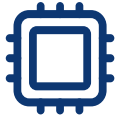




Hienfeld Cyberverzekering



Uw bedrijf is al een doelwit. De vraag is alleen of u het weet.

Welke cyberrisico's loopt mijn bedrijf?

In 2024 kreeg bijna twee op de tien Nederlandse bedrijven daadwerkelijk te maken met schade door een cyberincident. Denk aan financieel verlies, gestolen klantgegevens of een langdurige verstoring van de bedrijfsvoering. Bij grote bedrijven liep dat zelfs op tot drie op de tien. En dan gaat het alleen nog om de incidenten die ook echt worden gemeld.

Maar liefst 85% van de mkb-bedrijven heeft al minstens één cyberincident meegemaakt.

Toch denkt een kwart van de ondernemers nog altijd dat het risico voor hun bedrijf wel meevalt. Juist kleinere bedrijven onderschatten het gevaar vaak. Dat is begrijpelijk, want veel incidenten komen nooit in het nieuws. Niet omdat ze weinig voorkomen, maar omdat bedrijven de schade liever binnenskamers houden. Reputatieschade kan namelijk minstens zo ingrijpend zijn als de aanval zelf.

Ondertussen neemt nog altijd één op de vijf kleine mkb-bedrijven geen enkele maatregel tegen cyberrisico's.

Dat terwijl in 2025 bijna drie op de vier Nederlanders te maken kreeg met een poging tot cybercrime, zoals een phishingmail, een neptelefoontje van de bank of een valse

In deze brochure beantwoorden wij de volgende vragen:

- ✓ **Welke cyberrisico's loopt mijn bedrijf?**
- ✓ **Een cyberaanval... wat nu?**
- ✓ **Wat biedt de Hienfeld Cyberverzekering?**
- ✓ **Wat is de Hienfeld Cyber Assist lijn?**
- ✓ **Waarom Hienfeld?**

factuur. Cybercriminelen richten zich allang niet meer alleen op grote organisaties. Het mkb is juist aantrekkelijk, omdat de beveiliging daar vaak minder uitgebreid is en het bewustzijn niet altijd op hetzelfde niveau ligt.

Ongeveer 30% van de cyberincidenten begint bij eigen medewerkers.

Niet door opzet, maar door een menselijke fout. Eén verkeerde klik op een link, één gedeelde inlogcode of één overtuigende e-mail kan al genoeg zijn. Tegelijkertijd worden ook de wettelijke eisen strenger. De Autoriteit Persoonsgegevens treedt actief op bij datalekken en de boetes kunnen oplopen tot €20 miljoen of 4% van de wereldwijde jaaromzet.

De kans op een cyberaanval is bovendien veel groter dan veel ondernemers denken.

Die ligt rond de 1 op 5. Ter vergelijking: de kans op brand is ongeveer 1 op 8.000. Toch heeft vrijwel ieder bedrijf een brandverzekering. Zelfs wanneer u volledig in de Cloud werkt, betekent dat niet automatisch dat uw risico's zijn afgedekt. U blijft namelijk zelf verantwoordelijk voor de gegevens en systemen die u gebruikt en beheert.

Een cyberaanval... wat nu?

Cybercriminaliteit komt voor in veel verschillende vormen. Een aantal praktijkvoorbeelden:



U bent aan het werk en plotseling blokkeert uw computer. Er verschijnt een pop-up in beeld. U moet binnen 24 uur € 50.000 betalen. Doet u dat niet, dan worden al uw gegevens gewist.



Een hacker heeft toegang tot uw productieproces en vraagt losgeld. Als u niet betaalt legt hij uw bedrijf plat.



Een medewerker heeft op een foute link geklikt en daarmee een virus binnengehaald. Uw ICT'er legt per direct alle systemen stil om verdere schade te voorkomen.

De schade kan oplopen tot tienduizenden of zelfs honderdduizenden euro's.

U moet snel handelen om de schade te beperken. Daarnaast is het van belang dat u klanten, leveranciers, personeel en soms ook de media informeert over de situatie.

U wilt de beste specialisten om ervoor te zorgen dat uw bedrijf snel weer up and running is en om verdere problemen te voorkomen.

Maar waar vind je deze experts op korte termijn? En hoe weet je dat ze echt gespecialiseerd zijn in het oplossen van een cyberincident? Tijd om zorgvuldig onderzoek te doen is er dan niet!

Dan is het een geruststellende gedachte terug te kunnen vallen op de Hienfeld Cyberverzekering.

Hienfeld heeft afspraken gemaakt met de beste experts op het gebied van cybercriminaliteit binnen het MKB, verenigingen en stichtingen. Zij zijn direct beschikbaar als u ze nodig heeft.

De Hienfeld Cyber Assist lijn is 24/7 bereikbaar. U wordt in uw eigen taal te woord gestaan door uw persoonlijke crisiscoördinator. Samen bekijkt u welke specialisten het incident zo snel mogelijk op kunnen lossen.

Wat biedt de Hienfeld Cyberverzekering?

Een cyberverzekering is meer dan een dekking tegen de financiële gevolgen van cybercriminaliteit. Voorkomen is beter dan genezen! En, als het toch gebeurt is het zaak dat u zo snel mogelijk weer op een veilige manier aan de slag kunt.

Professionele assistentie tijdens en na een incident

Incident response

De eerste 48 uur zijn cruciaal om de schade te beperken. U kunt 24/7 contact opnemen met de Hienfeld Cyber Assist lijn. Uw persoonlijke crisiscoördinator neemt de situatie met u door en stelt in overleg met u een team van cyber experts samen: het incident response team. Dit team bestaat uit professionals die gespecialiseerd zijn in het helpen van het MKB, verenigingen en stichtingen. Zij gaan direct aan de slag om het incident op te lossen.

Hienfeld cyber specialisten

Wij werken uitsluitend met de beste in cyber gespecialiseerde professionals. Zij hebben affiniteit met het MKB, verenigingen en stichtingen. Specialisten die uw taal spreken!

- Persoonlijke crisiscoördinator
- ICT'ers
- PR-bureau
- Juristen
- Forensische experts

Ondersteuning om uw bedrijf te wapenen tegen cybercriminelen

Wij hebben een selectie gemaakt van diensten en specialisten die u helpen een cyberincident te voorkomen en de bewustwording van cyberrisico's te vergroten.

Een overzicht van deze specialisten vindt u [hier](#).

Een actueel overzicht met adviezen om uw organisatie beter te beveiligen tegen cybercriminaliteit vindt u [hier](#).



Financiële vergoedingen



Hacking en Systeem inbraak

- Forensisch onderzoek naar de oorzaak en omvang van een hack
- Herstel van hardware en software óf het verbeteren hiervan om een nieuw incident te voorkomen
- Communicatie met stakeholders
- Herstel van gestolen data of -software
- Geld dat door systeembreuk van uw rekening is gehaald



Digitale afpersing

- Schade door gijzeling van uw computersysteem of data
- Assistentie van security experts
- Het betaalde losgeld



Juridische assistentie bij aansprakelijkheidsstelling

- Aanspraken van derden in verband met een cyberincident of datalek
- Media-aansprakelijkheid
- Kosten van verweer



Verlies of diefstal van privacy gevoelige gegevens

- Onderzoek door bijvoorbeeld creditcardmaatschappijen of justitie
- Opgelegde boetes door toezichthouders of andere verplichte vergoedingen



Omzetverlies door cyberaanvallen

- Omzetverlies door een cyberaanval op uw computersytemen



CEO fraude en social engineering

- Verlies van vermogen
- Onderzoekskosten om te bewijzen dat iemand een onrechtmatige overeenkomst heeft gesloten, met vermogensschade voor u tot gevolg

Wat is de Hienfeld Cyber Assist lijn?

De eerst 48 uur na een incident zijn cruciaal. De Hienfeld Cyber Assist lijn is 24 uur per dag bereikbaar. U krijgt direct iemand aan de lijn die u in uw eigen taal te woord staat. Wij helpen u als volgt:



Waarom Hienfeld?

- ✓ 24/7 Hienfeld Cyber Assist lijn
- ✓ Eén persoonlijke crisiscoördinator
- ✓ Directe beschikbaarheid van cyberspecialisten op diverse terreinen. Hienfeld ontzorgt!
- ✓ Preventieve diensten om uw bedrijf te beschermen tegen cybercriminaliteit
- ✓ Hienfeld is expert op gebied van het cyberrisico voor het MKB
- ✓ De eerste 72 uur geen eigen risico bij inschakelen crisiscoördinator
- ✓ Dekking voor het verbeteren van uw computersysteem na een incident
- ✓ Dekking voor social engineering fraude

Wilt u meer informatie?

Neem contact op met uw verzekeringsadviseur.