Beveiliging 3.0

Beveiliging is van oudsher voornamelijk reactief en loopt vaak achter nieuwe zakelijke trends en technologieën aan. Security 3.0 moet hierin verandering brengen. Gartner-specialist Anthony Allan gaf hierover tekst en uitleg tijdens een rondetafelbijeenkomst. De nieuwe benadering van risico's heeft duidelijk niet de pretentie een antwoord te bieden op alle knelpunten binnen het securitybeleid, maar kan wel helpen bij het bepalen van de strategie. tekst Hotze Zijlstra fotografie Mark Nieuwenhuizen

Anthony Allan schetste aan het begin van zijn presentatie in de Amsterdamse Rembrandt Toren het beeld dat de meesten van ons zo onderhand wel kennen: de hoeveelheid (online) aanvallen neemt toe. Bovendien steken kraakpogingen slimmer in elkaar en worden ze niet langer ondernomen voor de kick, maar voor puur financieel gewin. Het woord cybercrime zegt het al: het is het domein geworden van de georganiseerde misdaad.
Allan: "Een bijkomende uitdaging is dat technologieën zoals ERP- en productiesystemen in toenemende mate aan internet gekoppeld worden. Omdat ze hier oorspronkelijk niet voor ontworpen zijn, kan dit nieuwe zwakke plekken opleveren."
De Gartner-man, uitgenodigd door rondetafelgastheer IBM, noemde verder de consumerization als risicovergrotende factor. "Het gebruik van mobiele privéapparaten, widgets en web 2.0 maakt organisaties kwetsbaarder." Toch moeten bedrijven hier een oplossing voor bedenken, willen ze althans een aantrekkelijke werkgever blijven voor de nieuwe generatie medewerkers.

SECURITY-NIEUWE-STIJL

Volgens Allan is het belangrijk dat beveiliging bij nieuwe producten of software standaard ingebakken wordt. "Zo niet, blijf je achter de feiten aan lopen." Wat hem betreft is het tijd voor security 3.0: "Security 1.0 was de strakke controle die de mensen in het datacenter hadden over het mainframe. Versie 2.0 is het ad-hocbeleid ten aanzien van virussen, identiteitsdiefstal en andere vormen van inbreuk – een dure manier van beveiliging omdat er telkens nieuwe gaten moeten worden gedicht. Bij Security 3.0 wordt er proactief opgetreden en is de beveiliging goeddeels geïntegreerd binnen het proces of de technologie."
Een ander onderdeel van security 'nieuwe stijl' is de implementatie van een risk & control assessment, een proces waarbij door middel van communicatie tussen de betrokkenen binnen de organisatie een risico- en beveiligingsbeleid op maat wordt opgesteld voor alle medewerkers en hun taken. Veel energie zou volgens de deskundige gestopt moeten worden in het trainen en het verhogen van de bewustwording bij de medewerkers.
Verder gloort er volgens Allan licht aan het einde van de tunnel. "Door de opkomst van gemanagede diensten zal een groot deel van de security worden gewaarborgd door de provider."

> "ER IS GEEN CORRELATIE TUSSEN INVESTERINGEN EN VEILIGHEID"

KOSTEN

Security wordt hierdoor meer en meer commodity en zal wellicht minder zwaar drukken op het IT-budget. Allan: "Je kunt de informatie binnen de organisatie niet beveiligen door alleen grote hoeveelheden geld aan security uit te geven. Er bestaat dan ook geen enkele correlatie tussen het aan beveiliging bestede geld en de daadwerkelijke veiligheid. Het verdient in veel gevallen de aanbeveling om er juist minder aan uit te geven, maar er meer bewust mee om te gaan."
Een punt dat dan ook nadrukkelijk ter tafel komt, is de cost effectiveness. In sommige gevallen, bijvoorbeeld bij dataverlies, kan het goedkoper zijn om dit eens in de zoveel tijd te laten gebeuren in plaats van voor veel geld alle risico's af te dekken. Een afweging die je volgens Anthony Allan kunt meenemen binnen het besproken risk assessment. Voor elke organisatie gelden namelijk andere uitgangspunten.
"Voorheen waren deze erg mathematisch van aard; er kwamen waarden uitrollen waar je eigenlijk weinig aan had. De trend gaat nu naar meer kwalitatieve modellen, waarin nog steeds is opgenomen wat je waaraan uitgeeft, maar die een realistischer beeld geven van de echte risico's."

WERKVLOER

"We hebben het nu vooral over de kantooromgeving. Maar hoe zit het met de beveiliging van de IT op de productie- of winkelvloer?", vraagt Arthur Govaert, general manager IT & IM Engineering Shell. "Personeel loopt er rond met laptops,