Nieuwe Risicoklassenindeling Digitale Veiligheid en pentest

Er is een sterke toename van Cybercriminaliteit. Zeker 50% van het MKB in Nederland krijgt te maken met fraude, diefstal en/of afpersing via internet. Dit komt natuurlijk door de steeds verdergaande digitalisering. Cybercriminaliteit heeft een enorme impact op de operationele continuïteit. Daarnaast leidt het ook vaak tot verlies van klanten, omdat het bedrijven bijvoorbeeld niet in dank wordt afgenomen als klantgegevens op straat komen te liggen door datalekken. Dat cybercriminaliteit een enorme kostenpost oplevert, zal niet verbazingwekkend zijn. Uit een onderzoek van Deloitte in 2017 is gebleken dat het MKB in Nederland jaarlijks wordt geconfronteerd met een waardeverlies van 1 miljard euro als gevolg van cybercriminaliteit.

Cyberverzekeringen

Vreemd genoeg heeft de toename van de cyberrisico's nog niet geleid tot veel meer vraag naar cyberverzekeringen. Ondanks diverse overheidscampagnes is het cyberrisicobewustzijn bij ondernemers in Nederland nog relatief laag. Ter vergelijking: het premievolume van cyberverzekeringen in Nederland bedroeg in 2019 slechts 17 miljoen euro tegenover 2,3 miljard euro in de Verenigde Staten. Er zijn blijkbaar nog steeds veel misverstanden over de cyberdekking op bestaande zakelijke verzekeringen. Daarnaast is het aanbod cyberverzekeringen in Nederland nog beperkt.

Risicobewustzijn rond cyberdreigingen

Om ervoor te zorgen dat het cyberrisicobewustzijn onder het MKB in Nederland toeneemt, heeft het Verbond van Verzekeraars aan een aantal initiatieven deelgenomen. Er kan daarbij worden gedacht aan:

- Het Actieprogramma Veilig Ondernemen 2019-2022 (het programma van het Nationaal Platform Criminaliteitsbeheersing waarmee met name cybercriminaliteit wordt aangepakt)
- De campagne Veilig Zakelijk Internetten (een campagne van MKB-Nederland en VNO-NCW waarmee bedrijven werden gewezen op het belang van veilig internetten)
- Het onderzoek Cybersecure MKB van de Haagse Hogeschool (een nulmeting van cybersecurity in het MKB)
- Het Risicomodel cyber, oftewel de Risicoklassenindeling Digitale Veiligheid

Risicoklassenindeling Digitale Veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) heeft in samenwerking met VNO-NCW, MKB-Nederland, het Verbond van Verzekeraars, de Nationale Politie, Cyberveilig Nederland, NLdigital, het CIO Platform Nederland, de Online Trust Coalitie, het Digital Trust Center en het Ministerie van EZK de Risicoklassenindeling Digitale Veiligheid ontwikkeld.

Met de Risicoklassenindeling kan de ondernemer op de website van het Digital Trust Center (www.digitaltrustcenter.nl/risicoklasse) een inschatting maken van de mate van cyberrisico's dat hij loopt. Aan de hand van 11 vragen wordt bepaald in welke risicoklasse de onderneming valt en welke beveiligingsmaatregelen de onderneming zou moeten treffen, om zijn digitale veiligheid te verbeteren.

De vragen gaan over de volgende onderwerpen:

- de omvang en jaaromzet van de onderneming
- de data (zoals gegevens van medewerkers, klanten en/of leveranciers) die de ondernemer in bezit heeft en de toegang tot deze data (wel of niet op afstand te benaderen)
- de bedrijfscontinuïteit na cybercrimes
- de bedrijfsactiviteiten (gevoeligheid voor politiek activisme, verkoop via een webshop, vestigingen in en/of omzet uit de VS, Canada en/of Australië)

Na het invullen van de online vragenlijst wordt een PDF-document gegenereerd, waarin de ondernemer een uitgebreide uitleg krijgt over de mogelijk te treffen beveiligingsmaatregelen. Daarbij wordt uitgegaan van de 5 basisprincipes van veilig digitaal ondernemen:

1. Inventariseer kwetsbaarheden
2. Kies veilige instellingen
3. Voer updates uit
4. Beperk toegang
5. Voorkom virussen en ander malware

Als extraatje staat er in het document een voorbeeld van een inventarisatielijst IT-onderdelen, om inzicht te krijgen in de mate van digitalisering. Ook zijn er voorbeelden van draaiboeken toegevoegd, die de ondernemer kunnen helpen als hij ondanks alle maatregelen toch het slachtoffer is geworden van een cyberincident.

Let op!

Het CCV heeft in het kader van cybersecurity ook het CCV-keurmerk Pentesten ontwikkeld. Bij een pentest (of penetratietest) zoekt een ethische hacker naar zwakke plekken van de website, applicatie of het hele IT-systeem. Met zijn bevindingen kunnen de cyberrisico's duidelijk in kaart worden gebracht en passende beveiligingsmaatregelen worden getroffen. Het CCV-keurmerk Pentesten is bedoeld voor cybersecuritybedrijven die pentesten aanbieden. Als zij het CCV-keurmerk dragen, mag de ondernemer erop vertrouwen dat er wordt voldaan aan bepaalde kwaliteitseisen.