ONDERNEMERS ADVISEREN OVER CYBERRISICO'S IS NIET MAKKELIJK. DE KANS IS NAMELIJK GROOT DAT UW RELATIE ZICH HIERVOOR LIEVER WENDT TOT ZIJN ICT-DIENSTVERLENER. TOCH IS ER EEN BELANGRIJKE ROL VOOR U WEGGELEGD. Ú BENT NAMELIJK RISICO-EXPERT; Ú DENKT NA OVER DE GEVOLGEN VAN EEN ONDERBREKING VAN DE BEDRIJFSCONTINUITEÏT. EN CYBERCRIME IS EEN VAN DE FACTOREN DIE IMPACTVOLLE GEVOLGEN KAN HEBBEN, HELEMAAL NU DOOR CORONA HET CYBERRISICO IS GEGROEID EN VERANDERD.

de Goudse verzekeringen

Tijd voor goed risicomanagement is nú

TEKST **PHILIP VAN GANGELEN, MANAGER VERKOOP DE GOUDSE**

Zoals gebruikelijk maken cybercriminelen gebruik van actuele ontwikkelingen om hun criminele acties aan op te hangen. Corona is voor hen een dankbaar onderwerp. Ieder mogelijk slachtoffer kent het, is zeer geïnteresseerd en is misschien zelfs een beetje bang. De kans dat iemand 'hapt' is dus groter dan ooit. Niet gek dat cybercriminelen hun pogingen flink opgeschaald hebben in de eerste helft van 2020. Bij de politie kwamen in mei 2020 volgens RTL Nieuws 6,8 keer zoveel meldingen van digitale misdaad binnen. Nepwebwinkels voor mondkapjes en desinfectiegel, antibacteriële bankpassen, nepmails uit naam van de World Health Organisation en het RIVM... ze schoten als paddenstoelen uit de grond.

ENORME VLUCHT

Door corona werkt een groot deel van Nederland nu thuis. Hoewel de versoepelingen langzaam opgeschaald worden, durf ik wel te stellen dat er voorgoed iets veranderd is. Zo meldt het Kennisinstituut voor Mobiliteitsbeleid dat 44 procent van de Nederlanders door corona is gaan thuiswerken en een kwart daarvan dat ook na de coronacrisis wil blijven doen. Hierdoor vindt communicatie veel minder plaats op kantoor. Vergaderen doen we via Zoom, Teams of Skype. Ook het brainstormen is gedigitaliseerd. Hingen post-its en je innovatieve ideeën vroeger relatief veilig aan de muur van je vergaderzaaltje, ze hangen nu via applicaties als Slack en Miro in cyberspace.

Maatschappelijk gezien is dit een prachtige ontwikkeling. We besparen veel kosten door een afname van de reistijd en mogelijk straks ook van de kantoorruimte, om over de verbetering van de luchtkwaliteit nog maar te zwijgen. Maar je hele bedrijfsvoering digitaal doen heeft ook keerzijdes. Want hoe meer we digitaliseren, hoe groter de kans op cybercrime. En als het dan misgaat, is je bedrijfscontinuiteït nog meer dan voor corona in het geding.

OP STEL EN SPRONG

Naast de toegenomen digitalisering is ook van belang onder welke omstandigheden die tot stand is gekomen. Door corona is dit namelijk, noodgedwongen, in allerijl gebeurd. Veel bedrijven zijn op stel en sprong overgegaan tot digitalisering van hun bedrijfsprocessen. Hierbij is de ondernemer in sommige gevallen ineens afhankelijk van de beveiliging van thuiscomputers van zijn medewerkers. Ook is onder de grote druk veel gebruikgemaakt van allerlei gratis (en dus wellicht minder beveiligde) apps. Zo gingen we massaal gebruikmaken van videobelapp Zoom, die vervolgens zo lek bleek als een mandje. Cybercriminelen maakten zo een half miljoen wachtwoorden buit. En die te betalen factuur die je baas vroeger met de pen aftekende, werd van de ene op de andere dag via de e-mail geaccordeerd.

Ik kan me goed voorstellen dat bij deze acute digitalisering risicomanagement een van de laatste zorgen van on-

dernemers moet zijn geweest. Maar het is wel de hoogste tijd om te beginnen met het managen van deze plots ontstane risico's. We stonden er voor corona namelijk ook al niet zo goed voor.

NUL TOT DRIE MAATREGELEN

Uit onderzoek blijkt dat ondernemers ervan uitgaan dat hun ICT-dienstverlener de cyberrisico's allemaal wel geregeld heeft. Ze vinden zelfs dat de ICT'er aansprakelijk is als er zich tóch een cyberincident voordoet. Nu blijkt óók uit onderzoek dat de gemiddelde ondernemer eigenlijk maar een paar cybermaatregelen treft. Een virusscanner en een Wifi-wachtwoord hebben de meeste ondernemers nog wel: circa 75 procent. Daarna wordt het al snel minder. Het CBS geeft aan dat circa 45 procent slechts nul tot drie maatregelen neemt. Uit eigen onderzoek van De Goudse komt eenzelfde beeld. Zo zien wij dat slechts 52 procent van de ondernemers dagelijkse back-ups laat maken en dat niet meer dan 34 procent aan bewustwording bij de medewerkers doet. Het belang van goede voorlichting van medewerkers, beveiliging en back-ups werd begin dit jaar nog maar eens aangetoond bij de Universiteit Maastricht. Op 2 januari 2020 meldden de media dat de universiteit slachtoffer was geworden van ransomware. Cybercriminelen waren diep doorgedrongen tot de systemen en blokkeerden de toegang tot e-mail, Windows en wetenschappelijke gegevens. De universiteit zag uiteindelijk geen andere mogelijkheid dan het betalen van losgeld van 197.000 euro om de controle over hun systemen terug te krijgen. De oorzaak? Eén phishing-mailtje.

Het gekke is dat back-ups en voorlichting juist vrij makkelijke en goedkope manieren zijn om je cyberrisico's te verkleinen.

> 'Perfect moment om een risico-inventarisatie onder de aandacht van uw relaties te brengen'

DÉ KANS VOOR RISICOMANAGEMENT

Tijdens deze coronacrisis staan ondernemers, wellicht onbewust, meer open voor risicomanagement. Er is in korte tijd veel veranderd en wellicht hebben ze het gevoel minder dan ooit grip op hun (cyber) risico's te hebben. Wellicht zijn ze ook, breder dan alleen het cyberrisico, op zoek naar hulp bij het inschatten van nieuwe risico's die nog op hen afkomen en horen ze graag hoe zij hier zo goed mogelijk op kunnen inspelen. Weinig ondernemers waren voorbereid op deze situatie en dat willen ze in de toekomst niet nog een keer laten gebeuren. Een perfect moment dus om een risico-inventarisatie onder de aandacht van uw relaties te brengen.

Zoals gezegd, zijn er relatief eenvoudige en betaalbare manieren voor ondernemers om het risico op en de gevolgen van een cyberincident te verkleinen. Toch kan het risico nooit helemaal worden uitgesloten. De bedrijfscontinuiteït kan ernstig in gevaar komen als er toch iets gebeurt. Het is dus altijd aan te raden om een cyberverzekering af te sluiten om de gevolgen hiervan te kunnen opvangen.

Veel succes bij uw advisering! ■