Virussen in mobiele omgev

E-mail lezen via de mobiele telefoon. Het koppelen van de PDA aan de PC op het werk. Het gemak dient de mobiele werknemer van vandaag. Besmetting met een specifiek op deze populaire communicatiemiddelen gericht virus is echter even gemakkelijk. Volgens IT-specialisten neemt de omvang van virussen voor GSM en PDA explosief toe. Het is dan ook zaak de kostbare hebbedingetjes afdoende te beveiligen.

Het aantal virussen dat het specifiek heeft gemunt op Personal Digital Assistants (PDA) en de nieuwste generatie mobiele telefoons zal de komende tijd explosief toenemen. Ook de huidige generatie WAP-telefoons loopt gevaar. De nieuwste types mobiele telefoons herbergen een flink aantal functies van een PDA. Deze toestellen communiceren zowel via de infraroodpoort (IR poort), docking stations, internet als draadloos via in opmars zijnde GPRS-netwerken. Hoewel er nu nog grote verschillen bestaan tussen de besturingssystemen en communicatiemethodes van de mobiele hebbedingetjes, gaan de ontwikkelingen op dit gebied zeer snel. De kans op besmetting groeit evenredig snel.

Management-summary

De nieuwste generatie mobiele telefoons is geschikt om mee te e-mailen, websites te bezoeken en voor benadering van documenten op bedrijfsnetwerken. Het aantal virussen dat zich specifiek richt op populaire communicatiemiddelen als GSM of PDA neemt fors toe. Bij besmetting werken soms alle programma's op de telefoon of PDA niet meer of wordt continu een hulpdienst gebeld. Het is dan ook zaak dat op het netwerk multiplatform antivirus software wordt geïnstalleerd en dat mobiele telefoons en PDA's worden bechermd tegen virussen, ook als zij hierdoor trager werken.

Virus, trojan of worm

Een computervirus is een klein computerprogramma dat meestal een saboterende werking heeft. Een groot aantal virussen 'verbergt' zichzelf in andere programma's om van daaruit ongezien de juiste werking van de software en het computersysteem te saboteren. Ook probeert het virus zichzelf te vermenigvuldigen. Dit om zijn besmettend werk te kunnen in- en voortzetten. Wie denkt dat het hierbij alleen gaat om Windows-systemen heeft het mis. De nieuwe generatie mobiele telefoons en PDA's gebruikt als operating system onder meer EPOC, PalmOS, Windows CE en Symbian. Deze besturingssystemen starten op vanuit een ROM-chip in plaats van een harddisk, en slaan hun gegevens op in een Flash-rom. De Flash-rom is het enige deel van een mobiele telefoon en/of PDA dat beschrijfbaar is en dat dus het risico loopt dat er zich een virus of trojan (horse) nestelt.
Een zelfstandig programma dat zich voordoet om een bepaalde nuttige en door de gebruiker gewenste taak te verrichten, maar dat ook saboterende acties verricht die de gebruiker niet wenst, wordt *trojan* genoemd. De naam verwijst naar het Trojaanse paard waarmee de Griekse soldaten werden binnengesmokkeld in Troje om zodoende de stad te veroveren. De term trojan wordt soms ook gebruikt voor programma's die virussen 'lanceren'.
Het zijn dan zelfstandige programma's die opzettelijk een virus bevatten en die dit virus in een computersysteem kunnen loslaten.
Zuiver technisch gesproken is een worm geen virus. Wormen verspreiden en vermenigvuldigen zichzelf gelijk aan een virus. Het verschil is dat een worm zich verplaatst van computer naar computer (en niet van bestand naar bestand), tot het volledige systeem is besmet. Wormen kopiëren zichzelf van de ene naar de andere computer via een netwerk, bijvoorbeeld via e-mail, ICQ of GPRS. Omdat wormen geen menselijke tussenkomst nodig hebben om zich te vermenigvuldigen, kunnen ze zich veel sneller verspreiden dan computervirussen.
Kwaadaardige software wordt ook wel *malicious code* genoemd. Virussen, trojans en wormen zijn hiervan voorbeelden. Malicious code is vaak geschreven om de veiligheid van systemen in gevaar te brengen.

WAP, WML en WML-script

Zoals GSM een standaard is voor mobiele telefonie, zo is WAP *(Wireless Application Protocol)* een standaard die het mogelijk maakt om informatie leesbaar te maken op mobiele telefoons en PDA's. Om van WAP gebruik te kunnen maken, is een 'micro browser' nodig. Deze is vergelijkbaar met een normale webbrowser, zoals de Internet Explorer. De micro browser is ingebouwd in de mobiele telefoon. Wereldwijd wordt er steeds meer informatie aangeboden in het WAP-formaat.
WML staat voor *Wireless Markup Language* en is onderdeel van het Wireless Application Protocol. WML wordt net als HTML gebruikt om internet webpagina's te maken en is integraal onderdeel van WAP. WML

ing

wordt gebruikt om het formaat en de presentatie van tekst te specificeren. Het heeft een bijhorende scripttaal WML-script dat veel weg heeft van Java-Scripts. Ook kunnen via WML functies worden aangesproken als het telefoonboek en sms. Met name door deze functies is het mogelijk om ongewenste zaken op de huidige generatie mobiele telefoons te laten plaatsvinden. Virussen, maar ook andere vormen van malicious code, kunnen hiervan gebruik maken.
Het succesvolle Symbian OS, wat onder andere wordt gebruikt in Nokia toestellen, is zo open dat alle Application Programming Interfaces (API's) eenvoudig kunnen worden benaderd. Ook kunnen er programma's in de achtergrond draaien. Een goede voedingsbodem voor virussen en malicious code.

Praktijk Het bekende 911-virus richt zich specifiek op I-mode telefoons. Dit virus belt het noodnummer 911. In Japan raken hierdoor de telefoonsystemen van de hulpdiensten overbelast. Het 911-virus is een script virus dat bij het bezoeken van een website via een mobiele telefoon of PDA een script in werking stelt dat de telefoons automatisch 110 (het alarmnummer van Tokio) laat bellen.
In het afgelopen halfjaar zijn er virussen, trojans en wormen gesignaleerd voor nieuwe generatie mobiele telefoons en PDA's. Deze worden vaak geschreven in generieke talen, soms in een 'taal' voor één bepaalde PDA en/of telefoon. Liberty Crack is een van de virussen voor EPOC, het operating system voor Psion PDA's. Het virus/trojan doet zich voor als een gratis versie van Gambit Studios Liberty Gameboy emulator. Zodra het virus wordt geactiveerd, kan het alle programma's op de zakcomputer verwijderen. Ook het besturingssysteem van Palm, (PalmOS) wordt getroffen door virussen. Zo is er Phage.936, een virus dat alle programma's in een Palm PDA beschadigd. Het zeer kleine programmaatje is in staat zichzelf te repliceren. Het gebruikt daarvoor de IR poort. Na besmetting weigeren alle programma's in de Palm dienst. Bij het opstarten van een programma verschijnt enkel een grijs scherm. Een besmette Palm kan worden 'gereanimeerd' door de beschadigde programma's te verwijderen en ze opnieuw van nul of van een back-up te installeren.

Antivirus Besmettingen vinden meestal plaats door wisselende contacten met andere, besmette computers en/of het gebruik van programmatuur van onduidelijke afkomst. Een PDA en/of telefoon kan 'besmet' raken via een attachment aan een e-mail of door synchronisatie met systemen die veelal al eerder zijn besmet. Virussen kunnen zich verplaatsen via internet, GPRS, maar ook via de IR poort, een cradle, docking station of tijdens PDA-synchronisatie met een PC. Maar ook door het surfen naar een verdachte WAP-site met daarop WML-scripts.
Bijna alle leveranciers van antivirus software hebben speciale versies ontwikkeld voor PDA's. Voor netwerken is het belangrijk dat multi-platform antivirus software wordt geïnstalleerd. Uiteraard is het regelmatig, liefst dagelijks, updaten van de software belangrijk. En als meest belangrijke geldt: gebruik bescherming tegen virussen! Ook als hierdoor de PDA of de GSM trager gaan werken.

Gebruik bescherming tegen virussen, ook als hierdoor de PDA of GSM trager gaat werken.

■ Ronald Eygendaal CSSM CISMP

Bronnen:
'Malicious Threats to Personal Digital Assistants.' Eric Chein, Symantec.
'Wap and viruses can your mobile phone get infected?' Mikko Hyppönen, F-Secure.

Wie is Ronald Eygendaal?

Ronald Eygendaal CSSM CISMP is werkzaam voor Getronics PinkRoccade als security consultant en heeft ruim twaalf jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder. Hij is tevens voorzitter van de vakgroep informatiebeveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN).