



ZURICH®



NORTHWAVE

#CyberComfort by Zurich

Voor, tijdens en na cyberincidenten

Cyberincidenten kunnen forse impact hebben op uw organisatie en de bedrijfsvoering voor lange tijd ontwrichten. Waar de meeste verzekeraars zich beperken tot het betalen van schade na een incident gaat Zurich verder. Wij investeren in de weerbaarheid van uw bedrijf zodat u cyberincidenten snel kan herkennen, melden en verhelpen. Gaat het toch mis? Dan valt u terug op onze ruime dekking en kan u gebruik maken van ons netwerk met experts onder leiding van een persoonlijke crisismanager.



Response-ability

De beste voorbereiding

Northwave is dé expert op het gebied van cyber security. Wij sturen de professionals van het **CERT** (Computer Emergency Response Team) van Northwave bij u langs om in gesprek te gaan over de belangrijkste risico's.

Centraal staat **Response-ability**: hoe kan uw organisatie het best reageren op een cyberincident.

De volgende elementen maken deel uit van uw pakket:

- **Rapid Response Plan**

Het draaiboek dat bij een incident wordt gebruikt. Een gepersonaliseerd plan om de hulpdiensten zo snel mogelijk op locatie te krijgen en schade te voorkomen.

- **Response-training**

Aan de hand van het responsplan traint Northwave uw vaardigheden aan de hand van relevante scenario's.

- **Northwave Threat Response**

Relevante werknemers kunnen worden aangemeld voor deze dienst die berichten verstuurd wanneer nieuwe dreigingen zich voordoen in uw branche of regio.

Zurich DigitalResolve

De beste crisishulp

Tijdens een incident bent u goed voorbereid. U belt het noodnummer zoals beschreven in uw responsplan en krijgt een **incidentmanager** toegewezen die u tijdens de crisis zal begeleiden.

Waar nodig komen de experts van **Northwave CERT** op locatie om de crisis te bestrijden. Fijn, want die kent u al.

Tijdens de crisisfase schakelt de incidentmanager met de nodige **experts** om de aanval op te sporen en verdere aanvallen te voorkomen.

Advocaten helpen bij vraagstukken over datalekken en daarbij horende meldingsplicht. Zo blijven claims in een later stadium tot een minimum beperkt.

Is de crisis afgewend, dan wordt gekeken naar **risicomanagement**. Wat kunt u doen om in de toekomst een hack, fraude of falen te voorkomen.

Northwave x Zurich

De beste afhandeling

Cyberincidenten kunnen leiden tot veel schade. U heeft bijvoorbeeld tijdelijk niet kunnen leveren of u wordt geconfronteerd met een veelheid aan claims.

Onze **schade-experts** zorgen dat uw bedrijf zo snel mogelijk weer operationeel is.

- Op basis van rapportages opgesteld door een forensisch accountant vergoedt Zurich uw bedrijfsstilstandsschade.
- **Verweer en onderzoek** naar de tegen u ingestelde claims en regresmogelijkheden.
- Vergoeding van noodzakelijke **verbeteringen** van uw systeem om toekomstige aanvallen te voorkomen.
- Vergoeding van **reputatieschade** en waar nodig ondersteuning van PR-bureaus.
- Ondersteuning bij strafvervolgning in geval van fraude.
- U ontvangt een **eindrapportage** van de incidentmanager met concrete handvatten om uw risico's beter te managen.

Voordelen van #CyberComfort

- Preventie, incidentmanagement en ruime voorwaarden onder een paraplu
- Maakt u gebruik van Zurich DigitalResolve, waaronder ook Northwave valt, dan is op die diensten geen eigen risico van toepassing gedurende de eerste 72 uur
- Wij leggen u geen beperkingen op, kiest u voor een eigen expert dan zijn ook die kosten verzekerd maar is het eigen risico van toepassing
- Bedrijfsschade wordt ook vergoed wanneer intern tot onderbreking wordt besloten of dit gebeurt op bevel van een toezichthouder
- Bedrijfsschade wordt ook vergoed wanneer de oorzaak ligt in een door u gekozen toeleverancier voor IT diensten
- Ruime definitie computersysteem waardoor ook industriële besturingssystemen onder de dekking vallen
- Standaard werelddekking

Onze dekkingen op een rij

Incidentmanagement

- Services bij en na een cyberincident en de kosten voor het oplossen van noodsituaties.

Eigen schade

- Bedrijfsstilstandsschade en extra kosten bij netwerkincident bij verzekerde en toeleveranciers, mogelijk uit te breiden met systeemstoring bij verzekerde of toeleveranciers.
- Vervanging en reconstructie van databestanden
- Vervanging van hardware en verbetering van computersysteem
- Cyberafpersing
- Reputatieschade
- Vermijding van aansprakelijkheid

Fraude

- Computer crime
- Social Engineering en CEO-fraude
- Opsporing van identiteitsfraude
- Telefoonhacking

Aansprakelijkheid

- Aansprakelijkheid tegen claims van derden
- Aansprakelijkheid in verband met bijvoorbeeld smaad of laster
- Verweer tegen onderzoek en boetes (ook GDPR, PCI-DSS)

Zurich Insurance plc, Netherlands branch
Prinses Margrietplantsoen 65,
2595 BR DEN HAAG
www.zurich.com

Meer informatie?

Neem contact op onze specialisten

Lennard Wit
lennard.wit@zurich.com
+31 (0)70 418 4021

Tjerk de Wilde
tjerk.dewilde@zurich.com
+ 31(0)70 418 4287

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 bijkantoor 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.