Mels Deels is ICT-journalist en schrijft al meer dan 20 jaar over ontwikkelingen en trends in onze branche.

Reageren? *Mail naar mels.dees@imediate.nl*

Security-wappies

Channelveteraan Johan Pellicaan (onder meer ex-Seagate, nu Scale Computing) viel onlangs tijdens een presentatie over malware terug op de digitale aanval op de Deense rederij Maersk. Ransomware legde het bedrijf, inclusief dochterondernemingen zoals een terminal in Rotterdam, stil. De impact van die aanval was groot.

Het is opvallend dat Pellicaan een voorbeeld uit 2017 in herinnering moest roepen om het belang van cybersecurity duidelijk te maken. Goed, de leveringsproblemen bij Albert Heijn ('lege kaasschappen') en de digitale inbraak bij Universiteit Maastricht staan ook in ons geheugen gegrift, maar verder blijven veel incidenten onbekend. Vooral als de getroffen ondernemingen niet beursgenoteerd zijn. En al helemaal in het mkb-segment.

Niet onschendbaar

In eerste instantie lijkt dat logisch: een bedrijf hangt niet graag de vuile was buiten. Uit schaamte, of vanwege het imago richting klanten, medewerkers en leveranciers. Die angst is gegrond, blijkt uit onderzoek van Kaspersky. Zo geeft meer dan de helft (57%) van de bedrijven aan nooit te zullen samenwerken met een onderneming waar een datalek heeft plaatsgevonden. Die houding is bepaald naïef. Al lang maken securityspecialisten duidelijk dat het niet de vraag is óf een onderneming wordt aangevallen, maar is alleen het moment onbekend waaróp het gebeurt. De wapens van cybercriminelen zijn inmiddels zo sterk, dat alleen security-wappies menen dat de eigen onderneming onschendbaar is. Wie zich bovendien realiseert dat onverlaten zich vaak al lange tijd in systemen van ondernemingen, en hun partners in de supply chain, bevinden, dan wordt duidelijk dat je eigenlijk helemaal niet kunt weten of een zakenpartner niet al dagelijks 'data lekt'.

> **"Meer openheid over incidenten op het gebied van IT-security stelt hele ketens in staat weerbaarder te worden"**

Samen weerbaarder

Sommige dieren die in groepsverband leven, zoals stokstaartjes, waarschuwen elkaar bij dreigend gevaar. Meer openheid over incidenten op het gebied van IT-security zou eenzelfde effect hebben en stelt hele ketens juist in staat weerbaarder te worden. Een geslaagde cyberaanval is vervelend en kost tijd, geld en moeite. Maar het is niet iets om je voor te schamen. In tegendeel, wie na een incident zijn beveiliging versterkt en de security-awareness binnen de organisatie verhoogt, zou juist meer dan ooit een aantrekkelijke partner voor andere ondernemingen moeten zijn.