GIDS

De complete gids voor cyberverzekeringen

Dekking, kosten, acceptatie-eisen, claimproces, marktoverzicht, NIS2 en DORA. Met actuele Nederlandse marktdata en bronvermelding.

Maart 2026

IBGIDS NL

INHOUDSOPGAVE

Kerncijfers op een rij

De Nederlandse cyberverzekeringsmarkt groeit, premies dalen en de noodzaak stijgt. Hieronder de feiten.

EUR 270K

Gemiddelde schade per cyberincident voor MKB in Nederland

Verzekercyber.nl [1]

77%

van het MKB heeft in de afgelopen 2 jaar te maken gehad met cybercrime

Vodafone Business [2]

EUR 111M

Bruto premie cyberverzekeringen Nederland (2024, +10% t.o.v. 2023)

Verbond van Verzekeraars [3]

-32%

Premiedaling internationaal (2025--2026) door overcapaciteit op de markt

Gallagher Re [4]

60%

van kleine bedrijven gaat failliet binnen 6 maanden na een ernstige cyberaanval

Laurus Verzekeringen [5]

EUR 690

Startpremie per jaar voor een cyberverzekering bij klein MKB

MKB Collectief Verzekerd [6]

Q2 2026

Verwachte inwerkingtreding Cyberbeveiligingswet (NIS2) -- ~10.000 bedrijven getroffen

Digitale Overheid [7]

1%

van alle bedrijven (2+ werkzame personen) was in 2023 slachtoffer van ransomware

CBS Cybersecuritymonitor 2024 [8]

1. Wat is een cyberverzekering?

Een cyberverzekering dekt de financiele gevolgen van cyberincidenten: van forensisch onderzoek en dataherstel tot gederfde omzet en claims van derden bij een datalek.

Het is geen vervanging voor goede beveiliging -- verzekeraars eisen basale security-maatregelen als voorwaarde. Maar het is een vangnet voor wanneer het ondanks die maatregelen toch misgaat. En dat gebeurt: 77% van het Nederlandse MKB heeft in de afgelopen twee jaar te maken gehad met cybercrime [2].

DRIE PIJLERS VAN EEN CYBERVERZEKERING

- **Hulpverlening (incident response)** -- 24/7 hulplijn met directe toegang tot forensisch team, juridisch advies en PR/communicatie. De waarde van deze diensten bij een incident: EUR 10.000--50.000+ [9]
- **Eigen schade (first party)** -- Kosten die je zelf maakt: forensisch onderzoek, dataherstel, bedrijfsstilstand, ransomware, crisismanagement
- **Aansprakelijkheid (third party)** -- Claims van derden: datalek bij klanten, privacyschending, juridische kosten, AVG-boetes

FIRST PARTY -- EIGEN SCHADE

COMPONENT	WAT HET INHOUDT
Forensisch onderzoek	Technisch onderzoek naar oorzaak, omvang en impact (~EUR 4.000/dag) [10]
Bedrijfsstilstand	Gederfde omzet en extra kosten door systeem-downtime (gemiddeld EUR 1.560.000) [11]
Ransomware / losgeld	Betaald losgeld, mits niet uitgesloten en als beste optie beoordeeld door IR-team
Data-herstel	Reconstructie van verloren of beschadigde data en systemen
Meldplichtkosten (AVG)	Juridische kosten, notificatie aan betrokkenen en Autoriteit Persoonsgegevens
Crisismanagement	PR, communicatie, reputatieherstel, call center voor getroffen klanten
Cyberafpersing	Kosten bij afpersing en dreigingen (breder dan alleen ransomware)

THIRD PARTY -- AANSPRAKELIJKHEID

COMPONENT	WAT HET INHOUDT
Privacyaansprakelijkheid	Claims van betrokkenen na datalek of privacyschending
Netwerkbeveiliging	Aansprakelijkheid als jouw systeem gebruikt wordt om derden te schaden
Juridische kosten	Advocaatkosten, verweer tegen claims en procedures
Boetes en sancties	AVG-boetes Autoriteit Persoonsgegevens (in NL onder voorwaarden verzekerbaar) [12]
Mediaschade	Aansprakelijkheid voor content op website of social media

STANDALONE VS MODULE VS ZELF DRAGEN

KENMERK	STANDALONE CYBERPOLIS	CYBERMODULE OP AVB/BAVA	ZELF DRAGEN
Scope	Volledig: first + third party + IR	Beperkt: meestal alleen third party	Geen overdracht
Dekking	EUR 250K--5M+	Vaak max EUR 50K--100K	Eigen draagkracht
Incident response	24/7 IR-team standaard	Zelden inbegrepen	Zelf regelen
Forensisch onderzoek	Volledig gedekt	Beperkt of niet	Zelf betalen (~EUR 4.000/dag)
Ransomware	Gedekt (mits voorwaarden voldaan)	Zelden gedekt	Zelf betalen
Bedrijfsstilstand	Gedekt na wachttijd (8--12 uur)	Meestal niet	Zelf opvangen
Premie indicatie MKB	EUR 1.500--10.000/jaar	EUR 200--500/jaar extra	Geen premie, wel reservering
Geschikt voor	Digitaal afhankelijk MKB/ enterprise	Laag digitaal risico	Enterprise met eigen IR + reserves

Wanneer kies je standalone?

Als je organisatie afhankelijk is van digitale systemen, persoonsgegevens verwerkt, bedrijfsstilstand direct omzetverlies betekent, of als opdrachtgevers een cyberverzekering als eis stellen. Een cybermodule op de BAVA is zelden voldoende voor een organisatie die digitaal werkt [13].

Waarom nu een goed moment

Na premiestijgingen van 20--25% in 2021--2022 door de ransomware-golf, dalen premies nu fors. Gallagher Re meldt internationaal een daling van 32% [4]. Bijna 40% van klanten kreeg premieverlaging bij verlenging [14]. Dit is het gunstigste moment in jaren om een cyberverzekering af te sluiten.

2. Waarom is het belangrijk?

De vraag is niet of je wordt aangevallen, maar wanneer. De cijfers laten zien waarom een cyberverzekering voor MKB-bedrijven geen luxe is maar noodzaak.

DE BUSINESS CASE

77% van het Nederlandse MKB heeft in de afgelopen twee jaar te maken gehad met cybercrime [2]. De gemiddelde schade per incident bedraagt EUR 270.000 [1]. 60% van kleine bedrijven gaat failliet binnen zes maanden na een ernstige cyberaanval [5]. De gemiddelde stilstandkosten alleen al bedragen EUR 1.560.000 [11].

Het CBS meldde in de Cybersecuritymonitor 2024 dat 1% van alle bedrijven met 2+ werkzame personen in 2023 te maken kreeg met ransomware [8]. Dat klinkt laag, maar bij meer dan 400.000 bedrijven in Nederland zijn dat duizenden getroffen organisaties per jaar. En ransomware is slechts een van de dreigingen -- phishing, datalekken, CEO-fraude en supply chain-aanvallen komen daar bovenop.

INCIDENT RESPONSE ALS KERNWAARDE

Veel adviseurs beschouwen incident response als de belangrijkste waarde van een cyberverzekering, boven de financiele dekking [9]. Bij een serieus incident heb je direct toegang tot:

- **24/7 incident response hotline** -- direct contact met specialisten
- **Forensisch team** -- analyse en stoppen van de aanval
- **Juridisch advies** -- direct beschikbaar voor meldplicht (72 uur AVG) en aansprakelijkheid
- **PR/communicatie** -- crisiscommunicatie naar klanten en stakeholders

De waarde van deze diensten bij een incident: EUR 10.000--50.000+. Dit is inbegrepen in je premie.

DRIE PRAKTIJKVOORBEELDEN

Marketingbureau -- ransomware (EUR 15.000)

Een marketingbureau werd getroffen toen de DGA zijn computer opstartte met een afbeelding van een grote sleutel op het scherm. Een hacker eiste een bedrag in crypto, anders zouden systemen versleuteld blijven. De cyberverzekering dekte de totale schade van EUR 15.000, inclusief forensisch onderzoek en herstel [15].

Productiebedrijf auto-onderdelen -- phishing (EUR 167.500)

Een werknemer klikte op een kwaadaardige link in een e-mail. Malware versleutelde alle gegevens op de server. Totale kosten: EUR 167.500 -- opgebouwd uit forensisch onderzoek, dataherstel, bedrijfsstilstand en juridische kosten [16].

Excluparts -- ransomware zonder cyberverzekering (>EUR 100.000)

Automaterialenbedrijf Excluparts werd in 2019 slachtoffer van ransomware. Cybercriminelen eisten bitcoins als losgeld. Het bedrijf verloor boekhoudgegevens, klantenbestanden en leveranciersoverzichten. Schade: meer dan EUR 100.000. Het bedrijf had geen cyberverzekering en moest alle kosten zelf dragen [17].

LES VAN EXCLUPARTS

Zonder cyberverzekering betaal je alles zelf. Een premie van EUR 2.000--5.000/jaar had Excluparts meer dan EUR 95.000 bespaard, plus directe toegang tot een IR-team.

ROI VAN EEN CYBERVERZEKERING

De rekening is simpel

Een MKB-premie van EUR 1.500--2.500/jaar tegenover een gemiddelde schade van EUR 270.000 per incident [1]. Dat is een factor 100x+ verschil. Bij slechts 0,6% kans op een serieus incident per jaar is de verwachte waarde al positief. 60% van kleine bedrijven gaat failliet na een ernstige aanval [5] -- een verzekering kan dat voorkomen.

3. Hoe werkt het? (het proces)

Van aanvraag tot claim: het acceptatieproces bepaalt je dekking en premie, en het claimproces bepaalt hoe snel je weer operationeel bent.

HET ACCEPTATIEPROCES STAP VOOR STAP

1. **Aanvraag**
   Contact met verzekeraar of intermediair. Eerste inventarisatie van je bedrijf, sector en omvang.

2. **Vragenlijst / risicoscan**
   Uitgebreide cyber-vragenlijst over je IT-omgeving, maatregelen en processen.

3. **Technische scan**
   Sommige verzekeraars voeren een externe vulnerability scan uit op je publieke aanvalsvlak.

4. **Risicobeoordeling**
   Score op branche, omvang en security-volwassenheid bepaalt je risicoprofiel.

5. **Premie en voorwaarden**
   Op basis van je risicoprofiel ontvang je een offerte met premie, dekking en voorwaarden.

6. **Verbeterpunten**
   De verzekeraar kan eisen stellen, bijvoorbeeld "MFA implementeren binnen 90 dagen".

7. **Ondertekening**
   Polis wordt ingangsdatum. Zorg dat je team weet wie te bellen bij een incident.

8. **Jaarlijkse review**
   Hernieuwde risicobeoordeling bij verlenging. Je risicoprofiel en premie worden opnieuw beoordeeld [18].

MINIMALE SECURITY BASELINE

Verzekeraars eisen basale security-maatregelen als voorwaarde voor een polis. Zonder deze maatregelen krijg je geen dekking of betaal je een forse toeslag.

MAATREGEL	STATUS	TOELICHTING
Multi-Factor Authenticatie (MFA)	Verplicht	Voor alle externe toegang, e-mail, VPN, admin accounts [19]
Regelmatige backups (3-2-1 regel)	Verplicht	Inclusief offline/immutable backups, periodiek testen
Patch management	Verplicht	Kritieke patches binnen 48--72 uur, regulier maandelijks
Endpoint protection (EDR)	Sterk aanbevolen	Traditionele antivirus onvoldoende, EDR steeds vaker vereist
Security awareness training	Sterk aanbevolen	Periodieke training en phishing-simulaties
Incident response plan	Sterk aanbevolen	Gedocumenteerd plan, jaarlijks getest
Netwerksegmentatie	Aanbevolen	Scheiding van kritieke systemen
Encryptie	Aanbevolen	Data at rest en in transit versleuteld
Logging en monitoring	Aanbevolen	Centraal logbeheer, detectie van afwijkingen
Toegangsbeheer (least privilege)	Aanbevolen	Minimale rechten per gebruiker [20]

IMPACT BEVEILIGINGSNIVEAU OP PREMIE

BEVEILIGINGSNIVEAU	EFFECT OP PREMIE
Alle baselines aanwezig	Standaardpremie, mogelijk 10--20% korting
Gedeeltelijk voldaan	Toeslag 20--50%, lagere verzekerde som
Niet voldaan aan minimale eisen	Afwijzing of alleen basisdekking beschikbaar

HET CLAIMPROCES BIJ EEN INCIDENT

Je hebt een cyberincident. Wat nu? Het claimproces bestaat uit negen stappen -- en snelheid is cruciaal.

1

Incident ontdekken

DIRECT

Verdachte activiteit, ransomware-melding, datalek of ongebruikelijke netwerkactiviteit.

2

Melden bij verzekeraar

BINNEN UREN

Bel direct de 24/7 hotline. Wacht niet tot het volgende moment -- elke minuut telt. Documenteer wat je weet.

3

Incident manager toegewezen

BINNEN UREN NA MELDING

De verzekeraar wijst een incident manager toe die het proces coordineert.

4

Triage

DAG 1

Ernst beoordelen, direct IR-team inzetten. Welke systemen zijn getroffen? Wat is de impact?

5

Forensisch onderzoek

1--4 WEKEN

Oorzaak, omvang en impact vaststellen. Hoe is de aanvaller binnengekomen? Welke data is getroffen?

6

Schadebeperking

PARALLEL AAN FORENSISCH

Systemen isoleren, herstellen, data terugzetten uit backups. Bedrijfsvoering hervatten.

7

Juridische stappen

BINNEN 72 UUR (AVG)

Meldplicht bij Autoriteit Persoonsgegevens (72 uur), juridisch advies over aansprakelijkheid.

8

Schadedocumentatie

2--4 WEKEN NA AFRONDEN FORENSISCH

Alle kosten documenteren en claimdocumentatie indienen bij de verzekeraar.

9

Uitbetaling

2--6 WEKEN NA COMPLETE DOCUMENTATIE

Verzekeraar beoordeelt de claim en betaalt uit. Totaal simpele claim: 4--8 weken. Complexe claim: 3--6 maanden [21].

DOCUMENTATIE IS ALLES

De doorlooptijd van je claim hangt sterk af van de compleetheid van je documentatie. Bewaar alles: screenshots, logs, tijdlijn van het incident, facturen van externe hulp, en communicatie met de verzekeraar. Onvolledige documentatie vertraagt uitbetaling.

4. Wat kost het?

Cyberverzekeringspremies varieren sterk op basis van omzet, sector en beveiligingsniveau. De markt is in 2025--2026 gunstiger dan ooit.

PREMIE PER BEDRIJFSGROOTTE

BEDRIJFSGROOTTE	PREMIE PER JAAR	VERZEKERD BEDRAG	EIGEN RISICO (INDICATIE)
ZZP / micro (1--5 pers.)	EUR 500--900 [6]	EUR 100K--250K	EUR 500--1.000
Klein MKB (5--25 pers.)	EUR 690--2.500 [1]	EUR 250K--500K	EUR 1.000--5.000
Middelgroot MKB (25--100 pers.)	EUR 2.500--10.000	EUR 500K--2M	EUR 5.000--15.000
Groot MKB / enterprise (100+ pers.)	EUR 10.000--50.000+	EUR 1M--5M+	EUR 10.000--25.000+

PREMIEBEPALENDE FACTOREN

1. **Omzet** -- primaire berekeningsfactor voor de meeste verzekeraars
2. **Sector** -- e-commerce (~EUR 2.097/jaar), zorg en financieel betalen meer [22]
3. **Verzekerd bedrag** -- van EUR 100K tot EUR 5M+
4. **Beveiligingsniveau** -- MFA, backups, EDR aanwezig = korting; ontbreken = toeslag of weigering
5. **Eigen risico** -- hoger eigen risico = lagere premie
6. **Schadehistorie** -- eerdere claims verhogen de premie significant

PREMIETREND 2020--2026

PERIODE	PREMIE-OMZET NL	TREND
2020	~EUR 25 miljoen	Jonge markt
2021--2022	~EUR 65--80 miljoen	Stijging 20--25%/jaar door ransomware-golf
2023	EUR 101 miljoen	+26% -- sterke volumegroei [23]
2024	EUR 111 miljoen	+10% -- premie per polis stabiliseert [3]

PERIODE	PREMIE-OMZET NL	TREND
2025 (schatting)	EUR 115--120 miljoen	+5--8% -- overcapaciteit, concurrentie
2026 (verwacht)	Verdere volumegroei	Premie per polis -32% internationaal [4]

De premie-omzet is meer dan verviervoudigd sinds 2020, maar de premie per individuele polis daalt nu door concurrentie en overcapaciteit op de markt.

EIGEN RISICO EN WACHTTIJD

Het eigen risico bij cyberverzekeringen varieert van EUR 1.000 tot EUR 25.000+, afhankelijk van bedrijfsgrootte en type incident. Bij ransomware is het eigen risico vaak hoger. Sommige verzekeraars hanteren geen eigen risico voor IR-kosten. De meeste polissen kennen een wachttijd van 8--12 uur voordat de dekking van bedrijfsstilstand ingaat.

> **Gunstig moment om af te sluiten**
>
> De markt kent overcapaciteit: meer verzekeraars bieden cyber aan dan er vraag is. Internationaal dalen premies met 32% [4]. Bijna 40% van klanten kreeg premieverlaging bij verlenging [14]. Dit maakt 2026 een gunstig moment om een cyberverzekering af te sluiten of je huidige polis te herzien.

5. Waar moet je op letten bij het kiezen?

Er zijn 17+ actieve cyberverzekeraars in Nederland. De keuze hangt af van je sector, omvang en gewenste dekking. Hieronder de criteria die ertoe doen.

SELECTIECRITERIA

1. **Dekking die past bij je risicoprofiel** -- niet elke polis dekt ransomware, bedrijfsstilstand of AVG-boetes. Stem de dekking af op je werkelijke risico's.
2. **Incident response kwaliteit** -- wie wordt er ingeschakeld bij een incident? Hoe snel zijn ze ter plaatse? Is het een 24/7 dienst?
3. **Eigen risico per type incident** -- het eigen risico voor ransomware is vaak hoger dan voor andere incidenten. Vraag een uitsplitsing.
4. **Uitsluitingen lezen** -- oorlogsclausule, bekende kwetsbaarheden, social engineering (CEO-fraude). De details staan in de polisvoorwaarden.
5. **Premie vs. verzekerd bedrag** -- niet alleen de goedkoopste polis kiezen, maar de polis met de meeste dekking per euro premie.
6. **Ervaring in jouw sector** -- een verzekeraar die jouw sector kent, begrijpt de risico's en kan gerichter adviseren.

10 VRAGEN OM TE STELLEN AAN JE VERZEKERAAR

1. Wat is het maximale verzekerd bedrag voor first party en third party apart?
2. Is ransomware losgeld gedekt, en onder welke voorwaarden?
3. Hoe snel is het IR-team ter plaatse na melding, en wie voert het uit?
4. Wat is het eigen risico per type incident (ransomware, datalek, stilstand)?
5. Zijn AVG-boetes van de Autoriteit Persoonsgegevens gedekt?
6. Hoe is de oorlogsclausule / state-backed attack exclusie geformuleerd?
7. Is schade via een leverancier (supply chain) gedekt?
8. Welke security-eisen stel je als voorwaarde voor dekking?
9. Wat is de wachttijd voor bedrijfsstilstanddekking?
10. Hoe verloopt de jaarlijkse hernieuwde risicobeoordeling?

RED FLAGS

> **WAAR JE VOOR MOET OPPASSEN**
>
> Geen 24/7 IR-dienst inbegrepen. Alleen third party dekking zonder first party. Verzekerd bedrag onder EUR 250K voor een MKB met digitale afhankelijkheid. Geen duidelijke uitsplitsing van het eigen risico per type incident. Polisvoorwaarden die niet beschikbaar zijn voor ondertekening.

TIP

Gebruik het acceptatieproces als roadmap voor je basisbeveiliging. Als je aan de acceptatie-eisen van een verzekeraar voldoet, heb je niet alleen een lagere premie maar ook een significant betere security posture.

6. Veelgemaakte fouten

Deze zeven valkuilen ondermijnen de waarde van je cyberverzekering.

1. Onderverzekerd afsluiten

Een verzekerd bedrag van EUR 100K klinkt veel, maar een gemiddeld incident kost EUR 270.000 [1]. De gemiddelde stilstandkosten alleen al bedragen EUR 1.560.000 [11]. Excluparts draaide na ransomware op voor meer dan EUR 100.000 aan schade -- zonder verzekering [17]. Bereken je maximale schade realistisch: forensisch onderzoek, stilstand, juridische kosten, notificatie en herstel.

2. Uitsluitingen niet gelezen

De oorlogsclausule, social engineering (CEO-fraude), supply chain-incidenten en toezichthoudersboetes zijn niet bij elke polis gedekt. De Merck/NotPetya-zaak (EUR 1,3 miljard schade) laat zien hoe groot de impact van een oorlogsuitsluiting kan zijn [24]. Lees de voorwaarden woord voor woord.

3. Security-eisen niet nageleefd

Als je bij het afsluiten aangeeft dat je MFA hebt maar het in de praktijk niet consequent gebruikt, kan de verzekeraar uitkering weigeren bij een claim. Een marketingbureau dat EUR 15.000 claimde na ransomware kreeg gelukkig wel uitbetaling [15] -- maar alleen omdat het aan alle voorwaarden voldeed. Documenteer alle beveiligingsmaatregelen en houd ze up-to-date [25].

4. Cyberverzekering als vervanging voor security

Een verzekering is een vangnet, geen alternatief voor goede beveiliging. Verzekeraars eisen basale maatregelen en weigeren dekking zonder. Het productiebedrijf dat EUR 167.500 schade leed door een enkele phishing-klik had de aanval waarschijnlijk voorkomen met security awareness training [16]. De combinatie is wat werkt: preventie plus verzekering [26].

5. Geen jaarlijkse review

Je risicoprofiel verandert: nieuwe systemen, meer medewerkers, andere diensten. Als de polis niet meegroeit, ben je onderverzekerd op het moment dat het ertoe doet. Herzie je dekking minimaal jaarlijks [27].

6. Supply chain niet meegenomen

Schade via een leverancier (software supply chain attack, cloud provider down) valt niet bij elke polis onder dekking. Third-party betrokkenheid bij datalekken is verdubbeld tot 30% in 2025 [28]. Controleer of supply chain-incidenten gedekt zijn.

7. Alleen financiele dekking gekozen

Sommige goedkope polissen bieden alleen financiele vergoeding achteraf, zonder incident response. De 24/7 IR-dienst is de grootste meerwaarde van een cyberverzekering -- bij een incident telt elke minuut [9]. Kies altijd een polis met directe hulpverlening.

7. Compliance: NIS2, DORA en AVG

Europese en Nederlandse wetgeving rond cybersecurity wordt strenger. Een cyberverzekering is niet verplicht, maar de relatie met compliance is sterk.

NIS2 / CYBERBEVEILIGINGSWET

De Cyberbeveiligingswet (Cbw) -- de Nederlandse implementatie van NIS2 -- treedt naar verwachting in Q2 2026 in werking. Ongeveer 10.000 Nederlandse organisaties vallen direct onder deze wet [7]. De relatie met een cyberverzekering is vijfledig:

1. **Risicoanalyse verplicht** -- NIS2 eist een formeel risicomanagementproces. Het offertetraject voor een cyberverzekering dwingt dezelfde inventarisatie af.
2. **Zorgplicht** -- NIS2 verplicht "passende maatregelen". Een cyberverzekering is een erkende risicomitigatiemaatregel.
3. **Meldplicht** -- NIS2 eist melding binnen 24 uur. Cyberverzekeraars bieden direct IR-ondersteuning voor deze strakke deadline.
4. **Supply chain** -- NIS2 eist compliance van leveranciers. Een cyberverzekering kan leveranciersrisico's afdekken.
5. **Aantoonbaarheid** -- Een polis toont aan dat je risico's serieus neemt richting toezichthouders [29].

> **BOETES NIS2**
> Essentiele entiteiten: tot EUR 10.000.000 of 2% van de wereldwijde jaaromzet. Belangrijke entiteiten: tot EUR 7.000.000 of 1,4% van de jaaromzet [30].

DORA (DIGITAL OPERATIONAL RESILIENCE ACT)

DORA is sinds 17 januari 2025 van kracht en richt zich specifiek op de financiele sector: banken, verzekeraars, beleggingsondernemingen en betaaldienstverleners. Toezichthouders in Nederland zijn AFM en DNB [31].

- **ICT-risicomanagement** -- DORA verplicht formeel ICT-risicomanagement, vergelijkbaar met de eisen die cyberverzekeraars stellen
- **Incidentrapportage** -- Verplichte rapportage van ICT-gerelateerde incidenten
- **Testen digitale weerbaarheid** -- Periodieke testen, waaronder threat-led penetration testing (TLPT)
- **Premievoordeel** -- DORA-compliance kan premieverlaging opleveren bij verlenging, omdat het een betere security baseline aantoont
- **Supply chain** -- Toeleveranciers van financiele instellingen worden indirect ook geraakt

AVG-BOETES: VERZEKERBAAR IN NEDERLAND

Boetes van de Autoriteit Persoonsgegevens zijn in Nederland onder voorwaarden verzekerbaar. Dit is opvallend: Nederland is een van de weinige landen in Europa waar dit mogelijk is. Voorwaarde is dat de boete niet voorkomt uit opzet of grove schuld, en het gaat om een bestuursrechtelijke boete [12]. Niet alle polissen dekken AP-boetes -- controleer de polisvoorwaarden.

RANSOMWARE LOSGELD: DE CONTROVERSIE

De meeste cyberverzekeringen in Nederland dekken betaald losgeld bij ransomware. Maar er is een keerzijde: verzekerde bedrijven betalen gemiddeld 2,8x meer losgeld dan niet-verzekerde bedrijven [5].

Onderzoekers van de Erasmus Universiteit pleiten voor een norm waarin niet-betalen de standaard wordt [32]. Het Verbond van Verzekeraars stelt daar tegenover dat verzekeraars juist helpen om niet te betalen, omdat IR-hulp en forensisch onderzoek losgeld vaak voorkomen [33].

VERWACHTING

NIS2 en DORA zullen de vraag naar cyberverzekeringen sterk aandrijven, vooral bij de ~10.000 bedrijven die direct onder NIS2 vallen, financiele instellingen onder DORA, en hun toeleveranciers.

8. Verschil met verwante oplossingen

Een cyberverzekering is niet de enige manier om met cyberrisico om te gaan. Hier vergelijken we de opties.

CYBERVERZEKERING VS ZELF DRAGEN (RESERVES)

ASPECT	CYBERVERZEKERING	ZELF DRAGEN
Kosten vooraf	EUR 1.500--10.000/jaar premie (MKB)	Geen premie, wel reserve nodig
Maximale schade	Overgedragen aan verzekeraar (tot verzekerd bedrag)	Volledig voor eigen rekening
Incident response	24/7 IR-team inbegrepen	Zelf regelen en betalen (~EUR 4.000/dag forensisch)
Juridische bijstand	Inbegrepen (AVG-meldplicht, aansprakelijkheid)	Zelf regelen en betalen
Geschikt voor	MKB zonder eigen IR-capaciteit	Enterprise met eigen IR-team, juridisch team en EUR 500K+ reserves

Zelf dragen is alleen verantwoord als je organisatie financiele reserves heeft om EUR 270.000+ schade op te vangen en beschikt over eigen forensisch, juridisch en PR-capaciteit [1].

MERCK/NOTPETYA: ILLUSTRATIE OORLOGSUITSLUITING

In 2017 trof de NotPetya-malware farmaceut Merck: 40.000 computers besmet, schade ~EUR 1,3 miljard. Verzekeraar Ace American beriep zich op de oorlogsuitsluiting omdat NotPetya een Russische statelijke aanval op Oekraine was. De rechter in New Jersey gaf Merck gelijk: de oorlogsuitsluiting vereist militaire actie, niet een cyberaanval op commerciele software [24].

Na deze zaak publiceerde Lloyd's Market Bulletin Y5381: alle standalone cyberpolissen moeten vanaf maart 2023 een expliciete state-backed cyber-attack exclusie bevatten. De Lloyd's Market Association publiceerde in 2024 negen nieuwe cyber war clauses [34].

STANDALONE CYBERPOLIS VS CYBERMODULE OP BAVA

ASPECT	STANDALONE CYBERPOLIS	CYBERMODULE OP BAVA
First party dekking	Volledig: forensisch, stilstand, ransomware, dataherstel	Zelden of zeer beperkt (max EUR 50K)

ASPECT	STANDALONE CYBERPOLIS	CYBERMODULE OP BAVA
Third party dekking	Volledig: privacy, netwerkbeveiliging, boetes	Basis: alleen privacyaansprakelijkheid
Incident response	24/7 IR-team standaard inbegrepen	Niet inbegrepen
Verzekerd bedrag	EUR 250K--5M+	Vaak max EUR 50K--100K
Premie MKB	EUR 1.500--10.000/jaar	EUR 200--500/jaar extra op BAVA

Een cybermodule op de BAVA is een budgetoplossing voor organisaties met minimale digitale afhankelijkheid. Voor MKB-bedrijven die serieus digitaal werken, is een standalone polis de aangewezen keuze [13].

9. Trends 2025--2026

Vijf ontwikkelingen die de cyberverzekeringsmarkt de komende jaren vormgeven.

1. Premiedaling door overcapaciteit

Meer verzekeraars bieden cyber aan dan er vraag is. Internationaal dalen premies met 32% [4], Nederland volgt met vertraging. Bijna 40% van klanten kreeg premieverlaging bij verlenging [14]. De markt is in 2025--2026 gunstiger voor kopers dan in de afgelopen vijf jaar.

2. AI-gedreven aanvallen en deepfake fraude

AI-gestuurde phishing is nauwelijks te onderscheiden van echte communicatie. Deepfake-fraude neemt toe: hyperrealistische video en audio voor CEO-fraude en identiteitsdiefstal. "Deepfake-as-a-Service" is in 2025 geexplodeerd als commerciele dienst [35]. Verzekeraars passen polisvoorwaarden aan om AI-gerelateerde aanvallen expliciet op te nemen [36].

3. Supply chain risico groeit

Third-party betrokkenheid bij datalekken is verdubbeld tot 30% in 2025 [28]. Hybride cloud-omgevingen en software supply chains worden primaire doelwitten in 2026. Verzekeraars scherpen supply chain-dekking aan: expliciete inclusie of exclusie in polisvoorwaarden.

4. Bundeling security en verzekering

Verzekeraars bieden steeds vaker cybersecurity-tools mee bij de polis: vulnerability scanners, awareness training platformen, security monitoring. Dit verlaagt het risico voor de verzekeraar en verbetert de security-baseline van de verzekerde. 37% van verzekeraars verwacht sterke toename cyberrisico in 2025 [37].

5. Ransomware-as-a-Service (RaaS)

Ransomware is geevolueerd tot een georganiseerd businessmodel met gedefinieerde rollen, servicestructuren en winstgedreven strategieen. RaaS verlaagt de drempel voor aanvallers en verhoogt het totale volume [38]. 2026 wordt het jaar van geindustrialiseerde cybercriminaliteit [36].

WAT BETEKENT DIT VOOR JOU?

De dreiging stijgt (AI-aanvallen, supply chain, RaaS), maar de premies dalen. Dit maakt 2026 het moment om een cyberverzekering af te sluiten of je huidige polis te herzien. Wacht niet tot de markt weer verhardt.

10. Aan de slag

Een cyberverzekering afsluiten is stap 1. Zo haal je er het maximale uit.

KEN JE POLIS

Zorg dat je team weet wat de dekking is, wat het eigen risico is, en wie je moet bellen bij een incident. De 24/7 hulplijn van je verzekeraar is je eerste contactpunt. Sla het nummer op in je telefoon en deel het met je IT-team.

VOLDOE AAN DE VOORWAARDEN

Houd je security-maatregelen op peil: MFA actief, backups getest, patches bijgewerkt. Een verzekeraar kan uitkering weigeren als je niet aan de gestelde eisen voldoet [25].

EVALUEER JAARLIJKS

Je risicoprofiel verandert. Groei, nieuwe systemen, andere sectoren -- herzie je dekking minimaal jaarlijks en pas aan waar nodig [27].

TEST JE INCIDENT RESPONSE

Voer jaarlijks een tabletop-oefening uit: simuleer een cyberincident en doorloop het claimproces. Weet iedereen wat te doen? Staan de juiste nummers klaar? Is de documentatie op orde?

Marktoverzicht: actieve cyberverzekeraars in Nederland

De Nederlandse cyberverzekeringsmarkt telt circa 17 actieve spelers. Dit is een feitelijk overzicht -- geen aanbeveling. De meeste cyberverzekeringen worden via intermediairs afgesloten.

VERZEKERAAR	DOELGROEP	TYPE
Hiscox (CyberClear)	MKB tot enterprise	Specialist cyber
Chubb	Middelgroot+	Internationaal
AIG (CyberEdge)	Enterprise	Internationaal
Markel	MKB	Specialist
Allianz	MKB tot enterprise	Breed
CNA Hardy	MKB tot enterprise	Professional lines
Zurich	Middelgroot+	Breed
HDI Global	Enterprise	Internationaal
De Goudse	MKB	Nederlands
NN (Nationale-Nederlanden)	MKB	Nederlands
VvAA	Zorg/medisch	Sectorspecifiek
De Vereende (BAVAM)	MKB	Beroepsaansprakelijkheid + cyber
Centraal Beheer (Achmea)	MKB	Nederlands, direct
Avero Achmea (CyberZeker)	MKB	Via adviseurs
Interpolis (Rabobank)	MKB	Via Rabobank
ABN AMRO Verzekeringen	MKB	Via ABN AMRO
Rabobank Cyberrisico	MKB	Via Rabobank

Dit overzicht is informatief. De meeste cyberverzekeringen worden via intermediairs afgesloten. Via **ibgids.nl/word-gematcht** word je gematcht met de adviseur die past bij jouw situatie.

Bronnenlijst

[1] **Verzekercyber.nl** -- Kosten cyberverzekering, gemiddelde schade EUR 270K. https://verzekercyber.nl/wat-kost-een-cyberverzekering/

[2] **Vodafone Business** -- 77% MKB cybercrime in afgelopen 2 jaar. https://www.vodafone.nl/zakelijk/inspiratie/mkb-doelwit-cybercrime-onderzoeken

[3] **Verbond van Verzekeraars** -- Bruto premie EUR 111M (2024). https://www.verzekeraars.nl/verzekeringsthemas/schade/cyber

[4] **Gallagher Re / Risk en Business** -- Premiedaling 32% door overcapaciteit. https://riskenbusiness.nl/nieuws/insurance/gallagher-re-cyberindex-meldt-premiedaling-van-32-door-overcapaciteit-verdere-verlaging-in-2026-verwacht/

[5] **Laurus Verzekeringen** -- 60% failliet na aanval, 2,8x meer losgeld. https://laurusverzekeringen.nl/cyberverzekeringen-onmisbaar/

[6] **MKB Collectief Verzekerd** -- Startpremie vanaf EUR 690/jaar. https://www.mkbcollectiefverzekerd.nl/cyberrisico/

[7] **Digitale Overheid** -- Cyberbeveiligingswet (NIS2), verwacht Q2 2026, ~10.000 bedrijven. https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

[8] **CBS Cybersecuritymonitor 2024** -- Ransomware 1% bedrijven, MFA-gebruik 76%. https://www.cbs.nl/nl-nl/longread/aanvullende-statistische-diensten/2025/cybersecuritymonitor-2024?onepage=true

[9] **Ekelenkamp** -- IR als kernwaarde cyberverzekering, waarde EUR 10K--50K+. https://www.ekelenkamp.nl/cyberverzekering/

[10] **Verzekering.nl** -- Dekking cyberverzekering, forensisch onderzoek ~EUR 4K/dag. https://www.verzekering.nl/veelgestelde-vragen/dekking-cyberverzekering/

[11] **Rabobank** -- Gemiddelde stilstandkosten EUR 1.560.000. https://www.rabobank.nl/bedrijven/verzekeren/verzekeringsnieuws/bescherm-je-tegen-cyberincidenten/

[12] **Aon / DLA Piper** -- AVG-boetes in Nederland onder voorwaarden verzekerbaar. https://www.aon.com/netherlands/newsroom/persberichten/2019/avg-boete-nederland-onder-voorwaarden-verzekerbaar/

[13] **Digital Trust Center (Min. van EZ)** -- Cyberverzekeringen: standalone vs module. https://www.digitaltrustcenter.nl/informatie-advies/cyberverzekeringen/

[14] **Risk en Business / Marsh** -- 40% klanten premieverlaging bij verlenging. https://riskenbusiness.nl/nieuws/insurance/verzekerden-aangespoord-om-te-onderhandelen-over-cyberdekking-nu-de-premies-stabiliseren/

[15] **Cyberadviseur.nl** -- Voorbeeld: cyberverzekering helpt na ransomware-aanval (EUR 15K). https://www.cyberadviseur.nl/voorbeeld-hoe-cyberverzekering-helpt-na-aanval-ransomware/

[16] **Cyberadviseur.nl** -- Schadevoorbeelden cybercrime en datalekken (EUR 167.500). https://www.cyberadviseur.nl/cybercrime/schadevoorbeelden/

[17] **CyberriskInsurance.nl** -- Excluparts: ransomware zonder verzekering (>EUR 100K). https://www.cyberriskinsurance.nl/kleine-bedrijven-slachtoffer-van-de-cyberaanval-ransomware/

[18] **Aon** -- AIC-rapport voor cyberverzekering, bedrijven tot EUR 250M omzet. https://www.aon.com/netherlands/bedrijfsrisicos/digitalisering/cyber-risicomanagement/cyberverzekering.jsp

[19] **Cyberadviseur.nl** -- Overzicht cyberverzekeraars en acceptatie-eisen. https://www.cyberadviseur.nl/cyberverzekering/verzekeraars/

[20] **AGConnect / PQR** -- De 13 minimale security eisen voor IT-omgevingen. https://www.agconnect.nl/partner/pqr-rustmakers-in-it/de-13-minimale-security-eisen-waaraan-elke-it-omgeving-moet-voldoen/

[21] **VNAB** -- Een kort begrip van de cyberverzekering (claimproces). https://www.vnab.nl/cache/een-kort-begrip-van-de-cyberverzekering.3730/een-kort-begrip-van-de-cyberverzekering.pdf

[22] **VMD Koster** -- Wat kost een cyberverzekering? Premiebepalende factoren. https://www.vmdkoster.nl/a-1541/wat-kost-een-cyberverzekering

[23] **VNAB** -- Cyberverzekeringsmarkt: van puber naar jong volwassene. https://www.vnab.nl/nl/actueel/nieuws/cyberverzekeringsmarkt-maakt-snelle-ontwikkeling-door-van-puber-naar-jong-volwassene/

[24] **Stibbe** -- Merck/NotPetya: oorlogsuitsluiting faalt, verzekeraar betaalt >USD 1 miljard. https://www.stibbe.com/publications-and-insights/reliance-on-war-exclusion-clause-after-cyberattack-fails-insurers-must/

[25] **HCA Groep** -- Voorwaarden van je cyberverzekering kennen. https://hcagroep.nl/waarom-je-je-moet-verdiepen-in-de-voorwaarden-van-je-cyberverzekering/

[26] **MKB Westland** -- Cyberweerbaarheid: waarom cyberverzekeringen alleen niet genoeg zijn. https://www.mkbwestland.nl/cyberweerbaarheid-voor-het-mkb-waarom-cyberverzekeringen-alleen-niet-genoeg-zijn/

[27] **De Zaak** -- Cyberverzekering voor bedrijven: jaarlijks herzien. https://www.dezaak.nl/verzekeringen/overige-verzekeringen/cyberverzekering-voor-bedrijven-onmisbaar-of-overbodig/

[28] **Auxis / Verizon DBIR 2025** -- Supply chain betrokkenheid verdubbeld tot 30%. https://auxis.com/10-cybersecurity-trends-defining-2026/

[29] **VNAB** -- Impact NIS2 op ondernemingen en verzekeraars. https://www.vnab.nl/nl/actueel/nieuws/wat-is-de-impact-van-de-nieuwe-europese-regelgeving-nis2-op-ondernemingen-en-verzekeraars/

[30] **NCSC** -- Cyberbeveiligingswet (NIS2): boetestructuur. https://www.ncsc.nl/over-ncsc/wettelijke-taak/wat-gaat-de-nis2-richtlijn-betekenen-voor-uw-organisatie/vragen-en-antwoorden/

[31] **Rijksoverheid** -- DORA: verordening ICT-bescherming financiele sector. https://www.rijksoverheid.nl/onderwerpen/financiele-sector/dora/

[32] **Erasmus School of Law** -- "Niet betalen van losgeld moet de norm worden". https://www.eur.nl/esl/nieuws/we-moeten-toe-naar-een-samenleving-waarin-het-niet-betalen-van-losgeld-de-norm/

[33] **Verbond van Verzekeraars** -- Losgeldverbod voor cyberverzekeringen is geen oplossing. https://www.verzekeraars.nl/publicaties/actueel/losgeldverbod-voor-cyberverzekeringen-is-geen-oplossing/

[34] **Browne Jacobson** -- Lloyd's Market Association: negen nieuwe cyber war exclusion clauses (2024). https://www.brownejacobson.com/insights/the-word-march-2024/lloyd-s-market-association-update/

[35] **Cyble** -- Deepfake-as-a-Service exploded in 2025. https://cyble.com/knowledge-hub/deepfake-as-a-service-exploded-in-2025/

[36] **Banken.nl** -- 2026 wordt het jaar van geindustrialiseerde cybercriminaliteit. https://www.banken.nl/nieuws/26681/2026-wordt-het-jaar-van-geindustrialiseerde-cybercriminaliteit-en-ai-agents/

[37] **Herenvest** -- Cyberverzekeringen in 2025: trends en strategieen. https://www.herenvest.nl/actueel/cyberverzekeringen-in-2025-trends-en-strategieen-voor-effectieve-bescherming/

[38] **CybersecurityAsia / Trend Micro** -- 2026 as year cybercrime becomes fully industrialised. https://cybersecurityasia.net/predict-2026-cybercrime-fully-industrialised/

[39] **Hiscox** -- CyberClear polis, 24/7 incident response. https://www.hiscox.nl/cyberverzekering-cyberclear-hiscox/

[40]

Beterverzekeren -- Cyberverzekering vergelijken 2026. https://www.beterverzekeren.nl/bedrijfsverzekeringen/cybercrime-verzekering/

[41] **Rabobank** -- Zo bereid je je voor op NIS2. https://www.rabobank.nl/bedrijven/verzekeren/verzekeringsnieuws/nis2

[42] **Grant Thornton** -- Cyber threat increases, preparedness falls short (MKB). https://www.grantthornton.nl/en/insights-en/research/cyber-threat-increases-preparedness-falls-short-a-wake-up-call-for-smes/