Gespreksgids Cyberverzekering

Voor de adviseur | MKB

Gebruik dit document om het gesprek met jouw klant te voeren wanneer hij of zij twijfelt aan de toegevoegde waarde van een cyberverzekering.

DEEL 1 — Veelgehoorde bezwaren & tegenargumenten

■ *Bezwaar: "Wij zijn veel te klein, hackers hebben geen interesse in ons"*

- Criminelen schieten met hagel. Geautomatiseerde tools scannen het hele internet 24/7 op kwetsbare systemen — het maakt ze niet uit hoe groot je bent.
- 77% van het MKB werd de afgelopen twee jaar minstens één keer getroffen door cybercriminaliteit. Kleine bedrijven zijn juist aantrekkelijk: minder beveiliging, maar wél waardevolle klantdata.
- Horecabedrijf de HALL (2024): 2 weken offline via een WordPress-lek. Geen groot bedrijf, wel €5.000–€10.000 schade.
- De vraag is niet óf het gebeurt, maar wanneer — en of je dan een vangnet hebt.
- *Tip: Vraag door: 'Hoeveel dagen kunt u uw bedrijf draaien als u niet bij uw computer kunt?'*

■ *Bezwaar: "Mijn IT-dienstverlener regelt alles, die zorgt voor mijn beveiliging"*

- Een IT-partij richt systemen in en beheert ze — maar geen enkele partij kan een aanval 100% voorkomen. Dat garandeert ook jouw IT-leverancier niet.
- Bij een aanval heb je naast IT-herstel ook hulp nodig bij: AVG-meldplicht, communicatie naar klanten, juridische ondersteuning en vervanging van omzetverlies. Dat regelt een IT-er niet.
- In Volendam (2025) werden tientallen MKB-bedrijven getroffen via één gehackt IT-bedrijf. Jouw IT-leverancier kan zelf het doelwit zijn.
- Een cyberverzekering en een goede IT-partner vullen elkaar aan — het één vervangt het ander niet.
- *Tip: Vraag: 'Heeft u afspraken met uw IT-partij over wat er gebeurt bij een aanval, en wie de kosten draagt?'*

■ *Bezwaar: "Wij werken alleen in de cloud, dus wij hebben geen risico"*

- De cloud beveiligt de infrastructuur — maar niet jouw accounts. De meest voorkomende oorzaak van cloudincidenten is een gestolen wachtwoord of phishingmail.
- Als iemand inlogt op jullie Microsoft 365, Google Workspace of boekhoudpakket met een gestolen wachtwoord, heeft de hacker toegang tot alles in de cloud.
- Cloudproviders zijn niet verantwoordelijk voor wat gebruikers doen of voor aanvallen via accountovername. Lees de kleine lettertjes.
- Ransomware treft ook cloudopgeslagen bestanden: sommige varianten versleutelen gesynchroniseerde mappen in OneDrive en Google Drive.
- *Tip: Vraag: 'Is op alle cloudaccounts twee-factorauthenticatie actief? Wat als iemand op een phishinglink klikt?'*

■ *Bezwaar: "Wij hebben niets te verbergen / wij bewaren geen bijzondere gegevens"*

- Elke ondernemer bewaart gegevens die criminelen interessant vinden: klantnamen, adressen, betaalgegevens, offertes, contracten, IBAN-nummers.
- Bij een ransomware-aanval is het niet relevant wát je bewaart — criminelen blokkeren alles en eisen losgeld voor de toegang, niet voor de inhoud.
- Onder de AVG bent u verplicht datalekken te melden. Een datalek zonder melding kan leiden tot boetes van de Autoriteit Persoonsgegevens.
- Reputatieschade bij klanten die horen dat hun gegevens zijn uitgelekt, is niet te onderschatten.
- *Tip: Vraag: 'Stel dat uw klantenbestand morgen op straat ligt — wat betekent dat voor uw relatie met uw klanten?'*

■ *Bezwaar: "Een cyberverzekering is te duur / dat verdien ik nooit terug"*

- ■ De gemiddelde schade per cyberincident bij MKB bedraagt €270.000 (bron: Cybercrimebeeld Nederland 2024). De premie is daar een fractie van.
- ■ Zelfs bij een kleine aanval — website plat, systeem down, AVG-melding — lopen de kosten voor IT-herstel, juridisch advies en omzetverlies snel op tot tienduizenden euro's.
- ■ Een cyberverzekering biedt ook 24/7 crisisondersteuning: forensisch IT-onderzoek, juridische hulp en communicatiebegeleiding. Die kennis en snelheid heb je bij een aanval hard nodig.
- ■ Bedrijven met een cyberverzekering herstellen gemiddeld significant sneller dan bedrijven zonder.
- ■ *Tip: Bereken samen: hoeveel omzet verliest de klant bij 1 week stilstand? Leg dat naast de jaarpremie.*

■ *Bezwaar: "Dat overkomt ons niet, wij zijn altijd voorzichtig"*

- ■ De meeste cyberincidenten beginnen niet met nalatigheid maar met een overtuigende nep-e-mail. Zelfs technisch onderlegde medewerkers trappen erin.
- ■ Bij de TU Eindhoven (2025) was één medewerker die zijn wachtwoord hergebruikte de ingang voor een aanval op het hele netwerk.
- ■ Voorzichtigheid verlaagt het risico — maar elimineert het niet. Een verzekering dekt het resterende risico dat altijd overblijft.
- ■ *Tip: Vraag: 'Wat is uw plan als het morgen toch misgaat?'*

DEEL 2 — Acceptatie-eisen van verzekeraars

Verzekeraars stellen minimale beveiligingseisen. Bespreek deze met de klant voordat u een aanvraag indient. Een 'nee' op een van deze vragen kan leiden tot afwijzing of een hogere premie.

■ Antivirusprogramma actief?	Is er door verzekeringnemer/verzekerde een antivirusprogramma van een gerenommeerde aanbieder (bijv. Eset, AVG, McAfee, Norton, Windows Defender) geinstalleerd en geactiveerd op alle (computer)systemen, inclusief Apple computers?
■ Wekelijkse back-up aanwezig?	Zorgt verzekerde er minimaal wekelijks voor dat een back-up wordt gemaakt van kritische gegevens en/of systemen, los van het computersysteem bewaard of in een erkende cloudoplossing (Microsoft OneDrive, Google Drive, iCloud, Azure Recovery Services, Vault of Amazon)?
■ Software-updates tijdig?	Voert verzekerde tenminste iedere 30 dagen nadat patches en software-updates door de fabrikant zijn uitgegeven, deze uit op de (computer)systemen?
■ Twee-factorauthenticatie (2FA)?	Wordt er binnen het computersysteem twee- of multifactor autenticatie (2FA) gebruikt om de toegang tot alle web-based (e-mail)accounts te beheren (bijv. Office 365, Gsuite, Azure, AWS, Salesforce) en om in te loggen op afstand in het computersysteem (remote acces)?
■ Minder dan 500.000 persoonsgegevens?	Verzamelt, verwerkt of bewerkt verzekeringnemer meer dan 500.000 unieke persoonsgegevens (incl. medische gegevens), inclusief de gegevens namens derden? — Antwoord moet 'Nee' zijn voor standaard acceptatie.

Praktijktip: Loopt de klant vast op een van deze eisen? Dat is juist een kans. Help hem of haar de beveiliging op orde te brengen — en adviseer daarna de passende dekking. Een 'nee' is geen afwijzing, het is het begin van het gesprek.

DEEL 3 — Openingsvragen om het gesprek op gang te brengen

Stilstand	Hoeveel dagen kan uw bedrijf draaien als u volledig niet bij uw systemen en bestanden kunt?
Back-up	Wanneer is uw back-up voor het laatst getest? Weet u zeker dat u erop kunt terugvallen?
Medewerkers	Weten uw medewerkers hoe ze een phishingmail herkennen? Is daar ooit aandacht aan besteed?
Klantdata	Stel dat uw klantenbestand morgen openbaar is — wat betekent dat voor uw klantrelaties?
Verantwoordelijkheid	Als uw IT-partij gehackt wordt en uw data daarbij betrokken is — wie draait dan op voor de schade?
2FA	Is twee-stapsverificatie ingeschakeld op uw e-mail en cloudomgeving? Op alle accounts?

DEEL 4 — Schadevoorbeelden uit de praktijk

Gebruik de onderstaande voorbeelden om de impact van een cyberaanval concreet te maken voor een ondernemer. Elk voorbeeld is gebaseerd op een gedocumenteerd incident uit 2024–2025.

Kapsalon — 3 medewerkers, eigen klantensysteem

Phishing → Ransomware

Een medewerkster ontvangt een e-mail die eruitziet als een factuur van de leverancier. Ze klikt op de bijlage. Binnen enkele uren zijn alle bestanden — inclusief het klantensysteem, de agenda en de financiële administratie — versleuteld. Het kapsalon kan drie weken geen afspraken maken, heeft geen toegang tot klantgegevens en moet een volledig nieuw boekingssysteem aanschaffen. De criminelen eisen €8.000 losgeld. Na overleg met de IT-specialist besluit de eigenaar te betalen omdat een back-up ontbreekt.

Losgeld betaald	± €8.000
Omzetverlies (3 weken dicht)	± €12.000
IT-herstel en onderzoek	± €6.000
Nieuw boekingssysteem	± €5.000
Reputatie- en klantverlies	± €7.000
Overige kosten (juridisch, AVG)	± €2.000
Totale schade	**± €40.000**

Les voor de adviseur: Dit begon met één klik. Vraag de klant: heeft u een recente, offline back-up? En weet uw team hoe ze een phishingmail herkennen?

Bron: Gebaseerd op gangbare schadegevallen MKB Nederland 2024 (Chubb / Hiscox schadestatistieken)

Horecabedrijf de HALL — website en reserveringssysteem

Hack via WordPress-lek

In september 2024 ontdekken de eigenaren van de HALL dat hun website volledig onbereikbaar is. Een automatische scanner had een bekende kwetsbaarheid in hun verouderde WordPress-installatie gevonden en misbruikt. De website — het centrale punt voor reserveringen, contactinformatie en evenementenkalender — lag twee weken volledig plat. Gasten konden geen tafels reserveren, de telefoon stond roodgloeiend en de reputatie liep schade op door negatieve reviews over de onbereikbaarheid.

Omzetverlies reserveringen (2 weken)	± €5.000 – €10.000
IT-herstel en websiteherstel	± €2.500
Reputatieschade / gemiste klanten	moeilijk te kwantificeren
Totale directe schade	**± €7.500 – €12.500**

Les voor de adviseur: Verouderde software is een open deur. Vraag de klant wanneer zijn website, kassasysteem of boekhoudsoftware voor het laatst is bijgewerkt — en door wie.

Bron: ABN AMRO — Iedereen kan slachtoffer worden (2024)

NRCollecties.nl — online webwinkel

Ransomware (groep: Ransomhub)

Op 17 augustus 2024 treft ransomware-groep Ransomhub de webwinkel NRCollecties.nl. Alle bedrijfsbestanden worden versleuteld: voorraadgegevens, klantorders, factuurhistorie en de gehele website-database. De webshop gaat onmiddellijk offline. Criminelen publiceren een losgeldeis. Het bedrijf kan geen orders verwerken, geen klanten informeren en heeft geen toegang tot zijn eigen data. De stilstand duurt meerdere weken. Klanten wenden zich tot concurrenten.

Losgeld (al dan niet betaald)	onbekend / vertrouwelijk
Omzetverlies webshop (weken offline)	hoog — afhankelijk van omzetsnelheid
IT-forensisch onderzoek	± €5.000 – €15.000
Herstel systemen en data	± €8.000 – €20.000
Klantcommunicatie en AVG-melding	± €2.000 – €5.000
Totale schade (schatting)	**± €30.000 – €60.000+**

Les voor de adviseur: Ransomware treft elk bedrijf dat digitaal actief is — van kapper tot webwinkel. Geen back-up betekent: betalen of alles kwijt. Vraag de klant hoe zijn herstelplan eruitziet.

Bron: ABN AMRO — Iedereen kan slachtoffer worden (2024)

ICT-dienstverlener Volendam — meerdere MKB-klanten getroffen

Ransomware via keten (supply chain attack)

In oktober 2025 wordt een lokaal ICT-bedrijf in Volendam getroffen door ransomware. Via een lek in de beheersoftware waarmee het bedrijf de systemen van haar klanten op afstand beheert, krijgen criminelen toegang tot tientallen aangesloten MKB-bedrijven tegelijk. Lokale ondernemers — winkeliers, installatiebedrijven, een tandartspraktijk — merken dat hun systemen opeens op slot zitten. Ze hadden zelf niets fout gedaan. De aanval was via hun vertrouwde IT-partner binnengekomen.

Omzetverlies per getroffen bedrijf	± €5.000 – €30.000
IT-herstel per bedrijf	± €3.000 – €15.000
Juridische aansprakelijkheidsvragen	lopend / complex
Totale ketenschade (meerdere bedrijven)	**± €200.000+ (schatting)**

Les voor de adviseur: Zelfs als jouw klant alles goed doet, kan hij slachtoffer worden via zijn IT-leverancier. Een cyberverzekering dekt ook dit soort ketenschade. Vraag wie de schade draagt als het via een derde partij binnenkomt.

Bron: Groot Waterland / NH Nieuws, oktober 2025

Wat de cijfers zeggen: 1 op de 5 MKB-bedrijven had in 2024 directe schade door cybercriminaliteit. De gemiddelde schade per incident bedraagt **€270.000**. 77% van het MKB werd in de afgelopen twee jaar minstens eenmaal getroffen. In 95% van de gevallen waarbij losgeld werd betaald, was er geen andere keuze om het bedrijf te redden.

Bronnen: MKB Servicedesk mei 2025 | NCSC Ransomware Jaarbeeld 2024 | Hallo.eu / Cybercrimebeeld Nederland 2024