# Cybersecurity belangrijke pijler in adviesgesprek

**'Gehackt bedrijf in Helmond slechts topje van de ijsberg: duizenden mkb'ers digitaal gegijzeld', schreef het Eindhovens Dagblad in augustus van dit jaar. En in juli kopte de Volkskrant: 'Hagaziekenhuis krijgt hoge boete na onbevoegd inkijken patiëntendossier Barbie'. Als ondernemers geen cybersecuritymaatregelen nemen, zullen dit soort koppen de komende jaren steeds vaker verschijnen.**

Uit cijfers blijkt dat bijna 7 op de 10 ondernemers in Nederland al eens te maken heeft gehad met een cybersecurityincident, zoals een hack of een datalek. En dat aantal is nog steeds groeiende, volgens informatiebeveiliger Northwave; het bedrijf meldde onlangs dat het aantal serieuze incidenten in de eerste twee kwartalen van 2019, ten opzichte van dezelfde periode vorig jaar, met bijna 200% is gestegen. Ook (cyber)verzekeraar Hiscox ziet de gemiddelde schadelast voor Nederlandse bedrijven en overheden nog steeds stijgen. Per incident bedraagt deze inmiddels ongeveer 300.000 euro (ten opzichte van 184.000 één jaar eerder). Toch is er ook goed nieuws te melden: volgens de Cybersecuritymonitor 2019 van het CBS nemen bedrijven steeds meer cybersecuritymaatregelen en maken vooral middelgrote bedrijven een inhaalslag.

## Checklist Aan de slag met advies cyberrisico's

Gezien de grote kans en impact van een cybersecurityincident hoort cybersecurity een prominente plek in te nemen in de adviesgesprekken die je als adviseur met je zakelijke klanten voert. Adfiz helpt adviseurs daarbij met een checklist 'Aan de slag met advies cyberrisico's'. Deze checklist is een waardevol handvat bij het aan de slag gaan met bestaande klanten.

### *Stap 1 – Analyseer je portefeuille*

Bepaal welke klanten in je portefeuille het grootste risico lopen en open staan voor advies over cyberrisico's. De praktijk leert dat het daarbij niet per se gaat om zaken als bedrijfsgrootte of de branche waarin een bedrijf actief is. Belangrijke segmentatiecriteria zijn:

- Het veiligheidsprofiel - heeft je klant zijn zaken technisch op orde?
- Het risicoprofiel - hoe groot is de kans op grote gevolgschade?
- Het begripsvermogen - is de klant thuis in de materie?
- De risicobereidheid - welke risico's is de klant bereid te lopen?

Wil je toch een analyse maken op bedrijfsgrootte en branche dan is de Cybersecuritymonitor 2019 van het CBS daarvoor een waardevolle bron (www.cbs.nl/nl-nl/publicatie/2019/37/cybersecuritymonitor-2019). Op pagina 42 en 43 worden incidenten (in %) naargelang de bedrijfsgrootte en per bedrijfstak genoemd.

### *Stap 2 – Bepaal hoe je je klanten gaat interesseren voor cybersecurity*

Uit de introductie van dit artikel bleek al dat veel bedrijven risico en impact onderschatten en niet goed voorbereid zijn op een cyberincident. Benut deze voorbeelden (en andere) en zorg dat uit je verhaal blijkt dat:

- de kans op een incident groter is dan de ondernemer denkt;
- de impact/schade van een incident groter is dan de ondernemer denkt;
- het handelingsperspectief groter is dan verzekeren;

Bied klanten hierbij een laagdrempelige eerste stap in de vorm van een (gratis) risicoscan (veel verzekeraars faciliteren dit).

Diverse verzekeraars (Allianz, Hienfeld) en andere partijen bieden gratis online cyber risicoscans waarmee je snel de risico's in kaart kunt brengen die je klant mogelijk loopt op het gebied van cyber en cybersecurity. Onthoud: voor bedrijven die niets of weinig hebben geregeld, is met kleine stappen vaak al een eerste verbetering te realiseren.

### *Stap 3 – Bepaal wat de belangrijkste risico's zijn voor je klant*

Bepaal welke bedrijfsactiviteiten kwetsbaar zijn voor welke cyberrisico's en hoe de beveiliging ervan tot nu toe is ge-

regeld. Onthoud daarbij dat cybersecurity niet alleen gaat over cyberaanvallen, maar ook over pc's, camera's, productielijnen of andere systemen die 'connected' zijn en die uitvallen als door een cyberincident zoiets simpels als data, telefonie of elektra eruit ligt.

Een hulpmiddel om inzicht te krijgen in de staat van de cyberbeveiliging van een organisatie (en dat vooral gericht is op middelgrote bedrijven) is de Cybersecurity Health Check (www.cybersecurityraad.nl/030_Publicaties/) van de nationale en onafhankelijke Cyber Security Raad.

### *Stap 4 – Breng de gevolgen van een cyberincident in kaart*

Bepaal hoe de in stap 3 gevonden kwetsbaarheden verschillende vormen van schade kunnen opleveren. Voorbeelden van mogelijke schades na een cyberincident zijn:

- Aansprakelijkheid, zoals boetes als gevolg van een datalek, aansprakelijkheid voor niet-elektronische gegevens en schending van de privacy
- Eigen schade, zoals netwerkonderbreking en diefstal van intellectueel eigendom

### *Stap 5 – Beheersmaatregelen treffen*

Door de juiste beheersmaatregelen te treffen, kunnen mogelijke risico's en schade flink worden beperkt. Niet voor niets maken preventie en incident managementdiensten vaak (verplicht) onderdeel uit van een cyberverzekering. Beheersmaatregelen zullen zich toespitsen op:

- Preventie, zoals antivirussoftware
- Detectie, zoals monitoringsoftware op computer-, server- en/of netwerkniveau
- Reactie & herstel, zoals een communicatieplan om belanghebbenden tijdig te informeren en een herstelplan om de bedrijfsvoering weer snel te kunnen hervatten

### *Stap 6 – Omgaan met de overblijvende risico's*

Sommige cyberrisico's zijn ook na het treffen van diverse maatregelen niet uit te sluiten. Voor deze risico's moet in kaart worden gebracht hoe hiermee om te gaan:

- Vermijden: de activiteit die samenhangt met het risico staken, uitbesteden of op een andere manier voortzetten
- Verminderen: door preventieve en schadebeperkende maatregelen de gevolgen van het risico kleiner maken
- Accepteren: goed bewust zijn van het feit dat het risico zich kan voordoen en wat daarvan de (financiële) consequenties zijn en bereid zijn de gevolgen te dragen
- Overdragen: de financiële gevolgen van het risico verzekeren. Diverse verzekeraars bieden inmiddels cybersecurityverzekeringen. Op www.poliskraker.nl vind je een vergelijking van 10 verzekeraars op 50 criteria.

### *Stap 7 - Blijf je klant actief volgen*

Cyberrisico's, cyberverzekeringen en cyberpreventiemaatregelen zijn volop in ontwikkeling. Monitor je klant daarom continu om te bekijken of er aanpassingen nodig zijn. <

*Dit artikel wordt u aangeboden door Adfiz*

## ADFIZ KENNISDOSSIER CYBERRISICO'S

De checklist Aan de slag met advies cyberrisico's is een onderdeel van het Adfiz Kennisdossier Cyberrisico's (www.adfiz.nl/dossiers/cyberrisicos). In dit dossier bundelen we alle kennis, informatie, tips en tools om als adviseur aan de slag te gaan met cyberveiligheid, zoals:

- Checklist Aan de slag met advies cyberrisico's
- Diverse hulpmiddelen om risico's in kaart te brengen
- Diverse checklists t.a.v. risico's en beheersmaatregelen
- Ledenvoordelen van diverse partners uit het Adfiz-netwerk voor tooling die kan helpen bij beheersmaatregelen en advies
- Modelbrief en infographic om onderwerp bij klanten op de agenda te zetten
- Module om gericht content te delen met (klant)groepen
- Verwijzingen naar relevante sites van derden.

Een deel van de informatie in het Kennisdossier Cyberrisico's is voor iedereen toegankelijk. Specifiek ontwikkelde tools, modeldocumenten en ledenvoordelen zijn uitsluitend beschikbaar voor Adfiz-leden.