Bestaande combinaties van beveiligingsproducten pakken probleem niet in de kern aan

Beveiliging netwerken is warboel

Voor het beveiligen van netwerken zijn maar weinig goede producten op de markt. De klanten zijn aan zet, zeggen **Maarten Oosterink** en **Leon Teheux**. Zij moeten investeren in innovatieve oplossingen in plaats van het in hapklare brokken naar binnen schuiven van halve oplossingen. Een compact, leesbaar manifest zou daarbij kunnen helpen.

ILLUSTRATIE: COMIC HOUSE/CLIFFHANGER

Ondanks het toenemende aantal berichten in de media over verloren bedrijfsgegevens blijkt dat het informatiebeveiligingsbeleid bij veel bedrijven vooral gericht is op dreigingen van buitenaf. Dit is opvallend, aangezien de dreigingen al lange tijd niet alleen maar van buitenaf komen: de afgelopen tijd is het aantal interne incidenten drastisch toegenomen. Er hoeft niet altijd sprake te zijn van opzet. Dankzij de complexiteit van hedendaagse besturingssystemen en applicaties ontwikkelen criminelen continu nieuwe en verbeterde vormen van malware (de verzamelnaam voor kwaadaardige software als virussen, trojans en spyware), die de computer van de werknemer als springplank gebruikt voor illegale activiteiten. Dit soort software trekt zich bijzonder weinig aan van traditionele maatregelen om ongewenste entiteiten buiten de deur te houden. Maatregelen zoals portiers, toegangspoortjes of sociale controle hebben geen vat op wat zich afspeelt binnen de digitale wereld.

Marktpartijen hebben elkaar in de houdgreep

Bestaande maatregelen die wel enigszins effectief zijn, baseren zich veelal op verouderde principes. Virusscanners en andere oplossingen die ons tegen malware moeten beschermen, vertrouwen bijna volledig op herkenning van digitale handtekeningen. Niet alleen is dit een reactief proces, dat dus per definitie achter de feiten aanloopt, ook het aantal handtekeningen is tot problematische hoeveelheden gestegen.
Als antwoord op de groter wordende dreigingen bieden leveranciers op het gebied van netwerken, besturingssystemen en virusbestrijding in toenemende mate oplossingen aan die de middelen van gebruikers aan een inspectie onderwerpen alvorens ze toegang tot het netwerk te verlenen. Zo levert Microsoft in de komende versie van Windows mogelijkheden om een computer eerst aan een gezondheidscontrole te onderwerpen, alvorens toegang tot het netwerk te bieden.
Hier is wel sprake van een kat die zijn eigen staart achterna zit. Het zijn immers dezelfde fabrikanten die ons recentelijk een VPN-oplossing verkochten, die nu een gapend gat in de firewall schieten. Naar analogie met de fysieke wereld hebben we ons eerst een bewaker laten aansmeren, om vervolgens dezelfde partij te vragen een tunnel te graven om zo, zonder lastige vragen, bij de schatkamer te kunnen komen.

Als we kijken naar de combinatie van beveiligingsproducten die we in hedendaagse netwerken tegenkomen, moeten we vaststellen dat het een slecht beheersbare brei van oplossingen is die zich vooral rond de periferie beweegt en het probleem niet in de kern weet aan te pakken. Die kern is namelijk het hart van een organisatie en dus datgene waarvoor al deze beveiliging in de eerste plaats noodzakelijk was: de informatie.
Dat er een probleem is waar nog geen bruikbare oplossingen voor zijn, is geen nieuws. Organisaties als Boeing, Proctor & Gamble en Rolls-Royce realiseren zich dit al enige tijd. Mede door oprichting van het Jericho Forum proberen ze naar een oplossing toe te werken. Met behulp van een elftal geboden (zie Automatisering Gids van 2 november 2007) wordt een ideaalbeeld geschetst hoe bedrijven waardevolle informatie zouden moeten beschermen.
Dit is een mooi uitgangspunt, maar hoewel leveranciers zich snel aansloten bij deze en soortgelijke groeperingen en lovende woorden spraken over wat er mogelijk zou worden in de nabije toekomst, is er tot op heden nog maar weinig concreets op de markt. Wat dat betreft bracht de beurs Infosecurity 2007, begin november in de Jaarbeurs Utrecht, vooral meer van hetzelfde uit de hoek van de leveranciers. Dit ondanks de duidelijk aantrekkende behoefte aan informatiebeveiliging en de bereidheid om hier geld aan uit te geven.

Een mogelijke verklaring hiervoor is de houdgreep waarin de betrokken marktpartijen elkaar houden. Denk aan de recente initiatieven van Microsoft op het gebied van antivirus, die de nodige discussie opleverde tussen allerlei mogelijke betrokkenen. Hieronder ook enkele gevestigde allianties op beveiligingsgebied, zoals de Trusted Computing Group en Microsofts SecureIT-alliantie. Dit zorgt ervoor dat innovatie bemoeilijkt wordt.
Een alternatieve verklaring zou kunnen zijn dat afnemers en integrators zich te veel laten leiden door het aanbod. Het is tegenwoordig vanzelfsprekend dat leveranciers in seminars of workshops aan klanten uitleggen welke problemen deze klanten hebben en hoe hun product of dienst dit kan oplossen. Een duidelijke vorm van 'technology-push' in plaats van 'market pull'.
De controle over wat er moet gaan gebeuren, ligt echter nog steeds bij de vragende partij. Als we al van oude principes en uitgangspunten willen uitgaan, dan maar van het principe van vraag en aanbod. De klant is aan zet om aan te geven welke problemen daadwerkelijk oplossingen behoeven en welke bereidheid er is tot investeren. Het wordt tijd dat men gaat investeren in innovatieve oplossingen voor de daadwerkelijke problemen in plaats van het in hapklare brokken naar binnen schuiven van halve oplossingen.
Een nuttige exercitie voor menig organisatie zou daarbij het formuleren van een informatiebeveiligingsbeleid kunnen zijn. Niet een honderden pagina's tellend document verstopt op een intranetsite, maar een compact, leesbaar en begrijpelijk manifest waarin beschreven staat welke informatie van waarde is voor de organisatie en welke zorgvuldigheid van eenieder verwacht wordt in de omgang. De vertaling van een dergelijk beleid naar technische oplossingen zal

Er is niet altijd sprake van opzet

menigeen versteld doen staan over hoe weinig effectief hedendaagse oplossingen eigenlijk zijn.
Wellicht is dit een goed moment om de rollen om te draaien en leveranciers uit te nodigen om met oplossingen te komen, in plaats van problemen. Een organisatie die zich positief wil onderscheiden bij de bescherming van waardevolle informatie zal bereid moeten zijn om te investeren in innovatieve oplossingen op basis van helder geformuleerde eigen behoeften. Deze durf om te pionieren zou weleens gunstig gewaardeerd kunnen worden door de eigen achterban. Bescherming van persoonlijke gegevens is immers een groot goed voor de hedendaagse consument.

Maarten Oosterink (maarten.oosterink@capgemini.com) en Leon Teheux (leon.teheux@capgemini.com) zijn beiden als consultant werkzaam bij Capgemini Nederland. Binnen de practice Architecture Governance & Infrastructure richten zij zich vooral op Identity Management en Security.

➲ Voor reacties en nieuwe bijdragen van deskundigen: Henk Ester (h.ester@sdu.nl, (070) 378 03 97).

OPLOSSINGEN

Malwarebestrijders

Aanbieders van software die malware moeten bestrijden hebben de afgelopen jaren een werkveldverbreding gehad van het eindpunt (de computer van de gebruiker) naar de rand van het netwerk. Oplossingen worden hierbij veelal als halffabrikaat ingezet, bijvoorbeeld op firewalls, security appliances en mailservers. Het probleem waar deze aanbieders mee kampen, is dat tot op heden alleen herkenning van malware op basis van digitale handtekeningen echt effectief is. Andere vormen van detectie van kwaadaardige acties ondervinden hinder van de fundamentele beveiligingsopbouw van hedendaagse besturingssystemen. Dit laatste is ook meteen het bestaansrecht van malwareaanbieders, wat het lastig voor hen maakt om met innovatieve oplossingen te komen. Een voorbeeld hiervan is dat er oplossingen voor smartphones geboden worden, maar de hoeveelheid malware kan de investering in een dergelijke oplossing moeizaam rechtvaardigen.

Netwerkleveranciers

De grote netwerkspelers bieden oplossingen om 'eigen' computers toe te staan op het netwerk en onbekende computers te weren of aan een inspectie te onderwerpen. Vrijwel alle oplossingen ondersteunen 802.1x, een industriestandaard voor authenticatie. Dit zegt niets over de 'gezondheid' van de computer en omdat het lastig is om alle computers binnen een modern netwerk te ondersteunen, wordt vaak van gebruik ervan afgezien. Cisco timmert al jaren aan de weg met zijn Network Admission Control (NAC) waarmee de gezondheid en veiligheid van clientsystemen vastgesteld kan worden. Bedrijven als HP en Juniper bieden vergelijkbare oplossingen.

Jericho Forum

Het Jericho Forum van de Open Group houdt zich bezig met het onderzoeken en ontwerpen van standaarden die het delen van informatie aanzienlijk moeten vergemakkelijken, waardoor bedrijven in de gelegenheid worden gesteld flexibeler en gemakkelijker samen te werken. Een eerste resultaat is het concept van 'de-perimeterization', waarmee grenzen om het netwerk worden vervangen door een systeem waarin de data zichzelf uiteindelijk moeten beschermen. Het voordeel is dat de transparantie en de mogelijkheden sterk toenemen. Kant-en-klare oplossingen conform deze ideeën zijn er nog niet, hooguit oplossingen voor een klein facet. Het concept wordt uitgedragen en ontwikkeld door organisaties als BP, Boeing, Microsoft en Capgemini.

Liberty Alliance

De Liberty Alliance heeft zich ten doel gesteld om te werken aan een alom verbonden wereld waarbij bedrijven, burgers en overheid eenvoudig kunnen communiceren, gebruikmakend van open standaarden. De privacy en vertrouwelijkheid van informatie moeten hierbij gewaarborgd blijven. Een van de peilers waarop deze alliantie bouwt, is het gebruik van federatie, een model waarbij entiteiten onderling verbonden zijn en waarmee zij een vertrouwensband kunnen opbouwen. Een goed voorbeeld hiervan is DigiD, het systeem dat door de overheid wordt gebruikt voor toegang tot overheidssystemen. Deelnemers zijn organisaties als Sun Microsystems, IBM, Novell, maar ook bedrijven als Boeing, Paypal en Mitsubishi.

Microsoft

Zoals het een grote aanbieder van ICT-oplossingen betaamt, maakt ook Microsoft deel uit van diverse bewegingen en allianties op het gebied van informatiebeveiliging. Begin dit jaar kondigden de Liberty Alliance en Microsoft aan samen te gaan werken. Microsoft is ook van de partij op bijeenkomsten van het Jericho Forum en werkt samen met Cisco waar het Cisco's NAC-initiatief betreft. Zelf heeft Microsoft zijn ideeën op dit gebied samengevat in Forefront, dat oplossingen biedt voor clients, servers en de rand van het netwerk. Het protocol Network Access Protection (NAP) is hier een voorbeeld van. Dit protocol verschaft, net als NAC, toegang tot het netwerk indien de gezondheid van de desbetreffende pc voldoende is.