

German
Data
Security



G Data Whitepaper 2009

Hoe komt malware terecht op
bedrijfscomputers?

Ralf Benz Müller & Werner Klier
G Data Security Labs



Go safe. Go safer. G Data.

Inhoud

1. Wat is het doel van malware?	2
2. Hoe verdienen cybercriminelen geld met malware?	3
2.1 Botnets	3
2.2 Spam	3
2.3 Afpersing	3
2.4 Gegevensdiefstal.....	4
2.5 Adware.....	5
3. Hoe komt malware terecht op een pc	5
3.1 Een verbinding is al voldoende.....	5
3.2 Via e-mail	6
3.3 Via Instant Messaging.....	8
3.4 Via file sharing services	8
3.5 Via gegevensdragers	8
3.6 Via lokale netwerken	9
3.7 Via websites	9
4. Hoe verloopt een typische infectiegolf	13
4.1 De voorbereiding	13
4.2 Uitvoering.....	14
4.3 De geïnfecteerde computer gebruiken.....	14
5. Hoe kunt u zich beveiligen	15

1. Wat is het doel van malware?

De laatste jaren is er een opmerkelijke verschuiving gekomen in de beweegredenen voor het maken en verspreiden van schadelijke software. In de beginjaren van de computervirussen ging het nog om een bijna sportieve strijd om de eer tussen computerspecialisten. Vandaag de dag staan vooral concrete financiële voordelen centraal.

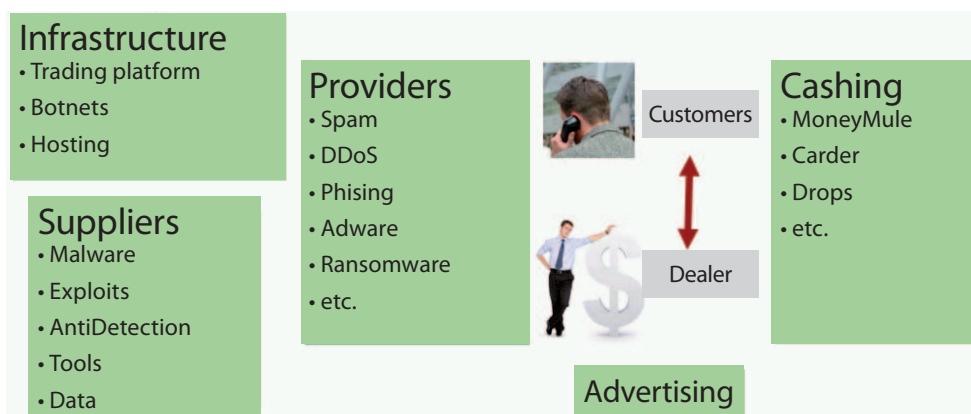
In de "digitale onderwereld" is een echte zwarte economie ontstaan, waarbij in strakke, keurig georganiseerde structuren malware wordt gemaakt, geperfectioneerd en verspreid.

Binnen de cybercrime-economie is een bloeiende handel ontstaan in alle mogelijke digitale goederen en diensten. Op speciale handelsplatformen is informatie verkrijgbaar over recent ontdekte veiligheidslekken en de daarbij passende malware. Soms geeft de auteur zelfs een functiegarantie en krijgen afnemers binnen de garantieperiode gratis aangepaste versies.

Legers van geïnfecteerde computers, die als zogenaamde zombies deel uitmaken van een botnet, worden per uur of per dag verhuurd. Zo kunnen spamcampagnes of doelgerichte aanvallen tegen onpopulaire websites of mailservers worden uitgevoerd.

En zelfs de laatste schakel in de criminele keten van toegevoegde waarde, namelijk het omzetten van de buitgemaakte informatie, zoals creditcardgegevens in contanten, wordt op de digitale markt van de cybercriminelen geregeld. Dat gebeurt door nietsvermoedende pc-gebruikers die als "financiële medewerkers" worden aangeworven bij dekmantelbedrijven. Deze stellen dan weer hun eigen bankgegevens voor dubieuze financiële transacties ter beschikking.

Vroeger was het hoofddoel van de aanvallen het creëren van schadelijke software, die uitsluitend ter verspreiding was bedoeld, maar dat is allang niet meer het geval. Nu wordt op steeds meer bedrijfsnetwerken ingebroken, om daar allerlei informatie te stelen waaruit munt is te slaan. Ook kan de infrastructuur van het aangevallen netwerk voor criminele doeleinden worden misbruikt.



Afb. 1: Overzicht van de verschillende delen van de e-crime-economie

Afbeelding 1 toont hoe de e-crime-economie een eng verweven netwerk van economische sectoren is. De eigenlijke spelers werken op de achtergrond. Zij leveren malware, kennis over nieuwe veiligheidslekken en handelen in gestolen gegevens. Die worden door tussenpersonen op gespecialiseerde plaatsen aan criminele "klanten" verkocht of verhuurd om ten slotte door aangeworven, meestal nietsvermoedende tussenpersonen in contant geld te worden omgezet (zgn. cashing).

2. Hoe verdienen cybercriminelen geld met malware?

Online-misdadigers maken op de meest uiteenlopende manieren winst. Het inzetten van een leger geïnfecteerde computers die onder controle van de aanvallers staan, is een belangrijke zet in het spel. Die zogenaamde botnets kunnen een flink aantal illegale activiteiten uitvoeren, waarmee in de digitale onderwereld veel geld te verdienen valt.

2.1 Botnets

Botnets zijn de draaischijf van de eCrime-infrastructuur. Ze worden niet alleen gebruikt voor het verzenden van spam en het uitvoeren van Denial-of-Service-aanvallen. Zombiecomputers worden ook ingezet als host voor phishing- en malwaresites en om de adressen van e-mail-servers op te sporen. Het is dan ook niet verwonderlijk dat het aantal botnetcomputers de laatste tijd zo sterk is toegenomen. Omdat botnets in kleinere eenheden van enkele duizenden zombiecomputers worden gesegmenteerd, is ook het aantal botnets aanzienlijk gestegen.

In het verleden gebeurde de besturing bijna uitsluitend via IRC (Internet Relay Chat, chatsysteem dat op tekst is gebaseerd). In de volgende ontwikkelingsfasen kwamen er steeds meer botnets bij die andere protocollen voor de besturing gebruiken. Moderne botnets, zoals het beruchte Storm-botnet, zijn als peer-to-peernetwerk (P2P) begonnen. Het eveneens machtige Zunker-botnet communiceert via http. Na het offline halen van de dubieuze Internet Service Provider McColo verloren een paar botnets hun commandocomputer en werden daardoor onbruikbaar. Het gevolg was het verdwijnen van de botnets Srizbi en Storm. Nieuwe botnets, zoals Waledac of Conficker, genereren nu veel verschillende contactmogelijkheden om altijd over botnets te kunnen beschikken. Bovendien worden de camouflagemechanismen steeds sluwder en met behulp van regelmatige updates en rootkits worden de backdoors op een efficiënte manier verborgen. De programma's en gegevens voor een opdracht worden eerst direct overgedragen en aansluitend opnieuw verwijderd.

2.2 Spam

Spam is big business. En niet alleen de aanbieders van de producten waarvoor reclame wordt gemaakt, verdienen hier geld aan. Het versturen van spam gebeurt meestal via botnets. Voor de verzending van 2 miljoen e-mails verspreid over 14 dagen telde de spammer Solomon \$195 neer. Aan 20 miljoen e-mails hing een prijskaartje van \$495. Op die manier is de handel in nutteloze pillen, gestolen software en minderwaardige kopieën zelfs bij de minste afzet

winstgevend. Die afzet blijft echter niet beperkt tot een minimum, integendeel. De semilegale producten, waarvoor reclame wordt gemaakt, hebben een klantenbestand dat groter is dan over het algemeen wordt gedacht. Zwendelaars verdienen niet alleen aan het verkopen van gebakken lucht. Jeremy Jaynes, in zijn tijd de achtste grootste spammer ter wereld, kreeg een salaris van zo'n \$750.000 per maand.

2.3 Afpersing

Als de webshop van een firma erg winstgevend is, of als een onderneming afhankelijk is van het tijdig verwerken van e-mails, kan de onderneming door aanvallen op deze diensten afgeperst worden. Aaneengeschakelde zombiecomputers van een botnet kunnen een website of een mailserver met zinloze verzoeken bestoken. Door de massale serververzoeken wordt een systeem in dergelijke mate overbelast, dat een normale werking niet meer mogelijk is.

Niet alleen bookmakers en onlinecasino's kunnen ten prooi vallen van deze verspreide overbelastingsaanvallen (in het Engels Distributed-Denial-of-Service, DDoS-aanval). Wie dagelijks met

vijf- en zescijferige bedragen bezig is of een spelcommunity van diensten moet voorzien, is zo nu en dan bereid om losgeld te betalen. Een bedrag dat vaak maar een fractie is van de omzet. In de meeste gevallen gaat het om 4-cijferige bedragen. Het aantal ongerapporteerde cijfers is zeer hoog.

DDoS-aanvallen worden ook voor politieke doeleinden gebruikt. Eind april en begin mei 2007 werden in Estland de servers van ministeries, overheidsinstanties, banken, kranten en ondernemingen lamgelegd. Het verwijderen van een Russisch gedenkteken voor soldaten veroorzaakte veel ongenoegen bij de Russische bevolking. Toen de demonstraties met geweld beteugeld werden, kwamen de botnets als politiek middel in actie.

Naast de DDoS-aanvallen zijn er nog andere mogelijkheden om slachtoffers van hun geld te beroven. Met ransomware, zoals GPCoder, wordt een aantal bestanden op een computer gecodeerd. Wie wil beschikken over de inhoud van zijn bestanden, heeft een decoderingsprogramma nodig. En dat kan tussen de \$12 en \$200 kosten.

Voor ondernemingen is er nog een aantal andere modellen beschikbaar. Een Trojaans paard kan kinderporno, illegale software en/of video- en audiobestanden die beveiligd zijn tegen kopiëren op een geïnfecteerde computer van een medewerker zetten. Nu heeft de aanvaller een wapen waarmee hij de medewerker kan uitspelen tegen diens baas of waarmee hij kan dreigen naar de politie te stappen.

2.4 Gegevensdiefstal

De handel in gestolen gegevens beperkt zich niet alleen tot gestolen creditcard- en bankgegevens. Ondertussen kunnen met behulp van phishing ook toegangsgegevens voor eBay, sociale netwerksites, online winkels, e-mailaccounts en nog veel meer worden gestolen. Met de zogenaamde "Keyloggers", die toetsenbordinput kunnen registreren, worden nog meer gegevens beschikbaar voor diefstal. Daartoe behoren toegangsgegevens voor firmaservers, online games, de inhoud van (vertrouwelijke) e-mails en documenten en de toegangsgegevens voor servers, forums en VPN's. Als een webserver net gedesinfecteerd is en na een paar dagen opnieuw geïnfecteerd is, kan het zijn dat de systeembeheerder zijn wachtwoord heeft prijsgegeven aan een keylogger. De logfiles van zulke keyloggers worden op underground-forums voor enkele honderden euro's per duizenden gigabytes verkocht. Vervolgens gebruiken andere groepen deze informatie en verkopen ze die verder.

De gestolen gegevens worden op verschillende manieren gebruikt:

- Creditcardgegevens worden gebruikt om vervalste kaarten te "drukken" of om bestellingen te plaatsen bij online shops.
- Bankgegevens worden gebruikt om ongeautoriseerde overschrijvingen uit te voeren. Aangezien bij bankgegevens van personen het overschrijvingsbedrag gelimiteerd is (vanaf 5000 euro gelden er speciale veiligheidsmaatregelen), is ook de buit gelimiteerd. Deze limieten zijn voor een groot aantal bankrekeningen van ondernemingen niet van toepassing. Daarom zetten online bankovervallers alle middelen in om aan dit soort toegangsgegevens te komen.
- Gestolen eBay-accounts worden gebruikt om via de aankoop van goederen gestolen geld wit te wassen.
- De toegang tot online games wordt gebruikt om online valuta en eigendommen te stelen.

- Met de toegangsgegevens voor e-mailaccounts en social netwerksites wordt in naam van het slachtoffer spam verstuurd.
- Met gestolen persoonlijke gegevens worden op het internet accounts op bepaalde forums aangemaakt. Deze accounts worden vervolgens voor illegale activiteiten en zwendel ingezet.

2.5 Adware

Adware registreert af en toe het internetgedrag van een gebruiker, toont reclame bij het openen van bepaalde websites of manipuleert zoekopdrachten. De betaling van adware gebeurt nadat een bepaald aantal klikken is bereikt (dan wordt bijv. de startpagina van de browser van aangetaste computers gemanipuleerd) of per geïnstalleerde versie. De overeenkomende partnerprogramma's bevinden zich in bepaalde online forums. Hoewel ook grote ondernemingen in de adwarebranche het voorbije jaar juridische nederlagen hebben moeten verwerken, is het aantal reclamemalware en potentieel ongewenste programma's in de afgelopen twee jaar meer dan vervijfvoudigd.

Besluit: Dit zijn zeker niet alle bedrijfsmodellen van de online criminelen. Maar ze tonen wel aan dat de online criminaliteit big business is. Met een schadeprijkaartje dat tot in de miljarden loopt, is deze sector lucratiever dan de drugsindustrie. De bovengenoemde sectoren vormen de zwaartepunten van de malwareverspreiding. Het belangrijkste instrument zijn de botnets. Van daaruit wordt spam verstuurd en vinden phishing-aanvallen plaats. Afpersing, de diefstal van gegevens en het invoegen van de gepaste reclame zijn andere zwaartepunten.

3. Hoe komt malware terecht op een pc

Na de toelichting over de motivatie van malwareverspreiders, is het nu de hoogste tijd voor het eigenlijke thema van deze studie. Er zijn talrijke manieren waarop malware op een bedrijfscomputer terecht kan komen. Soms is het al voldoende om een computer met het internet of het lokale netwerk te verbinden. Maar ook e-mails, file sharing services, instant messages en zelfs gegevensdragers kunnen schadelijke codes bevatten. Het grootste gevaar schuilt tegenwoordig in gemanipuleerde websites die ofwel meteen het geïnfecteerde bestand downloaden of ongemerkt op de achtergrond de computer infecteren als zogenaamde drive-by-download.

3.1 Een verbinding is al voldoende

De talloze internetwormen en bots die constant autonoom op het internet circuleren, vormen een continue bedreiging voor computers die met het internet zijn verbonden. Ononderbroken genereren ze min of meer willekeurig IP-adressen en controleren ze of de daarbijhorende computers kwetsbaar zijn voor veiligheidslekken. Vaak is de keuze aan IP-adressen beperkt, zodat enkel bepaalde netwerkbereiken van bijvoorbeeld een bepaalde internetprovider of een bepaalde regio worden gekozen. De veiligheidslekken die worden gebruikt, variëren van tijd tot tijd. Zelfs veiligheidslekken die al lang gedicht zijn, worden nog gevraagd, zoals die van Blaster (2003) en Sasser (2004). Frequente aanvalsdoelen worden in onderstaande lijst vernoemd:

- Plug'n'Play (MS05-039) via TCP/445, TCP/139
- RPC-DCOM (MS03-026/MS03-039) via TCP/135, TCP/445, TCP/1025
- LSASS (MS04-011) via TCP/445

- MySQL via TCP/3306
- Arkeia via TCP/617
- Veritas via TCP/6101
- Veritas via TCP/10000
- WINS via TCP/42
- Arcserve via TCP/41523
- NetBackup via TCP/13701
- Workstation Service (MS03-049) via TCP/135, TCP/445
- WebDaV via TCP/80
- DameWare via TCP/6129
- MyDoom-backdoor via TCP/3127
- Bagle-backdoor via TCP/2745
- IIS 5.x SSL PCT (MS04-011) via TCP/443
- Accounts met triviale wachtwoorden (verbinding via TCP/139 of TCP/445)
- MSSQL-server met alledaagse wachtwoorden (bijv. „SA“-account met leeg wachtwoord) via TCP/1433

In een studie werden over een periode van drie maanden aanvallen op verschillende computerarchitecturen gemeten. Computers met Windows werden ongeveer elke 38 seconden aangevallen. Veel systeembeheerders hebben al ondervonden dat een pas geïnstalleerde computer tijdens het downloaden van een patch na een paar seconden wordt aangevallen en overgenomen. Netwerken met veel klanten (zoals UPC) krijgen vaker dan om de 38

seconden aanvallen te verwerken. Daarbij komt nog eens dat de laatste jaren het vervaardigen van exploit-codes professioneler is geworden. Soms verschijnen exploit-codes voor veiligheidslekken al enkele dagen na de eerste berichten hierover. Ook worden er steeds meer exploits ontdekt terwijl ze door malware worden gebruikt (zgn. zero-day-exploits). Het recentste voorbeeld hiervan was de worm Conficker, die naast de automatische verspreiding ook lokale gedeelde items met zwakke wachtwoordbeveiliging en het automatische opstartmechanisme van USB-gegevensdragers gebruikt voor verspreiding.

Dit soort aanvallen gebeurt zonder toedoen van de pc-gebruiker en in de meeste gevallen ook zonder diens medeweten. Een goed geconfigureerde firewall of router beschermen tegen zulke aanvallen.

3.2 Via e-mail

Ook nu verspreidt veel malware zich via e-mail. De grote uitbarstingen van Loveletter, Melissa of Sobig en Netsky, die de mailservers gedeeltelijk op hun knieën dwongen, worden steeds zeldzamer en niet meer gebruikt voor de verspreiding van wormen. Sober, Nyxem en Warezov waren de laatste e-mailwormen die op grote media-aandacht konden rekenen. In plaats daarvan worden nu veel kleinere golven gestart die beperkt zijn in tijd en locatie. In tegenstelling tot de volledig automatisch werkende infecties door internetwormen, worden e-mailwormen pas gevaarlijk als de ontvanger de bestandsbijlage opent. Het ontvangen van een schadelijke e-mail alleen vormt geen gevaar op zich en in slechts een paar gevallen is het voldoende om de e-mail in de client te tonen (bijv. Bubbleboy en Klez). Bij het grootste deel van de e-mails moet de hulp van de ontvanger worden ingeschakeld. Die wordt via allerlei social engineering-

trucs aangezet tot het openen van de bijlage. Daartoe worden alle mogelijke gegevens van de e-mail-header vervalst. Vooral het adres van de afzender wordt vaak gewijzigd. Enkel de eerste generatie e-mailwormen werkte met de naam van het slachtoffer. Vandaag de dag bestaat er voor bijna alle afzenderadressen een vals equivalent.

Aangezien tegenwoordig uitvoerbare bestanden in e-mails worden weggefilterd (ofwel bij de gateway ofwel op de client) en de e-mailgebruikers zich meer bewust zijn van de risico's, zijn de malware-auteurs van strategie veranderd. Ze gebruiken niet langer bijlagen in e-mails maar links naar bestanden op het internet. Deze e-mails werden aanvankelijk niet als schadelijk herkend. In het beste geval kon een spamfilter ze eruit filteren. De werkwijze bleef voor de gebruiker echter ongeveer gelijk. Hij klikt op de link, de browser vraagt wat hij moet doen en of hij het bestand moet uitvoeren. Het duurde echter niet lang voor de directe links naar malware ook als schadelijk herkend werden. Daarom verwijzen malwareauteurs nu naar een website waar de ontvanger zelf iets moet downloaden, of waar de download na talrijke doorverwijzingen automatisch wordt opgestart.

De afzender, onderwerpregel en/of inhoud van de e-mail kunnen als lokaas worden gebruikt om het slachtoffer tot het uitvoeren van een bestand te brengen of tot het openen van een website (social engineering). Maar ook de naam van het bijgevoegde bestand, verdubbelde bestandsextensies, populaire pictogrammen of domeinnamen van een link kunnen de aanzet geven. Jordan en Goudey (2005) wijzen op de volgende twaalf psychische factoren waarop de meest succesvolle wormen tussen 2001 en 2004 zijn gebaseerd:

- Onervarenheid (inexperience)
- Nieuwsgierigheid (curiosity)
- Hebzucht (greed)
- Bedeesdheid (diffidence)
- Beleefdheid (courtesy)
- Ijdelheid (self-love)
- Lichtgelovigheid (credulity)
- Wishful thinking (desire)
- Lust en liefde (lust)
- Dreiging (dread)
- Wederkerigheid (reciprocity)
- Vriendelijkheid (friendliness)

M. Braverman vult aan:

- Algemene conversatie (generic conversation): Korte uitspraken zoals "cool", enz.
- Viruswaarschuwingen en softwarepatches
- Malware gevonden op de pc
- Viruscontrolebericht onderaan een e-mail
- Informatie of meldingen bij accounts: bijv. de telecom-trojaan, die zich als verhoogde telefoonrekening voordoe
- Foutmeldingen bij aflevering e-mail
- Lichamelijke aantrekkingskracht (physical attraction) (overlapt met het puntje Lust en liefde)

van Jordan & Goudey)

- Beschuldigingen (accusatory): bijv. de BKA-trojaan, die geeft aan dat er zogezegd illegale bestanden gevonden werden
- Recente gebeurtenissen
- Free stuff: Sommige mensen gooien alle voorzichtigheid over boord, zodra ze het woord "gratis" lezen

De pogingen om een slachtoffer te misleiden, houden niet op als de schadelijke code zijn doel bereikt heeft en uitgevoerd is. Na de succesvolle aanvallen mag het slachtoffer in geen geval merken dat er een infectie is. Foutmeldingen, afbeeldingen of (soms lege) documenten worden daartoe geopend. Sommige worms zoals Sircam en Magistr koppelen zich aan een bestand en als de schadelijke code wordt gestart, wordt ook het originele bestand geopend. Zo is er van de infectie niets te merken.

3.3 Via Instant Messaging

De meeste Instant Messaging-wormen sturen berichten met links naar websites. De mogelijkheid om rechtstreeks bestanden over te dragen, wordt nauwelijks nog gebruikt. Net als bij e-mails het geval was, zijn de aanvallen ook hier gebaseerd op social engineering. Sommige Instant Messaging-wormen bezitten zelfs chattoepassingen en kunnen korte gesprekken voeren om zo het vertrouwen te wekken.

Bedrijven die instant messaging gebruiken, kunnen het beste een client kiezen die het toelaat om inkomende bestanden te controleren. Bij enkele clients is het zelfs mogelijk om een virus-scanner via een opdrachtregel op te roepen

3.4 Via file sharing services

In een studie van G Data hebben we in P2P-file-sharing-services naar begrippen gezocht die gelinkt zijn aan de recentste top 20 van online games. Aan het begin van de studie bleek dat van de ongeveer 1000 gedownloade bestanden zo'n 33% schadelijke software bevatten. Iets meer dan twee derde (68%) van de schadelijke software bleek adware te zijn, 23% waren Trojaanse paarden en 5% backdoors.

In het verloop van de meer dan zes maanden durende studie was al meer dan de helft van de gecontroleerde bestanden uit P2P-file-sharing-services van schadelijke codes voorzien. Dit aandeel bereikte zijn piek aan het einde van het onderzoek met een topwaarde van meer dan 65% geïnfecteerde bestanden.

Deze cijfers tonen aan dat P2P-file-sharing-services erg geliefd zijn bij malware-auteurs. Wie van deze diensten gebruik maakt in een onderneming, kan zich hier maar beter tegen wapenen.

3.5 Via gegevensdragers

Het is schering en inslag dat gegevensdragers zoals harde schijven, dvd's of mp3-spelers bij het verlaten van het productiebedrijf met malware besmet zijn. Er zijn ook gevallen bekend waarbij op het parkeerterrein van een onderneming USB-sticks met daarop spyware worden gevonden. Sommige medewerkers zijn nieuwsgierig zijn naar de inhoud van de stick en infecteren op die manier hun pc met spyware.

Begin 2009 was de worm Conficker niet weg te denken uit het nieuws. Deze gebruikte onder andere de autorun-functie van Windows-besturingssystemen om zich via verwisselbare schijven te verspreiden. De worms van de autorun-familie gebruiken deze "functie" van Windows

ook en hebben sinds de tweede helft van 2008 voor een heropleving van wormen gezorgd. De raad om de autorun-functie simpelweg te deactiveren, leverde niets op, omdat dit pas mogelijk werd toen een betreffende Microsoft-patch beschikbaar was.

Deze voorbeelden tonen aan dat een onderneming die over waardevolle gegevens beschikt, ook vanuit andere hoeken een aanval kan verwachten.

3.6 Via lokale netwerken

Via gedeelde items in lokale netwerken kunnen ook verspreidingen plaatsvinden. Enkele wormen kopiëren zich naar alle toegankelijke gebieden. Vaak gebruiken ze daarvoor lijsten met gang-bare wachtwoorden. Conficker was ook een van de gretige gebruikers van deze zwakke plek. Daarom moeten in ondernemingen sterke wachtwoorden worden gebruikt en de goed-gekeurde software regelmatig, het liefst dagelijks, op schadelijke codes worden gecontroleerd. Enkele varianten van Rbot en Conficker gebruiken onder meer volgende logins:

```
„ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „COMPUTER“, „DATABASE“, „DB2“, „DBA“, „DEFAULT“, „GUEST“, „NET“, „NETWORK“, „ORACLE“, „OWNER“, „ROOT“, „STAFF“, „STUDENT“, „TEACHER“, „USER“, „VIRUS“, „WWWADMIN“
```

en wachtwoorden:

```
„0“, „000“, „007“, „1“, „12“, „123“, „1234“, „12345“, „123456“, „1234567“, „12345678“, „123456789“, „1234567890“, „12345678910“, „2000“, „2001“, „2002“, „2003“, „2004“, „ACCESS“, „ACCOUNTING“, „ACCOUNTS“, „ADM“, „ADMIN“, „ADMINISTRADOR“, „ADMINISTRAT“, „ADMINISTRATEUR“, „ADMINISTRATOR“, „ADMINS“, „BASD“, „BACKUP“, „BILL“, „BITCH“, „BLANK“, „BOB“, „BRIAN“, „CHANGEME“, „CHRIS“, „CISCO“, „COMPAQ“, „COMPUTER“, „CONTROL“, „DATA“, „DATABASE“, „DATABASEPASS“, „DATABASEPASSWORD“, „DB1“, „DB1234“, „DB2“, „DBA“, „DBPASS“, „DBPASSWORD“, „DEFAULT“, „DELL“, „DEMO“, „DOMAIN“, „DOMAINPASS“, „DOMAINPASSWORD“, „ERIC“, „EXCHANGE“, „FRED“, „FUCK“, „GEORGE“, „GOD“, „GUEST“, „HELL“, „HELLO“, „HOME“, „HOMEUSER“, „HP“, „IAN“, „IBM“, „INTERNET“, „INTRANET“, „JEN“, „JOE“, „JOHN“, „KATE“, „KATIE“, „LAN“, „LEE“, „LINUX“, „LOGIN“, „LOGINPASS“, „LUKE“, „MAIL“, „MAIN“, „MARY“, „MIKE“, „NEIL“, „NET“, „NETWORK“, „NOKIA“, „NONE“, „NULL“, „OAINSTALL“, „OEM“, „OEMINSTALL“, „OEMUSER“, „OFFICE“, „ORACLE“, „ORAINSTALL“, „OUTLOOK“, „OWNER“, „PASS“, „PASS1234“, „PASSWD“, „PASSWORD“, „PASSWORD1“, „PETER“, „PWD“, „QAZ“, „QWE“, „QWERTY“, „ROOT“, „SA“, „SAM“, „SERVER“, „SEX“, „SIEMENS“, „SLUT“, „SQL“, „SQLPASS“, „STAFF“, „STUDENT“, „SUE“, „SUSAN“, „SYSTEM“, „TEACHER“, „TECHNICAL“, „TEST“, „UNIX“, „USER“, „VIRUS“, „WEB“, „WIN2000“, „WIN2K“, „WIN98“, „WINDOWS“, „WINNT“, „WINPASS“, „WINXP“, „WWW“, „WWWADMIN“, „XP“, „ZXC“
```

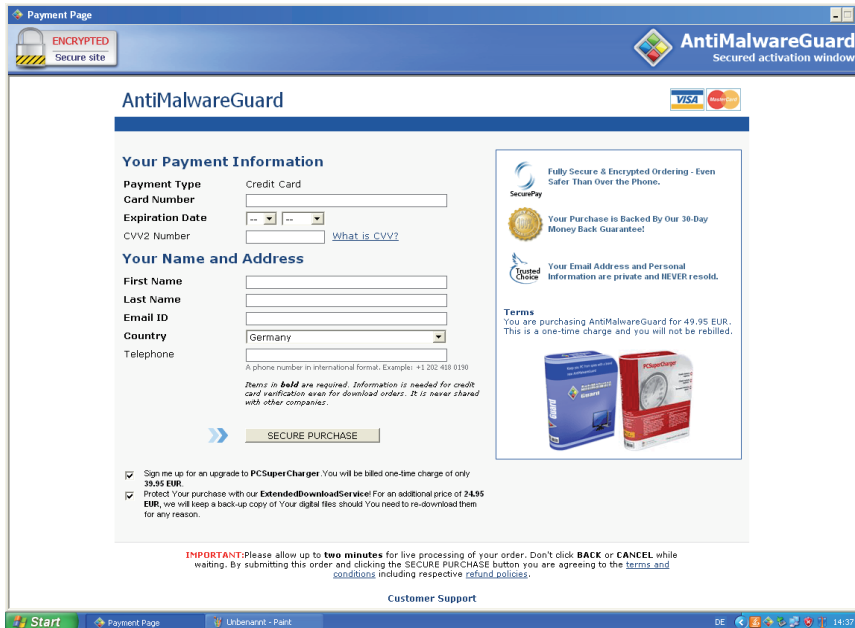
Gebruikers kunnen deze of vergelijkbare wachtwoorden, en hun Nederlandse vertaling, dus maar beter links laten liggen.

3.7 Via websites

De toegangspoort bij uitstek voor aanvallen zijn tegenwoordig websites. Er wordt gebruikgemaakt van een structureel lek in de werkwijze van virusscanners. Virusscanners controleren bestanden ofwel zodra een systeemcomponent toegang probeert te krijgen (OnAccess), of als dat gevraagd wordt (OnDemand). De controle gebeurt dus pas als de schadelijke code al als bestand beschikbaar is. Als de gegevens van de website nu via http naar de browser worden overgedragen, worden de html-codes en scriptopdrachten die daarin verwerkt zitten, eerst in het werkgeheugen van de browser geïnterpreteerd en uitgevoerd. Op een bepaald moment beslist de browser dan dat de inhoud op de harde schijf moet worden opgeslagen. En net dan kan het zijn dat de virusscanner alarm slaat. Maar dan zijn de schadelijke codes wel al uitgevoerd. Opdat een virusscanner voor schadelijke websites efficiënt kan beveiligen, moet de inhoud van de http-gegevensstroom gecontroleerd worden voor hij op de browser terechtkomt.

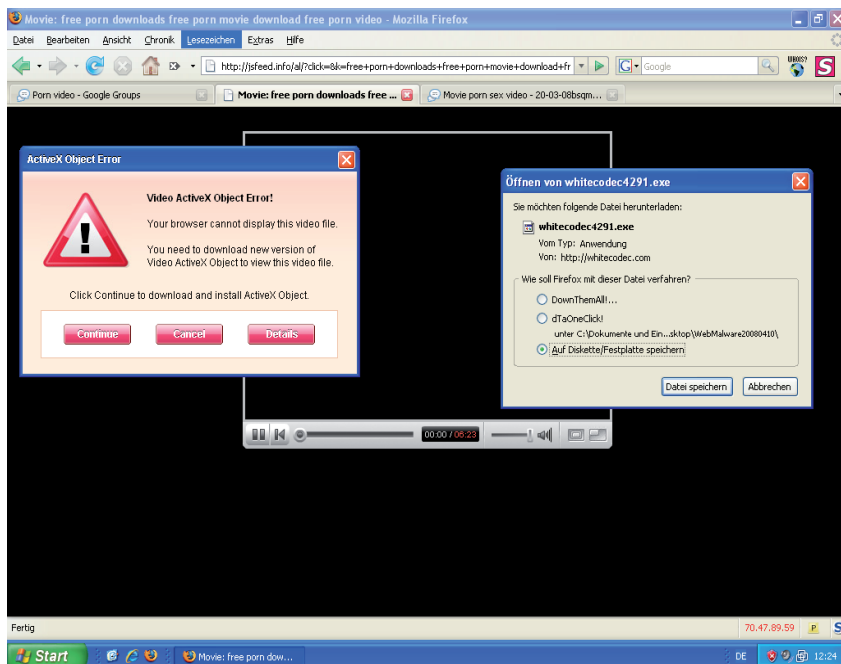
In het onderdeelje over e-mails werd al eens aangehaald dat schadelijke bestanden van websites kunnen worden gedownload. Dat gebeurt ofwel via een rechtstreekse link naar het schadelijke bestand, door het doorverwijzen naar andere links, of als de gebruiker onder valse voorwendsels wordt aangezet om het bestand met een klik op een knop of link te downloaden en uit te voeren.

Twee typische trucs waarmee gebruikers worden aangezet tot het downloaden en installeren van malware, worden hieronder kort beschreven. Zogenaamde scareware doet het slachtoffer door vervalste waarschuwingen geloven, dat zijn systeem met malware geïnfecteerd is. Om de infectie weg te kunnen werken, moet de gedupeerde zijn creditcardgegevens opgeven en zo'n 50 dollar betalen voor een "volledige versie" van een of andere scanner.



Afb. 2: Een scareware-website vraagt de creditcardgegevens van het slachtoffer

Een andere, erg geliefde truc is het slachtoffer naar een website lokken waar er schijnbaar een filmpje kan worden bekeken. Dit filmpje kan dan zogezegd een erotische inhoud bevatten of over een actueel thema gaan (natuurrampen, vliegtuigcrashes, presidentsverkiezingen, sport). Om het desbetreffende filmpje te kunnen bekijken, moet de bezoeker eerst een speciale videocodec of een nieuwere versie van de Flash Player installeren, waarin dan de schadelijke software verstopt zit. Achter deze link schuilt steeds malware die in plaats van de Flash Player op de computer wordt geïnstalleerd.



Afb. 3: Een zogenaamde videowebsite, die het downloaden van geïnfecteerde codecs vereist

Er is een aanvalstechniek waarbij het slachtoffer helemaal niets moet doen, namelijk de zogenaamde drive-by-downloads. Bij gewone downloads moet de bezoeker van een website zelf alles in gang zetten, maar bij drive-by-downloads, zoals de naam het al zegt, gebeurt dat allemaal onopgemerkt tijdens het surfen. Op een servercomputer, die wordt gecontroleerd door een malwareverspreider, worden scripts achtergelaten die allereerst controleren op welke browser en welk besturingssysteem de computer van de websitebezoeker draait. Vervolgens wordt er een schadelijke code geladen die hoort bij de betreffende combinatie. Die controleert de browser en zijn componenten op veiligheidslekken. Als het zoekresultaat positief is, wordt de schadelijke code overgedragen en worden de veiligheidslekken gebruikt om de controle over de computer over te nemen. Zulke schadelijke codes worden exploits genoemd. De meeste exploits in omloop zijn gemaakt voor Windows-computers met Internet Explorer. Maar ook de zwakke plekken van Firefox, Opera en Safari zijn niet veilig voor dit gevaar. De correcte installatie van de scripts gebeurt met tools als Mpack, IcePack en FirePack. Momenteel staan volgende veiligheidslekken bovenaan het lijstje van malware-auteurs:

- CVE 2007-0071 Adobe Flash
- CVE 2008-1309 RealPlayer
- ourgame_GLIEDown2 Internet Explorer
- CVE 2006-0003 MS06-01, MDAC
- CVE 2007-5601 RealPlayer

Als de server er eenmaal klaar voor is, moet de verspreider van malware enkel nog bezoekers naar zijn website lokken. Dat kan via spam-mails gebeuren, die met interessante nieuwtjes, speciale aanbiedingen of loterijprijzen de website een bezoekje waard maken. Maar er worden ook steeds vaker zoekopdrachten bij bekende zoekmachines als Google, Yahoo en Bing gemanipuleerd, zodat de schadelijke websites bovenaan in het zoekresultaat verschijnen. Ook een typfoutje bij de invoer van de link in de browser kan u al op weg helpen naar schadelijke sites. Twee voorbeelden: Met een schrijfwijze die lijkt op die van bekende websites worden domeinen als "mircosoft.com", "goggle.com" of "mcaffede" en nog vele anderen al jaren geregistreerd om er reclame te tonen. Nu kan er met de verspreiding van adware en malware nog meer geld

verdiend worden.

Het is echter nog efficiënter als de schadelijke code in de website van een bekend domein kan worden geïntegreerd. Als de aanvaller het voor elkaar krijgt om de webserver onder zijn controle te krijgen, wordt er met de bovenvermelde exploit-toolkits op elke website een regel toegevoegd, die schadelijke code van een andere server laadt (bijv. via IFRAME of SCRIPT). Er

bestaan nu ook al tools voor aanvallen op webserver. Die proberen met woordenboekaanvallen het wachtwoord van de beheerder te kraken. Op soortgelijke wijze worden veiligheidslekken in courante websoftware, zoals Content Management-systemen, blog- en forumsoftware en beheertools gebruikt, om de webserver over te nemen. In de meeste gevallen zijn de aanvallen niet beperkt tot een webserver, maar gebeurt dit en masse en automatisch. Het gevolg: Niet alleen in de donkere hoekjes van het internet loeren schadelijke codes op hun prooi, maar elk domein kan een potentieel gevaar bevatten.

Een andere mogelijkheid bieden de reclame-elementen op veelbezochte websites. Bijna alle populaire domeinen gebruiken reclame als manier om geld te verdienen met een website. De reclamebanners worden veelal via IFRAME op de pagina ingevoegd, zodat de gebruiker geen invloed heeft op de daar getoonde inhoud. Het is de taak van de adverteerder, de inhoud van de geleverde reclameboodschap te controleren. Dat is echter gemakkelijker gezegd dan gedaan. De schadelijke scripts, gemaakt met MPack of vergelijkbare tools, zijn in hoge mate gecamoufleerd en gecodeerd (het aanmaken van polymorfe schadelijke codes is ook mogelijk met scripttalen). Zo slagen schadelijke codes erin zich met legitieme websites te verbinden. Zo'n 80 % van alle drive-by-infecties gebeuren via legitieme websites.

Schadelijke codes kunnen echter ook worden overgedragen, zonder een webserver te kraken. Links op forums, blogs of e-mails kunnen ook schadelijke codes bevatten, die dan op de opgeroepen pagina worden uitgevoerd. Het interactieve "deelname"-internet beschikt over talloze discussieforums en wiki's, waarin de deelnemers zelf iets kunnen schrijven of bestanden kunnen invoegen. Op die plaatsen kan er ook wel eens malware geüpload worden of een link naar een schadelijke website worden geplaatst. Eén auteur is er een keer in geslaagd om op Wikipedia, in het artikel over de Blaster-worm, een link naar een removal-tool in te voegen, die later een Trojaans paard bleek te zijn. Op zulke forums zijn dus ook mensen (of hun machines) actief, die geen goede bedoelingen hebben. En met ontelbare gestolen identiteiten hebben ze er geen enkele moeite mee om tot de meeste plaatsen toegang te krijgen, waar ze dan heel goed verstopt zitten.

De schadelijke code hoeft niet noodzakelijkerwijs op een server te worden geplaatst. Een link op een willekeurige website is al genoeg om de schadelijke code te bevatten. Die leidt dan verder naar de doelpagina. Zo'n aanval wordt ook wel cross-site scripting (XSS) genoemd. XSS is mogelijk als de invoer van een gebruiker op een volgende pagina opnieuw wordt getoond en die invoer niet op uitvoerbare inhoud wordt gecontroleerd. Als bijvoorbeeld de naam van een formulier in de volgende bestelling opnieuw wordt aangegeven, is dat erg handig. Als een aanvaller in plaats van zijn naam een JavaScript-code invoert, wordt die door de browser uitgevoerd (behalve als deze wordt uitgefilterd). Een voorbeeld van cross-site scripting: In een formulier wordt een naam gevraagd. In plaats van zijn eigen naam in te geven, voert de aanvaller volgende code in:

```
<SCRIPT>alert(„You`re pwned“)</SCRIPT>
```

Na het versturen van het formulier wordt deze code op een volgende pagina niet weergegeven maar uitgevoerd. In het geval van dit voorbeeld verschijnt er een waarschuwing. Een echte aanval bevat gevaarlijkere code.

Zelfs als de formuliergegevens worden gefilterd, kan er nog steeds een schadelijke code rechtstreeks in de link van de opgevraagde pagina worden geschreven. En dat gebeurt zo:

```
http://www.myserver.dom/site.php?name=<SCRIPT>alert(„You`re pwned“)</SCRIPT>
```

Een dergelijke link kan zich achter iedere tekst verstoppen die op een forum of blog wordt geplaatst. Nog geniepiger is het als dergelijke XSS-links in de zoekresultaten van Google opduiken. De auteurs van malware optimaliseren de schadelijke blog-items voor de zoekrobot van Google. Maar hoewel Google hard werkt om dergelijke XSS-links op te sporen, krijgen auteurs met een paar camouflagetechnieken toch telkens weer de bovenhand.

Met de vele nieuwe mogelijkheden die Web 2.0 biedt, gaat het niet anders. Als u op het idee komt om de bedreiging af te slaan door de actieve inhoud of scripttalen niet meer toe te laten in de browser, sluit u ook de deur voor de ontelbare mogelijkheden van Web 2.0. Jammer genoeg zet een groot aantal van deze nieuwe functies wel de deur open voor misbruik en verhogen ze de kans op mogelijke veiligheidslekken. Eind 2005 verschaftte de XSS-worm van Samy hem via cross-site scripting (XSS) binnen 18 uur meer dan een miljoen vrienden op op Myspace. Cross-site scripting wordt nog erg onderschat.

Domeinen die schadelijke codes verspreiden, vindt men dus niet alleen terug in de duistere hoeken van het internet, op populaire downloadportalen (zoals Rapidshare) en op gehackte internetpagina's. Tegenwoordig zijn legitieme websites en zoekresultaten van Google ook niet meer zo veilig. In principe kunnen op elke website schadelijke codes verstopt zitten.

4. Hoe verloopt een typische infectiegolf

De meeste aanvallen door cybercriminelen hebben een vast patroon. Een typische infectie is de afgelopen jaren sterk veranderd. In het verleden waren er bijvoorbeeld de wormen NetSky en MyDoom die grote bijlagen hadden met monolithische schadelijke software met veel geïntegreerde functies. De laatste jaren komen vele kleine, compacte en zeer gespecialiseerde modules op. Die kunnen indien nodig flexibel worden geladen. De infectie gebeurt in meerdere fasen. Na de ontwikkeling van de schadelijke software en de keuze van een mogelijk slachtoffer, wordt de eigenlijke aanval uitgevoerd. Vervolgens kunnen de geïnfecteerde systemen, die voortaan onder de controle van de aanvaller staan, voor allerlei criminele activiteiten gebruikt en misbruikt worden.

4.1 De voorbereiding

Allereerst moet de schadelijke software, die men wil verspreiden, worden ontwikkeld. Dat is niet bij elke infectiegolf nodig. Wanneer de auteur van malware een schadelijke code eenmaal heeft ontwikkeld, kan hij hiermee met behulp van runtime packers, andere compilers en hulpprogramma's ter camouflage voor verschillende golven nieuwe varianten aanmaken, zolang tot ze door de gebruikelijke antivirusprogramma's niet herkend worden. Als de schadelijke code ervoor zorgt dat de virusscanner op de geïnfecteerde computers kan worden herkend, dan is het al voldoende om een versie in te zetten die de gebruikelijke virusscanners niet herkennen. Wie zijn handen daar niet zelf aan wil vuil maken, kan in de juiste "underground-forums" men-sen vinden, die de betreffende diensten gegarandeerd kunnen aanbieden voor een redelijke prijs.

Is de schadelijke software klaar, dan moet de aanvaller een (of meerdere) verspreidingsweg(en) kiezen. Zo kan hij bijvoorbeeld het schadelijke item door een automatisch uitgevoerde aanval

op een veiligheidslek doorvoeren. In dat geval merkt het slachtoffer helemaal niets van de aanval of infectie. Zijn voorkeur kan natuurlijk ook uitgaan naar een van de gebruikelijke trucs om de gebruiker er zelf toe aan te zetten de schadelijke software op te starten. In het eerste voorbeeld heeft de aanvaller een exploit nodig die de computer kaapt. In het tweede moet hij over een website en/of aanlokkelijke e-mail of instant message beschikken, die de gebruiker ertoe aanzet een bestand te downloaden en uit te voeren. Als het schadelijke item op een website moet worden gehost, dan moeten de domeinen geregistreerd worden en de bijpassende bestanden daar geplaatst worden. Voor de meeste van deze activiteiten bestaan er eenvoudig te gebruiken hulpprogramma's.

4.2 Uitvoering

Nadat de computer is overgenomen, wordt meestal eerst een Trojaans paard-downloader gestart. Die zorgt ervoor dat de schadelijke bestanden de computer kunnen binnendringen en worden opgestart. Eerst en vooral krijgt de auteur van de aanval informatie over het resultaat van de infectie en over het gekaapte systeem. Dan worden de beveiligingsinstellingen van de geïnfecteerde pc's uitgeschakeld. De computer is nu weerloos tegen verdere malware-activiteiten. Vervolgens wordt nog meer malware op de computer geladen. Hiervoor kunnen meerdere schadelijke bestanden worden gebruikt.

In de meeste gevallen is het eerste schadelijke bestand dat gedownload wordt, een backdoor. Die kan bijvoorbeeld met een rootkit worden verstopt en zo ongemerkt op de achtergrond lopen. Door dit achterpoortje krijgt de geïnfecteerde computer een nieuwe eigenaar, die nu naar believen met de computer kan werken. Zo kan dankzij deze backdoor de computer via IRC, P2P of http met vele andere pc's over de hele wereld worden gecoördineerd. Op die manier gaat een computer deel uitmaken van een soms enorm zombieleger. Na de installatie van de backdoor krijgt het geïnfecteerde systeem een grondigere inspectie en beslist de aanvaller wat hij met de computer wil doen. Met behulp van spyware worden de gekraakte computers gecontroleerd op waardevolle gegevens en/of met adware uitgerust. Beschikt de computer over een goede verbinding met het internet, kan hij voor het versturen van spam worden gebruikt. Andere mogelijkheden zijn het aanbieden van downloads voor illegale bestanden en het hosten van phishing- of malware-websites.

4.3 De geïnfecteerde computer gebruiken

Als de zombiecomputer van een botnet voor het versturen van spam zal worden gebruikt, zet de botnetbeheerder via een backdoor een malware-pakket op de geïnfecteerde computer. Dat bevat, onder andere, de e-mailtemplate, een lijst met e-mailadressen en de software voor het versturen van e-mails. Zodra het bestand is geïnstalleerd, wordt het opgestart en kan het verzenden beginnen. Nadat alle e-mails verstuurd zijn, worden de software en alle gegevens verwijderd van de computer. Alleen de backdoor blijft goed verstopt achter en wacht op verdere bevelen.

5. Hoe kunt u zich beveiligen

Het beveiligen van bedrijfscomputers tegen malware is maar een onderdeel van de IT-beveiliging, die altijd moeten worden beschouwd als de IT-beveiliging van de hele onderneming. IT-beveiliging is geen toestand maar een proces. Elke onderneming heeft risicogebruikersgroepen of -onderdelen die een bepaalde bescherming nodig hebben. In dit proces moet elke onderneming voor zich in allerlei opzichten een beslissing nemen om tot een individuele oplossing te komen.

Om te beginnen wordt beveiliging tegen malware gelinkt aan het gebruik van technische processen, die bescherming (zouden moeten) bieden tegen de gedefinieerde gevaren. De belangrijkste technische maatregelen zijn:

- **Virusbeveiliging**
Moet zowel op servers als op clients worden geïnstalleerd. Deze moeten bovendien de http-gegevensstroom en, indien nodig, de gegevens van chatsessies (ICQ, IRC) op schadelijke codes controleren.
- **Spambeveiliging**
Aangezien e-mails in plaats van bijlagen alleen nog maar links naar schadelijke websites bevatten, is de spambeveiliging tegelijkertijd ook een beveiliging tegen malware.
- **Firewall, Intrusion Detection/ Prevention**
Gegevens uit het netwerkverkeer kunnen worden gebruikt om gangbare aanvallen van internetwormen op te sporen en te verhinderen.

Er zijn nog andere technische maatregelen die een bijdrage leveren. De vanzelfsprekende veiligheidsmaatregelen worden aangevuld door patch management, virtualisatie van software, gebruikersrechten op bedrijfscomputers, toegangscontroles voor bestanden en bereiken van het netwerk, en nog vele andere voorzorgsmaatregelen. We zullen en kunnen hier niet dieper ingaan op de verschillende mogelijkheden.

Jammer genoeg zijn technische maatregelen niet voldoende om het netwerk van een onderneming efficiënt te beschermen. Medewerkers moeten de veiligheidsmaatregelen aanvaarden en ondersteunen. De met de directie afgesproken richtlijnen over de omgang met computers, gegevensdragers en andere beveiligingsrelevante informatie vormen hiervoor het kader. Juridische en ethische randvoorwaarden moeten daarbij in het achterhoofd worden gehouden. De beveiligingsmaatregelen moeten doorschemeren in de structuur van de organisatie. Zo moeten er bij overtredingen tegen de richtlijnen sancties horen. Last but not least moeten alle medewerkers worden geïnformeerd over de gevaren op het internet en in het bedrijfsleven. Wanneer waakzame medewerkers de technische maatregelen aanvullen, kan een bedrijf erin slagen zijn computers vrij van malware te houden.