

Artikel ICT-gevaar van binnenuit vele malen groter

Vooral overheid zwaar getroffen door gerommel met bestanden en diefstal

MarQit, Rotterdam, 19 mei 2006 – Organisaties hebben beduidend meer last van ICT-bedreigingen die veroorzaakt worden door hun eigen personeel dan bedreigingen die van buitenaf komen. Met name het doorsturen van zakelijke e-mails naar privé-adressen en diefstal van apparatuur zijn geen onbekende fenomenen. Dit blijkt uit een onafhankelijk onderzoek van Marqit, een informatieprovider die organisaties ondersteunt bij de oriëntatie op en selectie van ICT-oplossingen.

Marqit ondervroeg 843 ICT- en algemeen managers in diverse sectoren naar hun praktijkervaringen met security-problemen. Uit de antwoorden van respondenten komen de volgende opvallende feiten naar voren:

- Bedreigingen van binnenuit komen beduidend vaker voor dan externe;
- De overheid wordt het zwaarst getroffen door interne bedreigingen;
- Grotere organisaties zijn twee keer zo vaak slachtoffer van diefstal van computerapparatuur als het MKB.

Meer gevaar van binnenuit: mails doorsturen en diefstal

Meer dan de helft van de ondervraagde ondernemingen heeft al te maken gehad met het meest voorkomende type interne bedreiging: het doorsturen van zakelijke e-mails naar privé-mailadressen, 55 procent van de respondenten herkent dit. Opvallend is eveneens dat maar liefst 52 procent van alle organisaties al het slachtoffer geweest is van de diefstal van PC's, laptops en mobiele apparaten. Ook het opslaan van zakelijke bestanden op persoonlijke USB-sticks komt veel voor (47 procent). Ter vergelijking: externe bedreigingen zoals virusaanvallen, phishing en hacking kwamen in respectievelijk 50, 22 en 20 procent van de ondervraagde organisaties voor.

De overheid grootste slachtoffer

Bij de genoemde interne bedreigingen is het de overheid die daar veruit de meeste ervaring mee heeft. Diefstal van apparatuur springt eruit; maar liefst 59 procent van de ondervraagde overheidsinstellingen is daarvan het slachtoffer geweest, tegen 49 procent van de profit-organisaties. Ook worden er bij de overheid meer e-mails doorgestuurd naar privé-adressen (58 procent in vergelijking tot 53 procent bij profit) en blijken ambtenaren minder moeite te hebben met het kopiëren van bestanden op hun eigen USB-sticks (51 procent ten opzichte van 46 procent bij profit).

Grote organisaties; veel verduistering

De grootte van de organisatie blijkt ook een belangrijke factor in de aanwezigheid van interne ICT-bedreigingen. Maar liefst 66 procent van de organisaties met meer dan 100 medewerkers heeft al te maken gehad

met diefstal van apparatuur. Een groot verschil met het MKB, waar slechts 30 procent van de organisaties al eens bestolen is van binnenuit.

“De uitkomsten van ons onderzoek zijn confronterend, zeker gezien de verlies- en diefstalincidenten die we recentelijk in de pers hebben zien opduiken”, aldus Roderick Wijsmuller, managing director van Marqit.

“Voornamelijk bij de overheid blijkt de controle en kennis van wat wel en niet kan ondermaats en als daar niet snel wat aan gedaan wordt, zijn de gevolgen niet te overzien.”

UBM Global: als maatregelen ter voorkoming van dataverlies heeft DriveLock de volgende edities:

- *DriveLock Basic. Poort- en randapparaatcontrole en autorisatie plus netwerkprofielen.*
- *DriveLock Encryption. Versleutelen van informatie op verwijderbare drives.*
- *DriveLock Security Reporting Center. Verzamelen en rapporteren van DriveLock events.*
- *DriveLock Application Filter. Applicatiecontrole en -autorisatie.*
- *DriveLock Terminal Services. DriveLock functionaliteiten voor Terminal Server sessies.*