CYBERBEVEILIGING VOOR KLEINERE FINANCIËLE ORGANISATIES

CEO CHECKLIST: LEIDERSCHAP IN CYBERBEVEILIGING

BESTUUR

- ☐ Wijs een Chief Information Security Officer (CISO) aan als dit nog niet is gebeurd.
- ☐ Stel op basis van internationale, nationale en industrienormen en -richtlijnen een organisatiebreed, risicogebaseerd cyberbeveiligingsbeleid op en pas dit toe.
- ☐ Definieer rollen en verantwoordelijkheden voor alle medewerkers die betrokken zijn bij cyberbeveiliging. Werk samen met de CISO om de juiste cyberbeveiligingsrollen en toegangsrechten voor alle personeelsniveaus vast te stellen.
- ☐ Zorg ervoor dat u duidelijke communicatiekanalen hebt tussen verschillende eenheden of medewerkers die over verschillende aspecten van cyberbeveiliging gaan.
- ☐ Zorg ervoor dat de CISO weet bij wie hij moet zijn om u en de raad van bestuur tijdig op de hoogte te brengen van dreigingen.
- ☐ Vraag de CISO of ander technisch personeel om het senior management geregeld te briefen.
- ☐ Zorg ervoor dat het cyberbeveiligingsbeleid, normen en mechanismen uniform zijn binnen de hele organisatie.

RISICOBEOORDELING EN -BEHEER

- ☐ Voer in samenwerking met uw CISO of ander technisch personeel een cyberbeveiligingsrisicobeoordeling uit, die het volgende omvat:
  - Beschrijven van de activa van uw organisatie en de mate waarin deze afhankelijk zijn van technologie,
  - Beoordelen van de volwassenheid van uw organisatie en de inherente risico's die aan de technologische afhankelijkheid van haar activa kleven,
  - Bepalen van de gewenste volwassenheid van uw organisatie,
  - Begrijpen waar cyberdreigingen in de lijst met risicoprioriteiten van uw organisatie staan,
  - Vaststellen in hoeverre uw huidige cyberbeveiligingsstatus overeenkomt met de gewenste doelstatus,
  - Implementeren van plannen om volwassenheid te bereiken en in stand te houden,
  - Voortdurend opnieuw evalueren van de volwassenheid, risico's en doelen van uw organisatie op het vlak van cyberbeveiliging, en
  - Overwegen om beveiligingsmaatregelen te nemen, zoals de aanschaf van een cyberverzekering.
- ☐ Analyseer de resultaten en presenteer deze aan belangrijke belanghebbenden en de raad van bestuur.
- ☐ Houd toezicht op alle stappen, zodat de organisatie beter op cyberdreigingen kan reageren, en monitor de voortgang.

ORGANISATIECULTUUR

- ☐ Bespreek cyberrisico's en beveiliging regelmatig op leiderschapsniveau.
- ☐ Geef alle nieuwe medewerkers een cyberbeveiligingstraining en laat alle medewerkers documenten ondertekenen waarin ze toezeggen het cyberbeveiligingsbeleid van de organisatie na te leven.
- ☐ Laat alle medewerkers periodiek cyberbeveiligingstrainingen volgen.
- ☐ Zorg ervoor dat uw organisatie cyberbeveiliging altijd laat meewegen bij de keuze van potentiële leveranciers en het delen van gegevens met derden.
- ☐ Beoordeel jaarlijks het cyberbeveiligingsbeleid van uw organisatie.
- ☐ Moedig technisch personeel aan om vrijwillig informatie uit te wisselen over cyberdreigingen en incidenten.