Zelfscan 10 cruciale vragen om uw risico te bepalen

Gebruik deze ja/nee-vragen om te beoordelen hoe goed uw bedrijf is beveiligd:

1. Heeft u uw maximaal aanvaardbare downtime en financiële schade in kaart gebracht?
2. Heeft u een actueel informatiebeveiligingsbeleid?
3. Zijn al uw software en systemen up-to-date?
4. Worden er regelmatig back-ups gemaakt en worden deze actief getest?
5. Zijn uw medewerkers getraind in het herkennen van o.a. phishing?
6. Zijn alle systemen voorzien van next-gen endpoint protectie / EDR / firewall?
7. Heeft u een incident response plan (IRP)?
8. Worden uw netwerken en systemen regelmatig gecontroleerd op kwetsbaarheden?
9. Heeft u inzicht in wie wanneer toegang heeft tot welke systemen?
10. Heeft u uw IT-omgeving wel eens laten testen door een onafhankelijke deskundige?

Bonusvraag:
Heeft u als eindverantwoordelijke bij het beantwoorden van vragen aannames gedaan?
Zo ja, plan eens een **vrijblijvende brainstormsessie** in met één van onze experts!

Hoe meer **“nee”-antwoorden**, hoe groter uw risico!