Weerbaarheidscheck

15-minuten

Versie 1.0

CYBERBUSTERS B.V.

Hoe gebruik je deze check?

Beantwoord onderstaande 15 vragen eerlijk voor uw organisatie. Ken per vraag de volgende punten toe:

- **Ja** = 2 punten
- **Deels** = 1 punt
- **Nee** = 0 punten

De 15 Praktische Vragen

Vraag	Antwoordopties	Score
1. Is er een actueel en getest incident response plan aanwezig?	Ja = 2 pt Deels = 1pt Nee = 0 pt	
2. Weten medewerkers bij wie ze een (vermoedelijk) cyberincident direct moeten melden?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
3. Zijn de contactgegevens van externe experts (zoals IT-leverancier, cybersecurity partner en verzekeraar) direct beschikbaar?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
4. Worden er regelmatig back-ups gemaakt die offline of geïsoleerd worden bewaard?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
5. Is het herstellen van back-ups recentelijk getest op werking en snelheid?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
6. Is Multi-Factor Authenticatie (MFA) verplicht voor alle kritieke systemen en accounts?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
7. Worden beveiligingsupdates en patches automatisch of binnen korte tijd doorgevoerd?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
8. Krijgen medewerkers periodiek training over cyberrisico's zoals phishing en social engineering?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	

Vraag	Antwoordopties	Score
9. Is er een helder protocol voor het isoleren van besmette apparaten of netwerken bij een incident?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
10. Zijn de rechten en toegang van medewerkers beperkt tot wat noodzakelijk is voor hun functie (Least Privilege)?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
11. Is er zicht op alle apparaten en systemen die verbonden zijn met het bedrijfsnetwerk?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
12. Zijn er afspraken en protocollen voor communicatie naar klanten en leveranciers tijdens een crisis?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
13. Is bekend welke wettelijke meldplichten (zoals Autoriteit Persoonsgegevens) van toepassing zijn en binnen welke termijn?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
14. Worden kritieke bedrijfsprocessen en data regelmatig in kaart gebracht en gecategoriseerd op risico?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	
15. Evalueert en herziet de organisatie het cybersecuritybeleid na elk incident of minimaal jaarlijks?	Ja = 2 pt Deels = 1 pt Nee = 0 pt	

Uw Score

- **26–30 punten:** Weerbaar, uw organisatie heeft een uitstekende basis en weet wat te doen als het misgaat.
- **16–25 punten:** Gemiddeld, er zijn goede stappen gezet, maar er blijven cruciale kwetsbaarheden bestaan.
- **0–15 punten:** Kwetsbaar, directe actie is vereist om de continuïteit van uw organisatie bij een incident te waarborgen.

Disclaimer: Deze weerbaarheidscheck maakt onderdeel uit van een bredere inventarisatie en vervangt geen volledige audit of diepgaande risicoanalyse.

Wil je eens sparren over waar de grootste risico's of verbeterpunten zitten? Neem gerust contact op via: https://cyber-busters.com/contact