

Anneleen Dammekens
Attaché

Brussel, 25 november 2011

DOCUMENT

Commissie Bedrijfsbeveiliging

Hoe zich beschermen tegen de criminele cyberarchitectuur

Samenvatting

ICT-middelen maken ons het leven een stuk eenvoudiger. De Federale Gerechtelijke Politie wijst echter op de risico's verbonden aan het gebruik van ICT. ■

1. Algemene trends anno 2011

Onze wereld evolueert meer en meer in de richting van een e-maatschappij: iedereen is altijd en overal bereikbaar, een ongelofelijke hoeveelheid al dan niet beveiligde informatie is altijd en vanaf eender welke locatie consulteerbaar, meer en meer communicatie verloopt over het internet,...

Kortom de computer en het internet zijn vandaag de dag het geprivilegieerde medium van vele personen en bedrijven. De voordelen van ICT zijn dan ook talrijk: grote afstanden worden uitgevaagd, communicatie kan sneller en efficiënter dan ooit,...

Juridisch en Fiscaal
Departement
T + 32 2 515 08 38
F + 32 2 515 09 99
ada@vbo-feb.be

Helaas is er ook een keerzijde aan deze digitale medaille: een snel evoluerende cybercriminaliteit. Als gevolg hiervan is het internet niet alleen een zegen, maar meteen ook de achillespees van elk computersysteem.

Samen met de Gerechtelijke Politie, wil het VBO de aandacht van de bedrijven vestigen op het belang om zich bewust te zijn van deze cybercriminaliteit en van de risico's die verbonden zijn aan het gebruik van een ICT-systeem.

Vaak is het management van een bedrijf nog het meest kwetsbaar. Managers beschikken immers vaak over de belangrijkste gegevens en know how, maar



besteden soms omwille van gebrek aan tijd en/of kennis niet altijd even veel aandacht aan de toegankelijkheid van hun computer of ander ICT-materiaal. Op die manier kunnen ze een begeerde prooi worden voor cybercriminelen.

2. Cybercriminaliteit en cybercriminelen anno 2011

Cybercriminelen maken gebruik van de kwetsbaarheid van het internet en van het gebrek aan bewustzijn van de meeste internetgebruikers. Hiervoor heeft elke cybercrimineel een ander motief. De ene wil snel rijk worden op de kap van een ander. De andere krijgt een kick van het gevoel oppermachtig te zijn op het internet. Nog anderen willen eenvoudigweg de e-maatschappij destabiliseren omdat ze het kunnen.

Cybercriminaliteit neemt dan ook diverse vormen aan: internetfraude, spamming, hacking, DDoS¹,...

Ook de bedrijven blijven niet gespaard. Via allerlei manipulaties zoals malware, botnets, key loggers, enz. proberen cybercriminelen hetzij serversystemen te blokkeren, hetzij belangrijke (bedrijfs)informatie te achterhalen.

3. Waarom is het zo moeilijk om cybercriminaliteit te bestrijden?

De kennis en mogelijkheden van de cybercriminelen evolueren enorm snel. Cybercriminelen zijn steevast echte computerexperten. Om een voorbeeld te geven: een virus dat op een computer terechtkomt wordt elke 15 minuten geupdate via het internet. Het hoeft geen betoog dat een antivirusprogramma dat éénmaal per dag een update krijgt, daartegen niet is opgewassen.

De bestaande wetgeving is niet aangepast aan de snelheid en de flexibiliteit waarmee in cyberspace gewerkt kan worden. De politie en het gerecht beschikken op basis van de huidige wetgeving dan ook niet over voldoende mogelijkheden om doeltreffend te kunnen reageren tegen cybercriminaliteit. De aanpassing van deze regelgeving is dus noodzakelijk.

Het is echter moeilijk om de wetgever hiervan te overtuigen omwille van het gebrek aan correcte cijfers m.b.t. het aantal gevallen van cybercriminaliteit. Hiervoor zijn verschillende oorzaken. Enerzijds legt tot op heden slechts een klein percentage van

¹ **Distributed Denial of Service (DDoS)** attack is een Denial-of-Service-aanval op een computer of netwerk waarbij met een aantal computers, vanaf vele verschillende plaatsen op de wereld, -bestuurd vanaf een centraal punt-, zoveel verbindingsverzoeken naar de server van een of meer sites verstuurd worden, dat de service ervan tijdelijk niet beschikbaar is, of de server zelfs crasht.



de slachtoffers van cybercriminaliteit klacht neer. Vaak opereren cybercriminelen daarenboven vanuit het buitenland (de zogenaamde “safe haven landen”) en blijven zo buiten het bereik van de politie die door haar landsgrenzen gebonden is. Tenslotte zijn er te weinig onderzoekers bij de politie die voldoende gespecialiseerd zijn om een tegengewicht te vormen voor de expertise van de cybercriminelen.

4. Concluderend: enkele oplossingen

Om op te kunnen tegen de snel evoluerende cybercriminaliteit, dienen we als maatschappij de handen in elkaar te slaan. Zowel de overheid als de privé-sector kunnen werken aan een betere detectie van cybercriminaliteit door de opmaak van een lijst van de infrastructures die een groot risico lopen en door een consequente rapportering aan CERT²/de politie en een grondige bewijsgaring voor elk ernstig geval van cybercriminaliteit te verzekeren.

Op die manier zullen we een steeds beter overzicht krijgen van het cybercriminaliteitslandschap. Op basis daarvan kan dan effectieve actie ondernomen worden om de criminele cyberinfrastructuur te verzwakken en te ontmantelen.

Tenslotte dient preventief gewerkt te worden aan het bewustzijn en de responsabilisering van zowel individuen als bedrijven. Zo is bijvoorbeeld een goed paswoord geen overbodige luxe. Je paswoord regelmatig wijzigen is dat evenmin.

² Computer Emergency Response Team: <https://www.cert.be>