Column

Hardleers als altijd!

22 september 2020

Jean-Jacques Bistervels

Terugkijkend op de 'Apollo Vredestein' ransomware-casus, signaleerde het Financieel Dagblad (FD) recentelijk dat veel bedrijven de ICT-beveiliging niet op orde hebben.[1] Ik las dit artikel met een diepe zucht. Het bevestigde wederom wat ik allang vermoedde: in twintig jaar tijd is er in de *board of directors* van bedrijven niet veel veranderd! Focus op financiën, ja, maar ICT, data en beveiliging? Helaas.

Ik werk al een hele tijd in risk, compliance, audit, informatiebeveiliging. Maar toen ik na mijn studie met IT-auditing begon – destijds rond 2000 tijdens de internetbubbel (wie kent hem nog?) heette het nog EDP-auditing – was het niet anders. En de 'vertrouwde adviseurs' van die board, vaak accountants en 'internet visionairs', hadden er ook niets mee. Ja, enkele 'geeks': die paar accountants die destijds ook zo nodig 'RE' moesten worden, die wel natuurlijk. Werd je een 'RA RE' (snel omdraaien dan maar!). Maar het merendeel niet.

Tijden veranderen, zou je denken. In nog grotere mate dan rond 2000 is ICT in 2020 doorgedrongen in de kern van bedrijven. (Bijna) niks kan meer zonder. Hele bedrijfs- en verdienmodellen hangen af van de ICT. En toen COVID-19 dit jaar arriveerde, bleek het fileprobleem er ook mee op te lossen. Maar waarom zou je als board het onderwerp ICT-beveiliging anno 2020 belangrijk gaan vinden?

Ik heb afgelopen half jaar even geturfd: De universiteit van Maastricht trapte het jaar af met haar ransomware-incident. Daarna kwamen onderzoeksinstituut Wetsus, de University of California, postbedrijf Pitney Bowes (van eBay), Communications & Power Industries (CPI), accountantskantoor HLB Belgium, IT-dienstverleners Conduent en Cognizant, LG, softwarebedrijf Blackbaud, Garmin, onderzoeksbureau Nielsen, reisorganisatie CWT, Ruhr Universiteit Bochum, zorgverlener Regis, Canon… Het houdt niet op. Via mijn Linkedin heb ik ze allemaal gevolgd met likes: elke maand werd er meer dan één onderneming of instituut van naam getroffen door ransomware of malware. En lag de boel er plat. Forrester meldde dat zelfs 94 procent van de bedrijven afgelopen jaar is getroffen door een cyberaanval.[2] Big business, dus!

Ook verliepen alle incidenten in grote lijnen via het volgende stramien:

Eerst complete ontreddering: Alles ligt plat, systemen worden in paniek afgesloten. Data is weg, beschadigd, versleuteld. Waarom wij? Ons bedrijf was toch niet interessant genoeg? En de CISO had gemeld dat met het kleine, bescheiden budgetje (dat meestal dan werd beheerd door de directeur IT of CIO, als het er al was) het allemaal wel 'ok' was? Je zou eens anders hebben gerapporteerd, denk ik dan. Want meestal is dan niet het falend management de Kop van Jut.

Daarna complete radiostilte: Schaamte alom. De board wil niet dat de buitenwereld iets te weten komt. Liefst binnenskamers afhandelen en ontkennen. Maar helaas heb je klanten en journalisten, en die houden hun mond niet. En oh ja, dan ook nog die vervelende AVG: melden bij de toezichthouder! En eventueel ook nog je partners of – helemaal te gek voor woorden – je klanten.

Na een tijdje komt 'erkenning' en puinruimen: Tja, toch gehackt. Of 'malware'. Mogelijk 'ransomware'. En in dat laatste geval waren 'ze' al maanden actief in de systemen. Met datalek? Flinke kosten in ieder geval: het inhuren van een IT-beveiligingsbedrijf. Onderzoek doen, IT opnieuw opbouwen, 'assurance' verkrijgen. Vertrouwen herstellen. Beetje communiceren. Tonnen, soms miljoenen die er vervolgens tegenaan moeten om het allemaal op te ruimen en op te schonen. Oh, en eventueel nog wat losgeld. De criminelen moeten ook wat.

Ten slotte de 'evaluatie': Of kater? Men had toch altijd 'adequate beveiliging'? Bij klanten werd dit altijd zo benadrukt op beurzen en in 'meetings' (door de directeur nog wel die hier normaliter niet om maalde). De afdeling Communicatie is daar ook erg goed in. En de board en ook de commissarissen vertrouwden daarop. Want ze hadden voor die tijd andere en vooral ook veel leukere dingen te doen. En heb je natuurlijk om af te sluiten nog een interne zondebok nodig. Vaak de CISO of (de IT-auditor bij) Internal Audit. Slechts een enkeling maakt de publiceerbare *lessons learned* openbaar (Uni Maastricht, hulde!).

Kortom: je zou denken dat we inmiddels in 2020 ook in de board informatiebeveiliging en ICT (of *cyber*, wat je wil) hoog op de agenda hebben staan. Heeft het FD dan toch gelijk? Ik had als directielid toch hardop afgevraagd of we wisten wat we moesten doen. Of we onze data veilig konden herstellen, klantcommunicatie en verzekering op orde hadden, inclusief de voor de laatste geldende randvoorwaarden. En of we de gemaakte plannen al eens hadden geoefend. Maar nee, bij de boards lijkt het stil te blijven om dit soort risico's openlijk te bespreken. Totdat het mis gaat. Maar de cijfers liegen er niet om.

NOTEN

[1] FD: Hack bij Apollo Vredestein toont zwakke cyberbeveiliging Nederlandse bedrijven, 04-08-2020. https://fd.nl/ondernemen/1353014/hack-apollo-vredestein-legt-zwakke-cyberbeveiliging-bij-bedrijven-bloot?utm_source=nieuwsbrief&utm_campaign=fd-ochtendnieuwsbrief_#126;SYSTEM.CAMPAIGNID#126;_#126;SYSTEM.MAILID#126;&utm_medium=email&utm_content=20200804&s_cid=671, geraadpleegd op 31 augustus 2020

[2] Forrester: The rise of the business-aligned security executive, https://www.tenable.com/analyst-research/forrester-cyber-risk-report-2020, august 2020, geraadpleegd op 31

Ir. J.E. (Jean-Jacques) Bistervels RE CIA CCSA CRISC CDPSE CCP | informatiebeveiligingsmanager en privacyspecialist bij *Sanoma*

Jean-Jacques Bistervels is werkzaam als Informatiebeveiligingsmanager bij Sanoma. Daarnaast houdt hij zich bij Sanoma bezig met fraudebeheersings- en privacyvraagstukken. Na zijn studie Technische Bedrijfskunde aan de TUE is hij zijn carrière bij Ernst & Young gestart als IT-auditor. Hij heeft daarna ruim zeven jaar gewerkt binnen de farmaceutische sector en daarna ruim tien jaar in de financiële sector. Binnen NOREA is hij actief voor de kennisgroep Software Development en als redacteur voor de IT-auditor.