CYBERVERZEKERING

NUTTIG OF OVERBODIG?

DBA
verzekeringen | hypotheken | bankzaken

Cyberrisico's

Elk bedrijf kan getroffen worden door cybercriminaliteit. In deze brochure leest u waarom het zo belangrijk is om u te beschermen tegen cybercriminaliteit én hoe u dat doet. U vindt in deze brochure voorbeelden, tips, kosten van cybercriminaliteit en wat een goede cyberverzekering voor u kan betekenen.

Wilt u na het lezen van deze brochure een offerte voor een passende cyberverzekering? Neem dan contact met ons op.

DBA advies
info@dba-advies.nl
0342 404 180

Barneveld
Amersfoortsestraat 25
3772 CE Barneveld

Lunteren
Oranjestraat 6
6741 CW Lunteren

DBA
verzekeringen | hypotheken | bankzaken

Cyberverzekering: nuttig of overbodig?

"Wij hebben een deskundig ICT-bedrijf dat alles regelt. Waarom zouden wij dan een cyberverzekering nodig hebben?"

Uw bedrijf is hoogstwaarschijnlijk geen doelwit van criminelen. Maar **(cyber)criminelen worden door slechts één ding gedreven, geld.** En een geldstroom is aanwezig in elke onderneming. Indirect kunnen **klantgegevens en vertrouwelijke bedrijfsgegevens** ook geld opleveren. Als criminelen in het bezit van deze informatie komen, kunnen zij u afpersen.

Wanneer u een ICT-bedrijf inschakelt om uw ICT-zaken te regelen dan nemen ze u een hoop werk uit handen. Ze zorgen er bijvoorbeeld voor dat alle computers aangesloten zijn op internet. En bij storingen belt u het ICT-bedrijf waarschijnlijk als eerste op. **Cybersecurity is écht een andere tak van sport.** Stel uw bedrijf wordt gehackt en u kunt pas weer bij uw bestanden als u losgeld betaalt. Of uw bedrijf ligt drie dagen stil na een cyberincident. Dit soort incidenten kosten veel geld. Dan bent u bij het ICT-bedrijf niet aan het juiste adres. **Een cyberverzekering kan in die gevallen wél de hulp bieden die u op dat moment nodig heeft.**

Er verschijnen dagelijks berichten over cybercriminaliteit in de media. Voorbeelden bij grote bedrijven zijn er genoeg. Binnen het MKB zijn ze minder zichtbaar. Toch is de **schadelast voor het MKB gemiddeld tussen de € 50.000 en €74.000 per incident** (bron: Hiscox). Dat juist deze incidenten niet bekend worden gemaakt komt veelal door het taboe dat rond dit nieuwe risico hangt. Bedrijven vrezen voor reputatieschade en de gevolgen die dit heeft voor het krijgen en behouden van klanten.

Cybercrime vindt altijd plaats met behulp van internet, maar vaak **draagt een menselijke factor bij aan het succes van een crimineel,** veelal via een onbewuste actie. Bijvoorbeeld het openen van een bijlage van een e-mail waarin malware zit of het klikken op een link van een valse (bank)website. Ook als alles technisch gezien goed voor elkaar is, of als de administratie in de cloud staat, bent u niet 100% veilig.

DBA
verzekeringen | hypotheken | bankzaken

Voorbeelden

Laptop uit kofferbak gestolen

Een autoruit van een zorgmedewerker wordt ingeslagen. Zijn laptop in de kofferbak wordt gestolen waarna 1.300 patiëntgegevens op straat komen te liggen. Waaronder NAW-gegevens, maar ook BSN-nummers, voorgeschreven medicatie en diagnoses. De gegevens komen in verkeerde handen en worden openbaar gemaakt. De zorginstelling is verplicht aan alle patiënten melding te doen van de openbaarmaking. Daarop worden twee rechtszaken aangespannen. In een geval door een vrouw die haar baan zou zijn kwijt geraakt als gevolg van de openbaarmaking. In de tweede zaak wordt de praktijk verantwoordelijk gehouden voor identiteitsfraude die heeft kunnen plaatsvinden door het datalek. ***#datalek***

Ransomware bij administratiekantoor

Een medewerker van een administratiekantoor klikt op een schadelijke link in een e-mail en zo wordt malware gedownload op de server van het bedrijf, alle bestanden zijn versleuteld. Op het beeldscherm van de medewerker verschijnt de boodschap om binnen 24 uur een losgeldbedrag in bitcoins te betalen in ruil voor het ontsleutelen van de databestanden. Gespecialiseerde onderhandelaars en onderzoekers zoeken de ernst van de bedreiging uit om zo een beslissing te maken over het wel of niet betalen van losgeld. Het herstellen van de bestanden en het terugplaatsen van de back-up is een tijdrovende aangelegenheid. Als gevolg hiervan ligt het bedrijf enkele dagen stil. ***#phishing***

Schade door (ex-)medewerkers

Een recruiter werkzaam in opdracht van een garage-bedrijf stuurde per ongeluk het verkeerde bestand mee in een e-mail naar vier kandidaten. Het bestand bevatte namen, adressen en BSN-nummers van voormalige werknemers. Juridische adviseurs werden ingeschakeld om de met regelgeving samenhangende gevolgen te managen.

#datalek #reputatieschade

DBA
verzekeringen | hypotheken | bankzaken

Wat kost cybercrime?

Vanwege de serieuze en mogelijk verstrekkende gevolgen van cybercriminaliteit is het belangrijk een goede overweging te maken om wel of niet te verzekeren.

De helpdesk van de cyberverzekering zorgt dat u snel en adequaat kunt reageren. Hiermee beperkt u uw schade.

Deze hoge kosten kan een cyberverzekering voor u afdekken:

- Bedrijfsschade:
  - Uurtarieven medewerkers x aantal uren stilstand.
  - Webshop: aantal uren stilstand x gebruikelijke online omzet per uur.
- Forensisch onderzoek voor opsporen en bepalen omvang hack/lek: **€ 4.000 per dag.**
- Betalen losgeld.
- Herstel ICT-systemen: verwijderen malware, herstel en testen. Uurtarief ICT-expert: **€ 120.**
- Kosten PR en crisismanagement – als een cyberaanval publiekelijk bekend wordt zal uw organisatie kosten moeten maken voor het informeren van alle betrokkenen. Uurtarief PR adviesbureau: **€ 100.**
- Boete Autoriteit Persoonsgevens: maximaal **€ 10 miljoen** of 2% van de (wereldwijde) omzet.
- Inhuren juridisch expert: **€ 240 per uur.**
- Datalek: kosten van gestolen of verloren bestand: gemiddeld **€ 185 per bestand.**
- Reputatieschade.
- Aansprakelijkheidskosten en kosten van verweer.

DBA
verzekeringen | hypotheken | bankzaken

Preventiemaatregelen: 10 tips

1. Maak uw werknemers bewust van de cyberrisico's.
2. Gebruik een virusscanner, firewall, anti-spyware, advertentieblockers en veilige websites.
3. Houd systemen up-to-date. Download en installeer de benodigde updates.
4. Beveilig mobiele apparaten en draadloos internet.
5. Gebruik sterke wachtwoorden en update ze regelmatig.
6. Klik niet zomaar op links, afbeeldingen of video's. Kijk eerst naar de website of het bestand waar de link u naartoe stuurt door met je muis over de link te bewegen.
7. Blijf weg van toegestuurde of gedownloade bestanden met de extensie '.exe', '.vbs' en '.scr' als u niet 100% zeker bent over de herkomst van deze bestanden.
8. Maak regelmatig een back-up van al uw data. En test of het terugplaatsen van deze back-up werkt.
9. Als u een onbetrouwbaar of onbekend proces tegenkomt op uw computer, verbreek dan onmiddellijk de verbinding met het internet of andere netwerkconnecties. Dit voorkomt verspreiding van de infectie.
10. Bij twijfel: Google altijd eerst of er iets bekend is over de mail of site.

DBA
verzekeringen | hypotheken | bankzaken

Dekkingskenmerken cyberverzekering

Een cyberverzekering omvat veelal de volgende dekkingen:

Dekking voor eigen kosten als gevolg van inbraak op systemen of data.

Bijvoorbeeld kosten van forensisch onderzoek, kosten van communicatie met klanten, kosten van crisismanagement en reputatieherstel.

Dekking voor de gevolgen van gestolen privacygevoelige gegevens.

Bijvoorbeeld claims van individuele getroffen personen en boetes die zijn opgelegd door de Autoriteit Persoonsgegevens.

Beschermt bij afpersing.
U krijgt bijstand en eventueel betaald losgeld wordt vergoed.

Beschermt wanneer een afperser de website, het netwerk e.d. gijzelt en dreigt deze te beschadigen of te vernietigen of informatie openbaar te maken (ransomware).

Dekt omzetverlies veroorzaakt door cyberaanvallen.

Bijvoorbeeld wanneer door een DDos-aanval de webwinkel niet bereikbaar is.

De schade veroorzaakt door hackers is verzekerd.

Bijvoorbeeld reparatie of vervanging van websites en data, kosten van forensisch onderzoek naar de oorzaak van een hacking en advies in systeembeveiliging.

Dekt schade bij onbedoelde verspreiding van een virus.

Bijvoorbeeld als de website of een mail onbedoeld een virus verspreidt.

DBA
verzekeringen | hypotheken | bankzaken

Dit is een samenvatting van de geboden dekking. Hieraan kunnen geen rechten worden ontleend.
De exacte dekking leest u in de polisvoorwaarden. Deze kunt u downloaden via www.turien.nl/voorwaarden-documenten.

Misschien wel de belangrijkste reden om een cyberverzekering af te sluiten: hulpverlening

Een essentieel aspect, en volgens veel verzekerden zelfs hét belangrijkste aspect, van de cyberverzekering is de **hulpverlening**. Hiervan maakt u **gratis** gebruik wanneer u een cyberverzekering afsluit.

De hulpverlening is erop gericht om schade te beperken en bedrijfsactiviteiten snel te kunnen hervatten.

De hulpverlening bestaat uit:

- Een 24/7 helpdesk.
- Forensisch experts (voor het onderzoeken van de toedracht en de omvang en het herstel).
- De tijdige melding aan de Autoriteit Persoonsgegevens (AP) wordt gecoördineerd.
- Juridische bijstand.
- PR-bureau voor communicatie-advies.

De kosten voor forensisch **onderzoek bedragen vaak duizenden euro's per dag**. Ook juridische bijstand is erg kostbaar, maar essentieel wanneer u een cyberincident heeft. Deze mensen zijn bekend in het woud van regels en procedures en zijn de aangewezen personen om uw bedrijf weer snel productief te maken.

DBA
verzekeringen | hypotheken | bankzaken