# Cyberverzekering: vangnet of valse geruststelling?

In het digitale tijdperk is cybercriminaliteit helaas een deel van de realiteit. Een heuse cyberaanval kan verstrekkende gevolgen hebben voor de samenleving, voor individuen en voor bedrijven. Ransomware, datalekken, digitale pannes of sabotage, ziekenhuizen of luchthavens die lamgelegd worden. Zelfs wanneer je eigen digitale huishouding op orde is, kan een cyberincident bij een partner je eigen infrastructuur stevig treffen met aanzienlijke financiële, operationele en reputatieschade.

Om je daartegen te wapenen bestaat er zoiets als een cyberverzekering. Is het een nuttige buffer tegen dergelijke risico's, of geeft zo'n polis eerder een vals gevoel van veiligheid? In dit artikel leggen we uit wat het is, wat er bij komt kijken en welke incidenten wel of niet onder een cyberverzekering vallen.

## Wat is een cyberverzekering en wat dekt het?

Een cyberverzekering biedt dekking voor schade die ontstaat door cyberincidenten. Voor bedrijven en organisaties dekt zo'n verzekering bijvoorbeeld de kosten voor

- De heropbouw van IT-systemen,
- Juridische en technische bijstand,
- Crisiscommunicatie,
- Administratieve boetes (bijvoorbeeld in het kader van GDPR en NIS2)

Een cyberverzekering dekt **directe en indirecte schade**. 'Dat zit in drie delen: de hulplijn, de eigen schade en de schade aan derden,' vertelt **Tom Van Britsom**, cyberexpert bij verzekeringsmakelaar en risicoconsultant Vanbreda Risk & Benefits. 'Die hulplijn kan je vergelijken met pechverhelping voor de wagen. Wij zorgen voor de experten die de eerste noodzakelijke ingrepen doen na een incident, dat kan op IT-vlak zijn, maar ook juridisch of op vlak van PR. We brengen je bijvoorbeeld in contact met mensen die kunnen onderhandelen over losgeld dat wordt gevraagd.'

De 'eigen schade' is vaak een voortzetting van die hulplijn en gaat onder meer over experts die zich na de eerste zorgen inzetten om het bedrijf weer op de rails te zetten. 'Soms is dat enkele dagen, maar dat kan ook tot zes maanden duren en die kosten lopen vaak het hoogst op. Denk maar aan het herprogrammeren en herimplementeren van bepaalde zaken. Ook de tijd dat je als bedrijf niet operationeel bent zit daarin. Stel dat er bij een ransomware aanval losgeld wordt betaald, vergoedt de verzekeraar bijvoorbeeld bitcoins die ter beschikking worden gesteld door de professionele onderhandelaar.'

'Bij een verzekering is de financiële compensatie de meest voor de hand liggende. Maar die bijstand komt enorm van pas op juridisch vlak,' zegt Peter Vergote, Legal Advisor bij DNS Belgium. 'Stel dat je door een cyberincident naast de geleden schade ook verschillende claims krijgt van bedrijven die hierdoor schade ondervinden, dan helpt de expertise van je verzekeraar daar mee om te gaan. Op het moment van een incident wil je zelf vooral focussen op de dringende zaken, zoals je bedrijf weer op de rails krijgen.'

Verzekeraars vragen uiteraard dat je zelf voldoende maatregelen neemt om een cyberincident te voorkomen. De details kunnen verschillen, maar ze steunen meestal op deze vijf vereisten:

- Multi-Factor-Authentication (MFA)
- Back-ups die op twee fysiek gescheiden locaties worden bewaard
- Endpoint Detection & Response (EDR) en Managed Detection & Response (MDR)
- Vulnerability management
- Security awareness training & testing (met onder andere opleidingen en phishingtesten)

Heb je als bedrijf bijvoorbeeld nog geen MFA, dan wordt het al moeilijker om een verzekeraar te vinden. Maar Van Britsom benadrukt dat je nog steeds kan verzekerd worden. ‘Heb je nog niet alles op orde dan kom je nog steeds in aanmerking, maar je tarief zal hoger liggen, of je bent maar tot een bepaald bedrag verzekerd.’ Breng je nadien je veiligheidsprocessen in orde, dan kan je premie dalen.

**‘Een cyberverzekering is als een geneesmiddel. Het zal niet voorkomen dat een virus binnenkomt, maar het helpt je wel om vlotter te herstellen.’**

**Peter Vergote**
Legal Advisor DNS Belgium

‘De kost of inspanningen van die voorzorgen zijn niet de dealbreaker voor een cyberverzekering,’ vult Vergote aan. ‘Ze helpen je te wapenen tegen hackers, en zorgen er voor dat je voorbereid bent in het herstel dat na een cyberincident moet gebeuren.’ De nuance daarbij is wel dat zo’n verzekering geen *hacking* voorkomt. ‘Het is als een geneesmiddel. Het zal niet voorkomen dat een virus binnenkomt, maar het helpt je wel om vlotter te herstellen.’

Ondanks alle maatregelen zijn er wel een aantal elementen die niet onder een cyberverzekering vallen, maar daar hoort enige nuance bij. Het gaat onder meer over:

- Oorlog en terrorisme
- Fraude door eigen personeel
- Misleiding van het personeel
- Onvoldoende beveiligde systemen
- Reputatieschade of dalende beurskoersen.

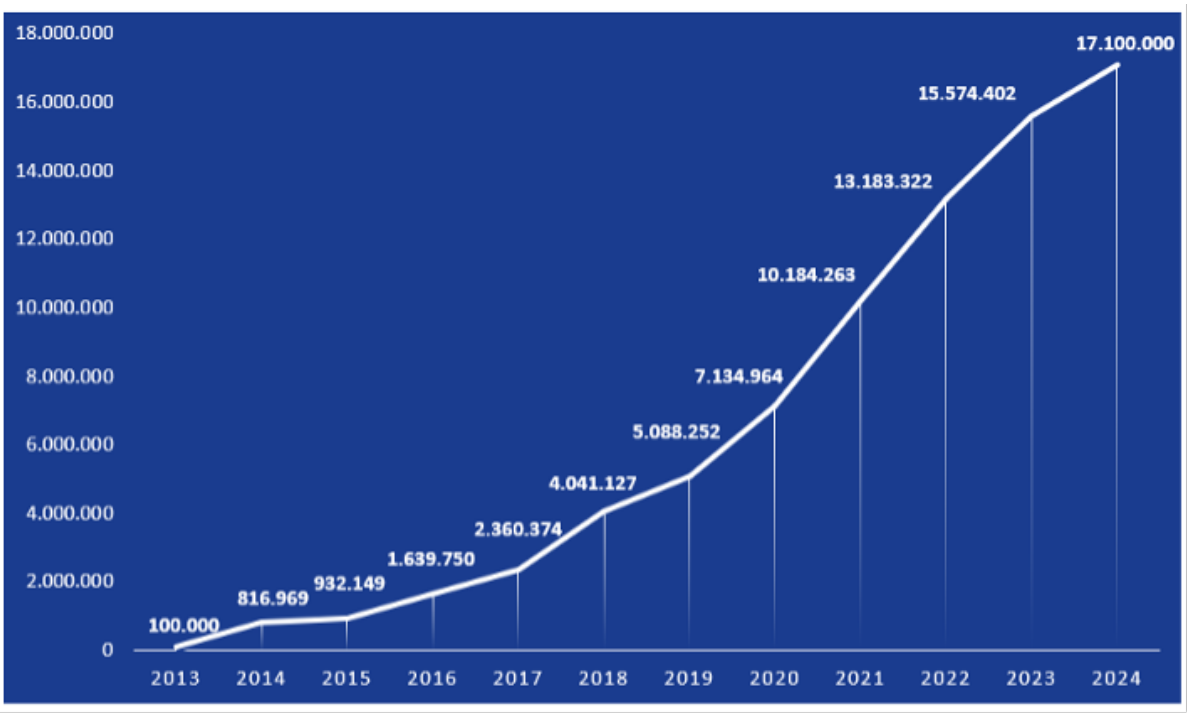
Terrorisme is daarbij een breed begrip. Wil dat zeggen dat een cyberaanval van een vijandig land of terreurgroep nooit gedekt is? ‘Standaard zijn oorlog en terrorisme uitgesloten bij verzekeringen. Maar een cyberverzekering bevat wel dekking voor cyberterrorisme. We hebben bedrijven gezien die zijn geïnfecteerd met NotPetya (*malware* die data versleutelt en vermoedelijk vanuit Rusland werd ingezet, nvdr), die bedrijven konden wel een beroep doen op hun polis. Ook al opereren de hackers in naam van een staat, dat valt voor de verzekering niet onder ‘oorlog’.’

## Inbreken in het systeem vs. inbreken in je hoofd

Wanneer een werknemer fraudeert of via de bedrijfssystemen schade veroorzaakt, wordt dat niet gedekt. Bij misleiding zit de nuance in de manier waarop het gebeurt. Klikt een werknemer per ongeluk op een phishinglink waardoor een hacker toegang krijgt totde systemen kan, dan is dat gedekt onder de cyberverzekering valt. Ook als diezelfde medewerker wordt overtuigd om op de phishinglink te klikken of via een nagemaakte pagina logingegevens invult, waardoor de dader toegang krijgt tot de systemen en hiervan misbruik maakt. ‘In dat geval is het de dader zelf die in de systemen prutst of betalingen uitvoert, dat is kwaadwillig gebruik en dat is effectief gedekt in de cyberverzekering.’

Wanneer een hacker diezelfde medewerker weet te overtuigen om een betaling te doen, dan wordt die medewerker om de tuin geleid en is het fraude. ‘Dat is als het ware ‘inbreken in je hoofd’, en dat valt niet onder de cyber-, maar de fraudeverzekering. Net als wanneer een crimineel met een mail, telefoontje of een deepfake video- of audiogesprek zich weet voor te doen als de CEO en vraagt om dringend een betaling te doen, dan is het de medewerker die de betaling uitvoert en dat valt onder de fraudeverzekering. Daar bestaat helaas veel verwarring over.’

In landen zoals de VS en het VK zijn cyberverzekeringen al veel langer gekend en relatief wijd verspreid, zelfs bij kleinere bedrijven. In België en Europa verzekeren we sinds 2010 bedrijven in cyber. Sinds 2020 is de markt stevig aan het groeien.  Van Britsom: "In onze klantenportefeuille van Belgische organisaties met meer dan vijftig medewerkers heeft één op twee een cyberverzekering. In organisaties met minder medewerkers ligt dat lager, maar we zien interesse in alle groottes en sectoren. Soms worden er ook polissen voor de hele sector afgesloten.



*Stijging premievolume cyberpolissen voorbije 10 jaar bij Vanbreda Risk & Benefits*

**Wie neemt een cyberverzekering?**

| | |
|---|---|
| 18 procent | Industrie |
| 18 procent | Groot- en detailhandel |
| 16 procent | Vrije beroepen |
| 12 procent | Informatie- en communicatiebedrijven |

Daarnaast sluiten sommige sectoren of federaties ook een polis af voor een groep van spelers of alle spelers.

## NIS2 en aansprakelijkheid

De nieuwe EU-wetgeving, de NIS2-richtlijn, verplicht bedrijven om zich te wapenen tegen cybersecurity voor de essentiële diensten die ze aanbieden. Opvallend is de expliciete en persoonlijke aansprakelijkheid van het management en bestuurders voor de naleving van de richtlijn.

Om aan haar verantwoordelijkheden te voldoen, moet het management:

- De risicobeheersmaatregelen omtrent cyberbeveiliging goedkeuren
- Toezicht houden op de implementatie van de richtlijn
- Verantwoordelijkheid nemen voor de naleving van de richtlijn.

Het is dus van belang proactief actie te nemen rond cyberbeveiliging en alert te blijven voor mogelijke dreigingen. Een cyberverzekering biedt extra bescherming, maar alleen als de basisbeveiliging in orde is.

‘Een cyberverzekering, inclusief de hulplijnen die daarbij horen, past in de NIS2-strategie,’ zegt Van Britsom. ‘Ook daar moet je een voorbereiding en een plan van

aanpak klaar hebben. Voor veel organisaties is een cyberverzekering daarom een deel van hun business continuity plan en cyberincident response plan.’

Vergote: ‘Je kan alle voorbereidingen inplannen, je bent beter voorbereid op een incident. Dat maakt dat het niet afsluiten van een cyberverzekering, zeker voor een technische instantie als DNS Belgium, bijna schuldig verzuim zou zijn.’

Doet een verzekering die losgeld betaalt meer kwaad dan goed?

Hoewel ransomware maar één van de situaties is waar een cyberverzekering van pas komt, is het wel het incident dat het vaakst opduikt in de media. Bedrijven moeten snel kiezen tussen veel geld betalen, doorgaans in cryptomunten, of hun bedrijfsdata verliezen of gepubliceerd zien.

**‘Veel organisaties schieten in blinde paniek en gaan snel betalen in de hoop snel weer verder te kunnen, maar betalen is niet altijd de beste of snelste oplossing.'**

**Tom Van Britsom**
Cyberexpert Vanbreda Risk & Benefits

Tegelijk roepen sommige cyberexperts op om nooit zomaar te betalen omdat je zo criminelen aanmoedigt om hun aanvallen verder te zetten. Zorgt een cyberverzekering en dan niet voor dat de criminele kassa blijft rinkelen?

‘Als er geen andere uitweg is, dan stelt de professionele onderhandelaar via de verzekering die bitcoins ter beschikking,’ zegt Van Britsom. ‘Maar als we naar de cijfers kijken dan betaalt gemiddeld één op twee het losgeld bij ransomware. Onder organisaties met een cyberverzekering is dat één op vier.’

Hier wijst de cyberexpert van Vanbreda Risk & Benefits naar de hulplijn met experts die de situatie mee inschatten. ‘Veel organisaties schieten in blinde paniek en gaan snel betalen in de hoop snel weer verder te kunnen, maar betalen is niet altijd de

beste of snelste oplossing. Begin dit jaar spraken we een klant wiens data versleuteld was. In ons onderzoek hebben we ontdekt dat de sleutel mee geëncrypteerd was. Betalen had in dit geval geen enkel verschil gemaakt. We hebben toen de keuze gemaakt om alles vanaf nul weer op te bouwen en dat was de beste oplossing.'

Het is dus niet omdat je je data meteen terug hebt, dat je een dag later weer op kruissnelheid bent. 'Als je betaalt en het herstel duurt drie maanden, of je betaalt niet en het heropbouwen duurt vier maanden, dan kan je die afweging maken.' Onderhandelen en mogelijke pistes bekijken samen met experts zorgen er dus voor dat er gemiddeld minder vaak wordt betaald, stelt Van Britsom.

## Cyberverzekering voor particulieren?

Als particulier kan je je ook laten verzekeren tegen schade door cybercriminelen maar het aanbod in België is beperkt. Vaak is het onderdeel van een gezinsverzekering of digitale bescherming die dekking biedt voor:

- Online oplichting
- Identiteitsdiefstal
- Reputatieschade
- Hacking

Deze verzekeringen zijn nog niet zo wijd verspreid als bij bedrijven, waardoor ze soms nog hiaten vertonen of niet volledig zijn afgestemd op de noden van een particulier.

Vergote: 'De hamvraag voor particulieren is hoe ver de dekking gaat. Ben je gedekt voor de situatie dat een cybercrimineel je kan misleiden waardoor hij duizenden euro's van je rekening kan halen? En in welke mate vervalt die dekking als je zelf onvoorzichtig bent geweest, bijvoorbeeld door wachtwoorden te hergebruiken?'

Hij maakt daarbij nog een belangrijk onderscheid tussen bedrijven en particulieren: 'Een bedrijf heeft een bepaalde reputatie en die kan bij een cyberincident aan diggelen liggen en gevolgen hebben voor de omzet. Bij een particulier ligt dat anders, daar gaat niemand je scheef bekijken als je slachtoffer bent geworden. Bovendien is de kans daar ook klein dat je er schade aan anderen mee berokkent.'

## Wat kan je zelf doen als individu?

Hoewel zo'n verzekering voor particulieren een nuttig vangnet kunnen zijn, moet je in de eerste plaats zelf instaan voor je veiligheid online. Dat doe je door je bewust te zijn van de risico's, de bestaande middelen optimaal te benutten en je toestellen en apps up-to-date te houden.

- Gebruik *tweestapsverificatie* (*2FA*, ook wel multi-factor authenticaton of MFA genoemd) in. Je moet dan naast je wachtwoord ook een code (per mail, sms, via een authenticator app) ingeven. Zo kan een hacker die je wachtwoord kan raden of onderscheppen niet zomaar in je account.

- Krijg je een telefoontje ‘van de bank’ of een Whatsapp van een onbekende die beweert een vriend of familielid te zijn? Dat kan een poging tot oplichting zijn.
- Krijg je van Itsme een vraag tot goedkeuring wanneer je dat niet verwacht? Weiger die dan.
- Gebruik voor elke account een verschillend en liefst moeilijk wachtwoord. Een *wachtwoordmanager* kan je helpen om voor elke website de verschillende wachtwoorden te bewaren.
- Verander je wachtwoorden regelmatig. Zeker bij accounts die geen 2FA hebben is het aan te raden om dit jaarlijks of sneller te doen.

**Bron**: website DNS Belgium
**Datum**: 20/10/2025