CYBER SECURITY Magazine

HOE JE NIS2 COMPLIANT WORDT

Auditeur Marc van der Zandt laat zien wat je moet doen.

GEHACKTE ONDERNEMER VERTELT

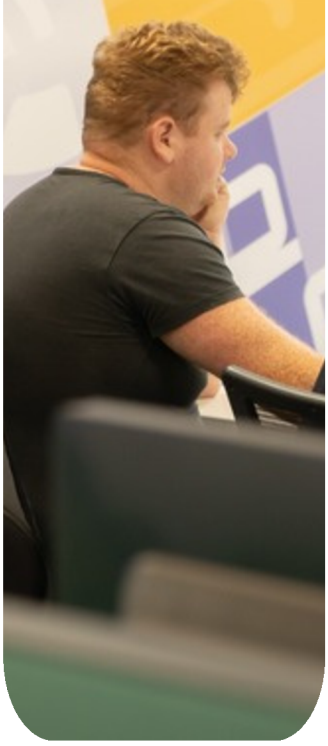
Xander Koppelmans deelt zijn verhaal en dat laat je niet meer los.

JE KENT HEM NIET, HIJ JOUW BEDRIJF WEL

Ethical hacker Jochen den Ouden laat zien hoe eenvoudig hij binnenkomt bij bedrijven.

TOP 5 CYBER SECURITY 'WAKKERLIGGERS'

WSB SOLUTIONS | Maakt ICT menselijk



Voorwoord

Eddy van de Lagemaat

Commercieel Directeur

De wereld van cyber security is de afgelopen jaren flink veranderd. Waar je vroeger verdachte e-mails nog redelijk makkelijk herkende en aanvallen sneller te herleiden waren, hebben we nu te maken met goed georganiseerde, professionele hackers. Hun doel: (veel) geld verdienen door bedrijven plat te leggen met bijvoorbeeld ransomware.

Gelukkig nemen steeds meer MKB-bedrijven hun cyber security serieus. Ze investeren in een veilige IT-omgeving en ontdekken dat dit niet alleen risico's verkleint, maar ook vertrouwen wekt bij klanten, partners en medewerkers.

Ondertussen scherpt de overheid de regels aan, zoals met de NIS2-richtlijn. En leveranciers bieden steeds meer deeloplossingen. Dat helpt, maar kan ook overweldigend zijn: wat kies je, wat heb je echt nodig en hoe houd je overzicht?

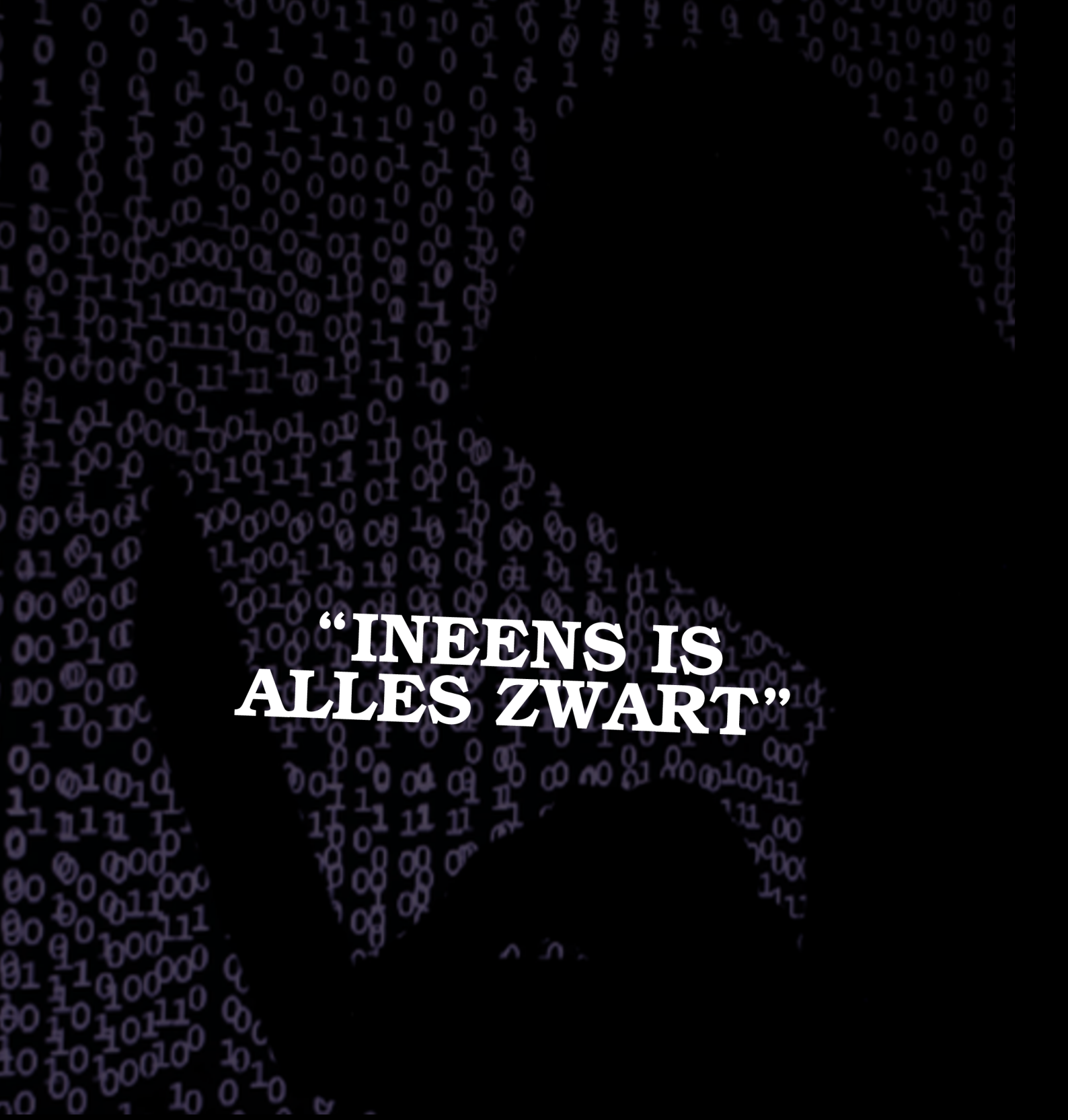
Daarom hebben we dit speciale Cyber Security Magazine gemaakt. Hierin helpen we mkb-bedrijven met:

- inzicht in de concrete risico's en dreigingen
- uitleg over de NIS2-richtlijnen
- overzicht van oplossingen en hoe wij je volledig kunnen ontzorgen

We spraken een hacker én een slachtoffer in openhartige interviews. Ook leggen we praktisch uit hoe je een sterke cyber security strategie opbouwt. En natuurlijk laten we zien hoe WSB Solutions je hierbij kan helpen.

Zo weet jij na het lezen precies waar je staat en welke stappen je vooruit brengen.

Veel leesplezier!


“INEENS IS
ALLES ZWART”

GEHACKT!

Je bent als laatste op kantoor. Klaar om naar huis te gaan en aan te schuiven voor een warme maaltijd. Nog snel wat facturen uitsturen en een paar laatste e-mails beantwoorden.

Je klikt op een link in een e-mail.

En dan – bam. Zwart scherm. Eén zin licht op:

"Al je bestanden zijn versleuteld. Maak 1 bitcoin over om weer toegang te krijgen."

Bedankt Rob voor de fantastische foto :)

Je hoofd maakt overuren.
Moet ik betalen? Krijg ik dan alles terug? Wat als ze blijven dreigen? Wat als ik niet betaal? Is dit het einde van mijn bedrijf?

Ransomware is al lang geen ver-van-je-bed-show meer. Sterker nog: het aantal incidenten steeg het afgelopen jaar met 300%. En het MKB is het favoriete doelwit. Jaarlijks krijgt 1 op de 4 MKB-bedrijven ermee te maken. Vaak met grote gevolgen: stilstand, schade, reputatieverlies. En soms is het zelfs einde verhaal.

Overheid grijpt in met NIS2

De overheid ziet dit gevaar ook. Daarom geldt er vanaf Q2 2026 nieuwe Europese wetgeving: NIS2. Deze verplicht bedrijven in essentiële en belangrijke sectoren om hun digitale veiligheid op orde te hebben. Denk aan technische maatregelen, meldplicht bij incidenten en beter toezicht.

Maar ook als toeleverancier kun je er niet omheen. Klanten gaan vragen stellen. Ben je veilig? Kun je aantonen dat je grip hebt op je risico's?

En dan?

Misschien denk je: Geldt dit ook voor mij? Wat gebeurt er als ik het niet regel? Ben ik dan als directeur aansprakelijk? En ook: Waar begin ik in hemelsnaam?

Goede vragen. Want er is veel: technische maatregelen, awareness training, certificeringen, tooling … En veel losse aanbieders. Het overzicht ontbreekt.

Rob van de Biezenbos
Accountmanager

Wat gaat er nu zo vaak mis bij bedrijven als het jouwe?

Cybercriminelen richten zich steeds vaker op het MKB. Eén klik op een verkeerde link en alles ligt plat.

We zetten de grootste bedreigingen op een rij. Met voorbeelden uit de praktijk en vooral: wat jij zelf kunt doen om schade te voorkomen. Want cyber security is niet alleen iets van IT. Het begint bij bewustwording. Bij jou.

“MKB-bedrijven denken vaak: Wij zijn te klein, waarom zouden hackers ons targeten?”

“Juist daarom ben je interessant: minder beveiliging, sneller binnen."

S	F	I	R	E	W	A	L	L	L	V	K	T	H	E	W	J	S
Z	P	R	W	A	C	H	T	W	O	O	R	D	R	J	A	W	M
T	E	U	P	D	A	T	E	W	B	U	Q	A	Y	X	U	I	U
N	O	M	E	N	D	P	O	I	N	T	W	I	C	J	D	W	L
E	G	B	I	U	X	D	Q	G	J	M	Z	B	A	A	I	E	T
D	G	V	N	R	A	O	N	U	O	D	E	R	V	H	T	D	I
I	C	W	P	T	C	I	U	S	V	2	R	Q	I	L	K	M	F
C	I	O	A	G	V	R	N	Z	O	S	O	M	R	C	N	D	A
N	C	L	M	E	N	A	E	W	M	I	T	R	P	Y	S	R	C
I	E	J	G	P	R	I	E	B	P	N	R	E	J	B	S	Q	T
K	B	T	S	C	L	R	R	H	Y	K	U	K	O	E	E	M	O
H	E	X	O	P	A	I	I	O	O	C	S	C	R	R	N	F	R
W	O	H	T	W	U	S	A	T	T	A	T	A	X	A	E	A	N
Q	G	Y	L	O	H	-	K	N	V	I	F	H	R	A	R	L	F
O	A	A	J	I	D	N	K	I	C	G	N	K	I	N	A	S	W
M	M	L	N	U	X	P	R	C	F	E	B	O	E	V	W	O	J
R	V	G	L	E	P	U	J	B	A	P	Z	J	M	A	A	N	H
O	H	M	L	K	S	B	C	U	D	B	Q	F	O	L	U	U	M

- AUDIT
- AWARENESS
- BACK-UP
- COMPLIANCE
- CYBERAANVAL
- CYBERCRIME
- DATALEK
- ENDPOINT
- FIREWALL
- HACKER
- INCIDENT
- MALWARE
- MDR
- MFA
- MONITORING
- MULTIFACTOR
- NIS2
- PHISHING
- PRIVACY
- RANSOMWARE
- UPDATE
- VIRUS
- WACHTWOORD
- WETGEVING
- ZEROTRUST

GROTE GEVOLGEN VOOR ONDERNEMERS

STILSTAND

Operatie ligt dagenlang plat, orders en facturen kunnen niet verstuurd worden.

FINANCIELE SCHADE

Omzetverlies, hoge herstelkosten, soms losgeld (ransomware).

IMAGO-SCHADE

Vertrek klanten door verlies vertrouwen, door negatieve berichtgeving raakt het bedrijfsimago beschadigd.

FAILLISSEMENT

Alle negatieve invloeden kunnen, zeker voor MKB-organisaties, leiden tot een faillissement.

CIJFERS OP EEN RIJ

MKB target cybercriminelen

25%

1 op 4 MKB-ers geeft aan afgelopen jaar schade opgelopen te hebben door cybercriminaliteit.

Phishing & Social Engineering

703%

In 2025 steeg het aantal aanvallen met gestolen inloggegevens, via phishing en social engineering, met 703%.

Schade per cyberincident

270k

Dit is het gemiddelde bedrag dat MKB-bedrijven kwijt zijn aan losgeld, herstel en stilstand bij een cyberincident.

Cyberaanvallen raken niet alleen techniek, maar ook mensen.
Ondernemer Xander deelt zijn verhaal.
Een confronterende wake-up call voor elke ondernemer
die denkt dat zoiets hem niet overkomt.

Xander Koppelmans

"VAN ZORGELOOS NAAR DAKLOOS. HOE ÉÉN HACK MIJN HELE LEVEN KANTELDE."

"Ik weet nog precies het moment waarop ik zag dat de eerste map verdween. Live. Gewoon voor onze ogen. Eén van mijn medewerkers stond naast me toen onze server zichzelf letterlijk leeg begon te trekken. Binnen een paar minuten verdwenen honderden klantmappen, werk van jaren. We dachten eerst nog: dit moet een systeembeheerder zijn die iets omzet. Maar dat bleek niet zo. 'Ik denk dat jullie gehackt worden', klonk het aan de andere kant van de lijn.

We lachten nog even. Want: wij? Wij waren een kerngezond MKB-bedrijf in Zeeland. Goed georganiseerd, professioneel, back-ups geregeld, niets om ons zorgen over te maken toch? We hadden 25 jaar opgebouwd aan reputatie en relaties. En toch... binnen een uur was het allemaal anders."

"Waarom ik? Wij zijn toch niet interessant?"

"Ik riep het regelmatig: 'We zijn te klein, te lokaal, te onbelangrijk voor hackers.' Maar dat is precies het probleem: dat valse gevoel van veiligheid, juist dat maakt MKB-bedrijven kwetsbaar. Want nee, je bent niet te klein. En nee, de cloud is geen magische ondoordringbare muur. Ook jouw Apple is te hacken. En ja, jouw back-ups zijn ook doelwit, zeker als je niet monitort of die nog veilig staan.

De hackers wisten precies wat ze deden: eerst de back-ups wissen, dan pas de server leegtrekken. En daar sta je dan. Met lege handen. En een volle agenda vol boze klanten."

De échte schade is niet digitaal

"Iedereen vraagt naar de financiële impact. Maar geld was niet het grootste verlies. De echte schade was persoonlijk. Na 25 jaar bouwen aan een bedrijf, aan vertrouwen, aan een team, voelde ik me ineens machteloos. Medewerkers die ziek uitvielen van de stress. Klanten die vertrokken, niet eens uit boosheid, maar uit angst. Leveranciers die zich terugtrokken. Partners die hun vertrouwen kwijtraakten.

En thuis? Mijn vrouw zei na een jaar dat de man waar ze mee getrouwd was niet meer bestond. De onbevangenheid, het plezier, het gevoel van controle... alles was weg. En dat raakte alles: ons huwelijk, ons huis, mijn gezondheid, mijn hele identiteit. Van ondernemer met personeel, een Audi en vier vakanties per jaar, naar een tweedehands auto, geen spaargeld en geen pensioen. Binnen twee jaar. Door één cyberincident."

Waarom ik wél mijn verhaal vertel

"Veel ondernemers zwijgen uit schaamte. Ik niet. Juist omdat ik weet hoe belangrijk het is dat anderen hiervan leren. Als het mij kan overkomen, dan kan het jou ook gebeuren. En het is een wonder als het jou nóg niet is overkomen.

Met 600 miljoen cyberaanvallen per dag is het niet de vraag of, maar wanneer. Tijd om wakker te worden. Tijd om te handelen."

Mijn belangrijkste tip? Gebruik een wachtwoordmanager.

"Vraag jezelf af: kan jij 100+ sterke wachtwoorden onthouden? Precies.
Zonder wachtwoordmanager hergebruik je wachtwoorden. En dat is de directe route naar een hack."

TOP 5

CYBERDREIGINGEN VOOR HET MKB: ZIT JOUW BEDRIJF IN DE GEVARENZONE?

1. Phishing & Social engineering

Phishing is slimmer en gevaarlijker dan ooit. Dankzij AI zijn aanvallen persoonlijk, overtuigend en bijna niet van echt te onderscheiden.

Denk aan e-mails, stem- of videoberichten die rechtstreeks lijken te komen van een collega of klant. In 2025 steeg het aantal aanvallen met gestolen inloggegevens met maar liefst 703 %. Mkb'ers zijn daarbij extra kwetsbaar door beperkte awareness en training.

> *Dagelijks worden wereldwijd 3,4 miljard phishingmails verzonden.*

Concreet MKB-voorbeeld:
Een medewerker van jouw boekhoudkantoor krijgt een e-mail die van de Belastingdienst lijkt te komen. De e-mail vraagt om "dringende verificatie van bedrijfsgegevens" via een link. De medewerker klikt en voert BSN-nummers en wachtwoorden in op een nepwebsite.

Resultaat: criminelen hebben nu toegang tot vertrouwelijke klantgegevens.

Wat kun je doen?

- Geef medewerkers praktijkgerichte training
- Gebruik tools die verdachte berichten automatisch signaleren
- Voer regelmatig nep-phishing campagnes uit om te testen en te leren

2. Ransomware (ook als dienst te huur)

Zodra hackers ransomware installeren, blokkeren ze je toegang tot je systemen en gijzelen ze je gegevens. Pas na betaling van losgeld (ransom) krijg je mogelijk weer toegang tot je data.

Een derde van de aanvallen is inmiddels gericht op het MKB. En dat werkt: in bijna de helft van de gevallen wordt het losgeld betaald.

Door Ransomware-as-a-Service (RaaS) zijn dit soort aanvallen zelfs beschikbaar voor iedereen, ook zonder technische kennis.

Concreet MKB-voorbeeld:
Een tandartspraktijk opent een bijlage in een e-mail die eruitziet als een factuur van hun leverancier. De bijlage installeert ransomware die alle patiëntendossiers versleutelt. De praktijk kan niet meer bij agenda's, röntgenfoto's of factuurgegevens. Criminelen eisen €300.000,- voor de sleutel.

Wat kun je doen?

- Zorg voor dagelijkse back-ups die je kunt terugzetten
- Houd systemen up-to-date met de nieuwste patches

3.

Malware vermomd als bekende software

Downloaders, Trojaanse paarden en adware blijven populair bij cybercriminelen. Ze stoppen hun malware in ogenschijnlijk legitieme programma's als Zoom, Teams of zelfs een nepversie van ChatGPT.

Eén ondoordachte klik en je zit met een geïnfecteerd systeem.

Concreet MKB-voorbeeld:
Een medewerker krijgt een overtuigende e-mail met een nep-update voor Microsoft Teams.

Hij klikt, installeert en haalt ongemerkt een Trojaans paard binnen.

Hackers kijken mee, onderscheppen projectoffertes en passen betaalgegevens aan. Klanten maken tienduizenden euro's over naar criminelen.

Wat kun je doen?

- Gebruik endpoint-beveiliging die malware herkent en blokkeert
- Laat medewerkers alleen software downloaden via goedgekeurde bronnen
- Stel duidelijke gebruikersrichtlijnen op

4.

Aanvallen via leveranciers

Je kunt je zaakjes goed op orde hebben, maar hoe zit dat met je IT-leverancier, softwarepartner of externe boekhouder?

Supply-chain aanvallen nemen toe.
Eén zwakke schakel en een hacker zit zo in jouw netwerk. Ruim een derde van de securityteams zag in 2025 zo'n aanval.

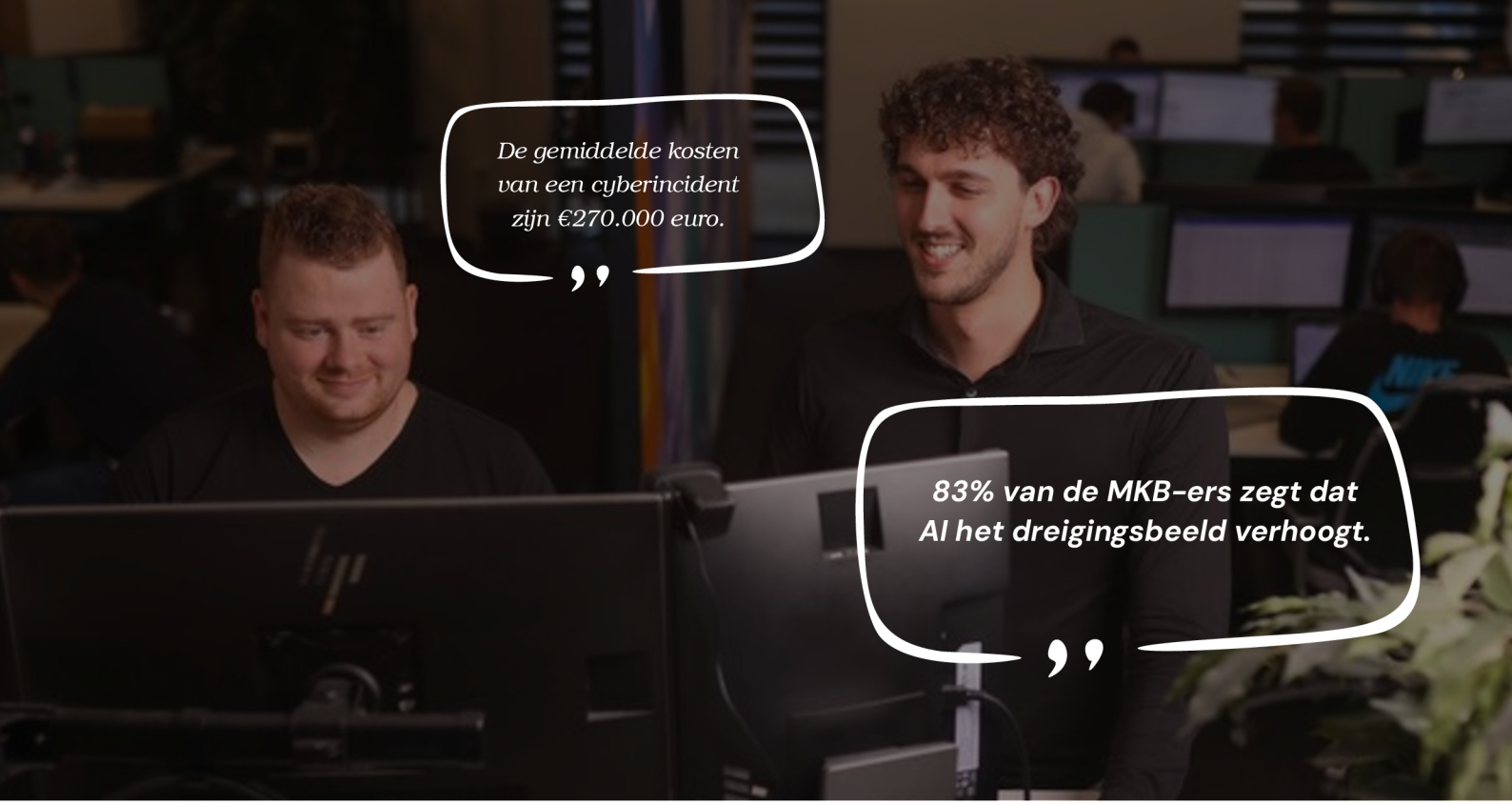
Wat kun je doen?

- Vraag leveranciers om inzicht in hun beveiligingsmaatregelen
- Leg beveiligingseisen vast in contracten

> *32% van alle ransomware aanvallen zijn gericht op het MKB.*

Concreet MKB-voorbeeld:
Een lokale webdesign-agency gebruikt een populaire WordPress-plugin voor alle klantwebsites.

Hackers beschadigen deze plugin en plaatsen malware die automatisch wordt verspreid naar alle websites die de agency beheert, inclusief die van een lokale bank en zorgverlener.



5.

AI en automatisering als aanvalswapen

Cybercriminelen gebruiken AI om sneller en slimmer aan te vallen. Ze scannen massaal netwerken (36.000 scans per seconde wereldwijd), kraken gestolen wachtwoorden en zetten geautomatiseerde aanvallen in. 83% van de mkb'ers ziet AI als extra risico, maar slechts de helft doet er iets mee.

Wat kun je doen?

- Maak gebruik van slimme monitoring en dreigingsdetectie (zoals MDR)
- Werk met een zero-trust aanpak: niemand krijgt zomaar toegang
- Bescherm accounts met sterke wachtwoorden en multi-factor authenticatie

Concreet MKB-voorbeeld:
AI analyseert het e-mailverkeer van een gehackte klant en schrijft vervolgens een overtuigende mail in diens stijl:

"Hé, kun je even dit conceptcontract checken voor 15u?" met een link naar een geïnfecteerd bestand.

De medewerker opent het zonder argwaan en geeft de aanvaller directe toegang tot vertrouwelijke klantdata.

Deze vijf dreigingen versterken elkaar

Phishing maakt de weg vrij, malware nestelt zich stilletjes, ransomware legt alles plat.

Cyber security is complex, maar jouw rol hoeft dat niet te zijn. Of je nu directeur bent, de financiën bewaakt of de IT beheert: iedereen kan iets doen.
We helpen je inzicht te krijgen in jouw risico's, zodat je stap voor stap kunt bijdragen aan een veiligere werkomgeving.

JE ROL BEPAALT JE RISICO

BEN JIJ JE BEWUST VAN DE RISICO'S DIE HOREN BIJ JOUW FUNCTIE?

Cyber security is allang geen exclusieve zorg meer van de IT-afdeling. In elke laag van de organisatie (van finance tot HR, van directie tot projectleiding) schuilen digitale risico's die misbruikt kunnen worden door cybercriminelen. En vaak is het niet het systeem dat faalt, maar de mens die een deur op een kier zet.

Weet jij welke risico's horen bij jouw specifieke rol? Of je nu beslissingen neemt, met gevoelige data werkt of toegang hebt tot kritische systemen: je bent een potentieel doelwit. In dit artikel lees je hoe cyberdreigingen zich richten op functiespecifieke zwaktes en wat jij concreet kunt doen om geen schakel te worden in een succesvolle aanval.

Directeur

Als directeur van een MKB-bedrijf ben jij verantwoordelijk voor de koers en continuïteit van de organisatie. En zowel de NIS2-richtlijn als de Cyberbeveiligingswet leggen een grote verantwoordelijkheid bij bestuurders, tot aan een persoonlijke aansprakelijkheid als onvoldoende maatregelen zijn genomen.

Een datalek of hack raakt niet alleen je IT, maar ook je reputatie. Klanten verliezen vertrouwen, projecten lopen vertraging op en je loopt het risico op forse boetes als je niet voldoet aan de AVG of andere wetgeving zoals NIS2.

Daarbij is het niet de vraag of je wordt aangevallen, maar wanneer. Juist als MKB'er ben je vaak een makkelijk doelwit: minder beveiligd, maar wel waardevolle data. Zorg dus dat je voorbereid bent. Niet alleen voor je IT-afdeling, maar vooral voor je organisatie en imago.

Cyber security is allang geen IT-zaak meer. Het is een directiedossier.

Stel jezelf deze vragen:

- Weet ik welke systemen en data kritiek zijn voor onze bedrijfsvoering?
- Hebben we een plan voor als we morgen platliggen door een cyberaanval?
- Voldoen we aan wetgeving zoals de AVG en (straks) NIS2?
- Wordt mijn managementteam actief meegenomen in cyberrisico's?

Financieel Manager

Als financieel manager bij een MKB-bedrijf sta je direct aan het front van cyberrisico's die je cijfers en processen kunnen verwoesten. Denk aan ransomware of cryptolockers: kwaadaardige software die je financiële data vergrendelt totdat je betaalt. Een databelemmering zoals deze blokkeert betalingen, vertraagt facturatie en geeft leveranciers en klanten een slechte indruk van je betrouwbaarheid.

Daarnaast loop je het risico op verstoring van je financiële data: corrupte of verdwenen gegevens kunnen de jaarrekening vervuilen, auditprocessen ontwrichten en zorgen voor complianceproblemen. In het ergste geval is terugdraaien van transacties onmogelijk, wat enorme impact kan hebben op je liquiditeit en groeiplannen.

Als financieel manager bewaak je niet alleen de cijfers, maar ook de continuïteit en integriteit van de financiële keten. Cyber security is tegenwoordig een cruciaal onderdeel van de financiële strategie.

Stel jezelf deze vragen:

- Wat is de impact op onze cashflow als onze systemen één dag niet functioneren?
- Kunnen we na een cyberaanval snel en veilig onze financiële data herstellen?
- Hebben we controle over wie toegang heeft tot bankgegevens en boekhoudsoftware?
- Is ons team getraind om phishing en frauduleuze betaalverzoeken te herkennen?
- Is cyber security een vast onderdeel van onze financiële strategie en begroting?

IT-manager

Als IT-manager in een MKB-bedrijf sta je dagelijks onder druk om systemen stabiel, veilig en schaalbaar te houden. Maar de dreigingen worden steeds slimmer. Denk aan supply-chain malware die via ogenschijnlijk betrouwbare leveranciers je netwerk binnensluipt.

Of APT's (Advanced Persistent Threats) die maandenlang onopgemerkt meekijken, op zoek naar gevoelige data of toegang tot klantomgevingen.

En dan is er nog de opkomst van AI-gedreven phishing. Waar klassieke phishingmails vol spelfouten stonden, zijn ze nu perfect getimed en gepersonaliseerd. Zelfs je collega van finance kan het verschil nauwelijks zien.

Jij bent de buffer tussen technologie en risico. Maar alleen red je het niet. Cyber security moet een gedeelde verantwoordelijkheid zijn binnen je hele organisatie.

Stel jezelf deze vragen:

- Hebben we zicht op kwetsbaarheden in onze softwareketen en leveranciers?
- Hoe snel detecteren we verdachte activiteiten, zoals APT's, binnen ons netwerk?
- Zijn onze toegangsrechten goed ingericht én up-to-date?
- Hoe effectief is onze security awareness training tegen AI-gedreven phishing?
- Betrekken we andere afdelingen actief bij onze cyber securityaanpak?

"ZOU JIJ HET OKÉ VINDEN ALS IEMAND ZONDER TOESTEMMING DOOR JE APPJES BLADERT?"

Die vraag stelde ik een paar jaar geleden tijdens een sessie over de AVG en het werd ineens stil. Die ene simpele vraag bracht iets in beweging. Niet alleen bij medewerkers, maar ook bij mij. Want echte security begint niet bij IT, maar bij bewustzijn.

Van keukentafel tot keten: waarom security steeds minder met IT te maken heeft
In 2017 sprak ik voor het eerst met WSB Solutions over de aangekondigde Algemene Verordening Gegevensbescherming (AVG). Die verordening was in het leven geroepen om de privacyrechten van de Europese burger beter te beschermen, een prachtig uitgangspunt.

Maar in de praktijk draaide het vooral om één ding: boetes voorkomen. Checklists werden opgesteld, verwerkersovereenkomsten getekend, registers gevuld en websites aangepast. Alles volgens de regels. Veel organisaties hadden het gevoel dat ze in korte tijd van al hun medewerkers mini-AVG-specialisten moesten maken. Alsof naleving alleen via kennis en procedures kon.

Maar ergens bekroop mij de vraag: we leggen medewerkers keurig uit wat ze juridisch wel en niet mogen, maar vragen we ook hoe zíj zouden willen dat er met hún gegevens wordt omgegaan? Die ene simpele vraag, "Zou jij dit prettig vinden als het om jouw data ging?", bleek een eye-opener. Niet alleen voor de ander. Ook voor mij en mijn collega's.

Dat moment markeerde het begin van iets wat ik nu zie als dé rode draad van onze aanpak: bewustwording begint pas echt als je het persoonlijk maakt. Als mensen zichzelf herkennen in de risico's en voelen dat het ook hún persoonlijke veiligheid raakt, thuis én op het werk.

En toen kwam de keukentafel
In 2020 werd die boodschap relevanter dan ooit. Tijdens de coronapandemie verhuisde het hele kantoor naar huis. Letterlijk. Partners, kinderen, buren (ja écht!) iedereen zat ineens op hetzelfde onbeveiligde wifi-netwerk te werken, te videobellen of games te downloaden met plugins van twijfelachtige herkomst.

Dat was geen theoretisch risico meer. Dat was de realiteit. De keukentafel werd een aanvalsvector. Eén geïnfecteerde laptop in het gezin, en een besmetting van de hele keten was een kwestie van tijd.

Organisaties zetten razendsnel technische oplossingen in: VPN's, cloudoplossingen, MFA. Maar ondertussen klikte diezelfde medewerker in joggingbroek nog altijd op die malafide-mail. Of gebruikte hij zijn privéwachtwoord, dat al jaren voorkomt in drie datalekken.

Wat we daarvan leerden? Gedrag is de kwetsbaarste schakel. En tegelijk de meest onderschatte.

Pieter Reners

BeveiligMij.nl

NIS2 en het geopolitieke speelveld
Fast forward naar nu. We zitten midden in geopolitieke spanningen: sancties, digitale sabotage, onderbrekingen in toeleverings-ketens. Europa staat onder druk en wil, nee moet, meer grip krijgen op zijn digitale infrastructuur. De NIS2-richtlijn is daar een rechtstreeks gevolg van. Vanaf 2026 moeten duizenden organisaties binnen de EU aantoonbaar werken aan digitale weerbaarheid. Niet alleen door hun techniek op orde te brengen, maar vooral door mensen actief te trainen, gedrag te veranderen en bewustzijn duurzaam te verankeren.

En dat is hard nodig. In Nederland werden in 2024 al 308 cyber-incidenten publiekelijk gemeld; meer dan genoeg om wakker van te liggen. Maar de eerste maanden van 2025 laten zien dat dit nog maar het begin was: begin mei lagen al 212 Neder-landse organisaties onder vuur, een stijging van 28% ten opzichte van vorig jaar.

Wereldwijd is de situatie nog alarmerender. In het eerste kwartaal van 2025 zagen organisaties gemiddeld 1.925 cyberaanvallen per week, een stijging van 47% ten opzichte van vorig jaar.

Ransomware vestigde een nieuw dieptepunt: 2.289 incidenten, een stijging van 126%, met gemiddeld $663.000 aan geëist losgeld en 1,58 terabyte aan buitgemaakte data per aanval.

De boodschap is glashelder: het is niet langer de vraag of je geraakt wordt, maar hoe vaak en hoe hard. Security is geen luxe meer. Het is een noodplan. En organisaties die dat nog niet zo zien, zijn eigenlijk al te laat begonnen.

Maar een noodplan werkt alleen als mensen weten hoe ze moeten handelen. Daarom stopt het niet bij techniek. Daarom draait het uiteindelijk altijd weer om gedrag.

Europese oplossingen, lokale verantwoordelijkheid
Gelukkig ontstaat er een stevig Europees ecosysteem van cloudproviders, securityaanbieders en soevereine opslag. Maar techniek is maar de helft van het verhaal.

De echte slag maken we pas als we ook het gedrag aanpakken. Als we inzien dat security niet ophoudt bij de voordeur van de IT-afdeling, maar begint bij de voordeur van je huis.

Daarom trainen wij medewerkers al lang niet meer alleen op de werkvloer. We laten ze ook ervaren hoe belangrijk hun digitale gedrag thuis is. Hoe veilig omgaan met data in je privésituatie direct impact heeft op jezelf én je organisatie. Niet omdat het moet. Maar omdat het logisch voelt.

Tot slot
Security is geen wedstrijd tussen IT-afdelingen. Het is een gezamenlijke inspanning, waarin gedrag, bewustzijn en samen-werking de hoofdrol spelen.

Van de juridische bewustwording in 2018, via de thuiswerkrealiteit van 2020, tot de geopolitieke verantwoordelijkheid van 2026: security is menselijker dan ooit.

Laten we vanaf nu niet alleen systemen updaten, maar vooral gesprekken voeren. Over gedrag. Over gewoontes. Over waarom het ook jouw data is die we beschermen.

3 lessen die ik nooit meer vergeet

1. **Maak het persoonlijk**. *Mensen veranderen pas als ze voelen dat het over henzelf gaat. De vraag "Zou jij dit willen?" werkt krachtiger dan duizend regels.*
2. **Kijk verder dan je eigen organisatie.** *Security is een ketenkwestie. Eén zwakke schakel bij een leverancier of gezinslid is genoeg.*
3. **Zet in op Europese oplossingen**. *Hosting in Europa is niet alleen veiliger, het verkleint ook de juridische en geopolitieke risico's.*

THE CYBER SECURITY CONFESSIONAL

Iedereen maakt fouten. Ook wij. Want hoe goed je processen ook zijn en hoe streng je beleid ook is, uiteindelijk zijn het mensen die op linkjes klikken, wachtwoorden hergebruiken of net iets te snel op “verzenden” drukken.

“Ik adviseer over multi factor-authenticatie, maar was laatst 10 minuten buitengesloten omdat m’n telefoon leeg was.”

“Ik schreef het wachtwoordbeleid van onze organisatie. Mijn eigen wachtwoord was jarenlang ‘Welkom123’.”

“Ik dacht ooit een slimme hack te analyseren... bleek het m’n dochter van 12 te zijn op het thuisnetwerk.”

“Tijdens een live demo over veilig werken, deelde ik per ongeluk mijn persoonlijke WhatsApp-scherm op groot scherm. Inclusief gênante groepsnaam.”

"Ik preek altijd over 'updates installeren', maar klik zelf structureel op 'morgen herinneren' als m'n laptop daarom vraagt."

"Ik waarschuw iedereen voor onbeveiligde USB-sticks, maar heb zelf ooit een gevonden stick wel in m'n laptop gestoken. Nieuwsgierigheid won."

"Ik geef presentaties over dataminimalisatie... maar bewaar zelf nog altijd m'n stageverslagen en tien jaar aan screenshots in m'n downloadsmap."

"Ik werk in cyber security... en moet elke maand m'n wachtwoord resetten omdat ik 'm weer vergeten ben."

"Ik leg uit hoe belangrijk fysieke beveiliging is... maar laat m'n badge standaard op mijn bureau liggen tijdens de lunch."

"Ik promoot digitaal welzijn... maar kijk dagelijks 6 uur naar 3 schermen tegelijk."

Als ICT-bedrijf met ruim 40 jaar ervaring in de IT weten we één ding zeker: niemand is perfect. Daarom delen wij hier met een knipoog onze eigen blunders. Niet om met de vinger te wijzen, maar juist om te laten zien dat fouten maken menselijk is. En stiekem... ook best herkenbaar.

DE DENKWERELD VAN EEN HACKER

Hoe en waarom jij als bedrijf op de radar komt te staan

Hoe komt een hacker eigenlijk binnen bij een bedrijf? Dat is misschien wel de belangrijkste vraag die je jezelf als ondernemer kunt stellen. Want nee, je hoeft geen internationale speler te zijn, geen bank, geen zorginstelling met tienduizenden patiëntgegevens. Ook jouw bedrijf, misschien met 20 man personeel, en een website die "ooit nog vernieuwd moet worden" is een aantrekkelijk doelwit.

Hoe een hacker denkt

"Ik word ingehuurd als hacker. Soms door bedrijven die een pentest nodig hebben voor hun ISO 27001-certificering. Soms omdat er investeerders aan boord komen. En steeds vaker: omdat een klant daarom vraagt. Maar het fijnst? Als een bedrijf écht intrinsiek gemotiveerd is om veilig te werken.

Hackers kijken anders naar een organisatie. Waar jij een mooie website ziet, zie ik een ingang. Een zinnetje als "binnenkort stappen we over op een nieuw systeem" kan voor een aanvaller betekenen: er zit een gat in je overgangsperiode.

Of: "onze IT is uitbesteed." Fijn, maar... aan wie? En hoe goed is die leverancier zelf beveiligd?"

Open poorten, oude software en post-its

"Verouderde software. Open poorten. Systemen die al maanden geen updates meer hebben gehad. Dat zijn de eerste dingen waar ik naar kijk. Maar ook naar gedrag. Wat medewerkers online zetten. Of je bedrijf zichtbaar is op social media. Welke tools je gebruikt."

Soms is een bedrijf geen direct doelwit, maar wordt het simpelweg gevonden. Via een geautomatiseerde scan. Een lijstje open poorten. Een vergeten VPN-server. En dan: bingo.

Ook menselijke fouten helpen een handje. Zoals een LinkedIn profiel waarop staat dat je met specifieke bedrijfssoftware werkt. Of een Instagram foto van je werkplek met een wachtwoord op een post-it. "Ja, dat soort dingen komen we echt tegen," zegt Jochen. "En ja, hackers kijken mee."

Ontmoet hacker Jochen Den Ouden.

Jochen is ethisch hacker en spreker die ingewikkelde IT-risico's simpel maakt. Met humor en scherpe voorbeelden laat hij zien hoe kwetsbaar bedrijven zijn. Zijn missie? Niet bang maken, maar wakker schudden.

Waarom juist MKB-bedrijven?

"Het is vaak makkelijker binnenkomen en de data is waardevoller dan je denkt."

MKB'ers onderschatten hun eigen waarde, stelt Jochen. "Ze denken vaak: we zijn te klein. Wat moeten ze bij ons halen? Maar je hebt klantgegevens. Toegang tot ketens. Soms toegang tot grotere klanten. En vooral: je hebt weinig verdediging.

Een groep van tien kleine bedrijven kan voor een aanvaller net zo interessant zijn als één grote multinational. Alleen met veel minder moeite."

Gedrag als kwetsbaarheid

De mens blijft de zwakste schakel. Vooral online gedrag van medewerkers maakt een bedrijf kwetsbaar:

- Medewerkers die zelf tools installeren en gebruiken (zonder beleid of toezicht)
- Te veel informatie op social media of in out-of-office replies
- Zwakke wachtwoorden op basis van persoonlijke voorkeuren ("RodeAuto2025")

Jochen lacht: "Iemand rijdt een leuke rode auto. Dan zou het wachtwoord zomaar eens 'RodeAuto2025' kunnen zijn. Het is echt geen grap."

Copilot: je beste vriend of je gevaarlijkste assistent?

"Bij steeds meer bedrijven zien we dat AI een rol speelt. Vooral Microsoft Copilot is populair. Superhandig, want je kunt vragen stellen en informatie opvragen uit je SharePoint."

Maar dat is ook een risico. "Wat als je daar ID-bewijzen, paspoorten of blauwdrukken van je machines in hebt staan? Dan was het al een risico. Maar met Copilot wordt het nog makkelijker gevonden, en zelfs actief gesuggereerd."

Volgens Jochen kwamen ze dit onlangs nog tegen bij:

- Een maakbedrijf dat werkte met machines op klantlocatie
- Een accountantskantoor met gevoelige klantdossiers
- Een softwarebedrijf voor zorginstellingen

"Ze dachten dat die documenten veilig stonden. Maar Copilot vond ze binnen seconden. En dus kan ik ze ook vinden."

Ben je na het lezen benieuwd hoe dit er in het écht aan toe gaat?

Scan de QR-code en luister de podcastaflevering, waarin Jochen vertelt hoe een hacker binnenkomt, welke verrassende ontdekkingen hij doet bij bedrijven én welke simpele maatregelen jij vandaag nog kunt nemen om je organisatie veiliger te maken.

Of klik hier

NIS2 uitgelegd in 3 minuten

“DIT IS NIS2”

NIS2 is de nieuwe Europese richtlijn voor cyber security. De afkorting staat voor ***Network and Information Systems Directive 2*** *en is de opvolger van de eerste NIS-richtlijn.*

Het doel? *Ervoor zorgen dat alle EU-landen hun digitale beveiliging op orde hebben. Zeker in sectoren waar uitval grote (maatschappelijke) gevolgen kan hebben, zoals energie, zorg of transport.*

De richtlijn verplicht organisaties om hun risico’s beter in kaart te brengen, cyber-incidenten te melden en structurele maatregelen te nemen. “Het mooie is, NIS2 gaat niet alleen over techniek, maar ook over processen, verantwoordelijkheden en bewustwording binnen je organisatie.”

Meretta Kouria
Cyber Security Consultant

Wat zijn de 5 belangrijkste onderdelen?

De kern draait om vijf pijlers. Begin met een risicoanalyse: welke dreigingen kunnen jouw organisatie raken, op korte én lange termijn? Werk daarna aan risicomanagement met duidelijke processen en verantwoordelijkheden. Zorg ook voor een meldplichtprocedure, zodat je cyberincidenten snel en correct rapporteert. Stel een incident responseplan op: wat doe je als het misgaat? Tot slot: neem de juiste technische en organisatorische maatregelen om je netwerk- en informatiesystemen te beveiligen en toon aan dat je die ook structureel uitvoert.

In welke sectoren voorziet NIS2?

De NIS2-richtlijn geldt voor essentiële sectoren als energie, transport, zorg, financiën en digitale infrastructuur. Ook kleinere organisaties krijgen ermee te maken doordat hun klanten strengere eisen stellen aan leveranciers.

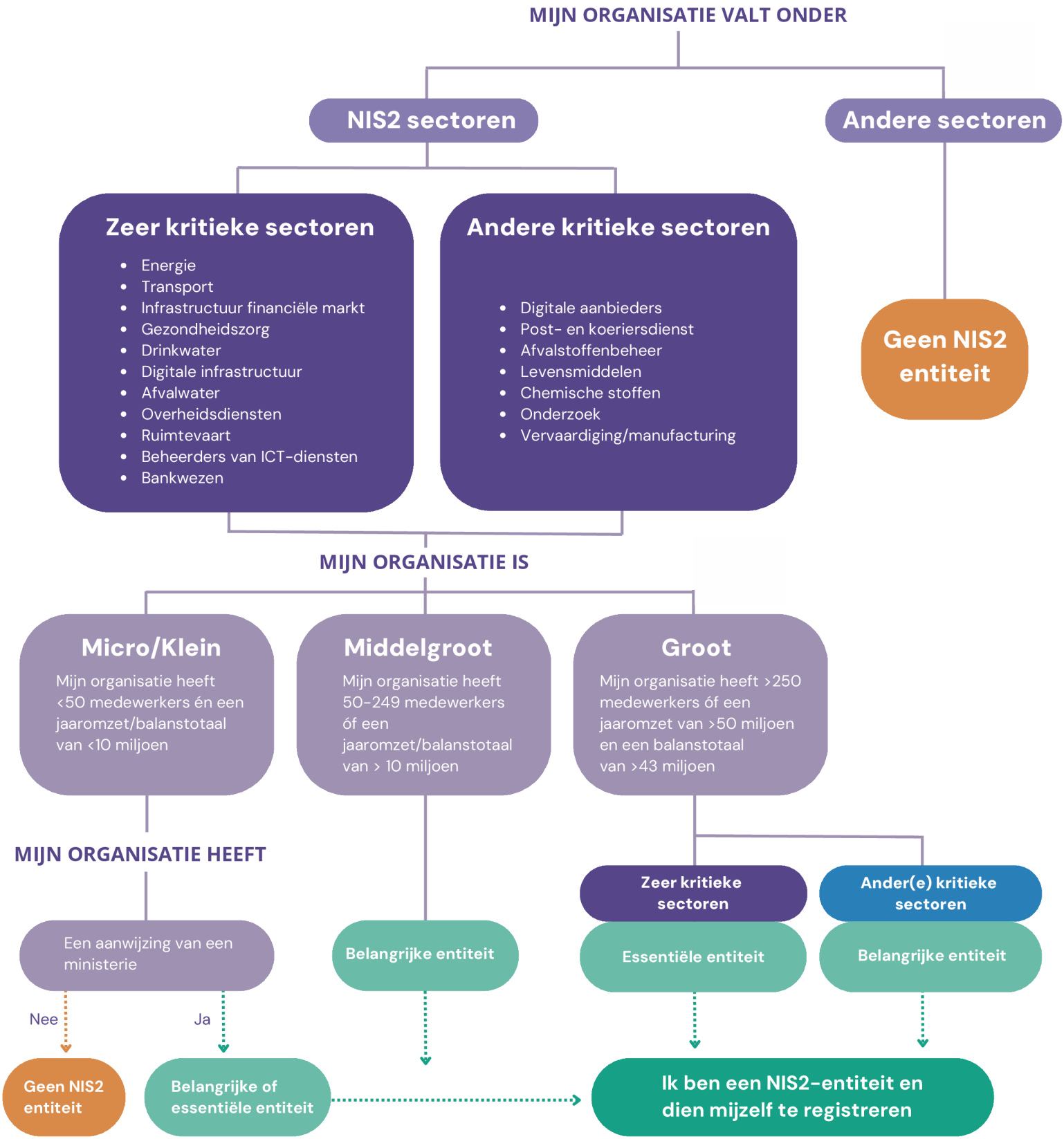
Hoe breng je je cyber security toonbaar op orde?

Het NIS2 Supply Chain helpt organisaties op een praktische manier te voldoen aan de NIS2-richtlijn. Deze in Nederland ontwikkelde standaard is gratis, toepasbaar in heel Europa en speciaal gemaakt voor het MKB.

De maatregelen zijn concreet, haalbaar en ontwikkeld door onafhankelijke cyber security experts. Ideaal voor audits én om je compliance aantoonbaar te maken.

“IS DE NIS2-RICHTLIJN VAN TOEPASSING OP JOUW ORGANISATIE?”

Martijn Furster
IT Consultant


MIJN ORGANISATIE VALT ONDER
NIS2 sectoren
Andere sectoren
Zeer kritieke sectoren
Energie
Transport
Infrastructuur financiële markt
Gezondheidszorg
Drinkwater
Digitale infrastructuur
Afvalwater
Overheidsdiensten
Ruimtevaart
Beheerders van ICT-diensten
Bankwezen
Andere kritieke sectoren
Digitale aanbieders
Post- en koeriersdienst
Afvalstoffenbeheer
Levensmiddelen
Chemische stoffen
Onderzoek
Vervaardiging/manufacturing
Geen NIS2 entiteit
MIJN ORGANISATIE IS
Micro/Klein
Mijn organisatie heeft <50 medewerkers én een jaaromzet/balanstotaal van <10 miljoen
Middelgroot
Mijn organisatie heeft 50-249 medewerkers óf een jaaromzet/balanstotaal van > 10 miljoen
Groot
Mijn organisatie heeft >250 medewerkers óf een jaaromzet van >50 miljoen en een balanstotaal van >43 miljoen
MIJN ORGANISATIE HEEFT
Een aanwijzing van een ministerie
Nee
Ja
Geen NIS2 entiteit
Belangrijke of essentiële entiteit
Belangrijke entiteit
Zeer kritieke sectoren
Essentiële entiteit
Ander(e) kritieke sectoren
Belangrijke entiteit
Ik ben een NIS2-entiteit en dien mijzelf te registreren

WETGEVINGEN EN NORMERINGEN:

HOE BLIJF JE COMPLIANT IN EEN STEEDS STRIKTER WORDEND CYBER SECURITY LANDSCHAP?

Wat betekent NIS2 voor jouw organisatie?

Cyber security is geen optie meer, maar een noodzaak. De nieuwe Europese NIS2-richtlijn verplicht organisaties met een essentiële of belangrijke rol om hun digitale beveiliging op orde te brengen.

Niet alleen grote bedrijven, maar ook MKB'ers in vitale ketens krijgen te maken met strengere eisen. Normen zoals ISO 27001 en NIS2 bieden houvast. In dit artikel lees je wat er verandert en hoe jij je organisatie voorbereidt.

ISO 27001: De basis voor informatiebeveiliging

Je hebt vast wel eens gehoord van ISO 27001: **de internationale norm voor informatiebeveiliging**. Deze norm helpt organisaties bij het opzetten en beheren van een Information Security Management System (ISMS). Vooral voor MKB'ers die omgaan met gevoelige data of werken binnen ketens met strenge beveiligingseisen is ISO 27001 cruciaal. Het biedt een gedetailleerde handleiding om risico's inzichtelijk te maken, processen vast te leggen en voortdurend te verbeteren.

Voor veel bedrijven en hun klanten is ISO 27001-certificering tegenwoordig een harde eis. Het behalen van dit certificaat toont aan dat je systemen veilig zijn en dat je processen effectief worden beheerd. Dit maakt ISO 27001 tot een must-have voor bedrijven die hun cyber security serieus nemen.

ISO 27005: Dieper in risico's duiken

Wil je een stap verder gaan in je beveiliging? Dan biedt ISO 27005 uitkomst. Deze norm focust op het beoordelen en beheersen van risico's. Het helpt organisaties niet alleen kwetsbaarheden in kaart te brengen, maar ook te prioriteren. Waar zitten de grootste dreigingen? Wat is de impact? En welke maatregelen zijn écht noodzakelijk?

ISO 27005 is vooral relevant voor bedrijven die in een risicovolle omgeving opereren en grote spelers in de technologie. Het implementeren van deze norm is intensief, maar het is onmisbaar voor organisaties die grip willen houden op hun digitale veiligheid.

NIS2: De nieuwe wetgeving voor vitale sectoren

Met de opkomst van steeds meer geavanceerde cyberdreigingen is er behoefte aan strengere wetgeving. De NIS2-richtlijn is een Europese maatregel die gericht is op het verhogen van de digitale weerbaarheid van organisaties in vitale sectoren, en hun toeleveranciers. Grote kans dat jouw organisatie hieronder valt.

Met NIS2 worden bedrijven verplicht om meldingen te doen bij cyberincidenten, risico's aantoonbaar te beheersen en passende beveiligingsmaatregelen te nemen. Dit maakt de richtlijn niet alleen een belangrijk stuk wetgeving, maar ook een kans om de beveiliging binnen je organisatie naar een hoger niveau te tillen.

Goed om te weten. Maar hoe breng je dit allemaal het beste in kaart? Dat doe je met een Security Framework.

NIS2 Supply Chain biedt hierbij houvast: het kwaliteitslabel (in 3 verschillende niveaus) helpt je te laten zien dat je voldoet aan de wet en dat je maatregelen effectief zijn.

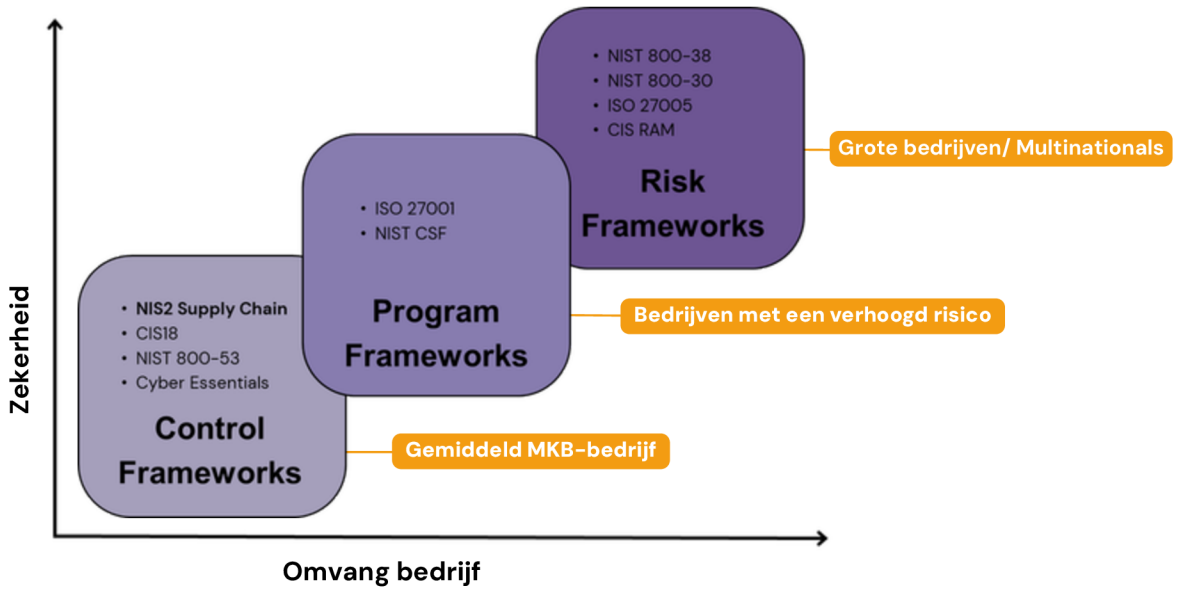
NIS2 komt eraan: Is jouw bedrijf klaar om te voldoen aan de nieuwe security eisen?

Kiezen voor het juiste Security Framework

Een Security Framework helpt je om je beveiliging goed in te richten en te behouden. Er zijn verschillende soorten frameworks, maar de belangrijkste voor de meeste organisaties zijn: **Risk Framework, Program Framework, en Control Framework.**

Microsoft kiest bijvoorbeeld voor een Risk Framework, passend bij hun enorme grootte en de risiconiveaus die zij lopen. WSB, ons eigen bedrijf, heeft gekozen voor het **Program Framework** en past de ISO 27001:2017 norm toe. Dit sluit aan bij de risico's die wij als IT-bedrijf lopen en biedt een solide basis voor beveiliging.

Voor de meeste niet-ICT-bedrijven is ISO 27001 vaak een stap te ver. Hier is een **Control Framework, zoals de NIS2 Supply Chain, de beste keuze**. Dit biedt een praktische en toegankelijke manier om aan de NIS2-richtlijn te voldoen. Het stelt je in staat om op een eenvoudige manier te bewijzen dat je voldoet aan de gestelde eisen en biedt tegelijkertijd de zekerheid van een robuuste beveiliging.



De rol van onafhankelijke audits

Ongeacht welk framework je kiest, het is belangrijk om te begrijpen dat de implementatie van een Security Framework niet stopt bij de invoering ervan. Het is essentieel om je maatregelen regelmatig te laten controleren door een onafhankelijke auditor. Deze audits garanderen dat je beveiliging niet alleen op papier goed geregeld is, maar ook daadwerkelijk effectief werkt in de praktijk. Na een succesvolle audit ontvang je een certificaat, dat je kunt gebruiken om klanten en stakeholders te tonen dat je aan de eisen van je gekozen framework voldoet.

De certificaten hebben echter een beperkte geldigheid: meestal één jaar. Na die tijd is het tijd voor een nieuwe audit en moeten eventuele verbeteringen of aanpassingen weer worden doorgevoerd. Dit zorgt ervoor dat je beveiliging altijd up-to-date en in lijn met de laatste normen blijft.

> *Een succesvolle audit levert een certificaat op en dat maakt aantoonbaar dat de juiste maatregelen zijn genomen om de beveiliging van netwerken en informatie te waarborgen.*

Conclusie

Of je nu kiest voor ISO 27001, ISO 27005, of de NIS2 Supply Chain, het belangrijkste is dat je actief werkt aan de beveiliging van je organisatie. Niet alleen om te voldoen aan de wetgeving, maar ook om je bedrijf, je klanten en je partners te beschermen tegen de steeds grotere cyberdreigingen.

Door het implementeren van de juiste normen en frameworks zorg je ervoor dat je goed voorbereid bent op de toekomst. En dat je niet alleen de wet naleeft, maar ook je digitale reputatie beschermt.

3 NIVEAUS

NIS2 SUPPLY CHAIN

“WELKE NIVEAUS KENT HET NIS2 SUPPLY CHAIN?”

NIS2 Supply Chain beoordeelt organisaties op zes gebieden: organisatorische, fysieke, mensgerichte, technologische, IT- en OT-maatregelen.

Zo wordt zichtbaar hoe volwassen je cyber security aanpak is en waar nog winst te behalen valt.

SC10

is bedoeld voor organisaties die zelf niet onder NIS2 vallen, maar wel leveren aan bedrijven die dat wel doen.

- *Gericht op organisaties met beperkte middelen of budgetten*
- *Een praktische instap, zonder zware investering*
- *Goede basis om later eenvoudig door te groeien naar SC20 of SC30*
- *Bestaat uit 17 maatregelen, waarvan veel gericht op organisatie en mens*
- *Maatwerk door risicoanalyse: alleen toepassen wat voor jou relevant is*

SC20

voor organisaties die wél onder de NIS2-richtlijn vallen, maar relatief beperkte risico’s lopen.

- *Gericht op organisaties met beperkte risico’s én budget*
- *Minimale NIS2-norm waaraan je op termijn moet voldoen*
- *Bestaat uit 19 aanvullende maatregelen bovenop het basisniveau*
- *Risicoanalyse bepaalt welke maatregelen voor jouw situatie nodig zijn*
- *OT-maatregelen alleen voor productiebedrijven*
- *IT-maatregelen alleen als je zelf software ontwikkelt of laat ontwikkelen*

SC30

voor organisaties die moeten voldoen aan alle eisen uit artikel 21 van de NIS2-richtlijn.*

- *Omvat alle verplichte maatregelen uit artikel 21*
- *In totaal 31 aanvullende maatregelen*
- *Risicoanalyse bepaalt welke maatregelen in jouw situatie relevant zijn*
- *OT-maatregelen alleen voor productiebedrijven*
- *IT-maatregelen alleen voor organisaties die software (laten) ontwikkelen*

Mark Krol

Technology & Innovation Lead

** Artikel 21 van NIS2 zegt in het kort: organisaties moeten passende technische en organisatorische maatregelen nemen om hun netwerk- en informatiesystemen te beveiligen, afgestemd op hun risico’s.*

Hoe kijkt een auditor naar cyber security?

WE VRAGEN HET AAN MARC

MARC VAN DER ZANDT IS CO-OWNER VAN SAFESECUR GROUP EN EXPERT IN INFORMATIEBEVEILIGING. HIJ VERTAALT COMPLEXE NORMEN ZOALS ISO 27001 EN NIS2 NAAR PRAKTISCHE, WERKBARE OPLOSSINGEN.

Q Wat is het belang van een cyber security-audit?

"Een cyber security-audit speelt een essentiële rol in het versterken van je organisatie. Het doel is helder: inzicht krijgen in kwetsbaarheden, verbeterpunten en eventuele risico's binnen je managementsysteem en technische maatregelen. En dat gebeurt volledig onafhankelijk.

Tijdens een audit wordt steekproefsgewijs bekeken of beleid en praktijk met elkaar overeenkomen. Staat er bijvoorbeeld in het beleid dat er dagelijks een incrementele back-up* wordt gemaakt en maandelijks een volledige? Dan moet dat technisch aantoonbaar zijn. Inclusief bewijs dat de back-ups ook daadwerkelijk werken.

Een externe blik doorbreekt bedrijfsblindheid. Iemand die tientallen organisaties per jaar ziet, herkent patronen en afwijkingen sneller. Dat helpt niet alleen om blinde vlekken bloot te leggen, maar ook om gevoelige of politieke onderwerpen bespreekbaar te maken. Zo'n audit is geen verhoor, maar juist een waardevol reflectiemoment om als organisatie sterker uit te komen."

> *Een audit brengt kwetsbaarheden én blinde vlekken aan het licht. Onafhankelijk, objectief en altijd met oog voor verbetering.*

Q Hoe werkt een audit voor NIS2 Supply Chain?

"Een audit voor NIS2 Supply Chain (SC10, SC20 of SC30) verloopt volgens een vaste structuur:

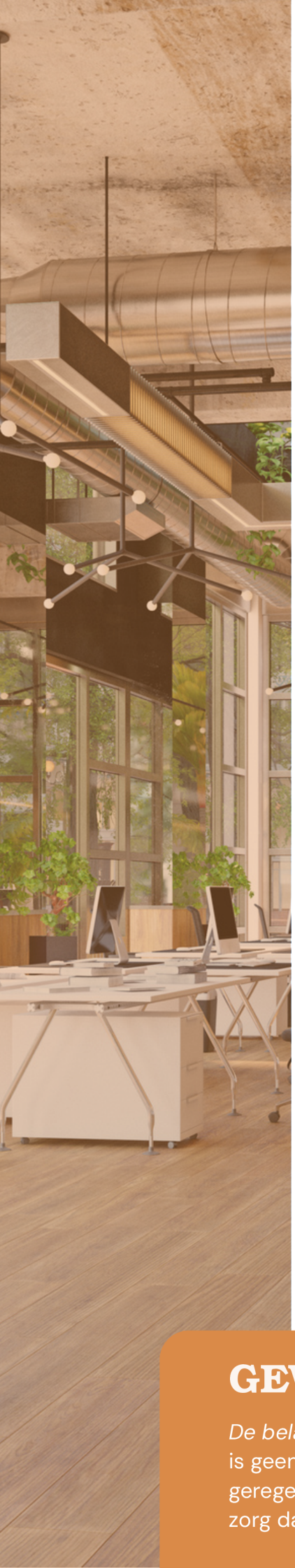
1. **Beleid bekijken** – Wat zijn de interne afspraken?
2. **Praktijk toetsen** – Wordt dat beleid ook daadwerkelijk nageleefd?
3. **Bewijs verzamelen** – Denk aan instellingen, systeemlogs of HR-documentatie.

De audits zijn opgebouwd als een groeipad: van SC10 (basismaatregelen) tot SC30 (uitgebreide, diepgaande controles). Hoe hoger je insteekt, hoe meer maatregelen er getoetst worden. Denk aan onderwerpen zoals endpoint-encryptie, netwerksegmentatie of het screenen van medewerkers.

De duur van een audit verschilt per organisatie. Voor kleine bedrijven volstaat vaak een halve dag. Grotere bedrijven met complexe IT- of OT-omgevingen kunnen rekenen op een meerdaags traject. Aan het einde volgt een eindgesprek waarin het oordeel wordt gedeeld: je voldoet, of je krijgt concrete verbeterpunten mee om alsnog aan de norm te voldoen."

Korte toelichting

** Een incrementele back-up slaat alleen de bestanden op die sinds de laatste back-up zijn gewijzigd of toegevoegd.*



Wat gebeurt er na een audit?

"Na de audit krijg je een afsluitende bijeenkomst waarin we de bevindingen bespreken. Stel je voor: je hebt alles goed gedaan, en je krijgt het Supply Chain label. Maar soms is er ook een moment waarop je nog wat dingen moet aanpassen.

Bijvoorbeeld, we hadden onlangs een situatie waarin een klant nog niet volledig voldeed aan bepaalde encryptie-eisen, maar het was duidelijk waar het misging en wat ze moesten doen om het op te lossen. Het leuke is dat als er nog verbeteringen nodig zijn, je precies weet wat je moet doen om het alsnog te behalen. Het is niet het einde van de wereld, maar een kans om sterker te worden.

Het is geen examen; het is een proces van constante verbetering."

Wat is de rol van de PDCA4YOU tool in het auditproces?

"De PDCA4YOU tool speelt een cruciale rol in het vereenvoudigen van het auditproces. Een van de grootste uitdagingen voor auditors is dat je altijd moet kunnen aantonen dat je voldoet aan alle normparagrafen. De tool biedt een oplossing voor dit probleem door het genereren van voorgestelde beleidsmaatregelen en operationele taken.

Bijvoorbeeld, als je beleid stelt dat alle apparaten met BitLocker moeten worden versleuteld, kan de tool een taak aanmaken om elke zes maanden te controleren of de encryptie op alle apparaten correct is toegepast.

Dit maakt het auditproces veel gemakkelijker voor de organisatie, omdat je niet door bergen documenten hoeft te bladeren om alles te bewijzen. Het maakt je managementsysteem niet alleen efficiënter, maar helpt je ook de juiste stappen te zetten voor verbeteringen."

Hoe werkt de begeleiding tijdens het gebruik van de PDCA4YOU tool?

"Bij WSB zetten ze alles voor je klaar in de PDCA4YOU tool, zodat jij je kunt richten op de uitvoering van de taken. Ze zorgen ervoor dat het beleid correct wordt ingesteld en alles gemonitord wordt. Jij voert de taken uit, zoals het controleren van encryptie, en zij zorgen ervoor dat alles in lijn is met de vereisten. Dit maakt het proces minder tijdrovend en zorgt ervoor dat je sneller kunt voldoen aan de auditvereisten."

Hoe vaak moet een NIS2-certificering worden geüpdatet?

"De NIS2-certificering moet jaarlijks worden geüpdatet. Als je stopt met het uitvoeren van de noodzakelijke audits, vervalt je certificering. Dit is vergelijkbaar met het ISO-certificaat: je moet je systematisch blijven verbeteren en de audits blijven uitvoeren om je certificering te behouden. Het is geen eenmalige taak, maar een doorlopend proces om je organisatie op het hoogste niveau van beveiliging te houden."

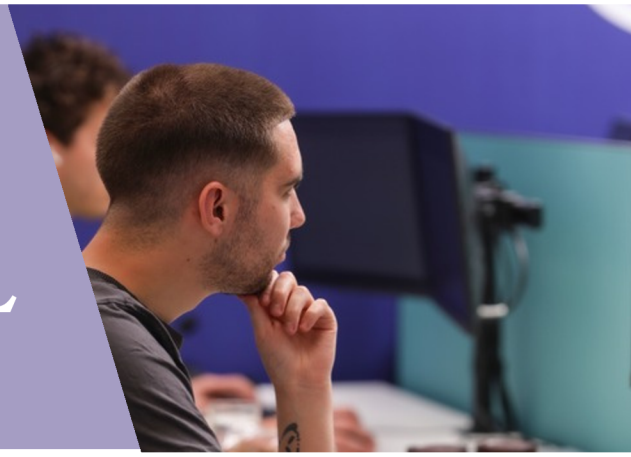
GEWOON BEGINNEN

De belangrijkste boodschap? Laat je niet afschrikken. Begin gewoon. Een audit is geen verhoor, maar een kans om beter te worden. Je hoeft niet alles perfect geregeld te hebben. Wel moet je kunnen aantonen dat je in control bent. "En zorg dat je een leuke auditor hebt," knipoogt hij tot slot, "dat helpt ook."

VAN ‘WE ZOUDEN MOETEN’ NAAR ‘WE HEBBEN GEDAAN’

Plan – Do – Check – Act

EFFICIËNT BEHEER VAN CYBER SECURITY MET DE PDCA4YOU TOOL



Wat is de PDCA4YOU Tool?

Met de PDCA4YOU tool neem jij de regie over je cyber security. Deze tool stelt jou in staat om je beveiligingsmaatregelen systematisch te verbeteren door de beproefde PDCA-cyclus (Plan-Do-Check-Act) toe te passen. Het resultaat? Niet alleen voldoe je aan de relevante wet- en regelgeving, maar je houdt je beveiliging continu op het hoogste niveau door altijd een stap voor te blijven op mogelijke dreigingen.

1. **Plan:** Bepaal je beveiligingsdoelen en stel een strategie op voor het realiseren van deze doelen.
2. **Do**: Implementeer de geplande beveiligingsmaatregelen binnen je organisatie.
3. **Check:** Evalueer en monitor de effectiviteit van je beveiligingsmaatregelen.
4. **Act:** Pas je maatregelen aan op basis van de evaluatie om de beveiliging te versterken en te optimaliseren.

Onze rol als ICT-partner

Als jouw ICT-partner zorgt WSB ervoor dat de PDCA4YOU tool naadloos wordt geïmplementeerd en volledig ingericht voor jouw organisatie.

Wij nemen het zware werk uit handen door het beleid samen met jou op te stellen en de tool te configureren, zodat jij je kunt concentreren op wat écht belangrijk is: je bedrijfsvoering beschermen en verbeteren.

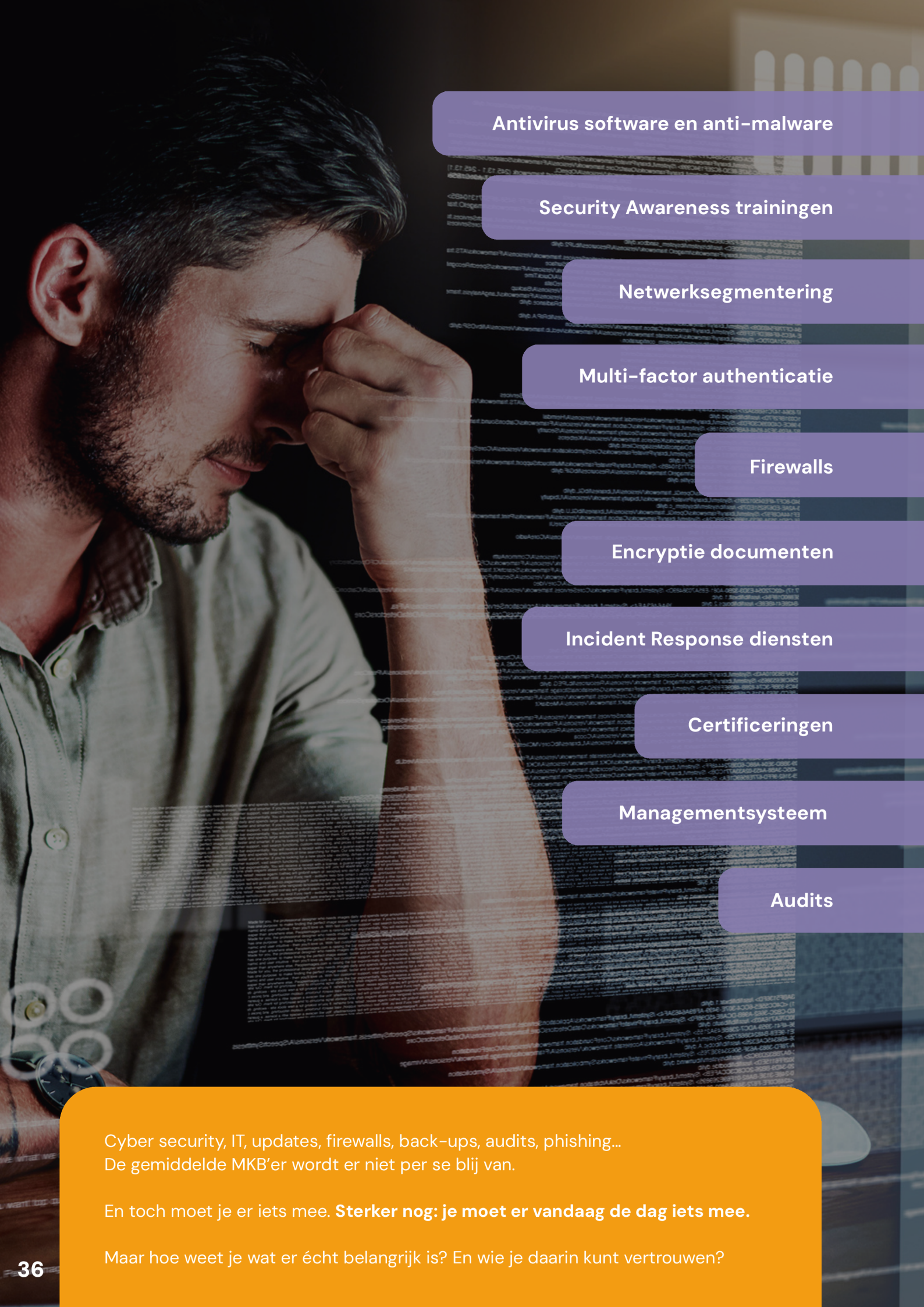
Waarom PDCA4YOU?

- **Eenvoudige integratie:** Dankzij de gebruiksvriendelijke interface kunnen organisaties eenvoudig de benodigde beveiligingsmaatregelen vastleggen, beheren en verbeteren.
- **Continue verbetering**: Het toepassen van de PDCA-cyclus zorgt voor een cultuur van voortdurende verbetering in je organisatie.
- **Compliance en Beveiliging**: De tool helpt je niet alleen te voldoen aan wet- en regelgeving, maar zorgt er ook voor dat je cybersecurity op de hoogste standaard blijft en is in te zetten om ISO-certificeringen te behalen.

Hoe werkt de tool?

PDCA4YOU maakt gebruik van een dynamische en gestructureerde aanpak om elke fase van je beveiligingsstrategie op te zetten en te monitoren. Via de tool kunnen teams hun processen beheren, taken toewijzen en snel ingrijpen als er een beveiligingsincident optreedt.

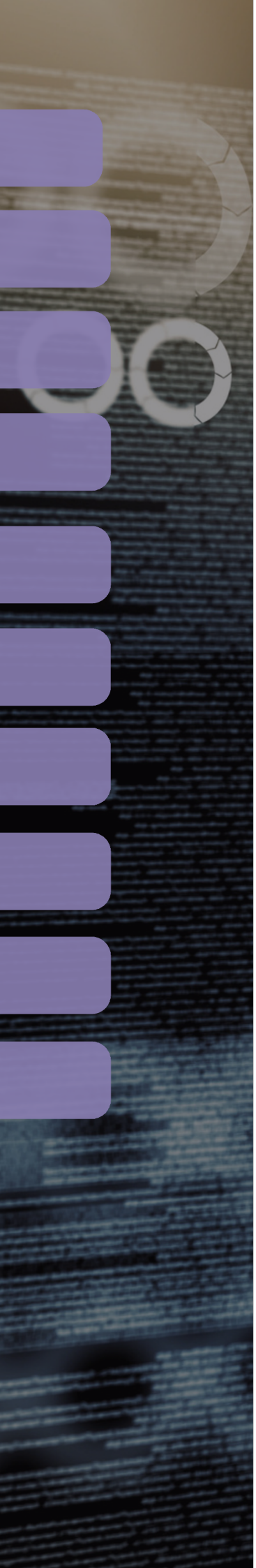
- **Beheer van beveiligingsmaatregelen:** Van technologie tot beleid, alle onderdelen van je cyber security strategie worden vastgelegd en beheerd.
- **Real-time feedback:** Krijg onmiddellijk inzicht in hoe goed je maatregelen werken, met de mogelijkheid om snel aanpassingen te maken.
- **Rapportages en analytics:** Met de ingebouwde rapportagetools kun je gemakkelijk prestaties volgen en compliance vereisen.



Cyber security, IT, updates, firewalls, back-ups, audits, phishing...
De gemiddelde MKB'er wordt er niet per se blij van.

En toch moet je er iets mee. **Sterker nog: je moet er vandaag de dag iets mee.**

Maar hoe weet je wat er écht belangrijk is? En wie je daarin kunt vertrouwen?



“WE BEGRIJPEN HET”

De wereld van IT-beveiliging is versnipperd. Er zijn tientallen losse puzzelstukken: van antivirussoftware en firewalls tot security awareness, encryptie en certificeringen.

Iedere leverancier heeft z’n eigen oplossing, taalgebruik of prioriteiten.

En dan sta jij daar, als ondernemer of IT-verantwoordelijke.
Met duizend vragen en nul tijd.

Misschien denk je:
“Kan ik dit niet gewoon zelf oplossen?”
“Begrijpen zij mijn bedrijf wel?”
“Wat als ik de controle verlies als ik een partij inschakel?”

Die twijfels zijn logisch.
Maar wij laten zien hoe je het wel kunt organiseren.

Cyber security ingewikkeld? Hoeft niet.

Wij zijn WSB. Geen helpdesk aan de andere kant van de lijn, maar een ICT-partner die met je meedenkt en jouw taal spreekt.

Geen losse tools of losse eindjes, maar één helder plan dat past bij jouw organisatie.

Eén aanspreekpunt
Eén route
Geen gedoe

We helpen je om keuzes te maken die bij je passen. Zodat jij weet waar je aan toe bent, zonder overspoeld te worden. En dat geeft ruimte. Om te ondernemen, om te focussen, om gewoon weer te doen waar jij goed in bent.

Op de volgende pagina nemen we je stap voor stap mee in onze aanpak.

Je leest hoe wij structuur brengen in je IT en cyber security,
hoe we zorgen dat je aan wet- en regelgeving voldoet,
en hoe we het voor jou vooral eenvoudig en behapbaar maken.

Geen wollig verhaal, maar een praktische route, afgestemd op jouw organisatie.

STAPSGEWIJZE AANPAK

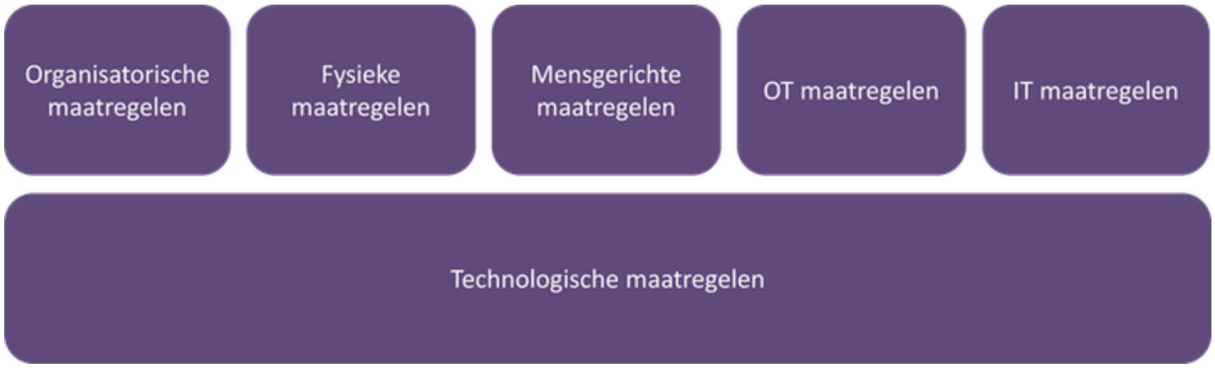
VAN CHAOS NAAR CONTROLE: JOUW ROADMAP

Je digitale beveiliging op orde

Als MKB-ondernemer weet je dat cyberveiligheid steeds belangrijker wordt. Met NIS2 wordt dit niet alleen belangrijk, maar verplicht. Gelukkig hoef je dit niet alleen te doen. Wij begeleiden je door het hele proces met onze bewezen aanpak.

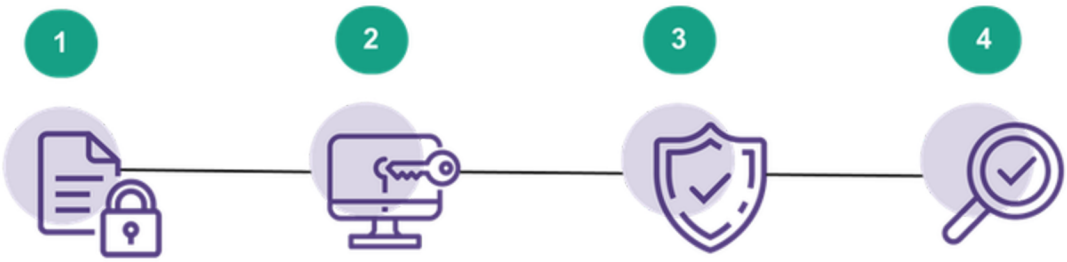
6 categorieën maatregelen. Wij regelen het allemaal.

NIS2 compliance bestaat uit maatregelen verdeeld over 6 verschillende categorieën. Afhankelijk van het NIS2 Supply Chain niveau dat je kiest (of moet behalen), neem je meer of minder van deze maatregelen. Het goede nieuws? Wij kunnen je helpen met alle benodigde maatregelen. Of je nu gewoon je beveiliging wilt verbeteren zonder NIS2, of volledig compliant wilt worden op niveau SC10, SC20 of SC30.



Technologische maatregelen: waar we beginnen.

We starten altijd met de technologische fundamenten van je beveiliging. Ons 4-stappenplan zorgt ervoor dat je IT-omgeving stap voor stap beter beveiligd wordt.



SECURITY SCAN | **BEHEER IT-OMGEVING** | **SECURITY LEVEL** | **INCIDENT RESPONSE MANAGEMENT**

ONZE AANPAK

1
STAP

SECURITY SCAN

Voordat we aan de slag gaan, willen we precies weten hoe je beveiliging er nu voor staat. Met onze uitgebreide Security Scan brengen we alle huidige beveiligings-maatregelen in kaart.

Voor nieuwe klanten is dit de startlijn. We ontdekken wat er al goed geregeld is en waar de grootste risico's liggen. Op basis van deze scan maken we een helder plan dat rekening houdt met zowel je specifieke risico's als je beschikbare budget.

Zo weet je precies welke stappen je moet gaan zetten om je beveiliging stap voor stap naar het gewenste niveau te brengen.

In deze stap installeren we monitoringsoftware op alle werk-plekken, servers en andere endpoints. Zo houden we zicht op wat er gebeurt en kunnen we zorgen dat systemen up-to-date en veilig blijven.

We voeren werkplek- en server-beheer uit op drie serviceniveaus (brons tot goud). We installeren en monitoren anti-virussoftware, voeren patchmanagement uit voor besturingssystemen en applicaties, en reageren snel op nieuwe dreigingen via Threat & Vulnerability Management (TVM).

Ook het netwerkbeheer pakken we aan: firewalls en andere netwerk-componenten worden actief gemonitord en bijgewerkt.

Daarnaast richten we een betrouwbare cloud back-up in voor servers, werkplekken en Microsoft 365. Door regelmatig hersteltests uit te voeren, weet je zeker dat je omgeving bij incidenten snel hersteld kan worden.

INRICHTEN BEHEER IT-OMGEVING

STAP
2

3
STAP

INRICHTEN SECURITY LEVEL

In deze stap richten we het gewenste securityniveau in, met als basis een uitgebreide set beveiligingsmaatregelen.

WSB biedt drie niveaus: Veilig, Extra Veilig en Super Veilig. Voor SC10/20/30 is Security Level 2 (“Extra Veilig”) vereist, gebaseerd op Microsoft 365 Business Premium.

We hanteren een vaste security baseline die we continu monitoren en twee maal per jaar actualiseren met nieuwe beveiligingsfuncties. Zo blijft de beveiliging ook op de lange termijn op niveau. Dankzij slimme tooling herstellen we afwijkingen automatisch, zodat je altijd verzekerd bent van een veilige digitale werkomgeving.

Met IT-beheer op zilver niveau én Security Level 2 voldoe je aan alle Technologische Maatregelen voor SC10. Zelfs als NIS2 (nog) niet van toepassing is.

3 LEVELS

Security Level 1 Veilig

Het minimale niveau om je bedrijf tegen cyberaanvallen te weren.

Zie het als een slot op je voordeur.

Security Level 2 Extra Veilig

Het aanbevolen niveau voor elk bedrijf dat zich wil wapenen tegen cyberaanvallen.

Zie het als een groot hek om je kantoor.

Security Level 3 Super Veilig

Het niveau wat we aanraden voor bedrijven die extra risico lopen zoals accountants.

Zie het als een 24/7 beveiligingssysteem met camera’s.

Bij afname Security Level 2 voldoe je aan de technologische maatregelen voor SC10.

STAP
4

INCIDENT RESPONSE MANAGEMENT

In de vierde en laatste stap richten we Incident Response Management in: een essentieel onderdeel om beveiligingsincidenten snel te detecteren en aan te pakken. We monitoren continu de IT-omgeving op verdachte signalen en grijpen direct in zodra dat nodig is.

WSB biedt drie niveaus van dienstverlening. De basis is de **XDR Service**, waarbij we signalen uit Microsoft Defender gebruiken om meldingen te analyseren en tijdens kantooruren op te volgen.

Bij de **MDR Essentials Service** wordt een extra detectielaag toegevoegd via een endpoint-agent, en worden incidenten 24/7 gemonitord en opgevolgd door een Security Operations Center.

Het hoogste niveau, **volledige MDR**, bevat aanvullende diensten zoals darkweb scanning, maandelijkse scans en beleid voor het blokkeren van apps, om risico's nog verder te verkleinen.

Incident Response Management is verplicht voor SC20 en SC30. Met de XDR Service voldoe je aan de minimumeis en ben je goed voorbereid op snelle respons bij dreigingen.

3 LEVELS

XDR

WSB verzorgt de monitoring en volgt incidenten binnen 8 uur op.

MDR Essentials

Een Security Operations Center met een team van speciale Security analisten volgt 24/7 proactief verdachte zaken op.
Bij een incident wordt er direct actie ondernomen.

MDR (Volledig)

Een nog uitgebreidere MDR-dienst met o.a. darkweb scanning, maandelijkse scans en beleid voor het blokkeren van apps.

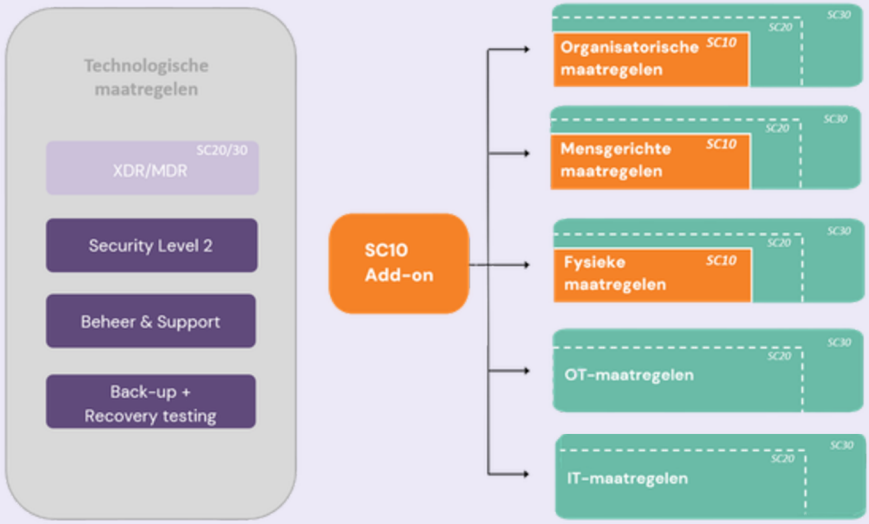
Om aan NIS2 SC20/30 te voldoen, is minimaal de XDR Service verplicht.

Waarschuwing: dit wordt een tikkeltje ingewikkeld.

In de volgende sectie gaan we dieper in op technologie en processen. Verwacht heldere uitleg, maar wel met inhoud. Want goede beveiliging is zelden simpel, maar wel cruciaal.

Voor NIS2 - SC10

Om aan NIS2 SC10 te voldoen, zijn naast technologische maatregelen ook 8 organisatorische, 1 fysieke en 3 mensgerichte maatregelen nodig. Hiervoor hebben we een SC10 Add-on: een vaste prijs, begeleiding door een Security Consultant, en ondersteuning via onze PDCA4YOU tool. Hiermee krijg je praktische voorbeelden, kun je taken verdelen en de voortgang van maatregelen volgen.

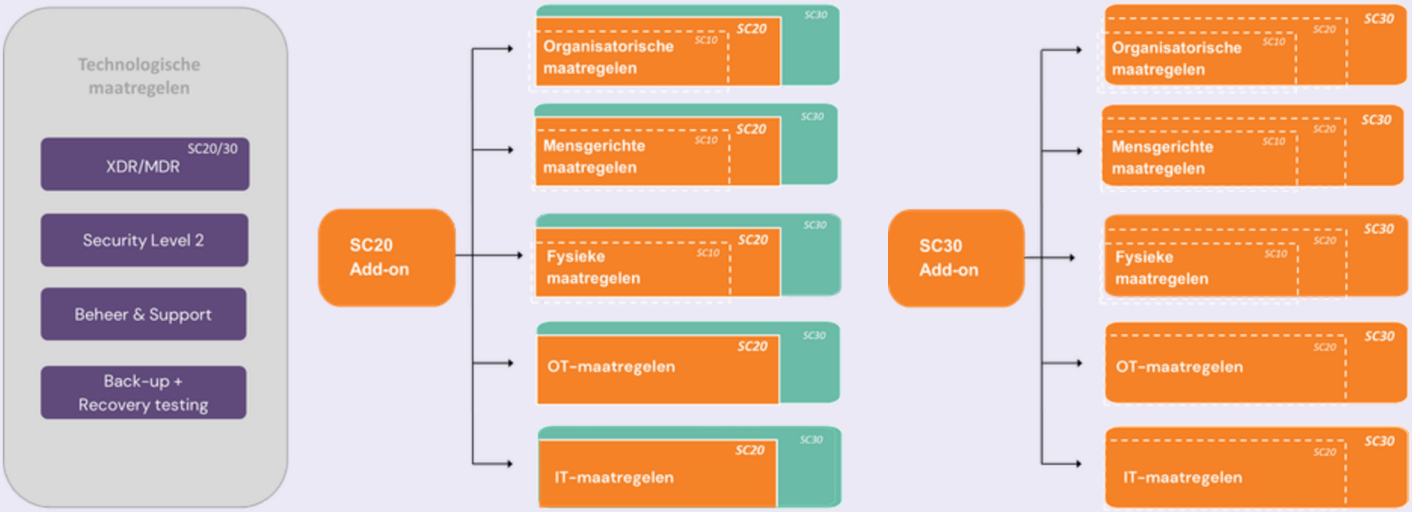


Voor NIS2 - SC20 en SC30

Voor SC20 en SC30 komen er 19 maatregelen bij bovenop de 17 van SC10, wat het totaal op 36 brengt.
Met de SC20 Add-on helpt een Security Consultant je om al deze maatregelen gestructureerd in te voeren via de PDCA4YOU tool. Deze add-on bestaat uit twee onderdelen:

1. Inrichting van aanvullende Technologische maatregelen
2. Ondersteuning bij het invullen van de overige maatregelen

Beide onderdelen worden aangeboden voor een vaste prijs. SC20 bevat ook maatregelen op het gebied van OT (voor productielijnen) en SC30 voor IT (voor softwareontwikkeling). Via een risicoanalyse bepalen we welke van deze maatregelen voor jouw organisatie relevant zijn. Zo richt je je alleen op wat echt nodig is.



“DENK NA VOOR JE KLIKT!”

Gedrag bepaalt of jouw organisatie veilig blijft.

Cybercriminelen gebruiken vaak valse e-mails, websites of berichten om je gegevens te stelen. Blijf alert. Trap er niet in.

Snelle tips:

- Deel nooit wachtwoorden of codes.
- Twijfel je? Check het e-mailadres of de link in je browser.
- Klik niet op onbekende links.

CYBER SECURITY AWARENESS TRAINING

Wat is het?

Cyber security awareness training is essentieel om je medewerkers bewust te maken van de risico's in de digitale wereld. Het doel? Ze leren malafide e-mails en verdachte links tijdig te herkennen, zodat ze een actieve rol spelen in de beveiliging van je organisatie.

Met NIS2 Supply Chain ben je verplicht om aan te tonen dat je medewerkers actief werken aan security awareness. BeveiligMij.nl, onze partner, biedt zowel klassikale als online trainingen, en phishing simulaties om medewerkers te trainen in realistische situaties. De resultaten bieden inzicht in wie extra ondersteuning nodig heeft, zodat je gerichte vervolgstappen kunt nemen.

Security awareness is geen eenmalige training, maar een doorlopend proces dat de digitale veiligheid van je organisatie versterkt.

BEVEILIGMIJ.NL
Security awareness

In 2024 was **95% van alle datalekken** het gevolg van menselijke fouten.
(Mimecast).

Tot wel 60% van de gehackte kleine en middelgrote bedrijven gaat binnen zes maanden failliet.
(National Cyber Security Alliance 2023).

Iedere dag worden er wereldwijd **600 miljoen cyberaanvallen** uitgevoerd op klanten van Microsoft.
(Microsoft Digital Defense Report 2024).

Van alle **identiteitsaanvallen** is 99% gebaseerd op wachtwoordaanvallen, zoals inloggen met gelekte wachtwoorden, password spray of phishing.
(Microsoft Digital Defense Report 2024).

Waarom je het nodig hebt

- **Mensen beïnvloeden de cyber security van je organisatie meer dan technologie of beleid.** Naast betrouwbare beveiligingssoftware moet je ook investeren in bewustwording en gedragsverandering om je IT-doelen te halen.
- Steeds meer Nederlandse overheidsinstanties **stellen cyber security training verplicht** voor hun medewerkers.
- **Verzekeraars kunnen security awareness training eisen** als voorwaarde voor dekking van cyberrisico's, ook voor het MKB.
- **Voldoen aan wet- en regelgeving** zoals de AVG, de NIS2-richtlijn en de Wet bescherming persoonsgegevens wordt eenvoudiger met een goede security awareness training.

Belangrijkste voordelen

- Maandelijks variërende thema's
- Leren in eigen tempo en locatie onafhankelijk
- Bedrijfsbreed inzetbaar voor ieder kennisniveau
- Van bewustwording naar gedragsverandering
- Toegang tot eigen rapportageplatform
- Themaposters

Q&A

MET PIETER REMERS

IN GESPREK MET CYBER SECURITY EXPERT PIETER OVER ACTUELE BEDREIGINGEN EN EFFECTIEVE AWARENESS-TRAINING

Q Wat is jouw advies als bedrijf gehackt wordt door ransomware. Betalen of niet?

"Dat is het duivelse dilemma. Ga je betalen? Dan houd je het verdienmodel van criminelen in stand. Ga je niet betalen? Dan kun je niet meer werken en ben je data kwijt. De laatste trend is dat cybercriminelen zeggen: 'Prima, jullie betalen niet, maar dan gaan we al jullie data gewoon publiceren.'

Wat je tegenwoordig veel ziet zijn bedrijven die een mediator in de arm nemen om te onderhandelen. Zorg er altijd voor dat je een specialist erbij hebt. Je moet van tevoren weten: hebben ze daadwerkelijk die gegevens en krijg je alles terug?"

Q Hoe professioneel zijn cybercriminelen tegenwoordig?

"Vroeger waren het zolderkamerhackers die puur uit vandalisme hackten.

> *Er gaat in cybercriminaliteit al jaren meer geld om dan in de hele drugscriminaliteit.*

Tegenwoordig zijn het hele serieuze bedrijven met callcenters en bitcoin-specialisten. Heb je problemen met betalen? Dan kun je gewoon rustig bellen: 'Heeft u verder nog vragen? We helpen u graag verder.' Er gaat in cybercriminaliteit al jaren meer geld om dan in de hele drugscriminaliteit."

Q Hoe gevaarlijk zijn deepfakes en AI voor cyber security?

"Het is heel eenvoudig om via AI iemands stem te klonen. Stel je voor: iemand belt naar je ouders met jouw stem waarin je in nood bent en er moet snel betaald worden. Wie zou dat niet doen?

De oplossing is een codewoord afspreken met je familie. Hetzelfde principe als met wachtwoorden. Voor bedrijven is het nog lastiger door fake nieuws en misleiding via social media."

Q Wat is het grootste probleem bij privacy?

"We hebben riskant gedrag ontwikkeld. Rond 2000 kwam iedereen massaal online. Toen was alles nieuw en spannend, maar ook onbeveiligd. Bedrijven leerden van fouten en gingen hun systemen steeds beter beveiligen.

Maar toen kwamen smartphones en social media rond 2008-2010. Plotseling deelden we weer alles: locaties, foto's, persoonlijke informatie. Alle voorzichtigheid die we hadden opgebouwd, gooiden we overboord voor gemak.

Gemak is de grootste vijand van veiligheid. Mensen willen met één klik inloggen, alles automatisch laten synchroniseren, en overal hun

gegevens delen. Het belangrijkste is dat je alert blijft en bewust keuzes maakt. Perfecte veiligheid bestaat niet, maar wees je bewust van wat je riskeert."

Q **Hoe train je mensen in cyber security awareness?**

"Het probleem is dat organisaties vaak denken dat één training voldoende is. Mensen zijn na een training heel enthousiast, maar na drie tot zes weken vallen ze terug in hun oude gedrag. Je moet cyber security awareness zien als een continu proces, niet als een eenmalige activiteit.

We beginnen laagdrempelig met wachtwoorden. Iets wat iedereen dagelijks gebruikt. Een gemiddelde Nederlander heeft veertig verschillende online accounts. Je e-mailwachtwoord is het meest cruciaal. Als iemand dat heeft, kan hij bij alle andere accounts via 'wachtwoord vergeten' functies.

Voor password managers geldt: begin klein en bouw het stap voor stap op. Ga je volgende week online bankieren? Verander dan dat wachtwoord en zet het in je password manager. Een week later doe je hetzelfde voor je LinkedIn-account of je verzekeringspolis. Op den duur wordt het een automatisme."

> *Gemak is de grootste vijand van veiligheid. Mensen willen met één klik inloggen.*

Q **Phishing simulaties. Wat is je gedachten hierover?**

"Veel organisaties zien phishing simulaties als de heilige graal, maar dat is onzin. We zijn geen voorstander van mensen lokken met cadeaus. Dat creëert wantrouwen. Wat we wel doen is mensen confronteren met realistische scenario's en een positieve meldcultuur stimuleren."

Q **Wat is je belangrijkste advies voor organisaties?**

"Richt je voor 70% op de privé-omgeving van gebruikers. Als mensen thuis veiliger gaan werken en intrinsiek gemotiveerd zijn, nemen ze dat gedrag mee naar kantoor. Het gaat niet om kennis toetsen, maar om gedragsverandering.

Cultuurverandering binnen de organisatie is het uiteindelijke doel. Een cultuur waarbij mensen durven te melden zonder zich te schamen. Denk aan de BOB-campagne, die draait 25 jaar en zit bij iedereen in het hoofd."

KERNBOODSCHAP

"Je bent waarschijnlijk geen doelwit, maar je kunt wel heel makkelijk slachtoffer worden. Blijf alert, weet waar je mee bezig bent, en als je weet dat iets een risico met zich meebrengt, wees je daar bewust van en maak dan de keuze."

CYBER SECURITY PODCAST

Episode #01

In het brein van een hacker: zo komt hij je bedrijf binnen.

Episode #02

Waarom je firewall niks waard is, als je mensen niet opletten.

Episode #03

De commerciële waarde van een veilige IT-omgeving

Duik dieper in digitale veiligheid met onze podcastserie

Cybersecurity wordt pas echt begrijpelijk wanneer je het hoort van de mensen die er dagelijks middenin staan. In onze podcastserie nemen we je mee achter de schermen van digitale veiligheid: van de denkwereld van hackers tot de kwetsbaarheden binnen organisaties en de praktische stappen die jij vandaag al kunt zetten.

Op deze pagina lichten we de eerste drie afleveringen uit. Elk met een uniek perspectief, concrete voorbeelden en inzichten die je als ondernemer of IT-professional direct verder helpen.

Ben je klaar om verder te luisteren, te leren en geïnspireerd te raken? Scan de QR-code en stap in de wereld achter cyberveiligheid.

Of klik hier

Gijs van den Berg - CFO bij Van Ballegooijen Foods

"We werken samen met WSB Solutions aan de veiligheid van onze IT- én OT-infrastructuur en zorgen tegelijkertijd dat we compliant zijn met de aankomende NIS2-wetgeving.

Door pragmatisch te focussen op wat écht belangrijk is, houden we het proces overzichtelijk en versterken we stap voor stap de continuïteit van ons bedrijf".

OOK AAN DE SLAG MET CYBER SECURITY?

"WE HELPEN JE GRAAG"

KLIK HIER

WSB Solutions
Kade 30, Hardinxveld-Giessendam
(0184) 61 88 37
info@wsb-solutions.nl
www.wsb-solutions.nl