CyberClear by Hiscox

U kunt op verschillende manieren met cybercriminaliteit te maken krijgen doordat uw:

- Computers/netwerken geïnfecteerd worden met computervirussen via internet, e-mail of USB-sticks;
- Systemen worden gehackt door phising, malware of ransomware;
- Laptops en/of USB-sticks zijn verloren of worden gestolen.

Wat zijn de risico's?

- Verlies van vertrouwelijke informatie zoals persoonsgegevens, medische gegevens, betaalkaartgegevens en/of bedrijfsgeheimen;
- Schade aan bestanden en systemen met het risico op omzetverlies;
- Reputatieschade.

CyberClear by Hiscox:

Deze verzekeringsoplossing beschermt uw bedrijf tegen de gevolgen van cyber en data risico's. Dit doen wij door middel van onze CyberClear services. Met deze services biedt Hiscox de mogelijkheid van preventieve maatregelen en staan wij u volledig bij met een netwerk van specialistische bedrijven indien zich toch een incident voordoet. Het enkel uitkeren van een bedrag is namelijk niet voldoende.

Als onderdeel van de CyberClear by Hiscox verzekering bent u verzekerd van:

- **Bescherming:** middels preventieve services zoals een security check of monitoring van uw systemen en het opstellen van uw verwerkersovereenkomst.
- **Verzekering:** dekking voor onder andere first party (uw eigen kosten) en third party (aansprakelijkheid derden).
- **Service:** bij een eventueel incident zullen wij u bijstaan samen met onze gespecialiseerde partners die u zullen adviseren en begeleiden.

Incident Response Plan

Het is mogelijk dat uw systemen zijn gehackt en/of er vermoeden bestaat dat uw data is verloren en/of gestolen. Indien dit gebeurt dan treedt voor u als verzekerde, met een enkel telefoontje, het Incident Response Plan in werking. Deze service is gebaseerd op het BVS principe (Bescherming, Verzekering en Service). U wordt volledig ontzorgd. Na het melden van de schade, zal het hele proces van hulp en advies worden begeleid door deskundige schadebehandelaars in samenwerking met onze partners.

Algemene Verordening Gegevensbescherming

Er zijn twee categorieën overtredingen en bijbehorende maximale boetes.
1) Verantwoordelijken (organisaties die persoonsgegevens verwerken) hebben onder de AVG bepaalde verplichtingen, zoals de verantwoordingsplicht.Komt een verantwoordelijke (een van) deze verplichtingen niet na? Dan kan de AP een boete opleggen van maximaal 10 miljoen euro. Of een boete van 2% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.
2) Overtreedt een verantwoordelijke de beginselen of grondslagen van de AVG? Of de privacyrechten van de betrokkenen (de mensen van wie de organisatie gegevens verwerkt)?Dan kan de AP een boete opleggen van maximaal 20 miljoen euro. Of een boete van 4% van de wereldwijde jaaromzet, mocht dat bedrag hoger uitkomen.

Preventieprogramma

Programma	Security Scan	Security Scan	Opstellen Verwerkers-overeenkomst	Disaster recovery maturity scan
Aangeboden door	Secureme2	RedSocks Security	ICTRecht	KPN
Doelgroep	Verzekerden tot een omzet van € 5 miljoen.	Verzekerden met een omzet vanaf € 5 miljoen.	Alle verzekerden.	Verzekerden vanaf een omzet van € 10 miljoen.
Verplicht?	Nee	Nee	Nee	Nee
Vorm	Online scan of via bezoek.	Online scan of via bezoek.	Beoordeling op afstand.	Op locatie.
Rapportage	In een persoonlijk gesprek.	In een persoonlijk gesprek.	Bespreking bij ICTRecht op kantoor.	Rapport
Kenmerken	De scan geeft inzicht in be-veiligingsmaatregelen en helpt uw cyberveiligheid vergroten.	De scan geeft inzicht in be-veiligingsmaatregelen en helpt uw cyberveiligheid vergroten.	hulp bij verkrijging van rechtsgeldige verwerkers-overeenkomst.	Een scan van de disaster recovey maatregelen dmv een 3 fase aanpak.
Kosten	Gratis	Gratis	Gratis	Gratis

HISCOX

Incident Response Plan

Hoe te handelen bij een incident?

Het Incident Response plan is een service die u door Hiscox wordt aangeboden. Het incident response team, een samenwerking tussen het gespecialiseerde schadeteam en professionals (op het gebied van forensisch onderzoek, juridische bijstand in het kader van de meldplicht, PR en het herstel van systemen en netwerken), is in staat snel te handelen in het geval van een beveiligingsincident met computers of netwerken.

Het doel is om de schade te beperken en snel hervatting van de bedrijfsactiviteiten te bevorderen. Naast reactie op incidenten richten onze partners zich ook op advisering, preventie en bescherming. Onze partners zijn onder andere: Deloitte, Smart & Able PR en Kennedy Van der Laan.

1.

AANLEIDING:
Een incident zoals een hack of een datalek heeft plaatsgevonden!

ACTIE VERZEKERDE:
Informeer direct uw adviseur en/of Hiscox. 24 uurs Incident Response alarmnummer: 0031 – 20 517 07 00.

2.

ONDERSTEUNING:
Hiscox schakelt forensisch specialisten in om mogelijk binnen 72 uur te bepalen wat de omvang en de oorzaak van het incident is.

Deloitte.

3.

ACTIE VERZEKERDE:
De Autoriteit Persoonsgegevens en mogelijk de betrokkenen worden geïnformeerd. Het incident response team adviseert u.

Kennedy Van der Laan

AUTORITEIT PERSOONSGEGEVENS

4.

ONDERSTEUNING:
Aansprakelijkheid en eigen schade zijn een grote zorg. Het Incident Response team staat klaar om u bij te staan.

Tevens bijstand van een PR bureau voor advies bij communicatie en hulp ter voorkoming van reputatieschade indien nodig.

SMART&ABLE
communicatie en lobby

5.

ACTIE VERZEKERDE MET ONDERSTEUNING:
Het herstellen van schade aan uw systemen en/of netwerk door specialisten.

6.

ACTIE VERZEKERDE EN HISCOX:
Eventuele evaluatie en nabespreking.

HISCOX