Verzekeren tegen cyberrisico's: nuttig of noodzakelijk?

Is het nog verantwoord om geen verzekering te nemen tegen cyberrisico's?

Een familiale BA-verzekering, dat vinden we allemaal vanzelfsprekend. Maar tegen informaticarisico's is het gros van de bedrijven, en dan vooral KMO's, niet voldoende verzekerd. Dat is deels te wijten aan naïviteit (*"mijn kleine bedrijf is vast niet interessant genoeg voor cybercriminelen"*), maar het is vooral ook een kwestie van onwetendheid. Kleine bedrijven hebben vaak minder krachtige beveiligingssystemen en beschikken doorgaans niet over een beproefd actieplan in geval van incidenten. Met andere woorden, ze zijn een vogel voor de kat.

Van een polis "Alle Risico's" naar een cyberrisicoverzekering.

Veel bedrijven heeft uiteraard wel een "Alle Risico's"-verzekering, die schade aan hun IT-apparatuur dekt. Hoewel een dergelijke verzekering noodzakelijk is, volstaat ze niet als bescherming tegen de golf van nieuwe cyberrisico's. De klassieke "Alle Risico's Elektronica"-verzekering dekt doorgaans schade bij ongevallen (brand, waterschade, diefstal enz.), maar schade door menselijke fout of vijandige aanvallen wordt in principe niet gedekt. Zelfs bij ongevallen stellen we vast dat de indirecte schade (bedrijfsverliezen, bijkomende kosten, terugzetten van gegevens, kosten voor herstel van de systemen enz.) meestal een veelvoud vormt van de materiële schade. Bij het aangaan van een polis wordt dit echter vaak over het hoofd gezien.

Bovendien is het informaticalandschap geëvolueerd...

Het informaticalandschap evolueert zo snel dat veel bedrijven, en vooral bedrijfsleiders, moeite hebben om bij te blijven. Informatici lanceren voortdurend nieuwe technologieën, zonder duidelijk zicht op de bijbehorende risico's. Cloudcomputing, mobiele technologieën (smartphones, tablets enz.) en de toenemende dematerialisatie van de activiteiten zijn slechts enkele voorbeelden. Bedrijven zijn steeds meer afhankelijk van hun informaticasystemen, met alle gevolgen van dien bij problemen. Elke bedrijfsleider zou zich voor elk IT-systeem de vraag moeten stellen: wat zijn de gevolgen voor mijn bedrijf als dit systeem een uur, een dag, een week of zelfs een maand onbeschikbaar is? Voor bepaalde bedrijfskritieke (vaak industriële) systemen zijn de gevolgen al na enkele minuten dramatisch.

Nieuwe risico's

De nieuwe vormen van cybercriminaliteit zijn zeer verontrustend: het verzamelen van bank- en andere vertrouwelijke gegevens, fraude, afpersing, malware, een Denial-of-Service-aanval op webshops, diefstal van materiaal en gegevens enz.
Ook menselijke fouten mogen we niet uit het oog verliezen: verlies van materiaal, doorsturen van onjuiste gegevens, phishing met het oog op het verduisteren van overschrijvingen of inbreuken in het systeem, ongewild aansluiten van een geïnfecteerde USB-stick enz.

De kosten lopen bij dergelijke incidenten al snel hoog op: interventie van gespecialiseerde technici om gegevens terug te zetten en de software en het informaticasysteem te herstellen, kosten voor experts om de oorzaken en gevolgen van het incident te onderzoeken, kosten voor juridisch adviseurs, eventuele kosten om alle betrokkenen op de hoogte te brengen van de diefstal van hun gegevens enz.

Een schadegeval kan zeer nadelige gevolgen hebben voor de reputatie en het imago van het bedrijf. Vaak moet dan ook een beroep worden gedaan op PR-consultants voor de coördinatie van de crisiscommunicatie en om de impact op het imago van het bedrijf te minimaliseren.

Schadelijke gevolgen, zegt u?

Een schadegeval kan ook nadelige gevolgen hebben voor derden waarbij het betrokken bedrijf burgerlijk aansprakelijk is.
Na een lange periode van terughoudendheid na de aanslagen van 11 september 2001 hebben een aantal verzekeringsmaatschappijen polissen uitgewerkt om hierop een antwoord te bieden.

De grote makelaarskantoren beschikken doorgaans over een afdeling die gespecialiseerd is in informaticarisico's, wat niet geldt voor kleinere makelaars, waar de nood aan informatie en opleiding vaak nog groot is.

Het beheer van IT-risico's start met een grondige analyse van de risico's waar het bedrijf aan blootgesteld is. Daarna moeten geschikte veiligheidsmaatregelen worden genomen. Het uiteindelijke doel is de risico's te identificeren die moeten worden verzekerd, zodat de kosten bij een schadegeval gedekt zijn.
Het is belangrijk dat ook de makelaars inzicht hebben in de informaticarisico's waarmee hun klanten worden geconfronteerd, zodat ze hen de polis kunnen aanbieden die het best aan hun behoeften voldoet.

Ir. Luc GOLVERS,
Gerechtsdeskundige informatica.
Voorzitter Belgische Club voor Informaticaveiligheid.
luc.golvers@skynet.be

CEPOM - Partner

Meer informatie

Wij hechten belang aan uw opmerkingen en opbouwende feedback. Aarzel dus niet om contact met ons op te nemen via http://www.cepom.be/nl/contact/

Voor verdere inlichtingen

Véronique Lagae – Opleidingscoördinator
Tel: +32 2 721 82 77 of veronique.lagae@cepom.be