

#CyberComfort by Zurich

Security & Privacy Verzekering

Productinformatie



#CyberComfort by Zurich

voor, tijdens en na een cyberincident de beste ondersteuning

In 2017 werden wereldwijd organisaties getroffen door de WannaCry en NotPetya malware aanvallen. Deze schadelijke programma's infiltreerden op verschillende netwerken waardoor kritieke databestanden konden worden gegijzeld en vernietigd. Hierdoor werden vele bedrijven geraakt en productielijnen stilgelegd. De totale kosten worden geraamd op honderden miljoenen euro's. De kans is groot dat opnieuw grote cyberaanvallen van deze omvang zullen plaatsvinden, maar ook op kleinere schaal vinden elke dag honderden incidenten plaats. Niet voor niets wordt een cyberaanval als grootste risicofactor gezien voor de bedrijfscontinuïteit van ondernemingen, dit geldt voor multinationals als voor het midden-kleinbedrijf.

Voor

Ondersteuning in preventiemanagement

Tijdens

Ondersteuning bij crisismanagement

Na

Ondersteuning bij het natraject



Al uw cyberrisico's ondervangen met één en dezelfde verzekering: #CyberComfort by Zurich

De Zurich Cyberverzekering beschermt bedrijven tegen de schadelijke gevolgen van cyberaanvallen en datalekken. In de verzekering worden verschillende elementen samengebracht die uitgesloten worden op traditionele verzekeringen, zo zijn uw eigen schade en de schade toegebracht aan derden op dezelfde polis gedekt.

Belangrijkste dekkingen en voordelen

Zurich biedt een totaalpakket aan waarbij u zelf kunt kiezen waartegen u zich verzekerd. Zo betaalt u nooit meer premie dan noodzakelijk.

De belangrijkste dekkingen:

Aansprakelijkheid

- Aansprakelijkheid en verweerskosten voor privacy en netwerkincidenten
- Verweerskosten bij formele onderzoeken
- Boetes die worden opgelegd door bijvoorbeeld de Payment Card Industry of de Autoriteit Persoonsgegevens in verband met de AVG/GDPR
- Media aansprakelijkheid

Eigen schade

- Kosten na incident, waaronder:
 - Forensisch IT-onderzoek
 - Pr-kosten
 - Notificatie, kredietmonitoring
- Bedrijfsstilstandschade, ook als deze ontstaan is door een incident op het netwerk van uw serviceprovider
- Datareconstructie
- Digitale afpersing en losgeld
- Reputatieschade die het gevolg is van weggelopen partners en klanten
- Social Engineering/CEO-fraude
- Kosten in noodsituatie

Aanvullende highlights

- Dekking bedrijfsschade ook wanneer intern tot onderbreking wordt besloten of door bevel van toezichthouder, de zogenaamde 'voluntary shutdown'
- Dekking voor onrechtmatig verkregen data
- Systeemfalen is als aanvullende dekking beschikbaar
- Ruime definitie van computersysteem, ook industriële besturingssystemen vallen onder de dekking
- Geen beperkingen op de experts die u inschakelt na een incident

Meer dan dekking; 24/7 een team van experts tot uw dienst met Zurich DigitalResolve

Met Zurich DigitalResolve heeft u altijd een crisismanager tot uw beschikking. Bij een incident belt u, dag en nacht, met het noodnummer. U krijgt een crisismanager aan de telefoon in de door u gekozen taal waarna een route wordt gekozen om de crisis zo snel mogelijk onder controle te krijgen. De crisismanager selecteert de experts die nodig zijn om het specifieke incident beheersbaar te maken en ondersteunt uw bedrijf waar nodig. Tot het moment dat het gevaar is afgewend is de crisismanager uw eerste aanspreekpunt.



01	Zoek zo snel mogelijk contact met DigitalResolve bij een incident, 24/7 365 dagen per jaar.
02	Incident manager aangesteld.
03	Forensisch IT-experts aangesteld (indien nodig) – inschalen en beperken van het incident – rapportage aan incident manager nadat incident onder controle is.
04	Incident manager bepaalt met u welke andere experts vereist zijn, denk aan advocaten en PR-consultants.
05	Reguliere discussies over de continuïteit van uw bedrijfsvoering met de betrokken partijen.
06	Andere experts aangewezen indien nodig, bijvoorbeeld voor de notificatie van klanten of kredietmonitorspecialisten.
07	Evaluatiegesprek en rapportage

De experts

Onze netwerkpartners zijn zorgvuldig uitgekozen en hebben verschillende expertises:

- Forensisch IT-experts en consultants
- PR-consultants
- Advocaten en experts op het gebied van cyberincidenten, datalekken en fraude
- Kredietmonitoring
- Forensisch accountants
- Onderhandelaren in het geval van afpersing
- Experts bij afhandeling privacy incidenten zoals de notificatieverplichting

Iedere partner in ons netwerk is geselecteerd op basis van bewezen diensten, ambitie en internationale mogelijkheden. Partners voldoen aan onze service standaard en rapportagenormen. Zo heeft u altijd toegang tot de beste dienstverlening.

Internationale mogelijkheden; lokale aanpak

Met Zurich DigitalResolve heeft u, indien nodig, toegang tot een internationaal netwerk. De crisismanager ziet erop toe dat de omvang van het incident snel in kaart wordt gebracht en regelt daarna dat u op locaties wereldwijd de hulp krijgt die u nodig heeft. Deze lokale benadering zorgt ervoor dat verdere cyberschade wordt voorkomen doordat data en andere informatie naar andere locaties moet worden verplaatst.

Een goede voorbereiding is het halve werk: preventief aan de slag met het Response-ability programma

Samen cyberrisico's beheersbaar maken, dat is waar wij voor staan. Daarom bieden wij onze nieuwe polishouders, als onderdeel van onze service, in samenwerking met Northwave, het Response-Ability Pakket aan. U maakt alvast kennis met de experts die u helpen na een cyberincident. Zij bereiden u zo goed mogelijk voor op een cyberincident zodat schadelijke gevolgen zoveel mogelijk beperkt kunnen blijven: dat noemen wij #CyberComfort.

Het Response-ability pakket

Optioneel, kunt u kosteloos* aanspraak maken op het Response-Ability programma:

- Een bezoek van het Northwave CERT-team. Samen met Northwave krijgt u inzicht in de mensen en de cultuur van uw organisatie. Zo proberen de experts inzicht te geven in de belangrijkste risico's voor uw onderneming. Centraal staat: hoe kan de organisatie zo goed mogelijk reageren op een cyberincidenten?
- Rapid Response Plan. U krijgt ondersteuning bij het opstellen van een realistisch crisisplan, zo weet u precies hoe u op een cyberincident moet reageren.
- Response-ability training. Aan de hand van het Rapid Response Plan traint Northwave de kernvaardigheden.
- Threat Response Abonnement. U kunt relevante medewerkers aanmelden bij de e-mailwaarschuwingdienst van Northwave. U krijgt een bericht wanneer zich een nieuwe dreiging voordoet, de ontvanger kan snel vaststellen of een dreiging relevant is voor de onderneming.
- Zurich Training: Cyber Crisis Management. U ontvangt vouchers voor gratis deelname aan de Training Cyber Crisis Management. Dit is een verdieping van de Response-ability training. Deelnemers gaan aan de slag met basisvaardigheden in een cybercrisis simulatie.

*bij een minimumpremie vanaf €2.000

Optimale bescherming bij cyberaanvallen en datalekken

Dit is Zurich DigitalResolve:

- Opsporing bron van de cyberaanval, falen of datalek.
- Bescherming van uw bedrijf tegen verdere aanvallen.
- Schadebegroting met hulp van een forensisch accountant.
- Reputatieschade beperkt met behulp van een PR bureau.
- Juridische ondersteuning bij compliance-vraagstukken.
- Hulp bij uitonderhandelen van cyberafpersingen.
- Notificatieverplichtingen vanuit PR- en wettelijk perspectief.
- Kredietmonitoring.
- Onderzoek naar regresmogelijkheden op nalatige derden.
- Risicomanagement na incident om verdere schade te beperken.

Meer informatie?

Neem contact op met onze specialist.

Sebastian Sieters

sebastian.sieters@zurich.com

+ 31(0)70 4184293

Zurich Insurance plc, Netherlands branch

Prinses Margrietplantsoen 65,

2595 BR DEN HAAG

www.zurich.com

De producten en diensten worden aangeboden of verricht door dochtermaatschappijen van Zurich Insurance Group. In Europa is dat met name Zurich Insurance Plc., een Ierse schadeverzekeraar. Het Nederlandse kantoor van Zurich Insurance Plc. handelt onder de naam Zurich Insurance Benelux. Dit document dient uitsluitend voor informatiedoeleinden. Producten en diensten kunnen van land tot land verschillen en zijn niet altijd in alle jurisdicties beschikbaar. De precieze omvang van de dekking en voorwaarden staan beschreven op het polisblad en in de daarbij behorende clausules, aanhangsels en polisvoorwaarden. Bepaalde producten en diensten kunnen worden geleverd via onafhankelijke derden. Verzekeringsproducten kunnen worden gedistribueerd via partners of onafhankelijke derde partijen.