#security

De ernst van cyberdreigingen neemt snel toe

Bestuurders moeten cyber-security-kloof dichten

De kloof tussen de bescherming van een traditionele cybersecurity-benadering en de cyberdreiging uit de praktijk wordt steeds groter, ook in Nederland. Dat vraagt om een andere en intensievere benadering van cybersecurity – vooral op boardroom-niveau.

Door **Eelco Stofbergen**, Thoughtleader Cybersecurity bij CGI Nederland.

ROTTERDAM – Digitale inbraken, DDoS-aanvallen, datalekken, phishing; er zullen weinig bedrijven meer zijn die niet bekend zijn met digitale dreigingen en geen maatregelen hebben genomen. De bescherming van informatiesystemen is onmisbaar en onontkoombaar in een zich sterk digitaliserende wereld. Cybersecurity is inmiddels een 'license to do business'. Een bedrijf beschikt immers over gegevens van klanten en partners, maar heeft ook steeds meer verantwoordelijkheden in een keten of netwerk. Andere organisaties en klanten rekenen erop dat uw bedrijf zijn verantwoordelijkheid neemt voor digitale veiligheid.

Standaardmaatregelen als een firewall, virus- en malwarebescherming, een goed wachtwoordenbeleid en versleutelde verbindingen – als ze al correct worden ingezet – zijn niet genoeg. Maar dat besef is nog lang niet overal doorgedrongen, blijkt uit recent internationaal onderzoek van CGI onder meer dan duizend beslissers. Die zien cybersecurity wel als een belangrijke trend – zowel vanuit IT- als vanuit zakelijk oogpunt. Nederlandse beslissers noemen cybersecurity zelfs de op één na belangrijkste trend (na de kostendruk), terwijl het wereldwijd de op vier na belangrijkste trend is. Maar diezelfde beslissers geven te weinig handen en voeten aan dat inzicht.

Ernst bedreigingen neemt toe

Waarom wordt het uitblijven van passende cybersecurity-maatregelen nu een steeds nijpender probleem? Het belang van een goede beveiliging neemt om een drietal redenen snel toe. Ten eerste is er een aantal innovaties gaande die een behoorlijke impact hebben op de digitale kwetsbaarheid. Met cloud computing komen veel gegevens buiten de bedrijfsmuren terecht. In het Internet of Things krijgt een snel groeiend aantal apparaten een verbinding met het internet. En voor big data worden nog meer verbindingen tussen gegevens aangelegd. Zo groeit het aantal nieuwe risico's exponentieel.

Daarnaast is er de reactie van overheden en toezichthouders op de groeiende cyberdreiging. De regelgeving rond de omgang met gegevens groeit, zowel op nationaal als op Europees niveau. Zo is sinds begin 2016 de meldplicht datalekken van kracht. Organisaties die te maken hebben met een ernstig datalek – het verlies van een USB-stick met klantengegevens is een voorbeeld – moeten dat melden aan de Autoriteit Persoonsgegevens, op straffe van een forse boete. Ook toezichthouders als De Nederlandse Bank en de Autoriteit Financiële Markten leggen een breed scala aan eisen op.

Maar de belangrijkste reden om cyberdreigingen meer aandacht te geven is het feit dat de ernst van die dreigingen zélf zo toeneemt. Het recente jaarverslag van de AIVD illustreert dat; de dreigingen komen overal vandaan en daarbij zijn zowel overheden als bedrijven doelwit. Volgens de AIVD was er in 2015 een recordaantal cyberspionage-aanvallen op Nederlandse overheidsinstellingen, maar hadden ook technologie- en nutsbedrijven en andere delen van de kenniseconomie daaronder te lijden. Aanvallers werken meer samen en worden helaas steeds vaker aangestuurd door de georganiseerde misdaad of door minder rechtschapen naties.

Ongefundeerd vertrouwen

Terug naar de resultaten van het onderzoek. Zeven op de tien Nederlandse beslissers blijken vertrouwen te hebben in de eigen mate van bescherming tegen cybercriminaliteit. Maar na enig doorvragen blijkt dat vertrouwen vaak niet terecht, als je uitgaat van het inzicht dat alleen een verdedigingslijn niet voldoende is. Welke bedrijfsmiddelen zijn er eigenlijk aantrekkelijk voor cybercriminelen? 43 procent van de Nederlandse organisaties en bedrijven heeft daar geen volledig overzicht van. En 45 procent beschikt niet over een goed responsplan om adequaat te reageren op een daadwerkelijk geslaagde inbraak of aanval. Er is dus kortom veel vertrouwen in de eigen cybersecurity-programma's, maar de benodigde maatregelen om echt beschermd te zijn tegen cybercriminaliteit ontbreken. Het is tijd dat organisaties op een aantal kritieke punten stappen gaan zetten.

Communicatieprobleem

Een fundamentele belemmering voor verbetering is het verschil van perceptie rond cybersecurity tussen de bestuurders en de lijnmanagers. De boardroom schat de cyberrisico's doorgaans lager in dan de lijnmanagers en heeft meer vertrouwen in de gebruikte bescherming tegen cyberaanvallen. Bestuurders hebben ook vaker privacy en gegevensbescherming als hun belangrijkste focus. In de praktijk is er bij cyberdreigingen vaak sprake van een technisch vraagstuk waar een strategisch geïnitieerde oplossing voor moet komen. Maar er is geen excuus voor het laten ontstaan van een communicatieprobleem hierover tussen bestuurders en werkvloer.

In een wat grotere organisatie kan een Chief Information Security Officer (CISO) zorgen voor de juiste beveiligingsaanpak. Maar die mag nooit de eigenaar van het probleem worden; het bestuur moet zich bewust zijn van het probleem, de verantwoordelijkheid nemen, de lijnen uitzetten en budget vrijmaken. En vooral het probleem goed snappen. Anderzijds moeten mensen aan de operationele kant van de organisatie begrijpen hoe ze moeten rapporteren richting bestuur, zodat men daar voldoende informatie heeft om die verantwoordelijkheid te kunnen nemen.

Plan van aanpak

Wat is nu in de praktijk de juiste aanpak? In ieder geval moet er een basisniveau aan beveiliging zijn ingericht, zowel aan de verdedigingskant – dus in de preventie – als aan de kant van monitoring en (insluip-) detectie. Dat moet 'business as usual' zijn, waarbij aanvallen gewoon worden gedetecteerd en afgehandeld. Daarnaast moet een organisatie afspraken maken over wat dan de situaties zijn die niet 'business as usual' zijn en hoe daarover moet worden gerapporteerd aan het management.
Een ander aandachtspunt is het daadwerkelijk kijken naar wat nu eigenlijk de kritieke assets zijn. Bedrijven hebben maar al te vaak niet goed geïnventariseerd wat ze aan waardevols te verliezen hebben. Dat kunnen recepturen van productieprocessen zijn, maar dat kunnen ook 'gewoon' klantgegevens zijn. Soms weten bestuurders wel hoe belangrijk die klantgegevens zijn, maar niet op welke plekken in hun systemen die zich allemaal bevinden.

Ook moeten organisaties die dat nog niet hebben gedaan een goed plan opstellen 'voor het geval dat'. Bijna de helft van de Nederlandse organisaties ontbeert een goed responsplan. Wat doe je bijvoorbeeld met je informatiesystemen als er meer aan de hand is dan een simpel af te weren aanval? Hoe hou je het in de gaten? Daar komen soms ook vaardigheden bij kijken die wellicht beter uitbesteed kunnen worden.

Ten slotte is het voor bestuurders een goede zaak om de financiële risico's van een (deels) geslaagde cyberaanval in kaart te brengen. Wat zijn de financiële gevolgen – direct en indirect – als bedrijfsactiviteiten in gevaar komen, intellectueel eigendom verloren gaat of de reputatie van het bedrijf een flinke knauw krijgt? Het is tegenwoordig goed mogelijk het bedrijf te wapenen tegen dergelijke risico's met een steeds populairder wordende verzekering tegen cybercriminaliteit. Maar dan moeten wel de juiste inventarisaties en responsplannen zijn opgesteld.

"Cybersecurity is een randvoorwaarde om succesvol zaken te doen"

Verantwoordelijkheid nemen

De toenemende innovatie, regulering en cyberdreiging vereisen dat organisaties hun digitale veiligheid versterken. Want cybersecurity is een randvoorwaarde om succesvol zaken te doen. Klanten en partners verwachten dat uw bedrijf opereert als een digitaal verantwoorde partij. Dat betekent voor bestuurders dat ze inzicht krijgen in wat hun organisatie te verliezen en dus te beschermen heeft, bewust hun cyberrisico's managen en de beveiligingsstrategie daarop afstemmen. Zodat de organisatie is staat is te groeien van een reactieve naar een proactieve cybersecurity-aanpak, die het verschil kan maken voor de business. En dat zal bestuurders als muziek in de oren klinken.