

# Cybersecurity assessment: Hoe u uw bedrijf veilig houdt

60 Procent van de mkb-bedrijven die een cyberaanval hebben meegemaakt, sluit binnen zes maanden de deuren. Check daarom welke securitymaatregelen bij uw bedrijf in orde zijn en welke niet. Gebruik daarbij deze Cybersecurity Assessment, onze eenvoudige checklist van zeven stappen. Met deze lijst weet u waar u op moet letten en hoe u uw bedrijf kunt beschermen.

## Meer weten?

Praat verder met onze adviseurs.  
[Bel, chat of maak hier een afspraak.](#)





# 1

## Bepaal de 'scope'

- Bepaal welk deel van uw bedrijf u wilt beoordelen: de hele organisatie, 'remote' teams, de toeleveringsketen of een specifiek systeem.
- Maak een lijst van de betrokken personen, processen, technologieën en derde partijen.
- Maak duidelijk wat wel en niet binnen de scope valt, zodat u niets vergeet.

# 2

## Identificeer en prioriteer uw assets

- Maak een lijst van alle bedrijfskritische apparaten: laptops, telefoons, servers, routers, enz
- Neem ook cloud platforms, e-mailsystemen en software op waar uw team dagelijks mee werkt.
- Geef alles aan wat gevoelige gegevens opslaat, verwerkt of opent.
- Rangschik ze op basis van hoe essentieel ze zijn of hoe schadelijk het zou zijn om ze te verliezen.

# 3

## Breng de risico's in kaart

- Identificeer mogelijke bedreigingen: phishing, malware, zwakke wachtwoorden, menselijke fouten, inbreuken op de toeleveringsketen.
- Stel voor elk bedrijfsmiddel de volgende vragen: wat is het risico? Hoe groot is de kans dat het zich voordoet? Wat zou de impact zijn?
- Benadruk uw grootste kwetsbaarheden. Waarschijnlijk: welke de grootste impact hebben.

### Meer weten?

Praat verder met onze adviseurs.  
[Bel, chat of maak hier een afspraak.](#)

# 4

## Controleer uw huidige beveiliging

- Controleer of uw antivirussoftware, firewalls, toegangscontroles en versleutelingshulpmiddelen actief en up-to-date zijn.
- Controleer de processen voor gegevensback-up en hoe snel u kunt herstellen van een verlies van data.
- Evalueer de training van uw medewerkers. Weten zij hoe ze bedreigingen kunnen herkennen en erop moeten reageren?

# 5

## Controleer de risico's van leveranciers en partners

- Maak een lijst van leveranciers, aannemers of dienstverleners die toegang hebben tot uw systemen of gegevens.
- Beoordeel bij elk van hen of ze aan uw beveiligingsverwachtingen voldoen.
- Controleer alle contracten en SLA's en zorg ervoor dat ze duidelijke beveiligingseisen bevatten.



# 6

## Stel uw actieplan op

- Stel een duidelijke lijst met prioriteiten op, te beginnen met snel te realiseren verbeteringen en risico's met een grote impact.
- Wijs taken toe aan mensen en stel een tijdschema op voor duidelijke verantwoordingsplicht.
- Controleer de voortgang met regelmatige check-momenten.

### Meer weten?

Praat verder met onze adviseurs.  
[Bel, chat of maak hier een afspraak.](#)



# 7

## Test uw reactieplan

- Voer een simulatie of een nepcyberaanval uit om te zien hoe uw team reageert.
- Controleer of uw incidentplan in het echt werkt en of iedereen weet wat te doen, wanneer dat te doen en wat er daarna gebeurt.
- Zorg ervoor dat back-ups, contactlijsten en responsrollen actueel en toegankelijk zijn.
- Pas het plan indien nodig aan.

## Klaar om van reactief naar proactief te gaan?

Cybercriminelen worden steeds geavanceerder en bedreigingen veranderen voortdurend. Het is dus essentieel om een stap voor te blijven.

Door deze checklist regelmatig door te nemen, kunt u zwakke plekken vroegtijdig opsporen, compliant blijven en betere bescherming inbouwen in uw dagelijkse activiteiten.

Hulp nodig om aan de slag te gaan? Neem contact op met [onze adviseurs](#) voor gratis persoonlijke ondersteuning.

### Meer weten?

Praat verder met onze adviseurs.  
[Bel, chat of maak hier een afspraak.](#)

# Meer hulp nodig bij het opstellen van een cyber- beveiligings- risicobeoordeling?

Onze adviseurs staan voor u klaar.  
Bel, [chat](#) of maak hier een afspraak.