Netwerkbeveiliging groeit veel bedrijven boven het hoofd

Veiligheidsrisico's steeds groter

LAURENS VAN AGGELEN

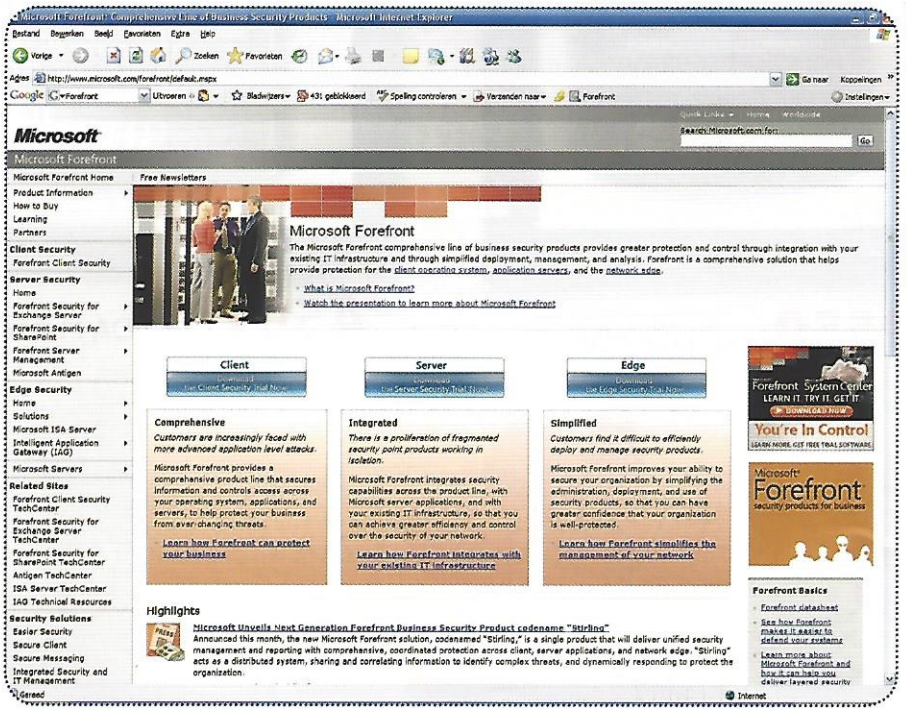
Hoe belangrijk een bedrijfsnetwerk is, wordt pijnlijk duidelijk wanneer er iets misgaat. De kans daardoor getroffen te worden, neemt steeds verder toe. Enerzijds doordat netwerken vaker en op meer manieren ook van buiten de bedrijfsmuren te benaderen zijn. Anderzijds doordat cybercriminaliteit lucratiever wordt. Met name kleinere bedrijven zien inmiddels door de bomen het bos niet meer, waardoor oplossingen vaak te laat worden ingezet en zij een gemakkelijke prooi zijn.

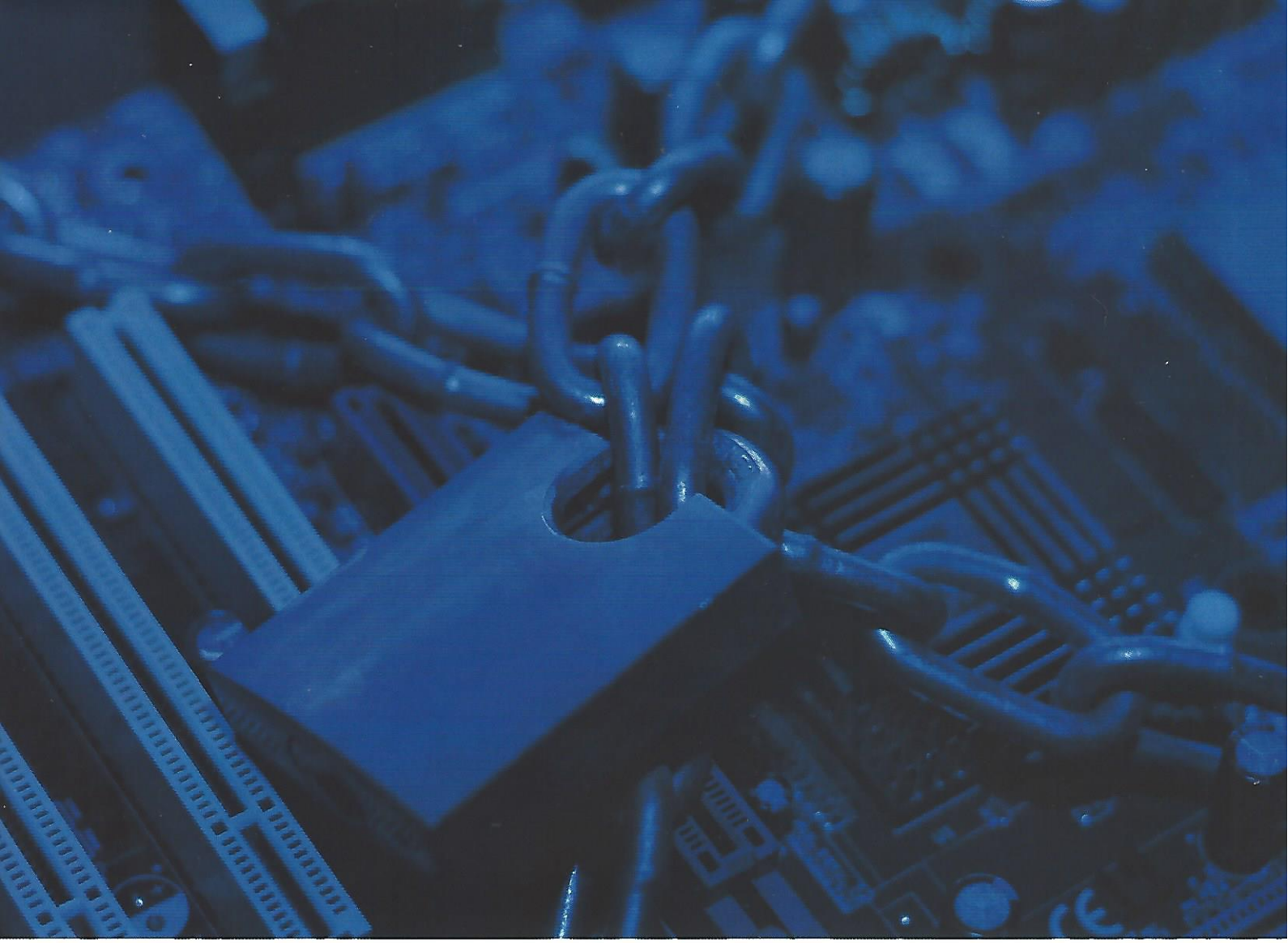
Bij de Infotheek Groep in Leiden, leverancier van hardware en ICT-diensten, weten ze er alles van. "We zien vooral aan de onderkant van het MKB nog heel veel misgaan. Met name doordat men in dit marktsegment de laatste jaren volop gebruik is gaan maken van internet en e-mail en men zich er tegelijkertijd niet van bewust is hoe afhankelijk men daarvan is geworden", vertelt directeur Duco van Leenen. "We zien dat kleinere bedrijven vaak nog slecht beveiligd zijn tegen het toenemende aantal virussen en andere bedreigingen. Bij grotere organisaties hoef je het belang van goede beveiligingssoftware niet meer uit te leggen, al zien we daar ook nog wel eens wat misgaan. Bijvoorbeeld doordat niet tijdig is voorzien in updates van deze software." Gaat het netwerk plat en raakt men data kwijt, dan blijkt ook vaak dat men niet op de juiste manier backups heeft gemaakt. "Pas bij het restoren blijkt dan vaak dat er iets mis is. Omdat het zelden of nooit wordt uitgetest, zoals eigenlijk zou moeten, komt dit kwaad pas aan het licht als het te laat is."

Uitbesteden

Bedrijven zouden zich volgens Van Leenen meer bewust moeten zijn van de slechte beveiliging van hun netwerken. "Zeker nu het alleen maar complexer wordt met de toename van e-mailverkeer, thuiswerken, VPN's en draadloze mobiele oplossingen. Hierdoor zie je dat de netwerken van veel bedrijven zo lek als een mandje zijn."

Van Leenen ontkent niet dat op afstand werken zo zijn voordelen kan hebben, maar is wel van mening dat je eerst een goede kosten-batenanalyse moet maken alvorens personeel uit te rusten met mobiele apparaten zoals notebooks, smartphones en PDA's. "Er wordt vaak te weinig gekeken naar wat het daadwerkelijk opbrengt en of personeel daarmee wel echt productiever wordt. Intussen investeert men er wel





in en worden vaak onnodige risico's genomen waardoor data en apparatuur gemakkelijk in verkeerde handen terecht kan komen." Bedrijven die zelf de kennis niet in huis hebben om voor een goede beveiliging van het bedrijfsnetwerk te zorgen, zouden er goed aan doen dit uit te besteden aan specialisten. "Het is zo ingewikkeld geworden dat we zelf al moeite hebben om alle ontwikkelingen bij te houden. Voor resellers is hier dan ook een mooie taak weggelegd. We zien overigens ook dat steeds meer bedrijven deze taken uitbesteden, omdat men het zelf niet meer aan kan en men zich liever op de corebusiness wil richten", aldus Van Leenen.

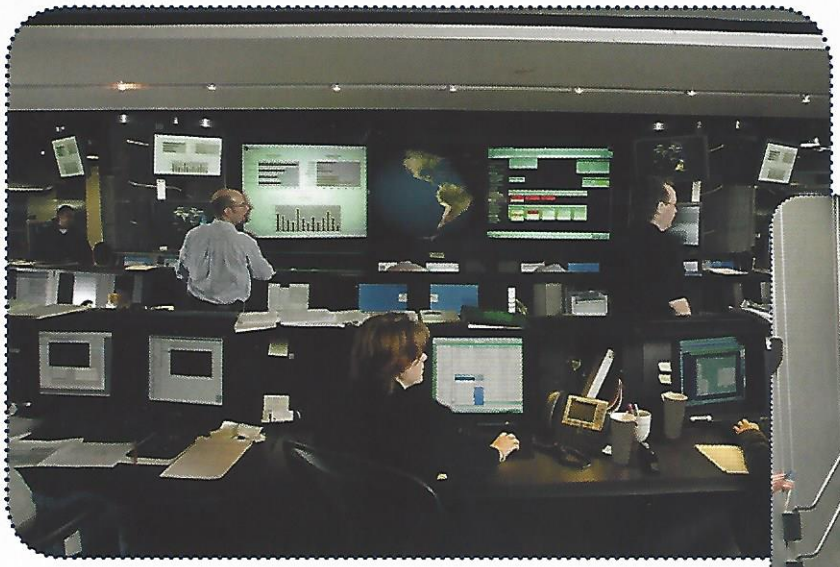
Microsoft Forefront

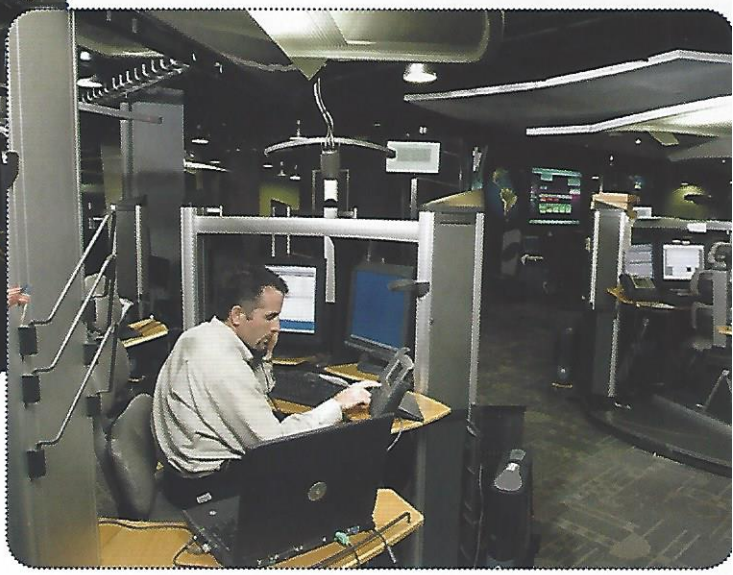
Resellers die op zoek zijn naar een mooie beveiligingsoplossing kunnen kiezen voor het onlangs geïntroduceerde Forefront van Microsoft. "De producten in deze serie bieden security-oplossingen op client-, server-, en edge niveau", schetst Bernard van der Feen, Product Solutions Manager van Forefront van Microsoft Nederland. "Ze zijn ontwikkeld om bedrijven bescherming te bieden tegen de voortdurende stroom aan nieuwe bedreigingen die op hen afkomt. Forefront zorgt voor een veilige toegang tot applicaties en data en zorgt er voor dat het beveiligingsbeheer eenvoudiger wordt."
Microsoft's CEO Steve Ballmer - die speciaal voor deze introductie naar Nederland kwam om meer gewicht in de schaal te leggen - sprak in zijn keynotespeech over de sterke toename van het aantal geavanceerdere veiligheidsbedreigingen. Ballmer: "Microsoft Forefront en Microsoft System Center zijn ontworpen om te voorzien in de toenemende behoefte van onze klanten aan veelomvattende en geïntegreerde beveiligingstechnologie die ze eenvoudig kunnen beheren en ze de beschikking geeft over

Microsoft System Center is een complete familie van oplossingen voor het end-to-end beheer van IT-infrastructuren, waarbij veel nadruk is gelegd op eenvoud, pro-activiteit en efficiency. De System Center-oplossingen verzamelen informatie over de infrastructuur, beleidsregels, processen en 'best practices', waarmee de IT-afdeling in staat is om beter beheerde systemen te bouwen en tal van processen te automatiseren. Zo kunnen organisaties de IT-kosten terugbrengen, de beschikbaarheid van bedrijfsapplicaties verhogen en de dienstverlening aan klanten verbeteren.

Controle

"Met Forefront kunnen we concurreren met een breed scala aan producten die het de gebruiker gemakkelijker maken om allerlei cruciale veiligheidsaspecten eenvoudiger te overzien. Bijvoorbeeld om te controleren of de firewall wel aanstaat en of patches wel gedraaid zijn", gaat Van der Feen verder. Toegang tot applicaties is hierdoor alleen mogelijk na een gedegen identificatie van de gebruikte pc en er wordt gekeken naar de locatie en het tijdstip waarop data of applicaties benaderd worden. "Maar ook wordt gecheckt of de computer die verbinding probeert te maken, zelf wel van adequate beveiligingssoftware is voorzien zodat deze geen bedreiging kan vormen voor alle andere op het netwerk aangesloten systemen." Forefront kan overigens geïntegreerd worden met Microsoft Exchange en de systeembeheerder wordt voorzien van uitgebreide rapportages, zodat kan worden toegezien op mogelijke verdachte acties die plaatsvinden op het netwerk.
"Voor resellers die gespecialiseerd zijn in security hebben we een speciaal partnerprogramma waarmee we hen in staat stellen hun klanten beter van dienst te zijn. Daarbij werken we met trainingen en is er een certificeringprogramma waaraan kan worden





Vanuit het Symantec Security Operations Center wordt gewaakt over nieuwe bedreigingen.

Toegangscontrole

Wie krijgt er toegang tot het netwerk en vanaf welke locatie? Ook bij ProActive Defense van ProCurve Networking draait alles om toegangscontrole. Binnen deze in april vernieuwde productlijn bevinden zich oplossingen als de nieuwe ProCurve Network Immunity Manager. Het gaat hier om een beveiligingsapplicatie die netwerkbedreigingen intelligent detecteert, afslaat en beheert, teneinde problemen zoals virus-aanvallen te voorkomen. "De wijze waarop deze software werkt, laat zich goed vergelijken met de douanecontrole op vliegvelden. Daarbij gaat het er niet alleen om wie je bent, maar ook hoe je je gedraagt en wat je bij je hebt", zegt Ton Serné, Country Manager ProCurve Networking, de netwerktak van HP. "Bij iemand die zich toegang wil verschaffen tot een netwerk is het niet anders. De verbeterde Identity Driven Manager baseert zich op gebruiker, apparaat, locatie, tijd en status van het client-systeem. Daarbij worden profielen vastgelegd en aangepast en wordt voortdurend gekeken of er niet op een verdachte manier van dit profiel wordt afgeweken. Hierbij valt te denken aan een gebruiker die zich vanaf een niet daarvoor geautoriseerde pc toegang probeert te verschaffen, of opvallend vaak pogingen doet om bij bepaalde data te komen. Zeker wanneer hij daar geen toestemming voor heeft of wanneer dit om allerlei andere redenen vraagtekens oproept."

In het derde kwartaal van dit jaar brengt ProCurve de versie 2.2 uit van de ProCurve Identity Driven Manager (IDM). Deze zal als gratis update aan klanten van IDM 2.0 worden aangeboden. IDM 2.2 werkt nauw samen met de nieuwe Network Access Controller 800 en biedt daardoor endpoint-integriteit op een eenvoudiger manier.

Intrusion-detection

De ProCurve Network Immunity Manager is een plug-in voor ProCurve Manager Plus 2.2 en detecteert en beantwoordt automatisch netwerkbedreigingen. Door informatie uit meerdere bronnen - zoals beveiligingsapplicaties van derden en ProCurve netwerkapparatuur - te analyseren, biedt deze oplossing bescherming tegen zero-day-aanvallen en bekende virusaanvallen op zowel bekabelde als draadloze netwerken. De Immunity Manager biedt ook uitgebreide rapportages om bedrijven te assisteren bij naleving van wet- en regelgeving.

"Door Network Immunity Manager aan ProCurve's ProActive Defense-portfolio toe te voegen, biedt ProCurve een beter inzicht in de gevaren die op het LAN rondgaan dan met in-line intrusion-detection apparatuur mogelijk is", aldus Serné. "Doordat Network Immunity Manager die gevaren op poortniveau bestrijdt, vormt dit een aantrekkelijke beveiligingsstrategie voor bedrijven."

ProCurve maakte enige tijd geleden ook bekend dat Fortinet, aanbieder van netwerkbeveiligingsproducten, is toegetreden tot de ProCurve Alliance. Deze alliantie verzorgt formele interoperabiliteitstesten en certificatieprogramma's, die uitgebreide en gekwalificeerde oplossingen opleveren voor resellers en klanten wereldwijd. De combinatie van Fortinet's FortiGate multi-threat beveiligingsapplicaties en de ProCurve Network Immunity Manager vormt een universele architectuur voor netwerkbeveiliging, waarmee de gebruikers hun netwerkbeveiliging kunnen

NAADLOZE INTEGRATIE

Naadloze integratie met het bestaande bedrade netwerk is waar veel bedrijven die steeds meer werken met draadloze oplossingen naar op zoek zijn. Niet-geïntegreerde draadloze LAN-systemen vormen een aanzienlijk probleem voor IT-beheerders die belast zijn met het beheer en de beveiliging van die netwerken. Het is immers van essentieel belang om zowel vaste als draadloze netwerken centraal te beheren om de totale eigendomskosten laag te houden en een netwerk betrouwbaar te laten draaien.

Met de Summit Wireless Mobility-producten van Extreme Networks kunnen IT-beheerders (via een enkele console) consistente beveiligings- en beheersmaatregelen doorvoeren in het gehele vaste en draadloze netwerk. De switches uit de Summit WM-reeks kunnen in combinatie met Altitude 350-2-toegangspunten een eenvoudig te beheren, veilige en schaalbare WLAN-oplossing bieden voor spraak-, video- en datatoepassingen.

De Summit WM-producten omvatten de Summit WM200- en Summit WM2000-switches. Voor kleinere installaties ondersteunt de Summit WM200 in de basisconfiguratie tot 50 toegangspunten, met de mogelijkheid de ondersteuning uit te breiden tot 100 toegangspunten. De WM2000-switch is schaalbaar en biedt ondersteuning voor grote WLAN-installaties met een capaciteit van wel 200 toegangspunten per controller.