HELPEN OM DE RISICO'S IN KAART TE BRENGEN

De vraag is niet of je wordt gehackt, maar wanneer. En als het dan gebeurt, zorg dan dat je er zo goed mogelijk op bent voorbereid. Bij Bol Adviseurs hebben ze de kennis in huis om ondernemers optimaal te adviseren over cybersecurity. En dan gaat het om veel meer dan hackpogingen alleen, legt EDP Auditor Thijs Peeters van Bol Adviseurs uit.

Thijs, jarenlang werkzaam geweest in de accountancy, heeft zich bij Bol Adviseurs gespecialiseerd in informatiebeveiliging. "Onze accountants zijn voor onze klanten een soort huisarts. Zodra zij problemen signaleren op het gebied van IT, informatiebeveiliging, cybersecurity, privacy of AVG, verwijzen ze klanten door naar de medisch specialist. Dat ben ik, samen met mijn collega's." Het liefst gaan ze bij de klant langs. "Omdat elk bedrijf zijn eigen risico's heeft en zijn eigen maatregelen moet treffen op het gebied van cybersecurity."

MENS, ORGANISATIE EN PROCES

Door middel van een Maturity Scan kijkt Bol Adviseurs hoe de informatiebeveiliging bij de klant is georganiseerd op strategisch, tactisch en operationeel gebied. Het begint bij de mensen. "Personeel moet snappen dat ze een sterk wachtwoord moeten kiezen en niet zomaar op een linkje moeten klikken. Daarnaast kijken we naar organisatie en proces: we kijken naar de risico's en adviseren welke procedures we optuigen om die risico's zo goed mogelijk te beheersen" Ten slotte speelt ook de component 'techniek' een rol. "Dan laten we een hacker proberen of hij van buitenaf kan binnendringen in jouw IT-omgeving."

Uit de Maturity Scan blijkt hoe volwassen een bedrijf is op het gebied van informatiebeveiliging. Het volwassenheidsmodel bestaat uit 5 niveaus: van beperkt tot heel uitgebreid. "Veel van onze klanten zitten op niveau 2: iedereen doet zijn ding, maar de documentatie laat te wensen over en een opvolgingsbeleid ontbreekt. Dan loop je het risico dat je van elkaar niet weet of bepaalde werkzaamheden zijn verricht. En in het geval iemand de organisatie verlaat, hij of zij de opgebouwde kennis meeneemt." Thijs adviseert klanten om te streven naar volwassenheidsniveau 3. "Daarbij zijn de belangrijkste werkprocessen uitgeschreven. Belangrijk is ook dat de HR-afdeling op basis van een blauwdruk of matrix weet welke rechten bij welk functieprofiel horen. En laat een afdelingshoofd een keer per jaar controleren of de rechten van de medewerkers kloppen."

RISICO'S VAN BUITENAF

Bij informatiebeveiliging is het daarnaast natuurlijk belangrijk om de risico's van buitenaf af te dekken. "Het is niet de vraag of je wordt gehackt, maar wanneer. Vaak denken klanten dat ze helemaal niet interessant zijn voor hackers. Maar die kijken juist naar hoe goed de beveiliging is. Wanneer het bij het ene bedrijf goed dichtgetimmerd is, kijken ze hoe het er bij de buurman uitziet. Als je alles goed beveiligd hebt, dan is de kans dat ze binnenkomen een stuk kleiner. Bedenk ook dat het voor hackers uiteindelijk draait om geld. Bijvoorbeeld door middel van ransomware te installeren. Dan moet je met bitcoins over de brug komen om weer toegang te krijgen tot je bestanden. Dat is geen sinecure om mee te maken, en komt echt veel vaker voor dan je denkt. Het maken van back-ups is echt geen overbodige luxe."

DE JUISTE KENNIS

Vanuit strategisch oogpunt is het volgens Thijs belangrijk om de verantwoordelijkheid voor de IT-beveiliging op de directietafel te leggen. "Vertrouw daarbij niet op één IT-medewerker. Uit onderzoek blijkt dat de grootste zorgen van bestuurders liggen op het gebied van cybersecurity en datamanagement, waaronder AVG. Zorg dus dat je de juiste kennis op de goede plek hebt in je organisatie. Of bindt daarvoor de juiste externe partijen aan je. Een must is daarbij een goede dienstverleningsovereenkomst, waarin duidelijk staat welke taken bij die externe partij liggen en hoe daarover wordt gerapporteerd."
De dienstverlening van Bol Adviseurs is erop gericht om klanten te helpen met het in kaart brengen van de grootste risico's, en hoe ze die op de beste manier kunnen borgen. Thijs: "Dan gaat het om *business continuity*: bedenk wat het ergste is wat je als bedrijf kan overkomen en hoe je dat dan gaat oplossen. Dan komt ook een stukje crisismanagement om de hoek kijken: je mensen moeten vanaf dan weten wat te doen om die crisis zo snel mogelijk af te handelen. Uiteindelijk is het onze rol om de klant te wijzen op de risico's. Het is aan de klant of hij die risico's wil accepteren", besluit hij.

BOLADVISEURS.NL