Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

CSR Cyber Security Raad

CYBERSECURITY HEALTH CHECK

- MIDDELGROTE BEDRIJVEN -

Oproep

Voor u ligt de Cybersecurity Health Check, een hulpmiddel dat u in staat stelt inzicht te krijgen in de staat van cyberbeveiliging van uw organisatie. Deze Health Check is vooral gericht op middelgrote bedrijven. Ook is het een leidraad voor controlerend accountants om met hun opdrachtgevers het gesprek over cybersecurity aan te gaan.

De Health Check is op verzoek van de Cyber Security Raad ontwikkeld door specialisten van vier grote accountantsorganisaties (Deloitte, EY, KPMG en PwC). De Koninklijke Nederlandse Beroepsorganisatie van Accountants (NBA) stelt de Health Check door middel van deze brochure beschikbaar aan haar leden en andere geïnteresseerden. De Health Check is geen uitputtende lijst, maar bedoeld als een goede start om de belangrijkste cyberrisco's in beeld te brengen en te mitigeren.

NBA-voorzitter **Marco van der Vegte**, benadrukt de signalerende en waarschuwende rol van accountants op het gebied van cybersecurity. "De accountant heeft zowel in zijn controlerende als adviserende rol aandacht voor de betrouwbaarheid en de continuïteit van de ICT-systemen waarbij het van groot belang is mogelijke cyberrisico's te identificeren. Daarbij is de mens vaak de zwakste schakel: cultuur en gedrag verdienen daarom de aandacht. Deze Health Check helpt om het gesprek over cybersecurity scherper te voeren."

Co-voorzitter van de Cyber Security Raad, **Jos Nijhuis**, vult aan: "Ook in de keten kunnen zwakke schakels zitten. Wanneer leveranciers zich bijvoorbeeld niet aan bepaalde basisnormen houden, dan kan dit een bedreiging zijn voor je eigen organisatie." Nijhuis is blij met de totstandkoming van de Health Check en de samenwerking met de accountants die hieraan voorafging. "Het aanpakken van cybercrime is geen gemakkelijke opgave. Een breed en niet aflatend maatschappelijk bewustzijn van de risico's op dit terrein is noodzakelijk om de cybersecurity in Nederland te verhogen."

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-hygiëne-maatregelen 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.

Algemene instructies

- Geef bij iedere vraag aan of dit voldoende is geïmplementeerd binnen uw organisatie en ga daarbij uit van de huidige stand.
- Bespreek deze vragenlijst met collega's en/of met uw accountant.
- Per categorie staan onderaan de potentiële risico's omschreven.

Cybersecurity: bewustwording als belangrijkste wapen

Cybercrime als tegenhanger van cybersecurity is big business. Malafide organisaties verdienen veel geld door organisaties te hacken. Vaak is het een kwestie van tijd voordat een organisatie te maken krijgt met cybercrime. En niet zelden ligt daar menselijk handelen aan ten grondslag. De vraag hoe organisaties zich tegen cybercrime kunnen wapenen is dan ook een terechte. Absolute veiligheid bestaat echter niet, maar bewustwording bij bestuurders en werknemers is nog steeds een belangrijk wapen in de strijd.

Cybersecurity Health Check

De accountant kan een belangrijke rol spelen bij die bewustwording, door de juiste vragen te stellen over cybersecurity. De Cybersecrity Health Check, die op initiatief van de Cyber Security Raad door specialisten van een aantal accountantskantoren (Inge Philips (Deloitte), John Hermans (KPMG), Douwe Mik (EY), Gerwin Naber (PwC)) is opgesteld, is daarvoor een doeltreffend hulpmiddel. Bedoeld als startpunt voor het gesprek tussen de accountant en zijn klant over cybersecurity. Dit ter verhoging van de digitale weerbaarheid, het vermogen om te incasseren en om snel te kunnen reageren.

NBA: thema maatschappelijke relevantie

Met deze brochure pakt de NBA haar proactieve rol op ten aanzien van actuele maatschappelijke thema's, waarvan cybersecurity er een is. Hierin past het signaleren van risico's die nadelig kunnen zijn voor de economie. In dit kader publiceerde de NBA eerder de Publieke managementletter: 'Van Hype naar aanpak' over risico's van cybersecurity (mei 2016). De Cybersecrity Health Check is daarop een logische vervolgstap.

Nuttige downloads / links

www.cybersecurityraad.nl

Download de ‘Handreiking cybersecurity voor de bestuurder’ gepubliceerd door de Cyber Security Raad.

www.nba.nl/projecten/kennis-delen/van-hype-naar-aanpak/

Download de door de NBA gepubliceerde Publieke managementletter over cybersecurity.

www.digitaltrustcenter.nl/

Lees de vijf basisprincipes van veilig digitaal ondernemen, waarmee ondernemers direct aan de slag kunnen.

MAATSCHAPPELIJKE RELEVANTIE

Deze brochure maakt onderdeel uit van de Vernieuwingsagenda Accountantsberoep; een initiatief van de NBA om de maatschappelijke relevantie van het accountantsberoep blijvend te verankeren in de samenleving. De essentie van ons beroep is het toevoegen van betrouwbaarheid aan informatie. Of het nou gaat om jaarrekeningen, bedrijfsprocessen, kredietrapportages, of belastingaangiftes: accountants voegen betrouwbaarheid toe. Op deze wijze dragen wij niet alleen bij aan het financieel welvaren van afzonderlijke organisaties, maar tevens aan het economische functioneren van onze samenleving.