Security-awareness bedrijven niet hoog genoeg

Wet Meldplicht Datalekken in de praktijk

Op 1 januari 2016 is de Wet Meldplicht Datalekken van kracht geworden als onderdeel van de Wet Bescherming Persoonsgegevens. In het kort stelt deze wet dat iedere ondernemer in Nederland verantwoordelijk is voor de (privacygevoelige) data in zijn organisatie. Bij overtreding van de wet kan de ondernemer een boete tegemoet zien. Ruim een half jaar later kunnen we voor het eerst de balans opmaken. Want werkt deze wet in de praktijk zoals hij op papier bedoeld is? Wat zijn de gevolgen van deze wet voor de ondernemer? En welke adviezen kunnen ICT- en securityprofessionals geven voor een veilige online bedrijfsomgeving?

tekst Frank Kemeling en Roger de Jonge

Ondanks dat de meeste ondernemers op de hoogte zijn van de Wet Meldplicht Datalekken, is in de praktijk de security-awareness binnen bedrijven niet hoog genoeg. Dit leiden we af uit het grote aantal meldingen over een inbraak in een bedrijfsnetwerk dat wordt veroorzaakt door een medewerker die per ongeluk op een besmet bestand klikt of een e-mail opent met een virus, malware of ransomware. Hoewel de ICT'er binnen de organisatie op de hoogte is van alle risico's en bedreigingen, kan het bij elke willekeurige medewerker fout gaan.

SPELFOUTEN

Daarbij zijn e-mails vol spelfouten verleden tijd en zijn de websites waar de nietsvermoedende internetsurfer heen wordt geleid steeds geavanceerder. Met andere woorden, de wet voorziet weliswaar in de behoefte om gegevens te beschermen, maar om een bedrijf te beschermen tegen cybercriminaliteit én sancties, moeten directie en de ICT'er op de hoogte zijn van de risico's, beschermende technische maatregelen genomen hebben en moeten de medewerkers afdoende worden ingelicht. Naast het naar behoren inrichten van ICT-faciliteiten moet het personeel getraind worden en bewust worden gemaakt van wat er mis kan gaan, en hoe dit kan worden voorkomen. In dit bewustzijn en in het implementeren van maatregelen valt nog veel winst te behalen, onder andere door het (laten) uitvoeren van phishing-campagnes en het volgen van security-awareness-trainingen.

LANGE TERMIJN ICT-STRATEGIE

Dat het overtreden van de wet ook een technische oorzaak kan hebben, waar uiteindelijk de ondernemer zowel verantwoordelijk voor is als de dupe van is, blijkt uit het feit dat veel systemen gehackt kunnen worden wanneer verouderde of juist heel nieuwe systemen niet meer aansluiten op de systemen van bijvoorbeeld leveranciers. Hackers, van wie de technische capaciteiten de laatste jaren aanzienlijk zijn toegenomen, kunnen op relatief eenvoudige wijze misbruik van deze mismatch maken. Het laatste half jaar is er een toename merkbaar van deze vorm van cybercriminaliteit in het MKB, met name omdat deze groep vaak geen ICT-meerjarenplan heeft en met verouderde systemen werkt die niet ingericht zijn op een veranderende omgeving. Dat maakt het MKB tot een relatief gemakkelijke prooi.

ICT-STRATEGIE

Organisaties in het midden- en kleinbedrijf zouden zich meer bezig moeten houden met hun ICT-strategie; welke technologie komt eraan, hoe bereid je je daarop voor als organisatie, wat past er bij je bedrijf? Een ICT-strategie die aansluit op een bedrijfsstrategie en -doelstelling ontbreekt bij de meeste MKB-bedrijven en kan daar-

mee technische problemen in de hand werken, met alle gevolgen van dien. Een ICT-meerjarenplan kan een onbewuste overtreding van de Wet Meldplicht Datalekken voorkomen.

HERSTELLEN VAN DE SCHADE

Een ander gevolg van het proces waarin een datalek schade aanricht in een organisatie, is dat wanneer een hacker eenmaal een systeem is binnengedrongen en er mogelijk bedrijfsgegevens op straat liggen. De gemiddelde systeembeheerder die verantwoordelijk is voor de dagelijkse gang van zaken, is niet altijd in staat om dit verantwoord op te lossen. Er zijn goed getrainde professionals nodig om de schade die aangericht wordt bij een lek en leidt tot het stilleggen van de bedrijfsvoering te herstellen én om de organisatie zo snel mogelijk weer operationeel te krijgen. Daar verkijken veel bedrijven zich op. Men is zich bewust van de wetgeving en de gevaren maar ondernemers zijn slecht voorbereid op de consequenties op lange termijn. De wet legt bloot waarin ondernemers tekortschieten, namelijk de noodzaak om te blijven investeren in ICT-kennis.

WAKE-UP CALL

Online security is niet alleen een IT-aangelegenheid en begint met het inventariseren van de bedrijfsprocessen en gegevensstromen. Juist in het MKB moet er een strategisch ICT-plan zijn dat onderdeel is van de bedrijfsstrategie en dat deel uitmaakt van de operatie. Dit gaat verder dan alleen wachtwoordbeheer en zou zich moeten richten op een betere opzet en (her) inrichting en beveiliging van (cloud) data, werkpleksecurity, actieve netwerkmonitoring, endpoint protection, phishing-campagnes, awareness-trainingen en het zwaarder inzetten op training van de ICT'er en het inschakelen van externe hulp- en kennisbronnen. Intern moet er duidelijker worden gecommuniceerd wat er door wie is geregeld. Medewerkers weten vaak niet hoe online security door een IT-afdeling is geregeld en moeten beter worden geïnformeerd. Bovendien hebben verschillende bedrijven verschillende behoeftes; een advocatenkantoor met vijf werkplekken vraagt een andere aanpak dan een verkooporganisatie met vijf werkplekken.

Het MKB heeft een wake-up call nodig en zou samen met een managed services provider of online securityspecialist moeten zorgen voor beleid op maat. Door binnen een bedrijf de krachten op organisatorisch en technisch vlak te bundelen, kan veel leed voorkomen worden en kan de wet zijn werk doen waarvoor deze bedoeld is. Niet als klokkenluider voor wat er schort binnen een organisatie of voor het bestraffen van ondernemers die hun zaken niet op orde hebben, maar als beschermer van privacygevoelige bedrijfsgegevens.

Frank Kemeling is online beveiligingsspecialist en manager bij BrainSec cybersecurity en Roger de Jonge is manager bij BrainCare managed ICT-services provider