Veiligheidstip: Bescherming tegen email virus

Op regelmatige tijdstippen duiken er email virussen op. Zo kregen onlangs een aantal BIN-leden een Engelstalige mail binnen met een link naar een geïnfecteerde website. Gelukkig hadden de meeste gebruikers een degelijke antivirus op hun computer zodat deze problemen snel ontdekt werden.
Niettemin blijft het opletten geblazen! Als BIN coördinator moet je extra waakzaam blijven.

De psychologie van een computervirus

Een computervirus heeft functioneel zeer veel weg van een menselijk virus. Het is immers per definitie een klein en onopvallend stuk programmeercode dat twee basisdoelen voor ogen heeft:
* **DOEL 1. Hoe kan ik best overleven?** Met andere woorden: hoe kan ik zoveel mogelijk opgestart worden zodat ik mijn programmeercode zo snel mogelijk kan verspreiden over zoveel mogelijk computers zonder opgemerkt te worden?
* **DOEL 2. Hoe kan ik best mijn taak volbrengen?** Virussen hebben altijd één of meer redenen van bestaan. Vroeger probeerde een virus vaak gewoon je computer stuk te maken door alle gegevens te wissen of te versleutelen (bv. cryptovirussen) maar tegenwoordig zijn programmeurs van virussen vooral uit op identiteitsgegevens, bankkaartgegevens, ... (bv. spyware) of op het gebruik van jouw computer om in een gezamenlijke aanval tegen welbepaalde doelen te gebruiken (bv. cybercrime bots).

Email om voort te planten

Email is een prima manier om jezelf als virus voort te planten naar andere computers.
Het versturen van een email vraagt immers zeer weinig programmeercode, het kan zeer onopvallend in de achtergrond gebeuren en email is ook per definitie een medium dat snel en veel computers met elkaar kan 'verbinden'.
Wanneer een nietsvermoedende gebruiker een email opent waarin een virus verscholen zit **als bijlage of als weblink**, dan nestelt het virusprogramma zich ergens in het actieve geheugen van de computer en bepaalt dan de beste strategie om te overleven. Het zorgt er o.a. voor dat het bij elke opstart van uw computer opnieuw geactiveerd kan worden zodat het zijn taken kan verder zetten.
Daarna gaat een mailvirus specifiek het adresboek van uw email uitlezen om zichzelf -verdoken in een emailbericht- opnieuw uit te sturen en zo weer andere computers te infecteren.
Maar de pret zou snel gedaan zijn, mocht iedereen onmiddellijk zien om welke email het gaat of vanuit welke computer die geïnfecteerde emails komen.
Daarom is een mailvirus intelligent genoeg om zichzelf steeds te versturen onder een andere naam. Het gaat vaak een willekeurig mailadres uit uw adresboek gebruiken om als verzender van de email te gebruiken (dat heet 'spoofing'). Vaak is het zelfs zo dat u er van uit mag gaan dat het verzender-adres in een geïnfecteerde email, net niet de bron is van de infectie.

Men kan proberen nagaan welke adressen allemaal de email hebben gekregen en op basis daarvan proberen achterhalen wie al die namen in zijn of haar adresboek kan hebben staan. Zelden verstuurt een email zich ook naar zichzelf. Een naam die ontbreekt is dus steeds een potentiële bron van infectie.
En wat de inhoud van de mail betreft zijn virussen intelligent genoeg om stukken tekst van het internet te plukken of om woorden lichtjes van plaats te veranderen zodat een antivirus ze niet snel kan detecteren. Wanneer je dus **een mail krijgt met wartaal** of met een nietszeggende boodschap, dan mag je er eigenlijk van uitgaan dat die drager is van een virus (als bijlage of als weblink).

Wat nu!

Eens een computer geïnfecteerd is, is het zeer moeilijk om zonder grondige informatica-kennis de omgeving echt 'clean' te krijgen. Een virus gaat er immers alles aan doen om ervoor te zorgen dat er geen enkele antivirus meer geïnstalleerd kan worden.
Onze raad is dan ook om uw computer **volledig uit te schakelen en binnen te brengen** in een gespecialiseerde computerfirma. Zij zullen de harde schijf uit uw computer verwijderen en als een tweede harde schijf aan een andere, sterk beveiligde computer hangen die alle virus-restanten zal proberen verwijderen.
Vergeet echter niet dat een virus vaak ook onherroepelijke schade aanbrengt aan 'gewone ' programma's zoals Word of Excel. Na een grondige cleaning krijg je 'kaas met gaatjes' terug. Waar een virus werd weggehaald, blijft gewoon blanco ruimte over. Hierdoor gaan bepaalde ponderdelen van programma's niet of onvolledig werken. Vaak is dan ook een volledige herinstallatie noodzakelijk.

Enkele TIPS voor BIN-coordinatoren

BIN-leden zitten vaak met elkaars contactgegevens in hun email-bestanden. Al te vaak heeft een BINco ooit zelf snel een mail gestuurd vanuit een mailprogramma naar een deel of zelfs de volledige groep. Daardoor kan een virus makkelijk iedereen van een BIN tegelijk aanvallen.
Indien je een email naar je BINleden wenst te versturen, hou rekening met de volgende tips:
1. Zorg dat je een professioneel (liefst betalend) antivirus programma hebt (bv. BitDefender, ESET, TrendMicro, Kaspersky, ...) dat minstens één keer per week updates krijgt. Vermijd de 'gratis' antivirus programma's (bv. MS Security Essentials, AVG, AVAST, ...) want deze beschermen gewoon onvoldoende.
2. Zet meerdere email adressen van bestemmelingen nooit in het 'AAN...' veld of in het 'CC...' veld van je mailprogramma maar in het 'BCC-veld' (Blind Carbon Copy). In Outlook kan je het BCC-veld zichtbaar maken door op de knop 'CC...' te drukken. Dit vermijdt trouwens 'kettingreacties' waarbij iedereen naar iedereen blijft sturen.
3. Stuur nooit een email naar meer dan 25 contacten tegelijk. Hierdoor zorg je dat je uit de blacklisting lijsten van providers blijft?
4. Stuur bij voorkeur enkel tekst-email (zonder afbeeldingen, kleuren, lettertypes of weblinks) in plaats van html-email.