

# Cybercrime wordt vorm van terreur”

Redactie economie

**AMSTERDAM** – Cybercrime dreigt een onbeheersbaar probleem te worden. Computercriminelen worden professioneler; een terroristische digitale aanval is denkbaar. „Voor de Nederlandse overheid schiet tekort in de beveiliging tegen computercriminaliteit.”

Dat blijkt uit de gisteren gepresenteerde resultaten van de ICT Barometer, uitgevoerd in opdracht van advies- en accountantskantoor Ernst & Young onder 600 managers bij de overheid en het bedrijfsleven.

Driekwart van de organisaties is in grote mate afhankelijk van ict. Hoewel de meeste bedrijven en overheidsorganisaties niet zonder ict kunnen, is de interesse in het voorkomen en aanpakken van cybercrime niet erg groot. Vier op de tien managers zeggen een noodplan te hebben voor het geval dat het kritische bedrijfsproces uitvalt of niet meer goed functioneert. Bij de overheid heeft driekwart geen noodplan klaar.

Monique Otten van Ernst & Young vindt dit „zorgelijk. Er moeten nu maatregelen worden getroffen om toekomstige terreuranslagen te voorkomen. Organisaties moeten hun ict-infrastructuur volledig beveiligen. In de VS is onlangs een succesvolle digitale aanval op een energiecentrale gedaan. Terreur via internet is dus geen fictie.”

Jacob Verschuur, directeur ict bij Ernst & Young, bevestigt dit. „Met vliegtuigen in een wolkenkrabber vliegen, is voorbij. Terroristen gaan aanslagen plegen via de digitale weg.”

## Fietsendiefstal

Sinds 2004 daalt het aantal managers dat last heeft van computervirussen van 28 tot 3 procent. Ook de hinder die organisaties hebben van computerinbraak is verminderd: van 5 procent in 2004 tot 0,4 procent nu. „Het lijkt erop dat we hackers te slim af zijn”, aldus Otten. „De praktijk is anders. Het is net als bij fietsendiefstal. In de loop van de jaren kijken we daar ook minder van op. We zijn gewend geraakt aan cybercrime en dat is eng.”

Op internet zijn bijna alle persoonlijke gegevens te zien, ook voor hackers. Otten: „De boodschappen die zijn gekocht bij Albert Heijn zijn zichtbaar; verzekeringen zijn op het web te regelen; de donorregistratie is online

te wijzigen. Veel burgers denken niet aan hun veiligheid; sommigen lenen zelfs hun DigiD, de digitale identiteit, uit aan anderen. Vroeger werden websites bijna alleen gebruikt om informatie te geven. Tegenwoordig is internet interactief. Dat vraagt om een betere beveiliging.”

Veel bedrijven maken nog steeds standaardfouten, aldus Otten. „Zo is via programmeertaal vaak gemakkelijk een werkende inlognaam en wachtwoord te maken.” Toch zien bedrijven de webapplicatie niet als grootste bron van zorg vanuit beveiligingsoptiek, blijkt uit de ICT Barometer. „Managers zien het zoekraken van usb-sticks als een veel groter probleem”, zegt Verschuur.

## Opsporing

Ruim 80 procent van de ondervraagden zegt weinig vertrouwen in politie en justitie te hebben bij de opsporing van computercriminelen. Het gros lost het probleem liever zelf op. Slechts een kleine groep doet aangifte (6 procent), terwijl twee op de tien bedrijven zelfs helemaal geen actie ondernemen.

De politie is er om „negatieve effecten van internetgebruik” aan te pakken, zegt Henk Klap van de politie. De leider van het Project Aanpak Cybercrime erkent dat het makkelijker moet zijn aangifte tegen computercriminaliteit te doen en dat het onderzoek daarna sneller moet. „Bedrijven hebben zelf ook een verantwoordelijkheid. De politie lost het veiligheidsprobleem niet op; organisaties moeten zorgen dat de beveiliging op orde is.”

De politie doet veel aan de aanpak van cybercrime. Klap: „Vijftien jaar geleden begonnen we experts aan te trekken. Nu hebben we er 250. Ook zijn inmiddels 2000 rechercheurs wegwijs gemaakt in de digiwereld. De komende jaren worden er nog meer geschoold. Zo kunnen we een aangifte sneller op waarde schatten en betere vervolgstappen zetten. En dat gaat makkelijker nu de burger zijn sporen overal op internet achterlaat.”

## ■ „Overheid faalt in strijd tegen internetcriminaliteit

