

Dat overkomt mij niet!



'Dat overkomt mij niet.' Dat is wat de meeste ondernemers denken als ze horen dat het netwerk van de burens is gehackt of dat er data is gelekt. Cybercrime ligt echter bij alle ondernemingen op de loer. Ook bij het MKB. Daarbij komt dat de cybercrimineel van tegenwoordig vernuftiger is dan ooit. Deze criminelen weten bijvoorbeeld in te breken in IT-systemen en een bedrijf tijdenlang te observeren, zonder dat iemand dat door heeft. Ze hebben zich bovendien goed verdiept in de psyche van de mens. Ze weten als geen ander hoe het menselijk brein werkt en hoe ze derden zover krijgen om geld over te maken. Gewoon, door gebruik te maken van gevoelens van twijfel, de wens om te 'pleasen' en tijdsdruk.



Snel handelen

Feit is: hoe beter een bedrijf beveiligd is, des te kleiner de kans dat dat bedrijf ten prooi zal vallen aan cybercriminelen. Maar als het dan toch gebeurt, bijvoorbeeld door een menselijke fout, dan is het zaak dat daar heel snel op gereageerd wordt om de schade zoveel mogelijk te beperken. Want dat scheelt niet alleen geld, het scheelt ondernemers ook enorm veel rompslomp en stress.

De juiste hulp op het juiste moment

Precies hiervoor kan een cyberverzekering afgesloten worden. Met de cyberverzekering van ACL Verzekeringen zijn ondernemers niet alleen gedekt voor diverse kosten, maar ontvangen zij voor, tijdens en na een incident ook hulp en advies.

-  Zij krijgen van tevoren hulp en advies om cybercrime te voorkomen. Zo krijgt iedere verzekerde die niet over een adequaat beveiligingssysteem beschikt, het Avast beveiligingssysteem tot zijn beschikking dat bestaat uit een firewall, een back-up systeem en antivirus software van goede kwaliteit.
-  Zij hebben 24/7 recht op hulp van een cyberrisk expert.
-  Zij krijgen advies en ondersteuning op tal van gebieden waaronder forensisch onderzoek naar de IT-systemen, analyse van de financiën, bewaking van de kredieten, juridische ondersteuning, crisiscommunicatie en PR.

Over welke risico's hebben we het zoal?

-  Ransomware (het encrypten van data die weer vrijgegeven wordt na betaling van losgeld)
-  Phishing
-  Onbeveiligde openbare wifi-netwerken
-  DDoS-aanvallen (aanval door een verzameling computers of andere apparaten die tegelijkertijd proberen om een computer(netwerk) of dienstverlening uit te schakelen)
-  Datalekken
-  Identiteits- of creditcarddiefstal
-  CEO fraude
-  Internet of Things (IoT) (waardoor criminelen zich via een device en WIFI netwerk toegang verschaffen)

Uitgebreide dekking tegen een concurrerend tarief

En de dekking? Die is bijzonder ruim. De cyberverzekering van ACL Verzekeringen dekt de wettelijke aansprakelijkheid, de bedrijfsschade en diverse kosten, zoals kosten van crisismanagement, data-herstel, forensisch onderzoek, rechtsbijstand, PR, verweer, PCI-boetes, cyberafpersing, melding en kredietbewaking. Het is dan natuurlijk wel van belang dat er gekozen wordt voor een verzekerd bedrag dat voldoende is om een solide dekking te bieden voor alle eerder genoemde risico's.

Er geldt bovendien geen eigen risico voor herstelkosten die gemaakt worden naar aanleiding van een dreigend of daadwerkelijk cyberincident. Kortom, een doordachte verzekeringsoplossing met verrassende verzekeringsvoorwaarden voor een zeer concurrerende premiestelling.



Een paar voorbeelden

Wanneer een medewerkster van een notariskantoor een, op het eerste oog, betrouwbare e-mail krijgt, klikt zij op de link om haar wachtwoord voor het intranet aan te passen. Achteraf blijkt dit een phishing e-mail te zijn waardoor cybercriminelen ongemerkt de systemen zijn binnengedrongen. De criminelen dreigen iedere dag een andere file openbaar te maken en eisen losgeld. Hierop dienen klanten een claim in voor het lekken van vertrouwelijke informatie. Met de criminelen moet bovendien onderhandeld worden over het geëiste losgeld.

Veel cyberincidenten doen zich geheel per ongeluk voor, veelal omdat een medewerker onachtzaam is. Bijvoorbeeld omdat een medewerker abusievelijk een vertrouwelijke e-mail naar een onjuiste mailinglijst stuurt, een zwak wachtwoord geraden wordt, iemand een laptop of USB-stick verliest, op een verkeerde link klikt of omdat een medewerker een oude harde schijf weggooit waar gevoelige informatie op staat. Het gevolg van al deze voorbeelden van niet bewust handelen is: een datalek.

Een medewerker verliest zijn telefoon en laptop, al dan niet door diefstal, met daarop persoonsgegevens van klanten en vertrouwelijke informatie van het bedrijf. Criminelen krijgen de telefoon en de laptop in handen en weten ze te ontgrendelen. Alle informatie komt op straat te liggen, waarop diverse klanten schadeclaims tegen het bedrijf indienen en het bedrijf bovendien reputatieschade oploopt.

Een oud-medewerker blijkt nog toegang te hebben tot alle bedrijfsgegevens en dus ook informatie van alle klanten. De medewerker chanteert hiermee het bestuur. Als het bestuur daar niet op ingaat verkoopt de oud-medewerker de gegevens door, waarop meerdere klanten schadeclaims indienen.

Een medewerker die in coronatijd thuiswerkt vindt het lastig om zich steeds weer opnieuw te moeten identificeren bij het inloggen op het bedrijfsnetwerk. Daarop bedenkt hij een workaround om gewoon lekker door te kunnen werken en gaat op zijn eigen laptop aan de slag. De beveiligingssoftware op de eigen laptop is echter niet optimaal en criminelen weten zich zo toegang te verschaffen tot zijn e-mailaccount.

Het computersysteem van een fabriek is gehackt. Pas na betaling van een som geld worden de systemen vrijgegeven. In de tussentijd kunnen de werkzaamheden geen doorgang vinden, waardoor de fabriek bedrijfsschade oploopt en achteraf ook nog eens geconfronteerd wordt met schadeclaims.

Zo ziet u maar: een cyberincident kan de beste overkomen. Gelukkig heeft ACL Verzekeringen speciaal voor het MKB een cyberverzekering ontwikkeld. Op de website kunt u heel gemakkelijk online een offerte opvragen.





ACL

ACL Verzekeringen

Postbus 314 | 7570 AH Oldenzaal | Tel: 0541-571179

E-mail: info@aclverzekeringen.nl | www.aclverzekeringen.nl