maar dragen ook bij aan SDG's, MVO en energie-efficiëntie. Wil je hier meer over weten? Bekijk dan onze vorige whitepaper over duurzaamheid:

<https://companyconnect.nl/whitepapers/>

Benieuwd wat wij voor jouw bedrijf kunnen betekenen? We denken graag met je mee.

Bel ons: 085 - 7500 505
Mail ons: salesdesk@companyconnect.nl

