Check: Hoe proactief is uw cybersecurity-advies?

Cybercriminelen gaan steeds verfijnder ter werk – mede dankzij kunstmatige intelligentie. Toch denken veel mkb'ers: mij slaan ze wel over. Ten onrechte. Dus hoe start u het gesprek over cybersecurity? Met de volgende tips zet u cyber hoger op de agenda van uw relaties.

1 Risicobewustzijn creëren

- ☐ Informeer mijn relatie over cyberrisico's, ongeacht bedrijfsgrootte.
- ☐ Corrigeer misvattingen, zoals dat alleen grote bedrijven doelwit zijn.
- ☐ Verhoog bewustzijn over aanvallen in de sector van de relatie.

2 Eerste beveiligingscheck

- ☐ Vraag naar basismaatregelen zoals back-ups, antivirus en firewalls.
- ☐ Moedig evaluaties van de huidige cybersecuritystatus aan.

3 Medewerkerstraining

- ☐ Bespreek het belang van cybersecuritytraining om phising en andere bedreigingen te herkennen.
- ☐ Adviseer specifieke trainingen voor alle medewerkers.

4 Beveiliging in de praktijk

- ☐ Benadruk het belang van sterke wachtwoorden, twee-factor-authenticatie en systeemupdates.
- ☐ Onderstreep het belang van regelmatige back-ups en offline bewaren.

5 Inzicht in gevolgen en kosten

- ☐ Bespreek financiële en operationele gevolgen van cyberaanvallen.
- ☐ Vermeld het risico van klantvertrouwenverlies.

6 Gebruik van diagnostische tools en assessments

- ☐ Gebruik tools zoals Risicoklassenindeling Digitale Veiligheid en Cyber Assessment van Avéro Achmea.
- ☐ Identificeer kwetsbaarheden met hacktests.