CYBERRISICO'S

CHECKLIST – AAN DE SLAG MET ADVIES CYBERRISICO'S

START

STAP 1

Analyseer je portefeuille

Je kunt niet alle klanten in één keer adviseren. 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 in de eerste plaats gaat om zaken als bedrijfsgrootte of de branche waarin een bedrijf actief is.

Belangrijke segmentatiecriteria zijn:

- **Veiligheidsprofiel:** heeft klant zaken technisch op orde
- **Risicoprofiel:** hoe groot is kans op grote gevolgschade
- **Begripsvermogen:** is de klant thuis in de materie
- **Risicobereidheid:** welke risico's is klant bereid te lopen

STAP 2

Pitch je verhaal

Bepaal hoe je het onderwerp bij de klant wilt agenderen. Veel bedrijven onderschatten het risico en zijn niet goed voorbereid op cybercrime. Met kleine stappen is dan al vaak een eerste verbetering te realiseren. Benut dit in je verhaal.

- Kans op een incident is groter dan ondernemer denkt (zie ook stap 3)
- Impact/schade van een incident is groter dan ondernemer denkt (zie ook stap 4)
- Handelingsperspectief is groter dan verzekeren (zie ook stap 5 en 6)
- Bied een laagdrempelige eerste stap in vorm van een (gratis) risicoscan (veel verzekeraars faciliteren dit).

Adfiz heeft diverse hulpmiddelen:

- Infographic cyberrisico's voor ondernemers
- Modelbrief
- Artikelen om te delen op Finfin van Adfiz
- Overzicht online cyberscans

Meer info adfiz.nl/cyber

STAP 3

Inventariseer de risico's

Bepaal waar de (belangrijkste) kwetsbaarheden zich bevinden en hoe die op dit moment beschermd worden.

- **Welke bedrijfsactiviteiten zijn kwetsbaar voor welke risico's?**
  Let op! Dit gaat niet alleen om informatie technologie (IT), ook het primaire proces is vaak 'connected'. Ook de operationele technologie (OT) kan blootstaan aan cyberrisico's.

- **Hoe is beveiliging geregeld?**
  - **Identificatie.** Risico: relevante dreigingen worden niet onderkend
  - **Bescherming.** Risico: een aanvaller krijg voet aan de grond
  - **Detectie.** Risico: incidenten worden niet tijdig opgemerkt
  - **Reactie.** Risico: inadequate reactie vergroot impact/schade
  - **Herstel.** Risico: inadequaat herstel vergroot impact/schade

*Tip! Gebruik de Cybersecurity Health Check van de Cyber Security Raad om beveiliging in kaart te brengen. **Meer info adfiz.nl/cyber***

CYBERRISICO'S

CHECKLIST – AAN DE SLAG MET ADVIES CYBERRISICO'S

VERVOLG

STAP 4

Breng mogelijke gevolgen in kaart

Bepaal hoe de kwetsbaarheden verschillende vormen van schade kunnen opleveren. In grote lijn zijn er twee categorieën:

- Aansprakelijkheid
- Eigen schade

Op **adfiz.nl/cyber** vind je een checklist met rubrieken en voorbeelden van mogelijke schades.

STAP 5

Tref mogelijke beheers-maatregelen

Cyber leent zich bij uitstek voor een meer risicomanagement georiënteerde aanpak. De juiste beheersmaatregelen kunnen de mogelijke risico's en schade flink beperken. Niet voor niets maken preventie en incident management-diensten vaak (verplicht) onderdeel uit van een cyberverzekering. Beheersmaatregelen zullen zich toespitsen op:

- **Preventie:** het voorkomen van incidenten door technische en organisatorische (be-schermings)maatregelen
- **Detectie:** het beperken van schade door incidenten snel te ontdekken
- **Reactie & herstel:** het beperken van schade door een goed incident response plan, her-stelplan en continuïteitsplan

STAP 6

Dek de overblijvende risico's af

Ook na getroffen beheersmaatregelen zijn cyberincidenten niet uit te sluiten. Zijn er andere manieren om risico's te vermijden, te verminderen, over te dragen of te accepteren? (zie ook het kennisdossier Risicomanage-ment). Vaak zal er de wens blijven om bepaal-de risico's af te dekken. Hiervoor zijn steeds meer verzekeringsoplossingen.

Ledenvoordeel

- Poliskraker: Polisvoorwaarden vergelijking van 10 verzekeraars op 50 criteria

Tips!

- *De eerder ingevulde Cyberscurity Health Check biedt hier een effectief startpunt*
- *Begin met de 5 basisprincipes van veilig digi-taal ondernemen, opgesteld door Digital Trust Center (onderdeel van ministerie van EZ)*
- *Bekijk de checklist beheersmaatregelen uit onderzoek dat Haagse Hogeschool met onder andere Adfiz heeft uitgevoerd.*
- *Kijk ook eens naar de Adfiz ledenvoordelen voor veilig communiceren van Safebay, SmartLockr en Zivver.* ***Meer info adfiz.nl/ledenvoordelen***
- *Wil je samenwerken met een cybersecurity dienstverlener? Check dan de brancheorgani-satie Cyberveilig Nederland (www.cyberveilignederland.nl)*

Aan de slag met cyberrisico advies

Koppen waarin gewag wordt gemaakt van een gehackt bedrijf, een universiteit die geconfronteerd wordt met ransomware of een ziekenhuis dat te maken krijgt met een datalek, (ont)sieren steeds vaker de krantenpagina's. Bijna zeven op tien ondernemers in Nederland heeft al eens te maken gehad met een cybersecurityincident en de gemiddelde schadelast voor Nederlandse bedrijven en overheden wordt geschat op ongeveer 300.000 per incident.

Gezien de grote kans en impact van een cybersecurityincident heeft cybersecurity

een volwaardige plek ingenomen in de adviesgesprekken die je als adviseur met je zakelijke klanten voert. Adfiz helpt adviseurs daarbij met de checklist 'Aan de slag met advies cyberrisico's'. Deze checklist is een waardevol handvat bij het aan de slag gaan met bestaande klanten om hen te doordringen van de noodzaak van het treffen van cybersecuritymaatregelen. Want getroffen worden door een cybersecurityincident is vaak niet iets wat bedrijven overkomt, maar wat ze hebben laten gebeuren. Met de juiste preventieve en schadelastbeperkende maatregelen, kunnen namelijk al veel cybersecurityincidenten voorkomen worden en kan de te verzekeren (financiële) schade beperkt blijven. ■

'Getroffen worden door een cybersecurityincident is vaak niet iets wat bedrijven overkomt, maar wat ze hebben laten gebeuren'