#ingezonden

Managed-securityservices verhogen weerbaarheid organisaties

Security verdient businessaandacht

Door **Sytse van der Schaaf**, research consultant en **Raymond Linkers**, director sourcing bij Metri

SCHIPHOL-RIJK - Bestuurders van organisaties leggen security veelal in handen van hun technische experts, terwijl zij het zelf als een bedrijfskundige kwestie aan zouden moeten pakken. In het aanbod van managed-securityservices is genoeg gerichte hulp van buiten te vinden waarmee de weerbaarheid effectief omhoog kan. Wat vooral nodig is, is een cultuurverandering in de directiekamer. Bestuurders moeten de agenda bepalen en security benaderen als hun probleem.

Cybersecurity is hoger op de strategische agenda komen te staan. Drie factoren zijn hierin essentieel: de ernst van de dreigingen, het toegenomen belang van IT en tot slot regelgeving. Bestuurlijk Nederland is cybersecurity serieus gaan nemen door aanvallen met de WannaCry- en Petya-ransomware medio 2017. Deze schadelijke software ontregelde de IT van toonaangevende organisaties als de APM-terminal in Rotterdam en TNT Express met aanzienlijke schadeposten tot gevolg.

Bedrijfskritische IT

De risico's zijn ook groter geworden doordat een vergaande digitalisering van bedrijfsprocessen de afhankelijkheid van bedrijfskritische IT heeft doen toenemen. Gedigitaliseerde overheidsdiensten, internetbankieren en e-commerce zijn gevoelig voor verstoringen door cyberaanvallen. De overheid onderkent dit economisch en maatschappelijk belang. Nieuwe regelgeving dwingt organisaties tot nieuwe maatregelen om de grote stroom datalekken en andere negatieve gevolgen van cybercrime in te dammen. De Algemene Verordening Gegevensbescherming (AVG) brengt het privacybelang van consumenten in balans met de dataverzamelwoede van de BV Nederland. Het dwingt organisaties bovendien om een informatiebeveiligingsplan in te stellen of het flink te herzien.

Aansprakelijk

Van een alarmerend gebrek aan urgentie rondom security is er nu opeens volop aandacht. Dat is op zich een positieve ontwikkeling, maar draagt ook risico's in zich. In 'Nederland verzekeringsland' zijn cyberverzekeringspolissen opeens ontzettend populair geworden. Bestuurders lopen het risico van persoonlijke aansprakelijkheid bij het niet melden van datalekken of claims rond onbehoorlijk bestuur als zij te weinig aandacht aan security hebben geschonken. Maar is de praktische weerbaarheid van organisaties werkelijk gediend met het afsluiten van dit soort kostbare polissen? Of wat te denken van de relatief nieuwe CISO en privacyfunctionarissen die in grote organisaties opduiken? Zitten zij werkelijk aan de directietafel en wordt er echt iets met hun input gedaan? Uit het 'Mind the breach gap'-rapport van Gemalto blijkt dat er vooral meer geld gaat naar gangbare technische securityoplossingen die in het huidige cloudtijdperk hun beperkingen hebben.

Zoden aan de dijk

Wat zet meer zoden aan de dijk? Behandel security als een gangbaar bedrijfsrisico en kom vooral met een praktische aanpak. Dat betekent dat er vanuit specifieke operationele risico's duidelijkheid komt welke systemen en data beveiligd moeten worden, wie waarvoor verantwoordelijk is inclusief de directie, hoe die beveiliging tot stand komt en wat dat mag kosten. Een belangrijk en bekend voorbeeld van zo'n aanpak komt van het National Institute of Technology and Standards (NIST), een organisatie die Amerikaanse overheidsinstanties bijstaat in cybersecurity. Er is net een nieuwe versie van dit raamwerk uitgebracht, op basis waarvan het Department of Defense voor het begin van de herfst een order met een geschatte contractwaarde van 10 miljard dollar gaat plaatsen voor het verhuizen van de eigen IT naar de public cloud. Dat staat en valt met goede security.

Expertise van buiten

Ook het afnemen van gerichte managed-securityservices kan een goed middel zijn om de eigen weerbaarheid aanzienlijk te verhogen. Voorbeelden van diensten zijn het beheer van firewalls, het aanbrengen van kritieke softwarepatches of realtime monitoring van de IT-omgeving op afwijkend gedrag. Een ander voorbeeld is deskundig advies bij de bouw van applicaties rond goede securitypraktijken. Een leverancier als Cast Software past dit medicijn toe door software tijdens de levenscyclus minder vatbaar te maken voor het uitbuiten van kwetsbaarheden. Door externe expertise en de overdracht van operationele taken aan een leverancier komt er meer tijd om security beleidsmatig aan te pakken en de business beter te ondersteunen. IT-adviesbureau METRI brengt binnenkort een rapport uit over het succesvol sourcen van managed-securityservices. Meer informatie is te vinden op www.metrigroup.com.

#strategicsourcing

Betere marktverkenning leidt tot betere outsourcing

Strategisch snuffelen (om niks te missen)

IT mag de laatste jaren weer helemaal meedoen in de boardroom. Los van cloud en 'as a service' zijn er allerlei nieuwe ontwikkelingen waarmee IT en aanpalende technologieën echte businessenablers zijn geworden. En soms zijn ze *zelf* de business. Tegelijkertijd is er een trend gaande waarbij weg wordt bewogen van outsourcing, of in elk geval van de term 'outsourcing'. De discussie over deze term leidt echter af van het echte probleem.

Door **Henk Pater**, CEO en oprichter van Outsourcing Hub

AMSTERDAM - Op zich begrijpelijk als je kijkt naar de klassieke definitie, waarbij men vaak denkt aan eerstegeneratie-outsourcingsdeals (met voor sommigen een nare bijsmaak). Maar deze deals zijn er nog genoeg in de midsize markt voor commodity-IT en in de gehele markt voor nieuwe IT-technologieën. Ze zien er alleen anders uit, maar wat ze gemeen hebben is dat het gaat om 'de eerste keer'.

Discussie voeren over de term outsourcing of over welke 'generatie' het betreft, leidt af van het echte probleem. Juist omdat de markt in zo'n rap tempo verandert, qua beschikbare technologieën en daarmee ook wat betreft spelers en hun aanbod, ontstaan nieuwe risico's en uitdagingen. Ik heb de indruk dat die te vaak worden weggewuifd onder het mom van 'het is geen outsourcing' of 'hebben we al vaker gedaan'.

Risico van uitsluiting

Bij deze problematiek hoor ik vrijwel altijd twee belangrijke oorzaken. Allereerst wordt er te weinig tijd en moeite gestopt in het grondig verkennen van de markt. Ten tweede is in het proces voorafgaand aan de formele (selectie)procedures vaak te weinig gelegenheid tot interactie met de markt.

Hierdoor loopt de vragende partij het risico dat leveranciers die goed zouden passen, onbewust of onbedoeld worden uitgesloten of afgeschrikt. Bijvoorbeeld omdat ze simpelweg niet in het vizier waren, of omdat eisen of tenderprocedures (onnodig) zwaar of ingewikkeld zijn gemaakt. Bovendien hebben IT-leveranciers niet altijd per direct tijd en resources beschikbaar en geven ze vanwege de 'luxe van keuze' vaker een no-bid af.

Snuffelen als oplossing

De oplossing zit 'm dus in het beter bijhouden van de markt en vooral in het eerder en meer interacteren met de markt. Klinkt simpel, maar het vergt een flinke bak aan discipline; we zijn met z'n allen kampioen uitstellen en 'druk zijn'. Dan is het gemakkelijk om terug te vallen in oude patronen.

Ik praat daarom liever over 'snuffelen', of beter gezegd *strategisch snuffelen*, want

Henk Pater

"Het belang van snuffelen was al groot en zal nog toenemen"

het snuffelen zelf moet interessant en leuk zijn, zonder al te veel inspanning en zonder keiharde verplichtingen. Maar ook strategisch, omdat het van essentieel belang is voor zowel IT als de business.

Daarbij zouden we eens naar een heel andere sector moeten kijken, namelijk die van het online daten. Om de ideale levenspartner te vinden kun je niet met iedereen praten, borrelen of een relatie aangaan. Tegelijkertijd vergroot je bij online daten de kans op succes door aan de voorkant te starten met zoveel mogelijk 'kandidaten'.

Online platforms

Slimme datingsites voorzien in een flinke lijst criteria die iedereen vooraf invult. Zo kan het matchingalgoritme bepalen wie voor elkaar een goede match vormen en wordt het kaf van het koren gescheiden. Beide gematchte personen beoordelen de kwaliteit van de match. Om te bepalen met wie je eventueel een borrel wilt gaan doen, ga je eerst eens wat chatten en e-mailen.

Snuffelen dus. Natuurlijk is de borrel het leukst en vergt het chatten en mailen wat tijd (dat voelt zeker zo als er *geen* borrel volgt), maar doe je dat goed, dat is de kans op een geslaagde borrel en een mooi vervolg veel groter. En zo voorkom je teleurstellende borrels of erger.

Dat is als je het mij vraagt precies wat we nodig hebben in de IT-sector. Bij het online daten werkt het uitstekend. Voor mij persoonlijk in elk geval, want ik ben vorig jaar getrouwd met mijn droomvrouw. Zij werd negen jaar geleden als goede match aan mij voorgesteld door zo'n slimme datingsite. Online platformen hebben de toekomst, ook voor IT en allerlei opkomende technologieën. En of je het nu outsourcing of sourcing noemt: het belang van snuffelen was al groot en zal alleen maar toenemen!