Binnen 4 stappen van **kwetsbaar** naar **weerbaar** op cybergebied

In onderstaand stappenplan bieden we jou praktische tips om jouw doel te behalen. Wij updaten deze stappenplannen regelmatig, dus check wanneer je het download en later aan de slag gaat altijd even of het plan nog up to date is.

Twee op de tien Nederlandse bedrijven leden afgelopen jaar schade door cybercriminaliteit. Bij grote bedrijven zelfs drie op de tien. Denk hierbij aan o.a. financiële verliezen, verloren klantdata en operationele verstoringen

Toch denkt een kwart van de MKB'ers dat cybersecurity "helemaal niet lastig" is. Terwijl 85% van hen ooit een cyberincident heeft meegemaakt. Ze vertrouwen op een firewall en antivirussoftware, maar detectie van inbraken? Een herstelplan? Die ontbreken in veel gevallen. Het gevaar zit vooral in het blind vertrouwen van de genomen beschermingsmaatregelen. Dat je geen cyberincidenten hebt gehad wilt niet zeggen dat je goed beschermd bent, al lijkt dat vaak wel zo.

Waar moet je verder rekening mee houden? De introductie van de NIS2 gaat ervoor zorgen dat grote klanten strenge eisen gaan stellen aan hun leveranciers. En de ontwikkeling van AI zorgt ook voor steeds slimmere cyberaanvallen.

Het is tijd om je digitale weerbaarheid serieus te nemen. Wij helpen je daarmee.

1 Stap 1: Breng in kaart waar criminelen naar op zoek zijn

Weet wat je moet beschermen
De eerste stap is kijken naar wat je precies moet beschermen. Niet alles in je bedrijf is even waardevol voor criminelen. Focus op wat écht telt.

Je digitale kroonjuwelen:

1. **Klantgegevens:** namen, adressen, betaalgegevens en je CRM
2. **Financiële systemen:** boekhouding, banktoegang
3. **Inloggegevens medewerkers:** wachtwoorden, pincodes
4. **Operationele systemen:** productie, communicatie, monitoring intellectueel eigendom

Bekijk voor elk systeem: wat gebeurt als het een dag plat ligt? Wat als data op straat komt te liggen? Hoeveel kosten de herstelwerkzaamheden?

Scan je zwakke plekken
Nu je weet wat waardevol is, wordt het tijd om te kijken hoe goed het beschermd is. Met onze cyberrisicoscan krijg je snel inzicht in je belangrijkste kwetsbaarheden.

Dit zijn enkele van de meest onderschatte risico's:

- Verouderde software
- Gebrekkig toegangsbeheer
- Leveranciers met systeemtoegang
- Back-ups op hetzelfde netwerk
- Zwakke wachtwoorden

MKB-bedrijven richten zich vaak op technische beveiliging zoals firewalls en antivirussoftware. Die zijn erg belangrijk, maar ook een back-up of herstelplan is cruciaal om de continuïteit van jouw organisatie te waarborgen.

Direct aan de slag:
Doe onze cyberrisicoscan

2 Stap 2: Bouw je digitale verdedigingsmuur

De basis moet op orde
Tijd voor actie. En nee, dat betekent niet meteen de duurste beveiligingssoftware kopen. Het betekent slim investeren in maatregelen die écht werken voor jouw situatie.

De onmisbare basis voor elk MKB-bedrijf:

- **Multi-factor authenticatie:** overal waar het kan, vooral bij banktoegang en admin-accounts
- **Automatische updates:** zet ze aan voor alle software, vooral Windows en Office
- **Aparte back-ups:** offline of in een andere cloud, dagelijks voor kritieke data
- **Toegangsbeheer:** medewerkers hebben alleen toegang tot systemen die ze nodig hebben voor hun taken
- **Endpoint protectie:** veel cyberaanvallen beginnen bij medewerkers, denk aan email bijlagen met malware.

Dit klinkt misschien technisch, maar het is de basis waarmee je jouw bedrijf digitaal beschermt. Dit kun je met je IT-leverancier bespreken.

Liever direct met een expert aan tafel? Onze cyber experts helpen je graag op weg.

Meer dan alleen preventie
Vrijwel alle bedrijven met personeel zijn ooit slachtoffer of doelwit geweest. De vraag is niet of je aangevallen wordt, maar wanneer. Verder gaan dan de basis is daarom nooit een slecht idee.

Deze vijf quick-wins kun je vandaag nog regelen:

- Schakel twee-staps-verificatie in op alle belangrijke accounts
- Installeer een wachtwoordmanager voor het hele team
- Plan een hacktest om je zwakke plekken te vinden
- Voorkom dat medewerkers zelf software kunnen downloaden en installeren.
- Test je back-ups. Lukt het om ze terug te zetten? En hoe lang duurt dat?

De grootste uitdaging voor MKB'ers? De snelheid waarmee nieuwe dreigingen opduiken. Meer dan de helft van de bedrijven noemt dit als grootste probleem.

Daarom kiezen steeds meer bedrijven voor managed security services. Laat experts meekijken, zodat jij je kunt focussen op ondernemen.

Direct aan de slag:
Plan een intake met een cyber expert
Download onze cyber voor MKB brochure

3 Stap 3: Maak je team cyberbewust

Medewerkers zijn favoriet doelwit
Harde waarheid: veel cyberaanvallen ontstaan door menselijke fouten. Die dure firewall? Die sterke wachtwoorden? Geen van beiden voorkomt dat malware wordt geïnstalleerd als medewerkers bijlagen met malware openen of op een link klikken die hen leidt naar een malafide website waarop ze hun inloggegevens intikken.

Phishingmails zijn met 52% de meest voorkomende aanval. De groeiende populariteit van AI zorgt ervoor dat deze mails ook steeds persoonlijker en dus gevaarlijker realistischer worden. Geen of weinig spelfouten komen niet meer voor en zelfs de toon van je vaste leverancier kan nagebootst worden.

Preventie is belangrijker dan ooit:

1. Herken phishing: check altijd het afzenderadres, klik niet zomaar op links
2. Een uniek wachtwoord per account, stimuleer het gebruik van een wachtwoordmanager
3. Creëer een meldcultuur: liever tien keer vals alarm dan één keer te laat
4. Blokkeer de toegang tot valse websites zodra die gemeld zijn door een medewerker
5. Geen privémail op de bedrijfslaptop

Maak cybersecurity leuk
Niet iedereen wordt enthousiast van een security training, maar je kunt het ook uitdagend maken. Organiseer bijv. de maandelijkse "phishing-loterij" waarbij degene die de meeste phishingmails correct meldt een kleine prijs wint.

De psychologie van cyberveilig gedrag:

- **Maak het makkelijk:** één klik om verdachte mails te melden
- **Beloon goed gedrag:** vier successen publiekelijk
- **Geen blame-cultuur:** fouten maken mag, niet melden niet
- **Herhaal de boodschap:** zet bijv. ieder kwartaal een ander cybersecurity thema in de spotlight
- **Maak het persoonlijk:** wat als jouw privégegevens op straat liggen?

Ondanks de pogingen om het "leuk" te maken, blijft cybersecurity een serieus onderwerp. Naast de algemene awareness is het goed om ook voor specifieke, "kwetsbare" functies extra training te bieden, zoals bijvoorbeeld de boekhouding afdeling.

4 Stap 4: Bereid je voor op een cyberincident

Wees realistisch:
Met maar liefst 85% van de MKB-bedrijven die al eens een incident heeft gehad, is een goed actieplan geen overbodige luxe.
Een goed Cyber Response Plan is als een brandblusser. Je hoopt hem nooit nodig te hebben, maar als het misgaat ben je blij dat hij er is.

Wat staat er in zo'n response plan?

1. **Detectie:** wie merkt de aanval op en hoe meld je dit?
2. **Isolatie:** hoe voorkom je dat het erger wordt?
3. **Communicatie:** wie informeer je wanneer (intern en extern)?
4. **Herstel:** hoe zet je systemen terug en test je of ze veilig zijn?
5. **Evaluatie:** wat leren we hiervan voor de volgende keer?

Vul het in met je team. Print het uit. Leg het in de la van elke leidinggevende.

En belangrijker: oefen het minimaal één tot twee keer per jaar.

De eerste 6 uur
75% van mkb-bedrijven kan binnen 6 uur reageren. Maar naast snelheid moet je ook de goede stappen zetten.

Doe het volgende:

- Isoleer getroffen systemen
- Controleer of de backup veilig is
- Maak screenshots
- Noteer wat er is gebeurd
- Bel je cyberverzekeraar
- Waarschuw IT-partners
- Informeer management

Ook met het oog op de aankomende NIS2 moet je dit op orde hebben.

Verzeker de potentiële klap
Een incident kost gemiddeld €270.000. Soms draait dat uit op een faillissement.

De juiste verzekering kan daarom het verschil maken. Deze dekt bijv. de herstelkosten van ransomware, forensisch onderzoek, juridische kosten, omzetverlies en eventuele schadeclaims van klanten.

Direct aan de slag:
Download de NIS2 praktijkgids

Van afwachten naar aanpakken

Cybersecurity is geen IT-probleem. Het is een bedrijfsrisico. Criminelen scannen massaal en automatisch. Ze zoeken de makkelijkste prooi, dus zorg dat jij dat niet bent.

De grootste valkuilen voor MKB bedrijven:

- Denken dat je te klein bent
- Alleen preventie, geen detectie
- Onderschatten menselijk risico
- Geen plan voor incidenten
- Wachten tot het gebeurt

Begin vandaag. Het beste moment om maatregelen te nemen was gisteren. Het op-één-na beste is nu.

Meer over cybersecurity:

- Lees Cybertrends 2025: alle cijfers
- Bekijk onze webinars: specifiek per sector
- Download de NIS2 gids

Zelf aan de slag:

- Doe de Cyberrisicoscan: krijg inzicht in 5 minuten
- Download Cyber Response Plan: wees voorbereid
- Download Employee Awareness: train je team

In gesprek met de experts:

- Bekijk Cybersecurity voor het MKB
- Plan adviesgesprek: persoonlijk advies van een expert

Klaar om de eerste stap te zetten?

Onze cyberexperts helpen je graag in kaart brengen waar jij de meeste meters kan maken.

Plan een vrijblijvend gesprek in →

Of bekijk onze MKB-oplossing

Wij horen graag je mening

Dit document is, na onderzoek, samengesteld met onze interne experts.
Uiteraard horen wij graag of het document je geholpen heeft en of je nog bepaalde dingen mist.

Laat je ons weten wat je ervan vindt?

Geef feedback