

CHUBB®

Cyberrisico's voorblijven.



Schaal je cyberbeveiliging
op met Chubb.

Inhoud

De evolutie van Chubb	P3
Cyberisicollandschap	P4
Huidige trends	P5
Dringende privacykwesties en meer	P6
Schadebeperkingsdiensten	P7
Threat Intelligence & Cyber Risk Advisory Team	P8
Incidentenresponsteam & schadeclaims	P9

Je cyberbeveiliging moet een sterk fundament hebben. Zoals alleen een wereldleider dat kan bieden.

De globalisering en digitalisering van het bedrijfsleven hebben een economisch klimaat gecreëerd waarin alle elementen sterk onderling afhankelijk van elkaar zijn. Een dergelijk klimaat zit vol risico's.

Chubb zorgt er al meer dan 25 jaar voor dat bedrijven cyberrisico's voorblijven. Vandaag de dag zijn we wereldleider op het gebied van cyberverzekeringen¹ – een positie die we hebben verdiend door consequent te innoveren op het gebied van dekkingsopties en beheerdiensten voor cyberrisico's om veranderende risico's het hoofd te bieden. Onze cyberschadespecialisten hebben wereldwijd al meer dan 32.500 cyberclaims afgehandeld en onderhouden nauwe banden met de beste responspecialisten die polishouders helpen om cyberincidenten te beperken en te beheren.

Of het nu gaat om polisbewoordingen waarin de nieuwste privacy- en cyberwetgeving is verwerkt, zorgvuldige dekkingsuitbreidingen of de persoonlijke selectie van cyberrisicodiensten om de risico's te beperken, Chubb biedt wat iedere klant vandaag én morgen nodig heeft.

Onze cyberschadespecialisten hebben al meer dan **32.500 cyberclaims** afgehandeld.

ONZE GESCHIEDENIS

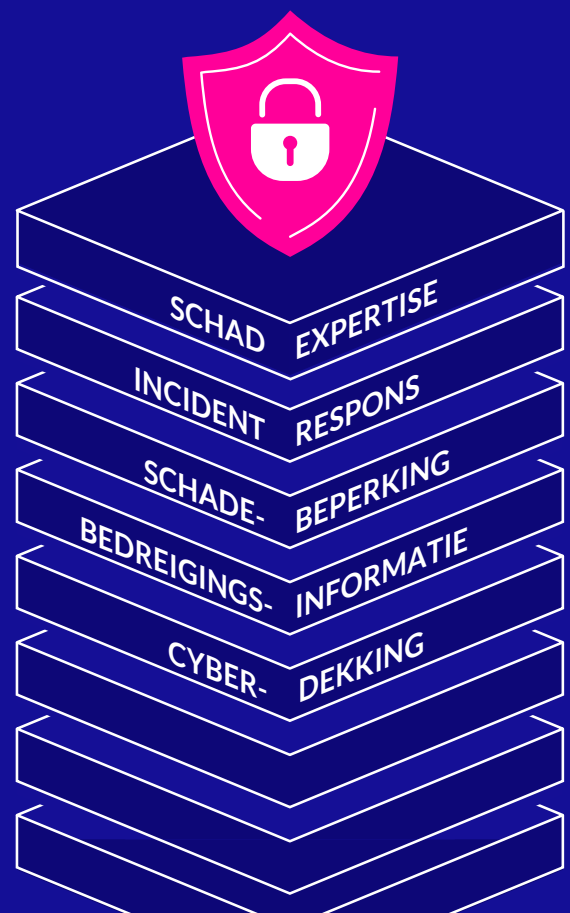
1998

Ons eerste cyberproduct uitgebracht.

2016

Cyber ERM en het Technology Master Package gelanceerd, bijna 20 jaar na de ontwikkeling van ons oorspronkelijke product.

Chubb is wereldwijd een van de grootste aanbieders van cyberverzekeringen, uitgaande van bruto geboekte premies.¹



5,4 miljard

internetgebruikers nu, ten opzichte
van 2,6 miljard 10 jaar geleden.²

280.000+

veelvoorkomende kwetsbaarheden
en risico's geregistreerd, terwijl **er dagelijks**
meer dan 100 bij komen.³

Cyberonveiligheid

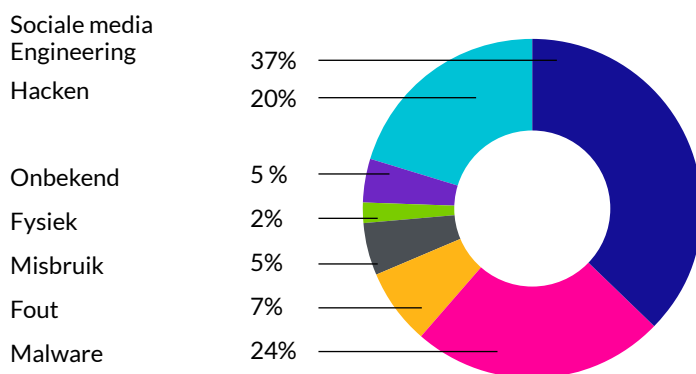
staat op de 4e plaats van de 10 grootste
risico's voor de samenleving.⁴

Als de risico's zich opstapelen, is het tijd om je beveiliging op te schalen.

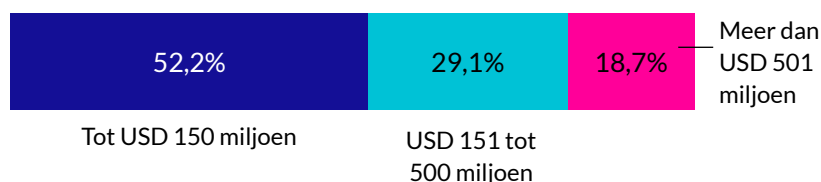
Trends in cyberclaims

Bedrijven van elke omvang hebben te maken met steeds geraffineerder wordende social-engineering-aanvallen, die tot datalekken, ontwrichtende ransomware-incidenten en zelfs reputatieschade kunnen leiden. Onze [cyberindex](#) heeft een inventarisatie gemaakt van triggers die tot dergelijke cyberincidenten leiden en geeft aan waarom bedrijven gebruik zouden moeten maken van de cyberdiensten van Chubb, waaronder de Chubb-cyberbeveiliging voor bedrijven met maximaal 100 werknemers.

Acties die cyberincidenten veroorzaken – 12 maanden Verenigde Staten, alle sectoren, omzet minder dan USD 150 miljoen



percentage jaarlijkse claims naar jaaromzet sinds 2023



Chubb cyberindex

Geeft realtime toegang tot de eigen claimgegevens van Chubb en geeft inzicht in actuele cyberbedreigingen, -trends en -kosten. Gebruikers kunnen perimeters instellen en historische trends bekijken op basis van het type bedreiging, de bedrijfsomvang en de bedrijfstak waarin het bedrijf actief is.

Ongelukken gebeuren:

Uit het Verizon Data Breach Investigations Report (DBIR)⁵ blijkt het volgende:

68% van de inbreuken betrof een niet-opzettelijk menselijk element

28% betrof fouten

15% betrof een derde

In de afgelopen twee jaar is het aantal aan privacy gerelateerde claims toegenomen met **210%**⁶



DRINGENDE PRIVACYKWESTIES EN MEER

De juiste cyberbeveiliging biedt ook dekking voor onbedoelde privacyschendingen.

Niet alle cyberrisico's zijn afkomstig van hackers. Technologische ontwikkelingen leiden ook tot veranderingen in de regelgeving. Als een van de grootste cyberverzekeringsteams ter wereld zijn we actief in meer dan 50 landen. We helpen onze klanten doorlopend bij het identificeren en beheren van de nieuwste risico's en bieden dekking voor risico's die met privacy verband houden.

Bij Chubb helpen we onze klanten niet alleen bij het identificeren en beheren van risico's, maar bieden we ook uitgebreide dekking voor een breed scala aan risico's. Onze veelomvattende verzekeringsoplossingen zijn afgestemd op de unieke behoeften van elk bedrijf.

AVG en BIPA

De AVG (Algemene verordening gegevensbescherming), die in 2018 van kracht is geworden, bepaalt hoe gegevens kunnen worden verzameld, gebruikt, opgeslagen en verwijderd. Het is gebruikelijk dat er wetten bestaan die slachtoffers van privacyschendingen de mogelijkheid bieden om als particulier een rechtszaak aan te spannen wegens geleden schade, in sommige omstandigheden zonder dat ze financieel verlies of aantoonbare schade hebben geleden.

Gegevenscategorieën zoals biometrische gegevens blijven op grond van de AVG een speciale gegevenscategorie, waarvoor vaak toestemming moet worden gegeven voor het verzamelen, gebruiken en verwerken daarvan. Voor bedrijven die met de Verenigde Staten te maken hebben, was de Biometric Information Privacy Act (BIPA, de Wet op de privacy van biometrische gegevens) die in 2008 in Illinois werd uitgevaardigd, de eerste wet waarmee een steeds populairder wordende standaard voor particuliere vorderingsrechten tegen organisaties werd ingesteld en die organisaties bij niet-naleving boetes oplegt.

Cookies, webbakens en pixels

Cookies, webbakens en pixels zijn codes die op websites worden gebruikt om de activiteiten van gebruikers te volgen ten behoeve van klantprofilering, gerichte reclame of gegevensanalyse. Om met behulp van deze trackingtechnologieën gegevens te verzamelen, is toestemming nodig. Als gebruikers niet om toestemming wordt gevraagd, houdt dat een schending in van de privacyregelgeving, zoals de AVG en de Privacy and Electronic Communications Regulations (PECR), een Britse wet die gebruikers privacyrechten

met betrekking tot elektronische communicatie geeft.

Voor polishouders met gebruikers in de Verenigde Staten zien we nog steeds claims wegens privacy-inbreuken op grond van de Video Privacy Protection Act (1988), de Amerikaanse wet ter bescherming van de privacy bij het kijken van video's. Over de hele wereld zien we dat steeds vaker rechtszaken worden aangespannen in verband met het onjuiste gebruik van deze technologie of openbaarmaking van videokijkgewoonten. Bij deze rechtszaken wordt aangevoerd dat zonder toestemming van de gebruikers persoonlijk identificeerbare gegevens zijn onthuld. Dit risico doet zich overal voor en de boetes kunnen hoog zijn.

Kunstmatige intelligentie (AI)

Terwijl het benutten van het volledige potentieel van AI voor organisaties over de hele wereld een belangrijke prioriteit blijft, blijft het – ondanks goedbedoelde inspanningen van overheden – lastig om doeltreffende AI-regelgeving in te voeren. Het beperken van aan AI gerelateerde beveiligingsrisico's is een proces van vallen en opstaan gebleken. Hoewel AI in sommige defensieve beveiligingstools is ingebed, wordt het ook gebruikt door degenen die juist schade willen aanrichten.

Digitale en operationele veerkracht

De regelgeving voor zowel digitale als operationele veerkracht blijft zich snel ontwikkelen. In de EU zijn de afgelopen maanden de Digital Operations Resilience Act ("DORA") en de NIS2-richtlijn van kracht geworden. Deze regelgeving is gericht op de financiële sector en kritieke infrastructuur en voorziet in strenge rapportagetermijnen en mogelijke boetes bij overtreding.

Je bedrijf is te belangrijk om geen sterke cyberbeveiliging te hebben.

Alle ERM-polishouders die een cyberdekking afsluiten, kunnen profiteren van gratis of scherp geprijsde* schadepreventiediensten die hen kunnen helpen om de meest urgente risico's te beperken en de risico's te verkleinen voordat er een cyberincident plaatsvindt.

De door Chubb aangeboden cyberdiensten zijn gebaseerd op de bedreigingsinformatie en claimservaring van Chubb:

- 1 Respons op cyberincidenten**
Een responsplan voor cyberincidenten opstellen, bijstellen of oefenen met alle betrokken partijen.
- 2 Beheer van cyberkwetsbaarheden**
Zwakke plekken in het netwerk van een organisatie opsporen om onjuiste configuraties en kwetsbaarheden proactief op te lossen.
- 3 Beveiliging van eindpunten**
Geavanceerde antivirussoftware en EDR-mogelijkheden (Endpoint Detection and Response) die helpen voorkomen dat cybercriminelen het netwerk van een organisatie binnendringen.
- 4 Gebruikersveiligheid en -bewustzijn**
Tools en training, zodat werknemers als eerste verdedigingslinie kunnen fungeren.
- 5 Privacyrisico**
De risico's en naleving van de regelgeving op het gebied van consumentenprivacy in het hele ecosysteem van een onderneming beheren.

*Waar de wet dit toestaat.

52%

van de doelwitten van cybercriminelen zijn kleine en middelgrote bedrijven.⁶

GRATIS CYBERBEVEILIGING VOOR MKB



Chubb- cyberbeveiliging

Een speciaal samengesteld **pakket diensten** dat wel EUR 27.000 aan jaarlijkse besparingen kan opleveren en via een netwerk van vertrouwde cyberbeveiligingsaanbieders wordt aangeleverd. Deze diensten zijn speciaal ontwikkeld voor bedrijven met 100 of minder werknemers en bedoeld om cyberincidenten te voorkomen, cyberrisico's doeltreffend te beheren en adequaat op incidenten te reageren.⁷



Speciale cyberexperts die zich toeleggen op het opschalen van je verdediging.

Vulnerability Management Outreach

Ons Cyber Intelligence Team bewaakt, scant en identificeert stelselmatig kwetsbaarheden en nieuwe kritieke bedreigingen om onze polishouders te beschermen. Polishouders worden geïnformeerd via:

Ons Outreach-programma

Cyberpolishouders en hun tussenpersonen krijgen bericht als tijdens hun polistermijn bekende kritieke kwetsbaarheden in hun omgeving worden aangetroffen die hoogstwaarschijnlijk zullen worden misbruikt.

Belangrijke meldingen

Worden verstuurd naar cyberverzekerden en hun tussenpersonen wanneer nieuwe kwetsbaarheden worden ontdekt die hoogstwaarschijnlijk zullen worden misbruikt en invloed op hun omgeving kunnen hebben.

Cyber Risk Advisory Team

Onze deskundige cyberrisicoadviseurs staan klaar om de juiste diensten aan te bevelen om de risico's voor polishouders te minimaliseren en hen te helpen bij het integreren van diensten in hun risicobeheerstrategie. Op onze [website](#) kan een afspraak worden gemaakt.



Een goede cyberbeveiliging beschermt niet alleen, maar reageert ook.

Incidentenresponsteam

Als er zich toch een cyberincident voordoet, staat ons deskundige incidentenresponsteam klaar om snel en efficiënt ondersteuning te bieden. Onze teams bestaan uit ervaren externe dienstverleners die advies- en andere diensten leveren op het gebied van juridische aangelegenheden, forensisch computeronderzoek, meldingen, callcenters, PR, crisiscommunicatie, fraude, kredietbewaking en identiteitsherstel.

Chubb Cyber AlertSM



Onze gratis Incident Response Mobile App verbindt polishouders 24/7/365 snel met een Chubb Incident Response Coach. Via de app kunnen ze onder andere foto's insturen om te helpen bij de beoordeling van de gebeurtenis en hun tussenpersoon op de hoogte stellen.

Download de app nu:



Wat maakt de claimafhandeling van Chubb anders?

Onze ervaren schadespecialisten begrijpen dat de afhandeling van claims de belangrijkste test voor onze service, ondersteuning en reputatie is.

Onze expertise is afgestemd op de cultuur en markt van onze klanten en het regelgevende klimaat waarbinnen ze actief zijn.

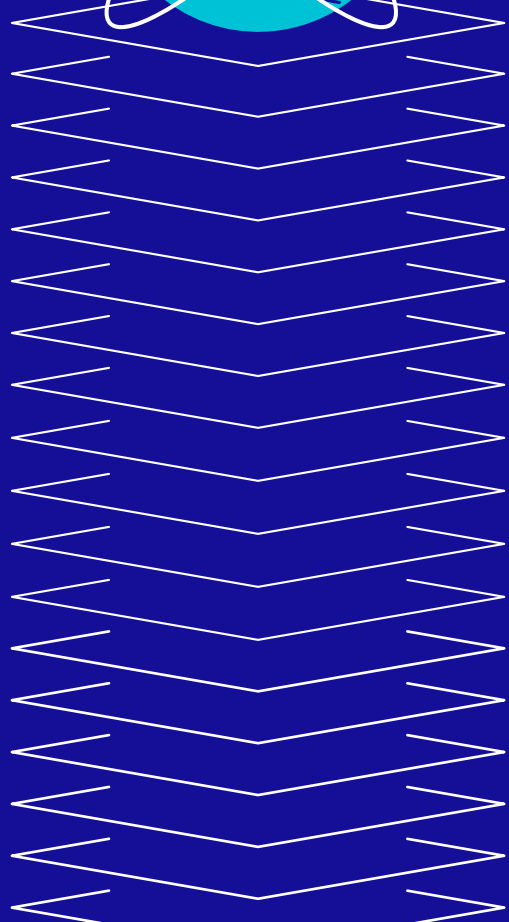
Flexibiliteit wanneer je die het hardste nodig hebt

Of je een incident nu via de hotline of via de Cyber Alert App meldt, je kunt zelf beslissen of je het incident als claim bij Chubb wilt indienen.

Dit team heeft al meer dan

32.500 cyberclaims afgehandeld

en kan ook jou bij jouw claim helpen.



Eindnoten

- ¹ Beinsure (<https://beinsure.com/global-ranking-cyber-insurers>)
- ² Forbes (www.forbes.com/home-improvement/internet/internet-statistics)
- ³ Nationale kwetsbaarheidendatabase van NIST (NIST) (<https://nvd.nist.gov/general/nvd-dashboard>) (vanaf maart 2025)
- ⁴ World Economic Forum - Global Risks Perception Survey, 2024 (<https://www.weforum.org/publications/global-risks-report-2024>)
- ⁵ Verizon Data Breach Investigations Report (www.verizon.com/business/resources/reports/dbir/)
- ⁶ Chubb-cyberindex (chubbcyberindex.com)
- ⁷ Voorwaarden zijn aan verandering onderhevig. De gratis diensten gelden voor een periode van één jaar en alleen voor polishouders die nieuwe abonnees/klanten zijn van de respectieve diensten. Bovendien mogen in aanmerking komende polishouders voor bepaalde diensten niet meer dan 100 werknemers hebben.

Bescherm je bedrijf met Chubb.

Klik op de QR-code of scan de QR-code voor meer informatie over Chubb Cyber:



Alle cyberdiensten zijn onderhevig aan wijzigingen. Eventuele wijzigingen in het dienstenaanbod worden weergegeven op het lokale webformulier voor cyberdiensten. Verzekeringssnemers zijn verantwoordelijk voor het controleren van de specifieke voorwaarden van elke cyberdienstverlener om in aanmerking te komen en op de hoogte te blijven van eventuele wijzigingen die zich kunnen voordoen.

MET KORTING AANGEBODEN CYBERDIENSTEN DOOR DERDE PARTIJEN:

Externe kwetsbaarheidsmonitoring, Veilige wachtwoordbeheerder.

De bovengenoemde cyberdiensten worden door derde partijen aangeboden aan Chubb-verzekeringssnemers voor de genoemde initiële periode, mits de verzekeringssnemer een nieuwe abonnee/klant is van de aangeboden cyberdiensten door de gekozen derde partij en de verzekeringssnemer voldoet aan de gestelde eisen. Na afloop van de genoemde initiële periode hebben verzekeringssnemers de mogelijkheid om hun cyberdiensten voort te zetten tegen een gereduceerd tarief bij verlenging. Houd er rekening mee dat de specifieke korting kan variëren per product en dienst. Kortingen op producten en diensten die worden aangeboden door cyberdienstverleners zijn alleen beschikbaar voor Chubb-verzekeringssnemers met lopende polissen en zijn onderhevig aan de toepasselijke verzekeringswetten. De producten en diensten die worden geleverd door derde partijen worden beheerst door contractvoorwaarden die de verzekeringssnemer aangaat met de derde partij. Chubb is niet betrokken bij de beslissing van de verzekeringssnemer om diensten aan te schaffen en is niet verantwoordelijk voor producten of diensten die worden geleverd door derde partijen.

Wij maken gebruik van door u aan ons [of, voor zover van toepassing, aan uwverzekeringstussenpersoon] verstrektepersoonsgegevensvoor de acceptatie, polisadministratie, schadebeheer, en andere verzekeringsdoeleinden zoals naderomschreven in ons Algemeen Privacybeleid, dat hier kan worden ingezien: www.chubb.com/benelux-nl/footer/privacy-policy.html