CyberCare Polis
PRODUCTOVERZICHT

Optimale ondersteuning bij online incidenten

De invloed van internet op ons dagelijks leven is groot. We brengen steeds meer tijd door op internet: we e-mailen, gamen, bankieren en shoppen, we onderhouden sociale contacten en zoeken naar informatie (bijvoorbeeld over medische zaken of reizen), we lezen het nieuws, bestellen eten, plannen routes en kijken naar TV-series en video's. Met onze smartphones zijn we fulltime met het internet verbonden en steeds meer huishoudelijke apparaten worden ook op het wereldwijde web aangesloten. Deze ontwikkeling is vooral positief, maar heeft ook negatieve kanten waaronder de opkomst van cybercrime.

Cybercrime: de snelst groeiende vorm van criminaliteit

Cybercrime, computercriminaliteit, digitale criminaliteit: allemaal termen voor deze vorm van criminaliteit die zich richt op computers of andere systemen zoals mobiele telefoons en tablets. Man of vrouw, jong of oud, hoog of laag opgeleid: iedereen loopt het risico om slachtoffer te worden van cybercriminelen. Cybercriminelen kiezen doorgaans geen specifiek doelwit, maar verspreiden hun malafide software zoveel mogelijk in de hoop veel apparaten te treffen. Phishing, ransomware, pinpas- of creditcardfraude, oplichting bij online aankopen of het klikken op een frauduleuze e-mail kan tot een financiële strop en veel zorgen leiden.

Hulpverlening
Met deze verzekering heeft u 24/7 toegang tot de helpdesk van CyberSupport. Ervaren cyber security professionals helpen u snel en doelgericht. Kijk voor meer informatie op www.cybersupport.nu.

Verzekerde cyberincidenten

Verzekerd zijn de hulpverlening en de schade die het gevolg zijn van één van de volgende cyberincidenten:

Cyberafpersing
Door hacking, phishing of malware worden persoonsgegevens of privacygevoelige gegevens buitgemaakt. U wordt gedwongen losgeld te betalen onder bedreiging dat deze gegevens worden vernietigd, beschadigd of openbaar worden gemaakt.

(e-)Reputatieschade
Uw goede naam wordt opzettelijk aangetast doordat iemand anders negatieve berichten online plaatst. Voorbeelden van negatieve berichten zijn: smaad, laster, belediging of het openbaar maken van privacygevoelige gegevens, zoals privéfoto's.

Verlies van geld (op rekening)
- Frauduleus gebruik van een bankpas of creditcard door een derde in de vorm van een contante opname en een contante aankoop van een dienst of goed.
- Schade door fraude met internetbankieren.
- Andere vormen van verlies van geld op rekening van een verzekerde door malware, phishing of door een hacker, bijvoorbeeld als u een geloofwaardige en gepersonaliseerde nepfactuur betaald.

Identiteitsfraude
Het misbruiken van identiteitsbewijzen van verzekerde.

Inbreuk op privacy
Verlies, diefstal of beschadiging van persoonsgegevens of privacygevoelige gegevens waardoor schade ontstaat die het gevolg is van het openbaar maken of verspreiden van die gegevens.

Aansprakelijkheid
- Aanspraken van derden als gevolg van identiteitsfraude.
- Aanspraken van derden als gevolg van verlies, diefstal of beschadiging van persoonsgegevens of privacygevoelige gegevens doordat die openbaar zijn gemaakt of worden verspreid.

Producteigenschappen

Verzekerd bedrag	Eigen risico	Verzekeringsgebied
Per gebeurtenis: max. € 50.000. **Per jaar:** max. € 100.000	€ 125 per gebeurtenis.	Werelddekking.
Premie Deze bedraagt **€ 12,50** per maand (exclusief assurantiebelasting). Op deze verzekering wordt 10% pakketkorting verleend als de polis onderdeel uitmaakt van de pakketverzekering van Turien & Co.		
Verzekerd Het hele gezin, incl. uitwonende studerende kinderen jonger dan 27 jaar. Alleen dekking voor schade in hoedanigheid van particulier.		

CyberCare Polis
PRODUCTOVERZICHT

Overzicht vergoedingen

- **Hulpverlening:** deskundige hulp van specialisten.
- **Computerhulp:** herstel van beschadigde gegevens en gegevensdragers na een cyberincident.
- **Onderzoekskosten:** forensisch onderzoek naar de oorzaak en de omvang van een cyberincident.
- **Kosten van preventiemaatregelen** na een cyberincident, bijv. het upgraden van het antivirusprogramma op het getroffen apparaat.
- **Schadevergoeding van het geldelijk verlies** in geval van het verlies van geld (op rekening) en betaling van losgeld.
- Vergoeding van kosten in verband met **aanspraken van derden** in geval van identiteitsfraude en verlies, diefstal of beschadiging van persoonsgegevens of privacygevoelige gegevens die openbaar worden gemaakt of worden verspreid.

Wat is niet verzekerd?

Niet alles is verzekerd. In de voorwaarden staan gebeurtenissen waarbij hulpverlening en schadevergoeding na een cyberincident niet verzekerd zijn. Raadpleeg de voorwaarden voor de exacte omschrijving.

- Schade door **ernstige conflicten** (molest), natuurrampen, atoomkernreacties, **fraude** en/of het niet nakomen van verplichtingen is niet verzekerd.
- Schade door **opzet, grove schuld of bewuste roekeloosheid** is niet verzekerd.
- Schade die **voorafgaand aan de ingangsdatum** van de verzekering heeft plaatsgevonden is niet verzekerd.
- Schade als gevolg van een cyberincident waarvan een andere verzekerde een **verdachte, dader of medepleger** is, is niet verzekerd.
- Schade als gevolg van het **ontbreken van passende beveiligingsmaatregelen** is niet verzekerd.

Passende beveiligingsmaatregelen

Onder passende beveiligingsmaatregelen verstaan wij tenminste het deugdelijk gebruik van wachtwoorden en het installeren en gebruiken van adequate en up-to-date antivirussoftware van een gerenommeerde leverancier (bijvoorbeeld van ESET, AVG, McAfee of Norton).

Wat is phishing?

Bij phishing proberen cybercriminelen via e-mail persoonlijke gegevens te ontfutselen. De e-mail is zo gemaakt dat deze van een echt bedrijf afkomstig lijkt. De internetgebruiker wordt in de e-mail bijvoorbeeld opgeroepen om een openstaande factuur te betalen. De links in de e-mail leiden de bezoeker vervolgens naar een valse website waar persoonlijke gegevens worden ontfutseld. Ook bevatten phishingmails vaak bijlagen, zoals een pdf of zip-bestand, waarbij automatisch schadelijke software (malware) wordt geïnstalleerd als de gebruiker deze opent.

Wat is malware?

Malware staat voor '**mal**icious soft**ware**'. Dit is een verzamelnaam voor alle software met een opzettelijk kwaadaardige werking. Dit wordt ook wel een virus genoemd. Het kan gegevens op de computer wijzigen of verwijderen, zoals persoonlijke foto's of belangrijke documenten. Daarnaast kan het bijvoorbeeld toetsaanslagen registreren, screenshots maken, de webcam aanzetten en zelfs geld van een bankrekening afschrijven.

Wat is ransomware?

Ransomware wordt ook wel 'gijzelingssoftware' genoemd. Het is een computervirus dat bestanden ontoegankelijk maakt – oftewel 'gijzelt' – en ze pas weer vrijgeeft als er losgeld is betaald aan de cybercriminelen die erachter zitten.

Een verzekering van:
TURIEN&CO ASSURADEUREN

Onze partner:
www.alertonline.nl

Meer info	Download de voorwaarden
Heeft u vragen, behoefte aan advies of wilt u een offerte? Neemt u dan contact op met uw assurantieadviseur.	Algemene voorwaarden Varia model 09-18 Bijzondere voorwaarden CyberCare Polis model 11.18