John Proctor, Vice-President Cyber Security bij CGI:

"ALLES DRAAIT OM RISICO-MANAGEMENT"

Tekst: Paul Teixeira

In onze digitale samenleving is alles met alles verbonden. Onderzoekers denken dat rond 2020 meer dan dertig miljard apparaten draadloos met elkaar zijn verbonden via *the internet of things*. Deze *hyperconnected* wereld zorgt voor economische en maatschappelijke groei, maar maakt organisaties ook kwetsbaar voor identiteitsdiefstal, cyberspionage en digitale oorlogsvoering. Dit laatste is volgens inlichtingendiensten zelfs een grotere bedreiging dan terrorisme. Volgens John Proctor, Vice-President Cyber Security bij de multionationale ICT-dienstverlener CGI, is *awareness* cruciaal om digitale dreigingen aan te pakken. "Organisaties moeten zich afvragen hoe secure ze zouden móeten zijn, niet hoe secure ze technisch kúnnen zijn."

Computercriminaliteit bestaat al sinds de jaren tachtig, toen ICT-oplossingen beschikbaar kwamen voor het grote publiek. Wat is er de laatste jaren veranderd?
John Proctor: "Cybercriminaliteit verschilt feitelijk niet van andere vormen van criminaliteit. Er is een slachtoffer voor nodig en een aanvaller die er op uit is om het slachtoffer schade te berokkenen. Maar waar het werkterrein van een zakkenroller beperkt is tot drukke winkelstraten, zijn cybercriminelen wereldwijd actief. En nu de hacker steeds professioneler en de technologie steeds complexer wordt, is het zaak je hiertegen te wapenen."

Wat zijn de voornaamste cybersecurityvraagstukken waarmee organisaties worden geconfronteerd?
"Vooral het professionalisme van de aanvallers en de complexiteit van zowel de dreiging zelf als de oplossing nemen de laatste tijd snel toe. Bedrijven en overheden moeten het met vaak beperkte IT-resources opnemen tegen mondiale bedreigingen. Maar gespecialiseerde IT-medewerkers zijn schaars en stakeholders eisen steeds minder risico en steeds meer compliancy aan wet- en regelgeving. Een flinke uitdaging, zeker gezien de huidige marktdynamiek waarin kostenreductie én performance-verbetering centraal staan."

Zijn bedrijven en overheden voldoende doordrongen van de urgentie van cybersecurity?
"Ze hebben in elk geval allebei belang bij cybersecurity. Ondernemingen investeren niet fors in R&D om vervolgens de concurrentie met waardevolle patenten aan de haal te laten gaan. *Due diligence* is ook van toepassing als het gaat om het verantwoord omgaan met bedrijfsinformatie. >>

OVER JOHN PROCTOR

John Proctor is een internationaal erkende security- en riskexpert. Na een carrière van ruim twintig jaar bij het Britse en Canadese leger – onder meer als human intelligence-specialist en personnel recovery-specialist – ging Proctor in 2011 bij CGI aan de slag als Vice-President Cyber Security. Onder Proctors leiding werden ook management en government van de 'human factors' van cyber security verankerd in CGI's securityservices.

‘Medewerkers moeten intrinsiek gemotiveerd zijn om verantwoordelijk met bedrijfsinformatie om te gaan’

Nalatigheid is niet alleen schadelijk voor de reputatie van een organisatie, maar kan bestuurders ook persoonlijk worden verweten, zoals een Canadese rechter onlangs oordeelde. Overheden willen een veilige leefomgeving en betrouwbare digitale dienstverlening voor hun burgers, maar kunnen digitale dreigingen niet alleen het hoofd bieden. De meeste publieke IT-infrastructuren worden geleverd door private partijen, dus is het logisch dat beide sectoren hierin nauw samenwerken. In verschillende Europese landen is dit afgelopen jaren ook gebeurd.”

Is cybersecurity een exclusieve aangelegenheid van IT-afdelingen of moeten organisaties er ook op corporate niveau mee aan de slag?
“Het stimuleren van *awareness* is een van de beste manieren om digitale dreigingen beter te kunnen weerstaan. Zoals de publieke en private sector samenwerken, zo moet ook binnen organisaties verder worden gekeken dan de grenzen van de eigen afdeling. Cybersecurity is niet alleen het domein van IT-afdelingen en CIO’s. Ook CFO’s en CSO’s moeten betrokken worden bij het opstellen en uitvoeren van veiligheidsregels en -beleid. En natuurlijk het personeel op de werkvloer. Bij IT-gerelateerde zaken hebben organisaties al snel de neiging zich eerst te richten op technologie en processen en pas daarna op hun medewerkers. En juist die moeten intrinsiek gemotiveerd zijn om verantwoordelijk met bedrijfsinformatie om te gaan. Beveiligingsprocedures worden vaak als omslachtig en onnodig gezien, maar medewerkers zijn al snel overtuigd van het nut ervan als ze beseffen dat ook hún loonstrook op het bedrijfsnetwerk te vinden is.”

Wat kunnen beslissers in bedrijfsleven en bij de overheid doen om hun cybersecuritystrategie te verbeteren?
“Organisaties moeten zich afvragen hoe secure ze zouden móeten zijn, in plaats van hoe secure ze technisch kúnnen zijn. Bij cybersecurity draait alles om risicomanagement. Als je besluit om de beveiliging van data en netwerken als een managed service te outsourcen, zoek dan een provider met een holistische benadering die de business echt begrijpt. Een provider die risico’s realistisch in kaart brengt en je helpt vast te stellen waar de kroonjuwelen van je organisatie zich bevinden. Ga voor een onafhankelijke partij die zijn oplossing aanpast aan jouw probleem, in plaats van andersom.” •

‘Als je besluit om de beveiliging te outsourcen, zoek dan een provider met een holistische benadering die de business echt begrijpt’