Ook mobiele terminals bedreigd door virussen

De toenemende integratie van PDA's en smartphones in bedrijfsnetwerken vergroot de dreiging van virussen voor organisaties. De eerste mobiele varianten zijn inmiddels al gesignaleerd. Bedrijven zullen dus maatregelen moeten nemen om hun mobiele systemen te beschermen tegen virussen, trojans en wormen.

Door Ronald Eygendaal

Op dit moment is er een klein aantal virussen bekend dat het vooral heeft gemunt op PDA's en de nieuwe generatie mobiele telefoons maar dat zelfs WAP-telefoons kan infecteren. De nieuwe generatie mobiele telefoons herbergt heel wat functies van PDA's. De toestellen communiceren draadloos via infrarood of Bluetooth, worden gesynchroniseerd via een *docking station* of zoeken mobiel verbinding met het internet, al dan niet via het GPRS-netwerk. De ontwikkelingen gaan zeer snel en gelijk aan deze trend zal ook het aantal softwarevirussen voor mobiele *operating systems* (OS) komend jaar explosief toenemen. Nu verschillen de besturingssystemen en communicatiemethodes nog teveel van elkaar om echt gevaar te lopen, maar hier komt snel verandering in. Zodra de uitwisseling van bestanden is gestandaardiseerd, zullen de mobiele virussen losbarsten.

Flash-ROM

Kwaadaardige software zoals virussen, trojans en wormen wordt ook wel *malicious code* genoemd. De softwarescripts zijn vaak geschreven om de veiligheid van systemen in gevaar te brengen. Wie denkt dat het hierbij alleen om Windows-systemen gaat, heeft het mis. De nieuwe generatie mobiele telefoons en PDA's gebruikt onder meer EPOC, PalmOS, Windows CE en Symbian als OS. De mobiele OS staat niet op een harddisk zoals bij computers, maar start vanaf een ROM-chip. De gegevens worden vervolgens opgeslagen in een Flash-ROM, het enige gedeelte van een mobiele telefoon of PDA dat beschrijfbaar is. Juist dit geheugen is gevoelig voor virussen of trojan horses.

Wireless Markup Language (WML) is een onderdeel van WAP en wordt net zoals HTML gebruikt om webpagina's te maken. WML specificeert het formaat en presentatie van tekst. De bijhorende scripttaal WMLScript heeft veel weg van Java-scripts. Ook kunnen functies zoals het telefoonboek en SMS via WML worden aangesproken. Virussen maar ook ander vormen van malicious code kunnen hier gebruik van maken. Zo is het succesvolle Symbian OS, wat onder andere wordt gebruikt in Nokia-toestellen, zo open dat alle *Application Programming Interfaces* (API's) eenvoudig kunnen worden benaderd. Ook kunnen er programma's op de achtergrond meedraaien, wat een goede voedingsbodem vormt voor virussen en malicious code.

Scripts

Een computervirus is een klein computerscript dat meestal een saboterende werking heeft. Een groot aantal virussen verbergt zich in andere programma's om vanuit daar ongezien de juiste werking van de software en het computersysteem te saboteren. Ook probeert het virus zichzelf te vermenigvuldigen om zijn besmettend werk te kunnen voortzetten.

Een trojan horse is een zelfstandig programma dat doet alsof het een bepaalde nuttige taak verricht, maar eigenlijk ongewenste saboterende acties onderneemt. De term trojan wordt soms ook gebruikt voor programma's die virussen lanceren. Het gaat hierbij om zelfstandige programma's die opzettelijk een virus bevatten en dus dit virus in een computersysteem kunnen loslaten.

Wormen zijn zuiver technisch gesproken geen virussen maar verspreiden en vermenigvuldigen zichzelf wel op dezelfde manier als een virus. Het verschil is dat een worm zich van computer naar computer verspreidt tot dat het volledige systeem is besmet, terwijl virussen zich

Ronald Eygendaal *is werkzaam als Security consultant voor Vodafone, heeft meer dan 10 jaar ervaring in beveiliging en informatiebeveiliging in het bijzonder; is voorzitter van de vakgroep ICT beveiliging van de Vereniging Beveiligingsmanagers Nederland (VBN), lid van het International Advisory Board van de International Foundation for Protection Officers (IFPO), is Certified Security Supervisor (CSS) en Certificate in Information Security Management Principles (CISMP)*

van bestand naar bestand verspreiden. Wormen kopiëren zichzelf van de ene naar de andere computer via een netwerk door middel van e-mail, ICQ of GPRS. Omdat wormen geen menselijke tussenkomst nodig hebben om zich te vermenigvuldigen, kunnen ze zich veel sneller verspreiden dan computervirussen.

Praktijk

De afgelopen zes maanden zijn er virussen, trojans en wormen voor de nieuwe generatie mobiele telefoons en PDA's gesignaleerd. Vaak worden deze geschreven in generieke talen, maar soms ook in een taal voor één bepaalde PDA of telefoon. Zo is *Liberty Crack* één van de virussen voor Psion's EPOC OS. De trojan doet zich voor als een gratis versie van Gambit Studios Liberty Gameboy emulator, maar verwijdert na installatie alle programma's op de zakcomputer.

Ook PalmOS wordt getroffen door virussen zoals het Phage.9360-virus dat alle programma's in de Palm PDA's beschadigt. Het zeer kleine programma is in staat zichzelf te repliceren via de infraroodpoort waarna alle programma's in de Palm weigeren te starten en het scherm enkel een grijs scherm toont. Een besmette Palm kan worden gereanimeerd door de beschadigde programma's te verwijderen en ze opnieuw vanaf nul of een back-up te installeren.

De afgelopen zes maanden zijn er virussen, trojans en wormen voor de nieuwe generatie mobiele telefoons en PDA's gesignaleerd.

Het 911-virus dat zich specifiek op i-mode telefoons richt, zorgde er in Japan voor dat de telefoonsystemen van de hulpdiensten overbelast raakten. Het scriptvirus stelde bij het bezoeken van een website een script in werking dat de telefoons automatisch 110, het alarmnummer van Tokio, liet bellen.

Het besturingssysteem voor PocketPC heeft ook een scripttaal waarin theoretisch een worm kan worden gebouwd. Het maken van een variant op *Melissa* en de *ILOVEYOU*-virussen is goed mogelijk maar in de praktijk zijn er nog geen virussen of andere ongewenste saboterende verschijnselen bekend.

Antivirus

Besmettingen vinden meestal plaats door wisselende contacten met andere besmette computers of het gebruik van programmatuur van onduidelijke afkomst. Zo kunnen PDA's of telefoons besmet raken via een attachment aan een e-mail of door synchronisatie met al eerder besmette systemen. Virussen kunnen zich verplaatsen via het internet, GPRS maar ook via de infraroodpoort, een *cradle*, docking station of tijdens PDA-synchronisatie met een PC. Zelfs het surfen naar een verdachte WAP-site met daar op WMLscripts kan een mobieltje besmetten.

Bijna alle leveranciers van antivirussoftware hebben speciale versies voor PDA's. Om besmetting via het netwerk te voorkomen moeten bedrijven multiplatform antivirus-software installeren. Uiteraard is het regelmatig, liefst dagelijks updaten van de software belangrijk. Maar gebruik bovenal bescherming tegen virussen, ook al vertraagt het de PDA of GSM. ■