

Yopmail: digitale vuilnisbelt voor spamberichten.

ntvangen". Vaak geef je spammers daardoor alleen maar de bevestiging dat je e-mailadres actief is, zodat er nóg meer ongewenste berichten je mailbox binnenrollen!

Updates & antimalware

een spammer die nu nog jouw e-mailadres te pakken kan krijgen? Vergeet het maar... ook je vrienden kennissen en vrienden durven je adres te geven – zonder dat ze zich van enig kwaad bewust zijn! Neen, we hebben het niet eens over de ergerlijke gewoonte om een ellenlange lijst met e-mailadressen in het CC-veld te ploffen, in plaats van het discretere BCC-veld (blind carbon copy) aan te spreken. We hebben het wél over gebruikers wiens pc als een zombie in een crimineel botnet is opgenomen. Hoe zit dat precies? Wie acht dat spyware, trojanen of wormen nog altijd een probleem zijn van enkele losgeslagen whizzkids, moet zijn mening dringend herzien! Het zijn deze verwoed werkende worden in handen van de meest maffiabendes, die zulke bollebozen inhuren. Ze gaan dan op zoek naar veiligheidslekken in je systeem of browser. Zodra ze die gevonden hebben, installeren ze heimelijk malware op je toestel. Als dat gelukt is, kan je geïnfecteerde pc contact opnemen met de hackers. Op hun commando voert jouw pc dan – samen met soms duizenden andere zombies – zowat alles uit waar zij zin in hebben. Typische voorbeelden zijn DDoS-aanvallen (Distributed Denial of Service), waarbij getracht wordt een of andere bekende server met talloze verzoeken te overstelpen, zodat die niet langer bruikbaar is) en... het verspreiden van spamberichten! Zo kan het gebeuren dat je spam ontvangt van een van je kennissen, wiens pc een willoze zombie is geworden. Wil

HET PROTOCOL EN DE WET

Zonde eigenlijk dat we ons als arme eindgebruikers het hoofd moeten breken om spam buiten onze mailbox te houden. Kan daar juridisch geen stokje voor gestoken worden, of valt dat niet met een technische ingreep te regelen?

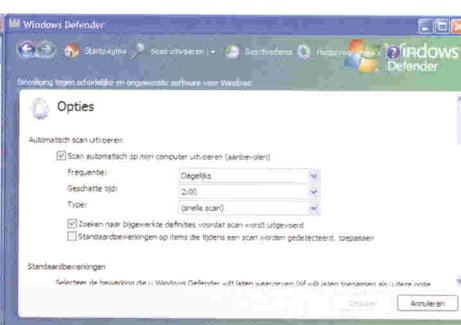
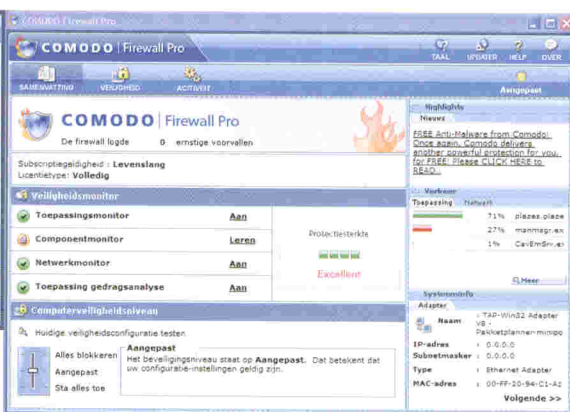
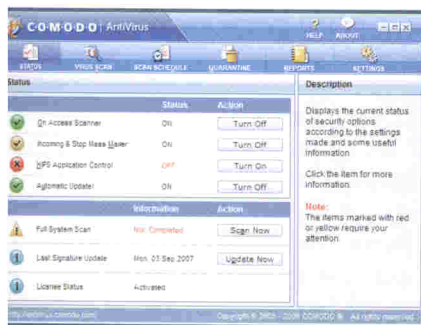
Beginnen we met de wet. Wie hierover alle details wil kennen, kan het boek 'Elektronische post juridisch bekeken. Praktische gids voor de onderneming en het bestuur' (Geert Somers en Jos Dumortier) raadplegen. In een notendop komt het hierop neer: de Belgische wetgever heeft binnen de Europese richtlijnen voor het zogenaamde opt-in principe gekozen. Dat houdt in dat "het gebruik van elektronische post voor reclame verboden is zonder de voorafgaande, vrije, specifieke en geïnformeerde toestemming van de geadresseerde van de boodschappen". Deze opt-in geldt echter niet als de elektronische contactgegevens onpersoonlijk zijn. Dus spam op adressen als info@ of klantendienst@ kan nog altijd, in tegenstelling tot privé-persoonen, die vooraf hun expliciete toestemming moeten geven. Wie in de fout gaat, riskeert € 50.000 tot € 125.000 boete. Deze regeling lijkt misschien waterdicht, maar de meeste spammers opereren vanuit het buitenland, waar de Europese – laat staan Belgische – regelgeving geen vat op heeft.

Het internationale karakter van het internet speelt onze wetgeving dus parten, maar hoe zit het met de techniek? Het grote probleem is dat het SMTP-protocol (simple mail transfer protocol), gebruikt om mail te versturen, nauwelijks of geen beveiliging kent. Meer bepaald ontbeert SMTP een degelijke controle op de authenticiteit van (de afzender van) het bericht. Voor spoofers is het dus een koud kunstje om een mail te sturen die van iemand anders lijkt uit te gaan. Intussen wordt er wel flink gesleuteld aan een of andere vorm van 'sender authentication', oftewel een identificatie van de afzender. Denk aan Microsoft met Caller ID – dat intussen met SPF, Sender Policy Framework, is samengesmolten – en Yahoo! met DomainKeys. De eindgebruiker hoeft hier geen extra inspanningen voor te leveren, maar de providers des te meer: hun mailservers zijn dan aan een stevige upgrade toe. Komt daarbij dat ook deze schema's niet waterdicht blijken én dat mailservers hierdoor vaak ten onrechte geblokkeerd worden. Kortom: lees de rest van ons artikel toch maar grondig door...

je vermijden dat ook jouw pc in zo'n crimineel botnet terecht komt, zorg er dan minstens voor dat je Windows en je browser altijd voorzien zijn van de laatste updates (veiligheidspatches). Even belangrijk is dat je een stevige firewall installeert – liefst een potiger exemplaar dan de ingebouwde firewall van Windows, zoals het gratis ZoneAlarm www.zonelabs.com of Comodo Firewall [\[www.firewall.comodo.com\]\(http://www.firewall.comodo.com\). Daarnaast beschik je liefst ook over een up-to-date antivirusprogramma – zoals het gratis Avast! Home Edition \[www.avast.nl\]\(http://www.avast.nl\) of Comodo Antivirus <http://antivirus.comodo.com> – en een up-to-date antispywaretool, zoals Windows Defender \[www.microsoft.com/netherlands/thuisgebruikers/beveiliging/spyware/software/default.aspx\]\(http://www.microsoft.com/netherlands/thuisgebruikers/beveiliging/spyware/software/default.aspx\) of Ad-Aware Free \[www.lavasoftusa.com\]\(http://www.lavasoftusa.com\).](http://www.personal-</p></div>
<div data-bbox=)



E-mailen en de wet: dit boek vertelt er je alles over.



Voor wie niet vies is van een gratis trio...