



# Cybersecurity belangrijker dan ooit!

Een universiteit wordt digitaal gegijzeld en betaalt omgerekend zo'n 200.000 euro losgeld, om weer toegang te krijgen tot hun eigen cruciale systemen en data en daarmee de continuïteit van onderwijs, onderzoek en salarissen te waarborgen. Een ziekenhuis ontdekt een digitale inbraakpoging en sluit uit voorzorg tijdelijk het dataverkeer met de buitenwereld af, waardoor patiënten niet bij hun elektronisch patiëntendossier kunnen, er geen dataverkeer mogelijk is met huisartsen en andere ziekenhuizen en werknemers niet vanuit huis kunnen werken.

## **Juist MKB'ers zijn een aantrekkelijk doelwit**

Wellicht denkt u: dat zijn grote organisaties, wij zijn een klein bedrijf, bij ons valt niets te halen. Internetcriminelen weten echter dat juist kleinere bedrijven vaak minder beveiligd zijn. Jaarlijks geeft dan ook meer dan 50% van het MKB aan doelwit te zijn geweest.

## **Niet alleen noodzakelijk, ook verplicht**

Beveiliging is niet alleen noodzakelijk, maar ook wettelijk verplicht. De Algemene verordening gegevensbescherming (AVG) eist bijvoorbeeld dat u moet kunnen aantonen welke organisatorische en technische maatregelen u heeft genomen om persoonsgegevens te beveiligen en dat u een protocol dient te hebben voor de afhandeling van datalekken en beveiligingsincidenten. Het niet voldoen hieraan kan leiden tot boetes, schadevergoedingen en zelfs persoonlijke aansprakelijkheid van bestuurders. Om niet te spreken over reputatieschade.

## **Goed onderhoud, veilig gedrag en de juiste cyber- en datariskverzekering**

Wat kunt u doen? Laten we het voor het gemak vergelijken met auto's, autorijden en autoverzekeringen. Veiligheid begint bij goed onderhoud en veilig gedrag van u en uw medewerkers. Maar dan nog zit een ongeluk in een klein hoekje. Bovendien heeft u vrijwel geen invloed op het gedrag van anderen.

Niet als een autoverzekering heeft een cyber- en datariskverzekering een WA- en casco-component:

1. Het 'WA-deel' biedt dekking voor schade die u onbedoeld veroorzaakt aan anderen, bijvoorbeeld na diefstal van privacygevoelige gegevens, het digitaal schenden van auteursrecht of het verspreiden van virussen. Deze schade valt niet onder de dekking van een reguliere bedrijfsaansprakelijkheidsverzekering;

2. Het 'cascodeel' biedt dekking voor schade die u zelf ondervindt, bijvoorbeeld door inbraak op uw systemen of data. Denk hierbij aan kosten van forensisch onderzoek, het inwinnen van advies, extra communicatie naar klanten, boetes opgelegd door toezichthouders, kosten voor reparatie of vervanging van websites, programma's of data, het betalen van losgeld en zelfs omzetverlies door cyberaanvallen.

Het kiezen van de juiste cyber- en datariskverzekering is echter altijd maatwerk. Laat u dan ook goed adviseren!

**Bert Zwier**  
*Teamleider Zakelijke Markt*  
*Kuiper Verzekeringen*