

DE CYBERHEALTHCHECK

STOOM JOUW ONDERNEMING KLAAR VOOR EEN GOEDE CYBERVEILIGHEID



Cybermindset

Integreer cyber-basisbegrippen in visie, missie en doel. Ken je digitale kernactiviteiten. Bepaal impact cyber-aanval op jouw bedrijf en reputatie.

Risicoanalyse

Inventariseer activa: mensen, kennis infrastructuur en technologie, processen en procedures, ... Focus op kernactiviteiten - hoe risico's indekken?

Back up

Bewaar data centraal. Sync naar meerdere plaatsen. Beveilig back-ups. Voorzie offline back-up. Test regelmatig je back-ups.

Check ook je partners

Welke maatregelen nemen zij? Bepaal contractueel, het recht om dit te controleren (right to audit). Controleer hun cyberreputatie (cfr financiële en beveiligings-doorlichting)

1

2

3

4

5

6

7

8



Verhoog jouw cyberkennis

Blijf op de hoogte via verschillende bronnen. Overleg binnen de sector. Evalueer medewerkers. Leg de cyber-lat voldoende hoog.

Cyberbudget

Bepaal het budget i.f.v. continuïteit kernactiviteiten. Focus op enkele maatregelen. Bepaal totale kost bij aanval. Cyber-verzekering afsluiten.

Loopt het toch fout?

Werk op voorhand een noodplan uit. Bewaar offline contactlijsten. Sluit op voorhand een contract af met cyber-experten. Contacteer "Cert.be".

Continue evalueren = blijven leren

Verbeter continue. Analyseer nieuwe activiteiten. Volg trends in technologie, medewerkers, bedreigingen. Verifieer regelmatig bestaande maatregelen. Bepaal focus next steps.