

Bedrijven spenderen meer aan printers dan aan netwerkbeveiliging

Onderzoeksbureau IDC vraagt om beveiliging op agenda directieraad te plaatsen

Diegem, 3 juni 2004

Volgens een studie die onderzoeksbureau IDC heeft gepubliceerd, nemen bedrijven de dreiging van computervirussen, -wormen en andere inbraakpogingen op het computernetwerk, niet voldoende ernstig. Dat wordt ondermeer aangetoond door de 42 miljard USD die vorig jaar in computerbeveiliging werd geïnvesteerd. Dat bedrag is minder dan vijf procent van de totale investeringen in computermateriaal. Het komt ongeveer overeen met de 43 miljard USD die vorig jaar aan printers werd uitgegeven.

Uit de studie blijkt dat menselijke fouten en het tijdverlies om het computernetwerk draaiende te houden na aanvallen, bedrijven het meest kwetsbaar maakt. De studie, gemaakt in opdracht van Cisco Systems, formuleert de belangrijkste aspecten van computerbeveiliging die elke manager zou moeten onderkennen:

- organisaties die het risico op computerinbraak willen minimaliseren, kunnen dat alleen door een alomvattende aanpak die het gehele computernetwerk beveiligt;
- meer dan 60% van alle gebruikers binnen een computernetwerk zijn niet meer actief; al die vervallen e-mailadressen maken bedrijven extra kwetsbaar en verhogen operationele lasten;
- ongewenste e-mail of spam kan nu al tot 80% van de binnenkomende mail bedragen; en spam is een mogelijke bron van inbraak;
- bedreigingen veranderen zo snel van aard, dat de effectiviteit van de beveiligingssystemen voortdurend beheerd moet worden.

IDC roept dan ook op om beveiliging op de agenda van de directieraad te plaatsen. Daarbij voorspelt het bureau dat tegen 2007 de bestedingen voor computerbeveiliging zullen oplopen van de huidige 4,8% tot zeven procent van het totale informaticabudget. Beveiliging voor mobiel computergebruik zal daarbij een sterke groei kennen, omdat meer en meer mensen zich van op afstand met het centrale bedrijfsnetwerk verbinden.

De vloedgolf van vorig jaar

Volgens IDC ondervonden we in 2003 een echte vloedgolf aan computervirussen. Het bureau poneert dat bedrijven zich moeten afvragen wat de impact van gegevensverlies voor hen zou kunnen betekenen. Omdat de computeraanvallen steeds gesofisticeerder worden, volstaan enkelvoudige beveiligingssystemen niet meer, zoals bijvoorbeeld alleen rekenen op anti-virussoftware. De beveiliging moet op de verschillende niveaus van het volledige computernetwerk actief zijn. Leveranciers van anti-virussoftware krijgen minder en minder tijd om te reageren op nieuwe types virussen, waardoor die laatste des te harder kunnen toeslaan.

IDC vraagt om eveneens rekening te houden met een adequate beveiliging van de computergegevens die bedrijven uitsturen. Indien die onvoldoende blijkt, kan het niet alleen productiviteitsverlies tot gevolg hebben, maar ook problemen met regelgevende instanties veroorzaken.

Om zowel het binnenkomende als het uitgaande gegevensverkeer voldoende te beveiligen, wijst IDC op de noodzaak om de beveiligingsmechanismen in het computernetwerk te integreren.

"Cisco heeft een beveiligingsarchitectuur ontworpen, het *self-defending network* genaamd, die volledig autonoom werkt en onmiddellijk kan ingrijpen als de veiligheid in het gedrang

komt," zegt Yves Mertens, technisch directeur van Cisco. "Daarmee kunnen onze klanten mogelijke menselijke fouten vermijden, wanneer men moet reageren op aanvallen."

Het volledige rapport van IDC kan je downloaden via
<http://files.quadrantcommunications.be/Quadrant.nsf/Pages/IDC>

Over Cisco Systems - "Empowering the Internet Generation" - NASDAQ:CSCO
Cisco Systems is wereldwijd marktleider in netwerksystemen voor het internet.
Meer info op <http://www.cisco.be> en <http://cisco.com>

Cisco Systems Belgium
Pascale Jacobs, marcom manager
Regentlaan 43, B-1000 Brussel
T: +32 (0)2 778 4662
F: +32 (0)2 778 4300
E: pjacobs@cisco.com

Contact voor journalisten:
Quadrant Communications
James De Paepe
Franklin Rooseveltlaan 348 H, B-9000 Gent
T: +32 (0)9 265 0226
M: +32 (0)477 544 388
F: +32 (0)9 256 4616
E: james@quadrantcommunications.be