Een cybercrisis is niet te voorkomen

We zien in de praktijk dat kantoren en hun klanten volledig afhankelijk zijn geworden van digitalisering. Daarmee stijgt het risico van een cyberincident, met alle verstoringen die dat met zich meebrengt. Welke preventieve maatregelen je ook genomen hebt om informatie te beveiligen, cyberincidenten zullen blijven voorkomen. Wat kun je dan nog doen?

Met die vraag hebben we ons in de afgelopen maand tijdens de IT-managementkring en de IT-auditkring beziggehouden. Dat deden we in samenwerking met informatiebeveiligingsspecialist Northwave.

Hacken of datalekken

Northwave ondersteunt bedrijven niet alleen bij het inschatten van risico's en het nemen van preventieve maatregelen, maar ook wanneer ze gehackt zijn of een datalek hebben. Dan rukt het computer emergency response team (CERT) uit. "We zien als Northwave CERT elke week weer nieuwe incidenten. Veel van die incidenten raken organisaties behoorlijk hard. Ze leggen processen lam en veroorzaken financiële schade. Wat we nu veel zien, is het fenomeen 'business email compromise', een manier van fraude waarbij gehackte e-mailaccounts een hoofdrol spelen. We zien op die manier tienduizenden tot honderdduizenden euro's verdwijnen." Aan het woord is Martijn Hoogesteger, hij is de teamlead van Northwave CERT.

Voorbereid op incident

Hoogesteger vervolgt: "De ontwikkelingen in cybercrime gaan gewoon erg snel. Daarom loop je met alleen preventieve maatregelen toch altijd een beetje achter de feiten aan. Het is daarom ook goed aandacht te geven aan detectie van hackers en de professionele reactie (incident response) daarop. Door je goed voor te bereiden op een incident, kun je de impact beperken en sneller weer je normale bedrijfsproces hervatten. Daarom is oefenen van wezenlijk belang. Als u dat langer dan zes maanden geleden voor het laatst gedaan heeft, dan wordt het hoog tijd."

Oefenen tijdens de kringbijeenkomst

Tijdens de IT-managementkring en de IT-auditkring hebben we daarom zo'n cyberincident geoefend. In groepen van zes deelnemers gingen we een uitgebreid scenario te lijf. Dat leverde veel inzichten op hoe belangrijk structuur in je aanpak en time management zijn. Belangrijkste inzichten: zorg dat je feiten van aannames weet te onderscheiden en houd een goed logboek bij van je beslissingen.

Verzekering

Naast voorbereiding kan natuurlijk ook het financiële risico worden aangepakt. Een aantal SRA-leden heeft daarom inmiddels een cyber risk-verzekering afgesloten. Zo'n verzekering vult de bestaande verzekeringen voor schade en (bestuurs-)aansprakelijkheid aan en biedt dus een goede manier om juist ook die risico's te dekken die niet met preventieve maatregelen worden ondervangen.

Tim van Lier, hij is underwriter bij Zürich Benelux en specialist op het gebied van het verzekeren van Security & Privacy-risico, zegt daarover: "Na een cyberaanval worden bedrijven geconfronteerd met extra kosten en mogelijke schadeclaims van derden. Productlijnen komen stil te liggen, computers raken onbruikbaar of gevoelige informatie ligt op straat. Een misvatting is dat de schade veroorzaakt door een cyberaanval is verzekerd via de traditionele schade- of aansprakelijkheidspolis. Doorgaans is dat niet het geval. Verzekeraars sluiten vaak cybergerelateerde schade uit. De kans dat men dan zelf met de kosten van de schade blijft zitten, is vervolgens groot."

Tijdens de oefeningen in de IT-management- en IT-auditkring hebben we die wisselwerking met een verzekeraar ook betrokken in het scenario. De verzekering dekt namelijk de bijstand van een computer emergency respons-team. Maar wanneer laat je zo'n team nu precies komen? Dat is ook een belangrijke constatering die de verzekeraar doet.

> Een cyberincident oefenen, is van wezenlijk belang

Samenwerking optimaliseren

Door de samenwerking tussen klant, verzekeraar en incident response te optimaliseren, daalt de schade en de duur van het incident. Los van de uitkering door de verzekeraar is dat natuurlijk altijd in het belang van het kantoor en de klanten van het kantoor. Zo snel mogelijk weer up & running zijn, dat is steeds de inzet. "We helpen onze klanten om het risico te beheersen door hen, voorafgaand aan een incident, al beter voor te bereiden. Mocht het komen tot een incident, dan wil je het bedrijf zo snel mogelijk weer terug op de rit hebben. We maken gebruik van uitgebreide netwerken waarin partners deelnemen die helpen bij de digitale-, juridische- en communicatieve afwikkeling van cyberincidenten", aldus Van Lier.

Speciale opleiding security management

Een goede voorbereiding is dus het halve werk. Daarom zal SRA u samen met Northwave verder faciliteren met kennis en kunde op dit gebied. In de tweede helft van dit jaar lanceren we bijvoorbeeld een speciale workshop security management voor accountantskantoren. Deze workshop stelt u in staat om op een goede manier de rol van security officer in te nemen. Alle elementen van security en privacy management komen aan de orde. Bovendien biedt meedoen aan de training ook meteen het gebruik van een online tool voor security en privacy management en een uitgebreide documentatieset, specifiek op maat gemaakt voor SRA-leden.

Meer informatie

Heeft u vragen over dit onderwerp, neem dan contact op met Tony van Oorschot, automatisering@sra.nl of 030 656 60 60.