Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

CYBERSECURITY HEALTH CHECK

- MIDDELGROTE BEDRIJVEN -

CSR Cyber Security Raad

IDENTIFICATIE

- ☐ Is de verantwoordelijkheid voor cybersecurity binnen de directie belegd en wordt cybersecurity periodiek binnen de directie besproken?
- ☐ Is binnen uw organisatie inzichtelijk wat uw belangrijkste kroonjuwelen zijn (webshop, operationele en financiële data, persoonsgegevens klanten) en wat het effect van een cyberaanval op deze kroonjuwelen kan zijn?
- ☐ Zijn de belangrijkste cyberrisico's en -dreigingen in kaart gebracht en worden deze periodiek geëvalueerd vanuit een strategisch, financieel, operationeel, reputatie en compliance (bv. AVG) perspectief inclusief derde partijen?

Risico
De relevante dreigingen worden niet onderkend. Daardoor is onduidelijk aan welke risico's het bedrijf wordt blootgesteld en welke maatregelen moeten worden genomen.

BESCHERMING

- ☐ Scholen uw medewerkers zich tenminste jaarlijks bij, om op de hoogte te blijven van recente ontwikkelingen en 'do's & don'ts' op securitygebied voor hun functie (zowel IT als non-IT)?
- ☐ Zijn de volgende basis IT-hygiënemaatregelen op orde bij zowel u als eventuele derde partijen:
  - patch management (bijwerken, testen en installeren van software);
  - toegangsbeheer (incl. intrekken toegang van gebruikers na functiewisseling of - beëindiging);
  - het maken van back-ups.

  Worden deze periodiek uitgevoerd en wordt de effectiviteit ervan regelmatig getest?
- ☐ Heeft uw organisatie effectieve maatregelen in gebruik voor netwerksegmentatie, endpoint security, en (D)DoS-mitigatie. Zijn systemen voldoende robuust en wordt gebruik gemaakt van 2FA (bv: wachtwoord en code via SMS) voor authenticatie op gevoelige systemen?

Risico
Een aanvaller krijgt voet aan de grond in uw organisatie. Bijvoorbeeld doordat medewerkers op links in phishingmails klikken, malware hun (onvoldoende gepatchte) endpoint infecteert en zich vervolgens ongebreideld door het (onvoldoende gesegmenteerde) netwerk kan verspreiden naar andere werkstations en servers.

DETECTIE

- ☐ Maakt uw organisatie gebruik van logging (log files), al dan niet centraal geaggregeerd? Wordt deze ook actief geanalyseerd, zodat monitoring van incidenten plaatsvindt?
- ☐ Is uw organisatie in staat om de volgende dreigingen te detecteren, bijvoorbeeld door het inzetten van monitoring software op computer-, server- en/of netwerkniveau?
  - Ransomware (WannaCry, Petya);
  - Virussen en Trojans (Remote Access Tools);
  - Diefstal van informatie (bedrijfsgeheimen);
  - Ongeautoriseerde toegang tot servers en/of informatie.
- ☐ Toetst uw organisatie de effectiviteit van de getroffen beveiligingsmaatregelen door het uitvoeren van beveiligingstesten, zoals:
  - Kwetsbaarhedenscan: het automatisch scannen van aan internet gekoppelde systemen en applicaties op de aanwezigheid van publiekelijk bekende kwetsbaarheden en configuratiefouten.
  - Penetratietesten: beveiligingstesten van aan internet gekoppelde systemen en applicaties en/of de kantoorautomatisering.
  - Red-teaming: op basis van scenario's tracht een hacker ongeautoriseerde toegang te verkrijgen tot uw informatie.

Risico
Incidenten worden niet tijdig opgemerkt, waardoor niet adequaat kan worden opgetreden en de incidenten (en impact daarvan) voortduren.

REACTIE

- ☐ Heeft uw organisatie een communicatieplan opgesteld om belanghebbenden (zoals de juridische afdeling, de pers, leveranciers, afnemers, personeel, overheid, Autoriteit Persoonsgegevens, etc.) tijdig en adequaat te informeren over een cyberincident?
- ☐ Heeft uw organisatie een crisisplan opgesteld om de impact van cyberincidenten te beperken en het incident zelf uiteindelijk te verhelpen en is helder wie welke rol daarin heeft?
- ☐ Oefent uw organisatie periodiek (bijvoorbeeld een keer per jaar) het reageren op een gesimuleerd cyberincident en bespreekt u de uitkomsten daarvan in het bestuur voor het verbeteren van het communicatie- en crisisplan?

Risico
Inadequate reactie heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.

HERSTEL

- ☐ Heeft uw organisatie een herstelplan opgesteld, dat u in staat stelt op tijd de bedrijfsvoering te hervatten (voordat de schade te groot is)?
- ☐ Zijn uw back-upvoorzieningen zodanig ingericht dat u snel en efficiënt getroffen systemen kunt herstellen naar normale operatie en test u dit regelmatig?
- ☐ Heeft uw organisatie processen en middelen om te leren van opgetreden cyberincidenten om deze in de toekomst te voorkomen, sneller te detecteren of beter op te reageren?

Risico
Inadequaat herstel heeft tot gevolg dat de impact van cyberincidenten groter is dan noodzakelijk.