

Virussen breiden zich uit naar mobieltjes

Door: Ronald Eygendaal

INLEIDING

Op dit moment is er maar klein aantal virussen bekend die het specifiek gemunt hebben op de Personal Digital Assistants (PDA) en de nieuwe generatie mobiele telefoons. Deze nieuwe generatie mobiele telefoons herbergen heel wat functies van PDA systemen. Het communiceren van de toestellen gebeurt zowel via de Infrarood poort (IR poort), een docking station, het internet en draadloos via in opmars zijnde GPRS netwerken. De ontwikkelingen gaan zeer snel. De verwachting is dat we komend jaar een explosie zullen zien van virussen die specifiek geschreven zijn voor de nieuwe generatie mobiele telefoons en PDA's. Momenteel zijn er nog veel verschillen in de besturingssystemen en communicatiemethodes van deze mobiele hebberdingetjes, edoch dit verandert snel waarna de mobiele virussen zullen losbarsten.

WAT IS EEN VIRUS

Een computervirus is een klein computerprogramma dat meestal een saboterende werking heeft. Een groot aantal virussen 'verbergt' zich zelf 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. Dit om zijn besmettend werk te kunnen in- en voortzetten. Wie denkt dat het hier alleen om Windows systemen gaat heeft het mis. De nieuwe generatie mobiele telefoons en PDA's gebruiken onder meer EPOC, PalmOS, Windows CE en Symbian, als operating systems. De OS'en 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 gedeelte van een mobiele telefoon en/of PDA wat beschrijfbaar is met het risico dat er zich een virus of trojan (horse) in kan nestelen.

WAT IS EEN TROJAN

Een zelfstandig programma welke zich voordoet om een bepaalde nuttige en door de gebruiker gewenste taak te verrichten, maar ook saboterende acties doet die de gebruiker niet wenst. De naam trojan verwijst door naar het Trojaanse paard waarmee de Griekse soldaten werden binnengesmokkeld in Troje en zodoende de stad veroverden.

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 dus dit virus in een computersysteem kunnen loslaten.

WAT IS EEN WORM

Zuiver technisch gesproken is een worm geen virus. Wormen verspreiden en vermenigvuldigen zichzelf gelijk aan een virus. Het verschil is dat, in plaats van zich van bestand naar bestand te verspreiden, een worm zich verspreidt van computer naar computer, totdat de worm(en) het volledige systeem besmetten. Wormen kopiëren zichzelf van de ene naar de andere computer via een netwerk, bijvoorbeeld via e-mail, ICQ, MSN, GPRS et cetera. Omdat wormen geen menselijke tussenkomst nodig hebben om zich te vermenigvuldigen kunnen ze zich veel sneller verspreiden dan computervirussen.

DE PRAKTIJK

Het bekende 911-virus richting zich specifiek op I-mode telefoons. Dit virus belt 911, in Japan raken hierdoor de telefoonsystemen van de hulpdiensten overbelast. Het 911 virus is een script virus wat bij het bezoeken van een website een script in werking stelt dat de telefoons automatisch 110 (het alarmnummer van Tokio) laat bellen. Vanuit deze wetenschap heeft concurrent Vodafone zijn Vodafone Live voorzien van virusscanning

Afgelopen 6 maanden zijn er virussen, trojans en wormen voor de nieuwe generatie mobiele telefoons en PDA's gesignaleerd. Vaak zijn deze geschreven in diverse talen sommige speciaal voor een bepaalde PDA en/of telefoon.

Liberty Crack is een van de virussen voor EPOC het operating system voor Psion PDA's.

Liberty Crack, is een virus/trojan en doet zich voor als een gratis versie van de Gambit Studios Liberty Gameboy emulator. Wanneer dit virus wordt geactiveerd kan het programma alle programma's op deze zakcomputer deleten.

Ook het besturingssysteem van Palm, (het bekende PalmOS) wordt getroffen door virussen. Zo is er Phage.936 een virus wat alle programma's in Palm PDA beschadigt. Het zeer kleine programmaatje is in staat zichzelf te repliceren, het gebruikt

Een computer-virus is een klein computer-programma dat meestal een saboterende werking heeft.



daarvoor de IR poort.

Na besmetting zullen alle programma in de Palm dienst weigeren. Na 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 herinstalleren.

Het besturingssysteem voor Windows CE/Pocket PC heeft ook een scripttaal. In theorie is het goed mogelijk om een worm te bouwen. Het maken van een variant op MELISSA en de ILOVEYOU is goed mogelijk. Echter in de praktijk zijn we nog geen virussen of andere ongewenste saboterende verschijnselen tegengekomen.

HOE RAAKT JE TELEFOON OF PDA BESMET?

Besmettingen vinden meestal plaats door wisselende contacten met andere, besmette computers en/of het gebruik van programmatuur van onduidelijke afkomst. Een veelvoorkomende manier waarop

een PDA en/of telefoon 'besmet' kan raken is: via een attachment aan een e-mail of synchronisatie met systemen die veelal eerder zijn besmet. Virussen kunnen zich verplaatsen via het internet, GPRS maar ook via de IR poort, een cradle, docking station of tijdens PDA-synchronisatie met een PC.

ANTIVIRUSBEVEILIGING

Bijna alle leveranciers van antivirus software hebben speciale versies voor PDA's. Voor netwerken is het van belang dat er multi-platform antivirus software wordt geïnstalleerd. Uiteraard is het belangrijk om zeer regelmatig, liefst dagelijks de virussoftware te updaten. En tot slot iets wat klaarblijkelijk maar al te vaak gebeurt: *Gebruik deze bescherming tegen virussen!* Ook al vertraagt dit de werking van uw PDA.

BRONNEN:

Malicious Threats to Personal Digital Assistants, Eric Chein, Symantec.

*Afgelopen
6 maanden
zijn er
virussen,
trojans en
wormen voor
de nieuwe
generatie
mobiele
telefoons
en PDA's
gesignaleerd.*

Wat de security manager zou moeten weten over de Euro

Door: Ronald Eygendaal & Ralph van Os

INLEIDING

Sinds de introductie van de Euro op 1 januari 2002 zijn er vooral amateuristische imitaties gevonden van Euro bankbiljetten, welke gemaakt zijn met behulp van een scanner of kopieer apparaat. De kwaliteit van deze nagemaakte biljetten is over het algemeen slecht te noemen. 'Bij de meeste Euro bankbiljetten kan iedereen zien dat ze vals zijn. Soms is op gewoon papier een kleurenkopie gemaakt.' Echter de laatste tijd duiken regelmatig 'professionelere' vervalsingen van met name de kleine eurocoupures op.

De vraag voor met name het security management is hoe deze valse eurobiljetten van echt te onderscheiden en direct gelieerd hieraan waar moet het personeel binnen een organisatie opletten om te voorkomen dat men transacties laat betalen middels valse eurobiljetten.

HOE HERKENT MEN DE ÉCHTE EURO-BANKBIJETTEN?

Sinds jaar en dag worden bankbiljetten beveiligd door een aantal doeltreffende beveiligingskenmer-

ken die het voor iedereen mogelijk maken het biljet op zijn echtheid te testen en te herkennen.

Deze beveiligingskenmerken zijn uiteraard ook in de nieuwe eurobankbiljetten verwerkt. De eurobankbiljetten zijn te controleren op een aantal specifieke echtheidskenmerken. Op basis hiervan kan men aan de eurobankbiljetten zien en voelen of ze echt zijn. Er is sprake van een gefaseerde graad van beveiliging, de lage coupures zijn anders beveiligd dan de hoge coupures. Echtheidskenmerken die voor alle eurobankbiljetten gelden alsmede hoe men deze kan vinden zijn:

VOELEN

De combinatie van met name het gebruik van uniek papier – gemaakt uit katoenvezels – met een voelbaar verhoogde opdruk op sommige delen maakt de biljetten voor iedereen duidelijk herkenbaar. Dit laatste is met name voor belang voor de blinden en slechtzienden in onze samenleving.

ZIEN

Als de bankbiljetten tegen het licht worden gehouden, ziet men o.a. het watermerk, de veilig-

