Formulier: Cybercrime risicoanalyse voor MKB'ers

Uit naam van Digiweerbaar.nl

Bedrijfsgegevens

Bedrijfsnaam: _____

Contactpersoon: _____

E-mailadres: _____

Telefoonnummer: _____

1. Inventarisatie bedrijfsmiddelen en data

Geef een overzicht van de belangrijkste bedrijfsmiddelen en data die potentieel kwetsbaar zijn voor cyberaanvallen. Geef per item aan of het kritiek is voor de bedrijfsvoering (Ja/Nee).

Bedrijfsmiddel/Data	Kritiek (Ja/Nee)

2. Identificatie cyberdreigingen

Geef een overzicht van de belangrijkste cyberdreigingen waaraan uw bedrijf blootstaat. Geef per dreiging aan wat de potentiële gevolgen zijn voor uw bedrijf.

Cyberdreiging	Potentiële gevolgen

3. Analyse bedrijfskwetsbaarheden

Geef een overzicht van de voornaamste kwetsbaarheden van uw bedrijf die cybercriminelen kunnen uitbuiten.

Kwetsbaarheid	Beschrijving

4. Risicoscore toekennen

Ken een risicoscore toe aan elk van de geïdentificeerde dreigingen en kwetsbaarheden op een schaal van 1 (laag risico) tot 5 (hoog risico).

Dreiging/Kwetsbaarheid	Risicoscore (1-5)

5. Implementatie beveiligingsmaatregelen

Geef een overzicht van de beveiligingsmaatregelen die u wilt implementeren, gebaseerd op de risicoscores. Geef per maatregel aan wat de verwachte implementatiedatum is.

Beveiligingsmaatregel	Verwachte implementatiedatum

6. Evaluatie en updates

Plan regelmatige evaluatiemomenten voor uw cybercrime risicoanalyse. Geef per evaluatiemoment de verwachte datum en eventuele actiepunten aan.

Evaluatiemoment	Verwachte datum	Actiepunten

7. Externe hulp

Indien u externe hulp overweegt, geef dan de contactgegevens van de externe partij en de diensten die zij zullen verlenen.

Naam externe partij: _____

Diensten: _____

E-mailadres: _____

Telefoonnummer: _____

8. Ondertekening

Datum: _____

Handtekening: _____

Naam: _____

Functie: _____

Dit formulier helpt u om een overzichtelijke cybercrime risicoanalyse op te stellen voor uw MKB-bedrijf. Door alle onderdelen zorgvuldig in te vullen en regelmatig te evalueren, zorgt u ervoor dat u altijd op de hoogte bent van de belangrijkste cyberdreigingen en kwetsbaarheden die uw bedrijf kunnen treffen.

Zodra u uw risicoanalyse hebt voltooid, is het belangrijk om actie te ondernemen en de geplande beveiligingsmaatregelen te implementeren. Houd er rekening mee dat de digitale wereld voortdurend verandert en dat het noodzakelijk is om uw risicoanalyse periodiek bij te werken om te zorgen voor de meest effectieve bescherming tegen cyberdreigingen.

Als u vragen heeft of hulp nodig heeft bij het invullen van dit formulier, aarzel dan niet om contact op te nemen met Digiweerbaar.nl. Wij kunnen u adviseren en begeleiden bij het uitvoeren van een grondige risicoanalyse en het implementeren van effectieve beveiligingsmaatregelen voor uw bedrijf.

Digiweerbaar.nl - Samen werken aan een veiligere digitale omgeving voor het MKB.