Groeiend aantal risico's vraagt om beveiliging

Safety first!

Dat we met z'n allen steeds afhankelijker worden van computers en mobiele apparatuur, betekent ook dat we het ons niet kunnen permitteren dreigende gevaren te onderschatten. Spam en virusaanvallen kunnen grote schade toebrengen.

Maar liefst 56 procent van de kleine en middelgrote bedrijven in enkele Europese landen en de VS is de afgelopen twaalf maanden slachtoffer geweest van een virusaanval. Dat blijkt uit onderzoek van Trend Micro, leider op het gebied van netwerkantivirus- en content-beveiligingssoftware. De meeste bedrijven waren in staat om de daaruit voortvloeiende problemen zelf op te lossen. Wel had men er gemiddeld een dag voor nodig om het netwerk weer werkend te krijgen. Hoewel bedrijven zich in toenemende mate bewust zijn van de gevaren die zij lopen, beschikken zij veelal niet over de tijd, middelen en mensen om hun netwerken te beschermen. De kosten en implementatie van de software zijn de belangrijkste drempels bij de aanschaf van een nieuw product. Slechts 77,5 procent van de MKB-bedrijven zou volgens het onderzoek een beveiligingsbeleid hebben om virussen, spam, hackers en ongewenste toegang tegen te gaan. Dat betekent dat bijna een kwart van alle bedrijven nu en dan flink schade oploopt door steeds agressiever wordende bedreigingen.

Dilip Timal: "We benaderen de markt pro-actief."

Compleet

Trend Micro was een van de eerste aanbieders van antivirussoftware voor pda's. Deze is nog altijd gratis te downloaden van de website. "Op dit moment zijn we aan het onderzoeken of we dergelijke software ook voor smartphones op de markt zullen brengen. Misschien is het daarvoor nog wat vroeg maar we streven er voortdurend naar om de markt pro-actief te benaderen", aldus Dilip Timal van Trend Micro Nederland. Eerder dit jaar introduceerde het bedrijf een compleet beveiligingspakket voor het MKB. Met de nieuwe Client Server Suite, Client Server Messaging Suite, InterScan VirusWall en NeaTSuite speelt Trend Micro in op de specifieke behoeften van vereenvoudigd beheer van desktop, server, gateway en beveiliging van Microsoft Exchange-mail. Timal: "Kleine en middelgrote bedrijven lopen net als grotere organisaties de kans op bedreigingen, bijvoorbeeld de MSBlast- en Sobig-F-wormen. Deze bedrijven zijn echter niet altijd voldoende ingericht om te kunnen omgaan met deze snel opererende virussen."

Een belangrijke aanbieder van geïntegreerde security-oplossingen is Symantec. Een succesvol product in die categorie is de Gateway Security 5400. Hiermee is de gebruiker verzekerd van bescherming tegen geraffineerde gecombineerde aanvallen zoals Blaster, Slammer en Sobig. "We zien dat het steeds belangrijker wordt om het toenemende aantal blended threats tegen te gaan", vertelt Steven Heyde van Symantec. "We willen de gebruiker vooral niet onnodig schrik aanjagen maar blended threats worden steeds gevaarlijker." Dit is een worm die gebruik maakt van gecombineerde aanvalstechnieken. Dat gebeurt doordat de worm kans ziet om misbruik te maken van programmeerfouten in software. Om een dergelijke worm buiten de deur te houden, is het verstandig om Windows, Outlook (Express) en bijvoorbeeld de Internet Explorer van Microsoft regelmatig te updaten. "Een blended threat laat eveneens zien dat de complexiteit van de bedreigingen toeneemt en deze zich steeds sneller weten te verspreiden."

Omdat zelfs een optimaal geüpdate systeem nooit in staat is om alle nieuwe gevaren meteen tegen te houden, moet de nieuwe generatie security-software ook in staat zijn om nieuwe gevaren beter te herkennen.

Brightmail

Was de Symantec Gateway Security 5400 bedoeld voor bedrijven met 25- tot 50 medewerkers. Inmiddels is er ook de Gateway Security 300, een wat minder uitgebreide variant. Deze serie is ideaal voor kleine bedrijven en combineert een uitgebreide beveiliging, een betrouwbare internetgateway en een optie voor een veilige draadloze LAN in één oplossing. De appliance bevat de allernieuwste inspectiefirewall, veilige IPsec VPN-verbinding, inbraakdetectie, inbraakbeveiliging en statische contentfiltering. Als het gaat om anti-spamsoftware, heeft Symantec inmiddels nieuwe troeven in handen gekregen. Eind mei werd namelijk Brightmail overgenomen, één van de grootste leveranciers van anti-spam technologie. Uit deze veelbelovende kruisbestuiving is een fraai nieuw product voortgekomen: Symantec Brightmail Anti-Spam 6.0.

Peer-to-peer

"Spam is op dit moment voor veel gebruikers een groeiend probleem aan het worden", vertelt Jan Leeflang van Aladdin Benelux. "Het is belangrijk om spam maar ook allerlei aanvallen en bedreigingen in een zo vroeg mogelijk stadium tegen te houden, liefst op gateway- en niet op desktopniveau. Met onze software proberen we bovendien ook alle nog onbekende gevaren tegen te gaan. Bij veel antivirussoftware zie je vaak dat er nog te veel gevaar schuilt in de tijd tussen twee updates. De software is te weinig pro-actief ingesteld om deze onbekende aanvallen in de tussentijd op adequate wijze te onderscheppen."

Andere gevaren schuilen volgens Leeflang

in het toenemende gebruik van peer-to-peer applicaties voor het uitwisselen van bestanden (Kazaa, Gnutella, eDonkey), maar ook door het gebruik van instant messengers (MSN, ICQ) lopen gebruikers risico.
Met de introductie van eSafe versie 4 Feature Release 2 (FR2), moeten gebruikers afdoende beveiligd zijn tegen deze relatief gevaarlijke applicaties, alsook tegen nog onbekende virussen. Naast bescherming tegen virussen en wormen, houdt eSafe ook het HTTP- en FTP-verkeer vrij van kwaadaardige codes, zonder hierbij de prestaties van het netwerk negatief te beïnvloeden. Een volledig overzicht van de eSafe4 FR2-features is te vinden op www.eSafe.com.

Norman SandBox

Een techniek die ook listig omgaat met nog onbekende gevaren is de Norman SandBox. Deze technologie wordt toegepast in Norman's antivirussofware. Hierbij worden alle gescande toepassingen uitgevoerd in een gesimuleerde computeromgeving waarbij onbekende gevaren worden gedetecteerd. Norman SandBox reageert op veel verschillende, vooraf gedefinieerde scenario's en merkt ze aan als 'beveiligingsrisico's'. Ze worden niet geïdentificeerd als virussen, maar als malware. Dankzij de simulatie van netwerken en verbeterde detectie van geavanceerde Win32-wormen kunnen onbekende wormen worden gedetecteerd voordat iemand ze ook maar heeft gezien. Op die manier vindt beveiliging plaats in een veel vroeger stadium dan voorheen.

Ook Microsoft staat niet stil als het gaat om het beter beveiligen van computers. Met het uitbrengen van Service Pack 2 voor Windows XP zal er op dit gebied het nodige verbeterd zijn. Ook ten aanzien van spam doet Microsoft het nodige (www.microsoft.com/spam). "De komende twaalf maanden zullen we enkele belangrijke nieuwe functies toevoegen aan de SmartScreen-filtertechnologieën om ze nog effectiever te maken. SmartScreen heeft het voordeel dat het kan putten uit miljoenen berichten die honderdduizenden Hotmail-gebruikers vrijwillig ter beschikking hebben gesteld en hebben gemarkeerd als spam of niet-spam. En omdat spammers steeds van tactiek veranderen om filters te ontwijken, zijn we van plan om SmartScreen-technologieën uit te rusten met functionaliteit voor automatische updates", aldus Bill Gates in een recente executive mail.

"We merken dat in het MKB veel aandacht is voor het tegenhouden van spam", zegt Marnix van Meer van Crypsys Data Security, distributeur en specialist in informatiebeveiliging. Van Meer is van mening dat eindgebruikers er niet per se naar zouden moeten streven om alle noodzakelijke security-software van één aanbieder aan te schaffen. "Wij bieden geen alles-in-één oplossingen omdat we vaak zien dat daarin altijd wel zwakke schakels zitten. Beter is het om van alles het beste te kiezen." Voor spam- en virusbeveiliging heeft Crypsys gekozen voor Sophos. Het bedrijf dat door marktanalist Frost & Sullivan onlangs nog werd benoemd tot Europees beveiligingsbedrijf van het jaar.

Wireless

Draadloos werken mag dan steeds populairder worden, wie zich niet voldoende beveiligt legt daarmee de sleutel onder de mat. De vraag is echter of het met beveiliging wel allemaal echt veilig genoeg is. "Honderd procent veilig is het nooit maar we zien wel ontwikkelingen die aangeven dat het steeds veiliger wordt", zegt Michel van den Berg van Netgear, aanbieder van geavanceerde netwerkproducten. "Het probleem ligt vaak bij de gebruiker. Die wil zonder veel rompslomp aan de slag en gaat snel voorbij aan de gevaren door een verkeerde manier van configureren", zegt Van den Berg.
Een notebook, pda of mobiele telefoon die op alle manieren is beveiligd tegen virussen en digitale dieven, kan natuurlijk ook nog gewoon gestolen worden. Steeds vaker gebeurt dat niet alleen omdat die apparaten zo begerenswaardig zijn, maar omdat bepaalde (bedrijfsgevoelige) gegevens nog veel meer geld opleveren. Om je als gebruiker ook daar tegen te wapenen is het verstandig om van toegangsbeveiliging en encryptie van data gebruik te maken. Control Break International (CBI) is een Nederlandse ontwikkelaar van software voor beveiliging van mobiele data. Onlangs nog introduceerde CBI SafeBoot voor Palm. Deze software beveiligt pda's tegen ongewenst gebruik van derden door de toegang tot de pda met encryptietechnieken te beveiligen. "We bieden encryptie-oplossingen voor alle soorten devices en toegangscontrole door middel van smartcards, fingerprint en wachtwoorden. Veelal in combinatie met elkaar", zegt Tom de Jongh van CBI. "Toegangscontrole alleen zou bijvoorbeeld nooit zinvol zijn als er ook niet wordt gekozen voor encryptie." Ook De Jongh is van mening dat de potentiële bedreigingen steeds groter worden.

Software van Sophos, Europees beveiligingsbedrijf van het jaar.

GSM-virus

Onlangs werd er in een actualiteitenprogramma op televisie uitvoerig stilgestaan bij de gevaren van virussen voor mobiele telefoons. Met name smartphones zouden er erg gevoelig voor zijn. "Ik zie het GSM-virus als een non-issue", zegt Marnix van Meer in een persbericht van Crypsys. "Dat nu ook mobiele telefoons al gevaar zouden lopen, wordt erg opgeblazen op dit moment. Mobiele telefoons zijn voor virusschrijvers minder interessant omdat ze nooit op alle telefoons schade aan kunnen richten en zich dus ook minder snel kunnen verspreiden. Ook zal een pc-virus meestal geen schade aanrichten op bijvoorbeeld een pda. We zien echter wel zwakke plekken waar virussen op termijn schade zouden kunnen aanrichten. We zullen daar tijdig een oplossing voor bieden maar willen vooral niet nu al gaan roepen dat gebruikers op hun hoede moeten zijn."