#secure!

Blijf weg van naming and shaming

Door **Jan Veldsink**, docent aan Nyenrode Business Universiteit waar hij Security and Cyber Risk doceert, een module binnen de Modulair Executive MBA in Business & IT

BREUKELEN - Steeds meer beroepscriminelen werken online. Dankzij eenvoudig te verkrijgen hacksoftware breken zij regelmatig in bij overheden en bedrijven. Het doel? Financieel gewin, datadiefstal of spionage. Het is daarom belangrijk dat organisaties zichzelf beter beschermen tegen digitale aanvallen.

Beroepscriminelen hoeven geen programmeur meer te zijn. Steeds vaker zijn het (internationale) misdaadsyndicaten die software of een dienst inkopen. Via malware worden deze programma's snel en goedkoop verspreid. De drempel is laag, de pakkans is bijna nihil. Het is moeilijk om de onderste steen boven te krijgen. Werkt een buitenlandse overheid mee om de vermeende hackers op te sporen, of is diezelfde overheid wellicht zelf de opdrachtgever? Het is daarom belangrijk om zelf de digitale dijken van de organisatie te bewaken.

Datalekken

De overheid heeft momenteel het meest te vrezen van het wegstromen van informatie. Lag in het verleden de nadruk op financiële zaken, nu draait het vooral om spionage. Hackers, regeringen en andere mogendheden willen een sterke informatiepositie om de publieke opinie te beïnvloeden. Denk daarbij aan nepnieuws verspreiden of misbruik maken van systemen. Gemeenten en ketenpartners van overheden zijn extra kwetsbaar. Zij hebben toegang tot allerlei landelijke informatie. Als een crimineel via een gemeente of lagere overheid binnenkomt, dringt hij wellicht direct de hele keten binnen.

> **"Zelfs meest ervaren IT-manager kan de mist in gaan met phishing"**

Chantage

Bedrijven hebben vooral last van diefstal gericht op financieel gewin. Denk aan diefstal van data om de eigen concurrentiepositie te verstevigen, maar ook aan het 'gijzelen' van computers. Ransomware is een programma waarmee iemand van buitenaf de computer of zelfs een heel systeem kan versleutelen. Daarmee wordt het onbruikbaar tot een bedrijf losgeld betaalt. Deze methode komt vrij vaak voor. Organisaties moeten zich vooraf bedenken: heb ik de juiste maatregelen getroffen? Is er een back-up? En stel dat je betaalt, kan je er dan van uitgaan dat het systeem daarna correct werkt? Een onzichtbare tegenstander biedt geen garantie.

Beveiliging

Organisaties moeten hun beveiliging goed op orde hebben. Zorg dat je systemen en beveiliging altijd up-to-date zijn. Wees daar proactief in. Bedenk ook waar je je cruciale gegevens opslaat. Waar is dat beveiligd? Wie kan daarbij? Denk daarom ook goed na over identity- en accessmanagement. Leg vast welke medewerkers toegang hebben tot welke informatie.

Zwakste schakel

De mens is altijd de zwakste schakel in cybersecurity. Criminelen gebruiken steeds vaker psychologische trucs om iemand te overtuigen om op een link te klikken of een spookfactuur te betalen. Iedereen is hier gevoelig voor, zelfs de meest ervaren IT-manager. We krijgen gemiddeld zestig tot tachtig spamsignalen per dag binnen, per e-mail, internet en telefoon. Hoe groot is dan de kans dat je per ongeluk eens op de verkeerde link klikt, waardoor malware wordt geïnstalleerd? Iedereen kent wel iemand die dat is overkomen. Daarom is het belangrijk dat de gehele organisatie doordrongen is van het belang van cybersecurity.

Bewustzijn

Wil je de veiligheid beter regelen, dan is het belangrijk om alle verdachte signalen en incidenten bespreekbaar te maken. Doe dat op het bewustzijnsniveau dat past bij iemands rol in de organisatie. Bespreek bij de financiële afdeling regelmatig signalen van spookfacturen. Vraag de schoonmaker of er onbekende mensen in het gebouw zijn geweest, want die kunnen fysiek een USB-stick in een van de computers hebben gestoken. Maar blijf weg van naming and shaming. Houd het bespreekbaar.

Strategie

Cybersecurity is niet alleen een onderwerp voor de IT-afdeling, maar ook voor de boardroom. Welke strategie zet je in? Moeten medewerkers eigenlijk nog wel per e-mail met elkaar communiceren of gaat de organisatie toe naar peer2peer-communicatie? Zorg dat cybersecurity altijd op de agenda staat van je organisatie. Zo houd je elkaar scherp.

#secure!

Vijf voorwaarden voor informatiebeveiliging tijdens digitale transformatie

Cybersecurity nauw verweven met digitale DNA

Door **Eelco Stofbergen**, thought leader Cybersecurity bij CGI

ROTTERDAM - Het grote succes van technologiegedreven bedrijven zoals Uber, Airbnb en dichter bij huis Coolblue dwingt andere organisaties om ook versneld te digitaliseren. Deze digitale transformatie vergroot het belang van ict binnen deze organisaties en daarmee ook het belang van cybersecurity. Vernieuwing van de informatiebeveiliging is hiervoor nodig. Vijf voorwaarden voor succesvolle cybersecurity in tijden van digitale transformatie.

Door digitalisering ontstaan nieuwe businessmodellen en vanuit het niets verschijnen nieuwe toetreders op de markt waardoor de concurrentie verhevigt. Klanten verwachten betere services die flexibel inspelen op hun wensen. Ondertussen verschuift digitale technologie van een technische oplossing naar de kern van het businessmodel. De digitale transformatie verhoogt de verandersnelheid van organisaties, maar de praktijk toont dat cybersecurity daar vaak niet in meegaat. Cybersecurity wordt binnen organisaties veelal als te statisch ervaren, een keurslijf dat verandering belemmert. Daardoor verliezen cybersecurityafdelingen de aansluiting en ontstaat het gevaar dat nieuwe diensten de juiste beveiliging ontberen.

Toenemende complexiteit

De uitdagingen van digitale transformaties worden versterkt door externe ontwikkelingen. Zo is er sprake van innovatie, waarbij nieuwe technologie steeds sneller wordt ingezet in organisaties. De ontwikkelingen gaan gepaard met toenemende connectiviteit en slimmere apparatuur en dit brengt beveiligingsuitdagingen met zich mee. Immers, slimmere apparatuur bevat sneller kwetsbaarheden en connectiviteit leidt tot blootstelling aan aanvallers.

Daarnaast neemt de wet- en regelgeving rond cybersecurity toe door de groeiende afhankelijkheid van informatie. Bijvoorbeeld de Wet bescherming persoonsgegevens (inclusief meldplicht datalekken), de Europese privacyrichtlijn (GDPR) en de aankomende meldplicht voor vitale sectoren. Maar ook vanuit branches zelf worden eisen gesteld.

Tot slot groeien de digitale dreigingen. Met de toenemende waarde en afhankelijkheid van gedigitaliseerde systemen neemt ook de belangstelling van kwaadwillenden toe. Cybercrime (bijvoorbeeld ransomware en phishing), digitale spionage en systeemverstoring (zoals een DDoS-aanval) vormen hier de belangrijkste risico's. Deze externe ontwikkelingen verhogen het belang van goede informatiebeveiliging, maar vergroten tegelijkertijd de complexiteit.

Voorwaarden

Organisaties worden geconfronteerd met uitdagingen rondom cybersecurity. Om deze uitdagingen het hoofd te bieden, moet cybersecurity binnen organisaties zich ontwikkelen. CGI ziet vijf voorwaarden voor adequate cybersecurity in tijden van digitale transformatie.

1 Sluit aan op doelen

Informatiebeveiliging moet een enabler zijn voor de organisatie en dus moet de beveiligingsaanpak in lijn zijn met de organisatiedoelstellingen. Daarbij moeten de te treffen maatregelen risicogebaseerd en passend zijn.

2 Speel in op omgeving

De snelle veranderingen door externe invloeden en interne behoeften maken dat informatiebeveiliging snel op de veranderingen moet kunnen reageren. Dat vereist continu risicomanagement, een lerende organisatie en het inspelen op risico's en kansen van technologische vernieuwing.

3 Blijf in control

De toenemende wet- en regelgeving en de hogere eisen die zowel de eigen organisatie als klanten stellen aan informatiebeveiliging, maken het noodzakelijk bewijsbaar 'in control' te zijn. Dat vereist de borging van de juiste beveiligingsmaatregelen, inzicht in de staat van informatiebeveiliging en rapportages daarover naar stakeholders.

4 Gebruik je verstand

Informatiebeveiliging moet nadrukkelijker kennis- en informatiegestuurd gaan werken. Dat betreft niet alleen kennis van het vakgebied en nieuwe ontwikkelingen, maar ook up-to-date inzicht in de eigen omgeving (situational awareness) en actuele informatie over dreigingen (threat intelligence) waarmee detectie wordt gevoed.

5 Zoek verbinding met partners

In de hedendaagse wereld kan geen enkele organisatie de informatiebeveiliging geïsoleerd aanpakken. Optimale informatiebeveiliging betekent dat moet worden gewerkt in verbinding met partners (intern en extern) in het digitale ecosysteem. Daarbij is het delen van kennis en informatie een randvoorwaarde.

Digitale DNA

De digitaliserende maatschappij maakt de digitale transformatie van organisaties onvermijdelijk. Maar diezelfde maatschappij verwacht van organisaties dat zij zorgvuldig met informatie omgaan. Cybersecurity zal daarom ook een transformatie moeten ondergaan, zodat wordt voldaan aan de voorwaarden voor succesvolle cybersecurity en security onderdeel wordt van het digitale organisatie-DNA.