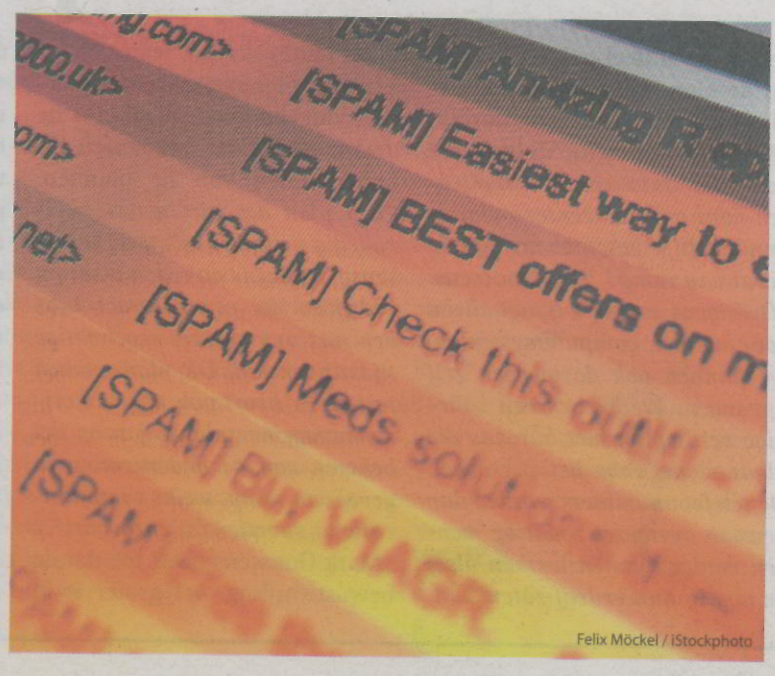
# Malware een halt toeroepen

TEKST: FRANS GODDEN

Eddy Willems, IT Security Evangelist bij Kaspersky Labs

Malware is eigenlijk de verzaMalware is eigenlijk de verzamelnaam voor al wat gevaarlijk is voor je PC. Vroeger had het vooral betrekking op virussen, maar die vertegenwoordigen nu nog amper 5 tot 7% van alle problemen. Nu spelen eerder Trojaanse paarden, adware en spyware de hoofdrol. *"Malware groeit nog steeds exponentieel"*, zegt Eddy Willems, IT Security Evangelist bij Kaspersky Labs. *"Begin vorig jaar werden 500.000 gevallen geregistreerd, maar tegen het einde van het jaar waren dat er al 2 miljoen. En onze prognoses voor dit jaar voor het tienvoudige lijken te gaan uitkomen want we zaten vorige week al aan 17,5 miljoen stuks. Daarbij gebruikt malware steeds vaker technieken om onzichtbaar te worden, om onder de radar te blijven, zoals rootkit technologie. Alleen het doel van malware blijft ongewijzigd: geldgewin!"*.

Het is dan ook duidelijk dat hier nieuwe technieken nodig zijn, de klassieke firewalls en anti-virusdefinities volstaan niet meer. Willems: *"Naast intrusion protection, waarbij we malware gaan blokkeren en hacking proberen te voorkomen, maken we nu ook gebruik van een nieuwe technologie, white listing. Daarbij wordt je hele PC één keer afgescand en als het ware een portret gemaakt van alle programma's die op je PC staan. De minste wijziging die zich dan voordoet aan die programma's, wordt onmiddellijk gesignaleerd en de verdediging kan in actie komen"*.

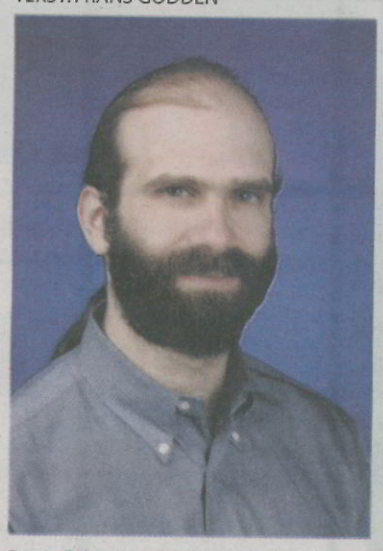



Felix Möckel / iStockphoto

# Diefstal van identiteit duidelijk in de lift

Precieze cijfers zijn er niet maar alle specialisten zijn het erover eens dat de diefstal van identiteit een bijzonder snelgroeiende plaag is geworden. Niet alleen neemt het aantal mogelijkheden om zich uit te geven voor iemand anders toe, maar ook de manier waarop identiteitsdiefstal kan gebeuren wordt steeds gevarieerder.

TEKST: FRANS GODDEN



Bruce Schneier, Chief Technical Officer van BT Counterpane

Bruce Schneier, Chief Technical Officer van BT Counterpane, de divisie van British Telecom die zich toelegt op beheerde securitydiensten, windt er geen doekjes om: de diefstal van identiteit is de nieuwste misdaad van het Internettijdperk. Een crimineel verzamelt daarbij voldoende persoonlijke gegevens over het slachtoffer om zich te laten doorgaan als de ander bij banken, kredietkaartfirma's of andere financiële instellingen. Hij plundert dan de rekeningen van het slachtoffer en verdwijnt met de cash.

Dergelijke praktijken komen natuurlijk meer voor in landen waar geen identiteitskaarten bestaan zoals Groot-Brittannië of de Verenigde Staten – daar zijn zelfs gevallen bekend van criminelen die zich voordeden als iemand anders en op het postkantoor het adres van het slachtoffer lieten veranderen. Maar met de opkomst van het Internet zijn ook andere landen niet langer immuun. Volgens Bert Van Beeck, Identity Specialist bij Sun Microsystems, moet je wel een onderscheid maken tussen een hack, waarbij met criminele bedoelingen ingebroken wordt in computersystemen om kredietkaart- of andere identiteitsgegevens te stelen, en phishingaanvallen, waarbij mensen misleid worden om persoonlijke gegevens op het Internet in te vullen en door te sturen, ogenschijnlijk naar een betrouwbare bestemmeling maar in feite naar een site die door criminelen opgezet werd.

> **"De diefstal van identiteit is de nieuwste misdaad van het Internettijdperk"**

Phishing kan je vermijden door nooit in te gaan op oproepen via e-mail om vertrouwelijke gegevens door te sturen, al dan niet via een Website die er vertrouwd uitziet. Je zal overigens op de Website van elke bank kunnen lezen dat zij nooit mails sturen waarin je bankgegevens gevraagd worden. *"Maar er is nog een ander aspect dat met identiteit te maken heeft, namelijk identity management"*, zegt Van Beeck. *"Stel, je wordt gepromoveerd in het bedrijf waar je werkt, krijgt nieuwe rechten in je nieuwe afdeling maar men vergeet je oude rechten in je vroegere afdeling te schrappen. Het resultaat is dat je dan misschien rechten hebt die niet met elkaar verenigbaar zijn, en dan krijg je conflicten rond de segregation of duties, een van de basisconcepten van interne controles. Iets wat te allen prijze moet vermeden worden want dan wordt de poort wagenwijd opengezet om bepaalde transacties te laten plaatsvinden, zonder dat er nog controle over is. Daarom heb je producten als identity managers nodig om manuele controles te kunnen uitvoeren"*.

Jill Fromer/iStockphoto