



Trends in security

Nieuwe techniek, nieuwe uitdagingen

Security is één van de meest zichtbare en relevante onderdelen van IT. Gevraagd naar de impact van een service-oriented architecture, virtualisatie of Web 2.0 moeten directieleden het antwoord vaak schuldig blijven. Wanneer er echter wordt gesproken over datalekken of het verliezen van intellectuele eigendommen, is de aandacht snel getrokken. *Kim Loohuis*

De IT-beveiligingssector lijkt vooralsnog niet onder de gevolgen van de economische malaise gebukt te gaan. Volgens Watchguard-CEO Joe Wang is dat logisch. "Bedrijven kunnen niet snijden in hun securitybudget vanwege de risico's die ze vervolgens lopen." Deze sector groeit als eerste en er wordt pas als laatste op bezuinigd. Dat wil niet zeggen dat de economie helemaal geen vat op security heeft. "Als de economie goed was geweest, was de sector harder gegroeid," aldus Wang.

Additionalen beveiliging

Wang ziet dat bedrijven steeds meer verschillende technologieën gebruiken, waardoor de noodzaak voor additionele beveiliging stijgt. "Door het gebruik van onder meer Skype en sociale netwerken worden er deuren geopend voor bedreigingen van buitenaf," aldus Wang. "De beveiliging hiervan vormt een uitdaging voor leveranciers. Het overgrote

merendeel is bijvoorbeeld nog niet in staat om VoIP-beveiliging te leveren." Dat onderschrijft ook Jonathan Penn, analist bij Forrester Research. Hij ziet bedrijven focussen op vier zaken: het beschermen van data, het stroomlijnen van kostbare of arbeidsintensieve taken, het zorgen voor beveiliging voor een zich steeds verder ontwikkelende IT-infrastructuur en het zowel begrijpen als beheren van IT-risico's binnen een groot enterprise-framework. "De belangrijkste kwestie van security is het beschermen van data, niet het weren van bedreigingen of het voldoen aan reguleringen. Steeds meer bedrijven realiseren zich dat het beschermen van het netwerk of de IT-infrastructuur alleen niet genoeg is om de onderneming te beschermen."

End-point-security

Op het gebied van datasecurity is eindpuntbeveiliging van groot belang. "Tot nu toe bleef de beveiliging van notebooks

en smartphones eigenlijk een beetje achter," zegt Patrick Dalvinck, general manager Benelux bij Trend Micro. "Veel bedrijven beschikken over een klassieke antivirusoplossing, maar daar houdt het wel mee op. Het eindpunt is één van de belangrijkste punten die beveiligd moet worden, zowel tegen potentiële inbraken als het infecteren van de systemen, waardoor het later kan worden gebruikt voor allerlei kwalijke doeleinden. Ook moet het zo beveiligd worden dat vertrouwelijke data het bedrijf niet kunnen verlaten via usb-stick, e-mail of instant messaging, zonder dat het aan de beveiligde voordeur wordt gecontroleerd." Veel bedrijven hebben inderdaad zo'n goed beveiligde gateway. Dat is echter verre van voldoende wanneer medewerkers met mobiele apparaten data van het systeem kunnen halen om vervolgens op een andere plaats verbinding te maken met het internet en zo de data zouden kunnen verspreiden. "Meerlagige beveiliging op verschillende systemen is waar het om draait," aldus Dalvinck. "Waar bedrijven naartoe moeten is dat ze een opeenstapeling van securitycomponenten op ieder eindpunt moeten hebben. Dat moet goed te beheren zijn en goed geïntegreerd." Dat is op zich niet moeilijk realiseerbaar.

Toch maken veel bedrijven het zichzelf onnodig moeilijk door verschillende oplossingen te kiezen voor verschillende eindpunten van verschillende leveranciers, omdat het op dat moment het goedkoopst is of het beste uitkomt. Het aanschaffen van security voor eindpunten wordt veelal ad hoc gedaan, waardoor integratie vervolgens lastig wordt, om van beheer nog maar te zwijgen. "Als je honderden end-points hebt, wordt het al gauw onoverzichtelijk. Wij raden klanten altijd aan een geïntegreerde suite te kopen met centraal management, zodat de verschillende componenten samenwerken en op elkaar afgestemd zijn," zegt Dalvinck.

Malwareoplossingen

Een bijkomende complexiteit is de hoeveelheid malware op internet. Hierdoor hebben antimalwareoplossingen steeds meer resources nodig. Dalvinck: "Twintig jaar geleden, bij de oprichting van Trend Micro, telden we nog geen tweeduizend nieuwe malwares in het eerste jaar. In 2006 waren dat er al 600 duizend. Afgelopen maand hebben we 1.053.000 nieuwe stukken malware gemeten, in één maand!" Deze explosieve groei heeft vooral te maken met het feit dat criminelen internet hebben ontdekt als manier om goed en snel geld te verdienen.

"Er wordt grof geld verdiend met het schrijven en distribueren van malware. Dat is een gigantische uitdaging voor de antimalware-industrie," zegt Dalvinck. Voor systeembeheerders betekent dit dat ze vrijwel continu zouden moeten bezig zijn met het updaten van hun systemen – en niet alleen de eindpunten, maar ook de servers en alle andere systemen die onder hun beheer vallen. Daar waar ooit één update per week volstond, is er nu sprake van een update per twee uur. "Dat betekent dat je vandaag de dag op elk moment een additioneel risico hebt van drie- à vierduizend nieuwe malwares die je niet kunt afvangen. Dat is het *window of vulnerability*." Bijkomend probleem is dat de antimalwarepakketten steeds

zwaarder worden en meer resources vragen. Dalvinck schat dat er dit jaar zo'n vijftien miljoen nieuwe stukken malware worden gedetecteerd, die in de herkenningssystemen van de antimalwaresoftware moet komen. "De slechte eigenschap van die software is dat het die herkenningssystemen in zijn geheugen moet laden om real-time te kunnen scannen. Het gevolg is dat de produc-

Positief gevolg van uitbesteding aan de cloud is dat de belasting van de lokale systemen enorm wordt verminderd.

De door Trend Micro gebruikte technologie is gebaseerd op reputation-databases. In het datacenter staan drie verschillende reputation-databases waarvan alle klanten gebruikmaken. Het gaat om een mail-, een web- en een file-reputation-database. "In de mail-

Meerlagige beveiliging op verschillende systemen is waar het om draait

ten meer geheugen en cpu-power gaan gebruiken, waardoor weer zwaardere systemen nodig zijn of de levensduur van een systeem wordt ingekort omdat er een stuk capaciteit wordt besteed aan het bestrijden van malware."

In de cloud

Een mogelijke oplossing voor de vele kwaadwillige software ligt in de cloud. Volgens Jonathan Penn van Forrester groeit de vraag naar beveiliging in een SaaS-model. "De vraag naar managed security services komt niet alleen van kleine organisaties die geen security-expertise in huis hebben en qua budget op de kleintjes moeten letten, maar ook van grote enterprises die zo groot, gefragmenteerd en complex zijn dat managed security de enige redelijke oplossing is."

Volgens hem profiteren alle ondernemingen van kostenbesparingen en verminderde complexiteit wanneer ze kiezen voor een SaaS-oplossing.

Ook Trend Micro heeft die ontwikkeling gezien en startte vier jaar geleden met de ontwikkeling van een cloud client-systeem. Dalvinck: "Van alle verwerking die op de individuele systemen van de klanten afgewerkt moet worden, zorgen wij ervoor dat minimaal 85 procent van alle checks en scans op onze systemen in ons datacenter gebeurt."

reputation-database hebben we een verzameling van ip-adressen van waaruit ooit spam is verstuurd. Wanneer er naar één van onze klanten een e-mail voorbij komt die afkomstig is van een ons bekende spammer, wordt de mail niet doorgestuurd naar de klant."

Tegenwoordig bevatten e-mails niet zo vaak meer geïnfecteerde bestanden, maar wordt de lezer door een link in het mailtje verleid een website te bezoeken waar hij vervolgens wordt geïnfecteerd. De web-reputation-database analyseert alle url's die in e-mails zitten verborgen. Wanneer een url uitkomt op een website met malware, wordt vervolgens vanuit de security-labs gekeken welke malware dit is. De url krijgt vervolgens een slechte reputatie, waardoor een volgende mail met een dergelijke link kan worden afgevangen. Slechte bouwstenen van files op de geïnfecteerde systemen worden toegevoegd aan de file-reputation-database.

"In de praktijk betekent dat wanneer een klant een webpagina wil bezoeken en hij de url intikt, er niet alleen een aanvraag naar internet wordt verzonden, maar parallel een aanvraag naar de reputation-database. Indien blijkt dat de pagina op dat moment een slechte reputatie heeft, kan die pagina niet worden bezocht." Doordat de systemen continu worden ge-update, hebben

de klanten ook altijd de meest actuele informatie, zonder zelf op lokale systemen updates te hebben uitgevoerd. "Er zal altijd sprake blijven van een window of vulnerability, maar doordat het cloud-systeem continu wordt ge-update, wordt dat risico verkleind," zegt Dalvinck.

Zorgwekkende trends

Andere trends op securitygebied noodzaken systeembeheerders en ondernemingen hun visie op beveiliging te herzien, betoogt Penn. "De netwerk-omgeving valt uiteen. Het huidige bedrijfsnetwerk in de vorm zoals we die nu kennen, sterft uit door initiatieven rondom externe toegang, mobiliteit en Software-as-a-Service. Organisaties laten steeds meer partners op hun netwerk, terwijl medewerkers meer gebruikmaken van mobiliteit. Daarnaast heeft de organisatie niet altijd meer vat op de apparatuur waarmee gebruikers het bedrijfsnetwerk op gaan. Het lokale bedrijfsnetwerk wordt minder relevant wanneer organisaties voor SaaS-oplossingen of services in de cloud kiezen. Door die ontwikkeling moeten IT-afdelingen een nieuwe omgeving zien te creëren rondom applicaties en security." Ook Penn waarschuwt voor de enorme toename aan malware. Traditionele beveiligingsmanieren zoals url-filtering en antivirus op de gateway zijn niet meer toereikend. Het benutten van kwetsbaarheden op legitieme websites, phishing-aanvallen gecombineerd met *drive-by* downloads en aanvallen via sociale netwerken dwingen bedrijven ertoe real-time webcontent te analyseren. "Het gaat niet meer om wel of geen toegang tot Facebook, MySpace of Google, maar het gaat erom te weten welke content er op de pagina's staat die medewerkers bezoeken," aldus Penn. Tot slot waarschuwt hij voor virtualisatie. "Dat ontwricht beveiligingsmodellen." Virtualisatie is in opmars, mede doordat het de mogelijkheid biedt datacenterbeheer te stroomlijnen en efficiënter gebruik te maken van computerkracht. De gesprekken die er nu worden gevoerd over de beveiliging

in een gevirtualiseerde wereld, gaan voornamelijk over de beveiliging van de hypervisor (virtualisatielaag) en het beheer en de integriteit van VM images. "Maar door virtualisatie moeten organisaties hun security opnieuw onder de loep nemen. Ip-adressen en netwerksegmenten waren voorheen de grenzen van de beveiliging, maar nu er omgevingen zijn waar verschillende virtuele

machines op één fysieke machine kunnen draaien, is er geen sprake meer van zulke duidelijk gedefinieerde grenzen." Ook Patrick Dalvinck houdt op dat vlak zijn hart vast. "Bij fysieke servers was een geïnfecteerd systeem te isoleren. Bij virtualisatie draaien er misschien wel vijftien systemen op die ene fysieke server. Malware kan via de hypervisor makkelijker verspreid worden." Daarnaast waarschuwt hij voor een overload op de fysieke machine. "Wanneer er een scan op een fysiek apparaat wordt uitgevoerd, wendt die machine alle resources aan om dat proces zo snel mogelijk achter de rug te hebben. De virtuele machines vechten tegelijk om die resources, wat kan leiden tot een enorme overload op de fysieke machine."

Data-leakage

Hoewel de afgelopen maanden geen nieuwe gevallen de media hebben gehaald, kennen we allemaal het verhaal van officier van justitie Tonino, wiens computer bij het vuilnis werd aangetroffen met daarop honderden pagina's vertrouwelijke documenten. Een ander bekend geval is dat van de medewerker van de inlichtingendienst die twee diskettes met daarop vertrouwelijke informatie in een leaseauto liet liggen. Zoals eerder al werd geconstateerd door Forrester-analist Penn, gaat

het in toenemende mate om de bescherming van bedrijfsgegevens. Uit zijn onderzoek blijkt dat veel organisaties zich in toenemende mate zorgen maken over data-leakage, maar dat ze voornamelijk de kat uit de boom kijken. "Data leak-preventie (DLP) is een technologie die erop gericht is de gevoeligheid van data binnen een bedrijf in te schatten en daarnaast bijhoudt waar medewer-

Het huidige bedrijfsnetwerk in de vorm zoals we dat nu kennen sterft uit

kers deze data opslaan of naartoe zenden. Het gros van de bedrijven maakt zich zorgen over de beveiliging van hun data en houdt de ontwikkeling van DLP nauwgezet in de gaten, maar het wordt nog weinig daadwerkelijk ingezet." Volgens de Forrester-analist zou DLP moeten zorgdragen voor vier fundamentele behoeftes: het signaleren en classificeren van gevoelige data; het opstellen van beleid en regels voor verschillende data-buckets; regulering via middelen als blokkeren en encryptie; en auditing en incidentrapportages. "Data leak-preventie zal geen technologie op zichzelf blijven zoals nu het geval is," zegt Penn. "DLP zal met andere technologieën integreren in drie fases. De eerste fase, waarin we momenteel zitten, behelst het verbreden van DLP-mogelijkheden om naadloze beveiliging in te sluiten van data in beweging (DIM), data in gebruik (DIU) en data in rust (DAR). De tweede fase, die nu start, focust op het integreren van DLP met andere beveiligingsoplossingen, zoals encryptietechnologieën. De derde en laatste fase van DLP-integratie, die over een jaar of vijf volwassen zal zijn, zal DLP integreren in informatie- en contentmanagement." Zowel Dalvinck als Penn onderstreept de noodzaak om vertrouwelijke data te beschermen en de blik te richten op integratie in de toekomst. «