DATALEKKEN VOORKOMEN MET EEN GOEDE CYBERSTRATEGIE

Voorkom dat het beeld op zwart gaat

Werkt u als marketeer met persoonsgegevens, dan geeft de nieuwe Meldplicht Datalekken u extra verantwoordelijkheden. Zo zult u moeten nagaan of de IT-afdeling van uw bedrijf wel voldoende maatregelen heeft genomen om een hack het hoofd te kunnen bieden. Maar om dat te kunnen, is het goed als u zelf ook iets weet van de risico's.

Ongetwijfeld leest u het met meer dan gemiddelde interesse als bij een collegabedrijf een bestand met onversleutelde wachtwoorden is 'buitgemaakt'. Misschien wordt u dan overvallen door het gevoel 'daar doe je toch niets tegen'. Die gedachte is echter niet helemaal terecht, en vaak wordt deze ingegeven door een gebrek aan technische kennis.

Basiskennis

Is dit bij u ook het geval, probeert u dan snel enige basiskennis te verwerven. De recente hack (april 2015) van het Franse TV-station TV5 Monde toont duidelijk aan dat de impact van een incident groot kan zijn: het beeld stond anderhalve dag op zwart. Net als bij diefstal mag het motto 'het is niet de vraag of je gehackt wordt, maar wanneer' dan wel gelden; het is een must dat uw bedrijf een goede strategie heeft om goed voorbereid te zijn en de schade te kunnen beperken.

Kerntrekbeveiliging

Wat zijn de ingrediënten voor een goede cyberstrategie? De meeste mensen wapenen zich op zijn minst tegen woninginbraak door de woning op slot te doen bij vertrek. Nu dieven steeds vaker woningen binnen komen door simpelweg de cilinder uit het slot te trekken, schaffen meer mensen sloten aan met kerntrekbeveiliging. Een kleinere groep gaat nog verder en installeert een alarmsysteem, al dan niet met camera's. Dit laatste gebeurt overigens vaak pas nadat er ingebroken is.

Een continue drie-eenheid

Uiteraard houdt het niet op bij de implementatie van de gekozen oplossingen. De in dit artikel beschreven stappen vormen een continue drie-eenheid, zoals u in bijgaande grafiek kunt zien.

Afweging

Iedereen maakt een afweging tussen de kans op woninginbraak en de kosten die nodig zijn voor preventie. Dit is in feite ook de eerste stap bij het opzetten van een cyberstrategie. Inzicht in de bedreigingen voor uw databases met klantgegevens en de kwetsbaarheden daarvan, biedt de mogelijkheid om het risico van cyberaanvallen in te schatten. Het gewenste rendement op de investeringen die nodig zijn om deze risico's te verminderen, bepaalt vervolgens hoe hoog deze investeringen moeten zijn. Slechts weinig mensen zullen onmiddellijk alle sloten vervangen zodra ze horen dat dieven nieuwe technieken gebruiken om in te breken.

Moedwillig

Bij de inschatting van de kans op datalekken van uw kostbare gegevens, is het van belang om niet alleen te kijken naar bedreigingen van buitenaf. Ook bij cybersecurity spelen bedreigingen vanuit de eigen organisatie een grote rol. Medewerkers hebben immers makkelijker toegang tot vertrouwelijke gegevens dan personen van buitenaf; bij moedwillig misbruik speelt dat een belangrijke rol. U zult niet de eerste zijn die te maken krijgt met een medewerker op de afdeling die bij zijn ontslag de complete klantendatabase mee naar huis neemt op een usb-stick. Veel beveiligingsinci-

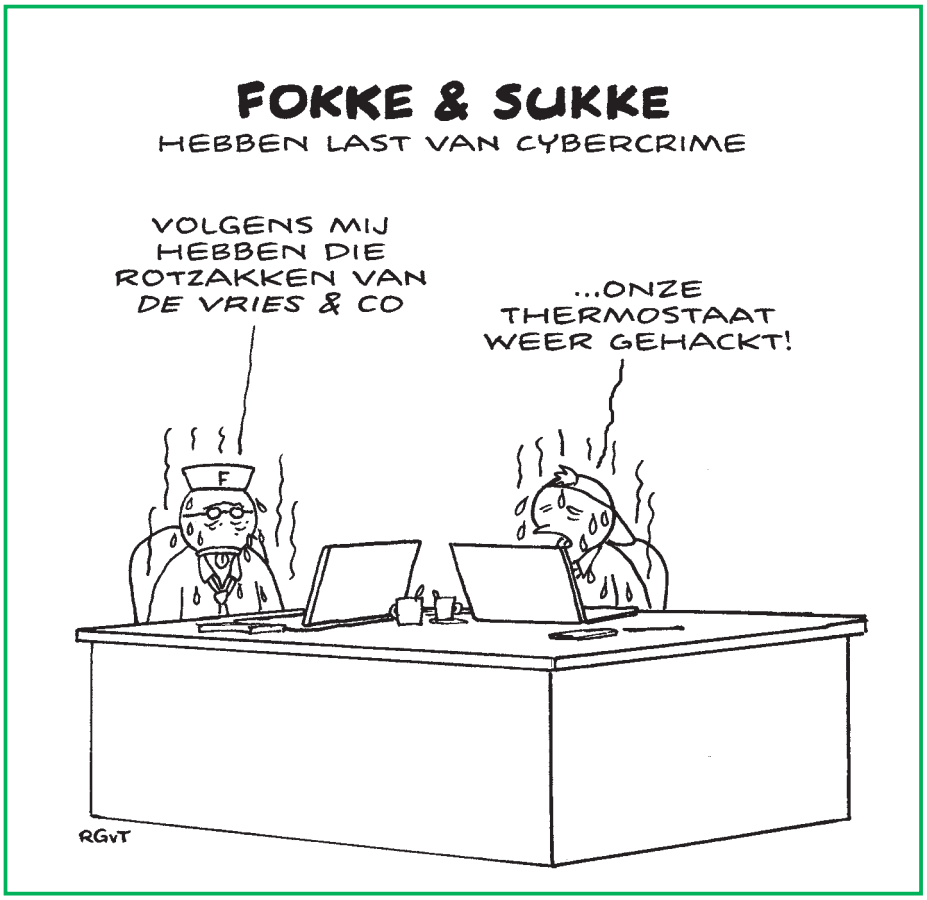
denten hebben echter hun oorsprong in gebrek aan bewustzijn: met alle lijntjes die tegenwoordig ook 'naar buiten' lopen, is het van belang dat uw collega's zich voldoende bewust zijn van de risico's die het werken met (gevoelige) bedrijfsinformatie met zich meebrengt. De ontvanger van een mail met vertrouwelijke informatie kan deze bijvoorbeeld doorsturen. Vaak staan zelfs IT-medewerkers er niet bij stil dat socialmediatools die ook veel in zakelijk verband gebruikt worden, zoals Yammer en Whatsapp, vrijwel alle gegevens van een telefoon (adresboek, foto's, films) kopiëren naar een eigen server en er geen inzicht in geven wat met die gegevens wordt gedaan.

Omvang

Tot slot is er natuurlijk ook nog wet- en regelgeving waaraan u moet voldoen. In de afweging van risico's en maatregelen moet uw bedrijf ook nog beantwoorden aan de actuele eisen op het gebied van privacy en bescherming van gevoelige bedrijfsgegevens.
Als de risico's bekend zijn, komen de oplossingen en maatregelen in beeld. Voordat u daar keuzes in kunt maken, moet u de nodige vragen beantwoorden over de mogelijke gevolgen van een cyberaanval of -fraude. Denk hierbij aan vragen over de omvang van een datalek, of aan de periode dat de bedrijfssystemen na een geslaagde aanval niet beschikbaar zullen zijn. Welke effecten kan dit hebben voor het imago en de financiële situatie van uw organisatie?

Veelomvattend

De risico's, de eisen van de organisatie én het beschikbare budget bepalen uiteindelijk welke technische oplossingen u kiest en op welke manier het bedrijf de procedurele aanpassingen invoert. De ketting is zo sterk als de zwakste schakel. Een cyberstrategie om datalekken te voorkomen, kan dus zo veelomvattend zijn dat deze de gehele organisatie raakt. De invoering ervan neemt daarom de nodige tijd in beslag en kan ook van diverse kanten op weerstand van medewerkers rekenen. Mensen raken immers per definitie bepaalde vrijheden kwijt.



Klok

Het personeelsbestand verandert, de technische mogelijkheden nemen toe, zowel van de daders als van de slachtoffers, en de motieven van de daders verschuiven eveneens. Zorg daarom dat u continu de risico's monitort en adequate maatregelen neemt.
In het verleden werd dit vaak op periodieke basis gedaan, bijvoorbeeld één keer per maand. Gezien de aard van de risico's en het feit dat de afhankelijkheid van IT zo groot is geworden, zal dit voor veel organisaties niet meer voldoende zijn. De klok rond bedrijfskritische middelen blijven monitoren, is voor steeds meer bedrijven een must.

> **"De klok rond blijven monitoren is bijna een must"**

Agenda

Als u afhankelijk bent van IT – en welke organisatie is dat niet tegenwoordig – zult u moeten nadenken over een cyberstrategie. De continuïteitsrisico's worden te groot! Zo'n strategie heeft invloed op de hele organisatie en gaat verder dan de implementatie van een tool. Houd de strategie bovendien regelmatig tegen het licht om te zorgen dat deze actueel blijft. Maar houd ook rekening met andere eisen, zoals efficiënte processen en kostenbewustzijn. Uw bedrijfsprocessen moeten daarom nieuwe ontwikkelingen omarmen, maar wel op een veilige manier.

Robert Heines is Principal Business Consultant Cyber Insurance bij CGI. Postbus 8566, 3009 AN Rotterdam, www.cginederland.nl, tel.: +31 (0)88 564 0000