Koninklijke Nederlandse Beroepsorganisatie van Accountants

NBA

ABN·AMRO

NEDERLANDS CYBER COLLECTIEF

SAMEN · VEILIG · VERBONDEN

+

DIGITALE VEILIGHEIDSCHECK MKB

+

Digitale veiligheidscheck MKB

Digitale veiligheid is cruciaal in het bedrijfsleven. Niet alleen voor grote, internationale ondernemingen, maar ook voor mkb-bedrijven. Hacks en datalekken hebben vaak grote gevolgen. Wat als geld verdwijnt naar verkeerde rekeningen? Wat als de website wordt gehackt of niet meer functioneert? En wat als vertrouwelijke informatie het bedrijf uitlekt? Dat kost niet alleen geld, maar ook de reputatie bij klanten en afnemers staat op het spel.

Deze veiligheidscheck is ontwikkeld voor de mkb-accountant. Het is bedoeld als een goede start om de belangrijkste cyberrisico's in kaart te brengen en aan te pakken. Deze check geeft u handvatten om het gesprek aan te gaan over digitale veiligheid. Uw rol als 'Trusted Advisor' kan per klant verschillen. U kunt met deze veiligheidscheck het onderwerp in ieder geval bespreekbaar maken en tips geven. Indien uw klant sterk afhankelijk is van zijn geautomatiseerde systeem, zoals bij een webshop, zal uw rol meer ondersteunend zijn en zullen er andere specialisten worden ingeschakeld. U bent tenslotte geen cybersecurity-specialist.

MKB
accountant

Cybersecurity: bewustwording als belangrijkste wapen

Malafide organisaties verdienen veel geld door bedrijven te hacken. Vaak is het een kwestie van tijd voordat een organisatie te maken krijgt met cybercriminaliteit. In de meeste gevallen is een hack of datalek terug te leiden naar een menselijke fout. Cybercriminelen gaan zo geraffineerd te werk, dat zelfs de meest oplettende medewerker alsnog een verkeerde link opent. De vraag hoe ondernemers zich tegen cybercriminaliteit kunnen wapenen, is dan ook een terechte vraag. Absolute veiligheid bestaat niet, maar bewustwording bij ondernemers en werknemers is nog steeds een belangrijk wapen in de strijd.

Digitale veiligheidscheck MKB

Veilig ondernemen vergt een hoog bewustzijn van de risico's en een uitgedacht actieplan op de plank. De accountant kan een belangrijke rol spelen bij die bewustwording. En door de juiste vragen te stellen, door advies te geven (eventueel om een deskundige in te schakelen). Deze digitale veiligheidscheck MKB is daarvoor een doeltreffend middel. Bedoeld als startpunt voor het gesprek van de mkb-accountant met zijn klant over cybersecurity om de veiligheid van zijn onderneming te waarborgen.

NBA: thema maatschappelijke relevantie

Met deze brochure pakt de NBA haar proactieve rol op ten aanzien van actuele maatschappelijke thema's. Cybersecurity is hier een van. Bij deze rol past het signaleren van risico's die nadelig kunnen zijn voor de economie.

De brochure kwam tot stand in nauwe samenwerking met het Nederlands Cyber Collectief en ABN-AMRO.

IDENTIFICATIE

- [ ] Wat zijn de digitale kroonjuwelen van het bedrijf? Dit zijn de digitale onderdelen of de bedrijfsgegevens, die cruciaal zijn voor het functioneren van het bedrijf. Onderdelen waarvan de continuïteit van het bedrijf afhankelijk is of die mogelijke reputatieschade tot gevolg hebben. Het is zaak deze kroonjuwelen te beschermen voor cybercriminelen én onhandigheden van medewerkers.

- [ ] Is er een noodplan aanwezig bij geval van hack of datalek? Ook buiten de kantooruren? Is een lijst van de belangrijkste IT leveranciers aanwezig? En is bekend bij welk incident, welke IT leverancier moet worden benaderd?

Risico
Als niet alle cruciale IT onderdelen en bedrijfsgegevens binnen een bedrijf in kaart zijn gebracht, zijn mogelijk ook de juiste veiligheidsmaatregelen niet getroffen. Het bedrijf is op deze onderdelen kwetsbaar.

BESCHERMING

- [ ] Controleert de onderneming regelmatig of de basisveiligheid nog op orde is:
  - Wordt software automatisch geüpdatet?
  - Worden dagelijks back-ups gemaakt die buiten de onderneming worden bewaard?
  - Wordt periodiek getest of het terugzetten van back-ups lukt?
  - Is het gebruik van sterke wachtwoorden verplicht? Moeten deze regelmatig worden gewijzigd? Wordt gebruik gemaakt van Two-Factor Authentication?

- [ ] Worden de meest veilige instellingen gekozen voor apparatuur, software en internetverbindingen?

- [ ] Wijzigt men de standaard wachtwoorden van aan het netwerk en internet verbonden apparaten (zoals een beveiligingscamera) direct?

- [ ] Worden de toegangsrechten tot systemen aangepast als een medewerker een andere functie krijgt of vertrekt?

- [ ] Zijn de ruimtes met serverapparatuur en andere randapparatuur afgesloten? En dan niet alleen voor klanten maar ook voor onbevoegde medewerkers?

- [ ] Is de meest recente update voor de gebruikte antivirussoftware geïnstalleerd en zijn de firewalls up-to-date?

Risico
Bij onvoldoende bescherming zijn alle servers en computers in een netwerk door een cryptoware besmetting binnen een handomdraai onbruikbaar. De kosten om dit te herstellen kunnen behoorlijk zijn.

DETECTIE

- [ ] Zijn de medewerkers in staat om diverse vormen van fraude te herkennen? Bijvoorbeeld CEO-fraude door het herkennen van valse e-mail adressen, onjuiste domeinnamen en afwijkende schrijfstijl.

- [ ] Wordt door de onderneming periodiek gecontroleerd op de aanwezigheid van illegale software op de computers van de medewerkers? In veel gevallen is illegale software voorzien van malware.

- [ ] Worden logbestanden van systemen gecontroleerd op aanwijzingen van hacks en andere beveiligingsproblemen?

- [ ] Is de ondernemer in staat om de volgende bedreigingen te ontdekken, bijvoorbeeld door het inzetten van monitoring-software op computer-, server- en/of netwerkniveau? Voorbeelden zijn:
  - Ransomware (gijzelsoftware) en cryptoware
  - Virussen
  - Trojaanse paarden
  - Spyware

Risico
Als een incident niet tijdig wordt opgemerkt, kan de impact van dit incident enorm toenemen.

REACTIE

- [ ] Weten de medewerkers wat te doen als zij zijn gehackt? Ook buiten de kantooruren?
- [ ] Is er een beleid dat medewerkers worden beloond bij het melden van beveiligingsincidenten? Ook als de melder zelf de veroorzaker is?
- [ ] Weet de ondernemer wat te doen als het bedrijf is gehackt? Bijvoorbeeld dat bij een datalek, waarbij persoonsgegeven openbaar zijn geworden, hij contact moet opnemen met de Autoriteit Persoonsgegevens?
- [ ] Worden cyberincidenten periodiek door de onderneming gesimuleerd? Worden de reacties met de medewerkers besproken en indien noodzakelijk bestaande instructies aangepast?

HERSTEL

- [ ] Weet de systeembeheerder wat hij moet doen na een cyberincident? Is er bijvoorbeeld een stappenplan?
- [ ] Kunnen back-ups snel worden teruggezet? Is vervanging van de systeembeheerder geregeld, als hij niet aanwezig is?
- [ ] Worden cyberincidenten achteraf met het personeel geëvalueerd? Worden indien nodig de instructies aangepast?

- [ ] Wordt elke dag gecontroleerd of aanwezige pinautomaten niet zijn geskimd, door te controleren of er geen opzetstukken zijn gemonteerd?
- [ ] Is men alert op het gebruik van juiste webadressen? Begint het webadres met 'http' dan is de internetverbinding niet beveiligd.
  - De 's' in 'https' staat voor 'secure'(veilig). Toch blijft het ook hier oppassen: er zijn ook phishingwebsites die beginnen met 'https://.

Risico
Inadequaat of te traag optreden verkleint de kans op herstel. Bijvoorbeeld dat bij CEO-fraude de bank probeert het gestolen geld terug te halen.

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

Nuttige downloads / links

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

Download de door de NBA gepubliceerde Publieke managementletter over cybersecurity.

https://www.nba.nl/themas/mkb/informatie-voor-mkb-accountants/cybersecurity/

https://digitaltrustcenter.nl

https://www.abnamro.nl/fraude

https://nederlandscybercollectief.nl/

De Cyberwacht -de hack-hulplijn van het Collectief- is direct bereikbaar onder nummer 070 513 55 55 (€ 1,49 per minuut).

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. Eerder brachten de Cyber Security Raad en de NBA een soortgelijke brochure uit getiteld: ‘Cybersecurity Health Check voor middelgrote bedrijven’ en geschreven door specialisten van Deloitte, EY, KPMG en PwC.