DIGITAAL GESPUIS WORDT MOBIELER

Virussen loeren op geavanceerde telefoons

Mobiele telefoons worden steeds geavanceerder, maar daardoor ook kwetsbaarder. Meer mogelijkheden om informatie te benaderen, biedt immers ook meer mogelijkheden voor hackers. Een mooi voorbeeld daarvan is Bluesnarfing waarbij de mobiele telefoon wordt binnengedrongen via Bluetooth. En ook virussen gaan niet meer voorbij aan mobieltjes.

Door Ronald Eygendaal

Naast fysieke diefstal, fraude en oplichting liggen er vooral bij de nieuwe generatie mobiele telefoons andere gevaren op de loer. Namelijk het digitale ongedierte beter bekent als virussen. Op dit moment is er maar klein aantal virussen in omloop dat het specifiek gemunt heeft op de Personal Digital Assistant (PDA) en de nieuwe generatie mobiele telefoons zoals smartphones. Maar ook de huidige generatie van WAP-telefoons loopt gevaar.

Afgelopen jaar zijn er virussen, Trojans en wormen voor nieuwe generatie mobiele telefoons en PDA's gesignaleerd. Vaak worden deze geschreven in generieke talen, soms in een taal voor één bepaalde PDA of telefoon.

Een bekend virus is *911 dat* zich specifiek richt op i-modetelefoons in Japan. Dit virus belt het alarmnummer waardoor de telefoonsystemen van de Japanse hulpdiensten overbelast raken. Het gaat hier om een scriptvirus dat bij het bezoeken van een website een script in werking stelt dat de telefoons automatisch 110 (het alarmnummer van Tokio) laat bellen.

Besmetting

Besmettingen vinden meestal plaats door wisselende contacten met besmette computers of het gebruik van programmatuur van onduidelijke afkomst. Een manier waarop een PDA of telefoon *besmet* kan raken, is via een attachment aan een e-mail of synchronisatie met systemen die veelal al eerder zijn besmet. Virussen kunnen zich verplaatsen via internet en GPRS maar ook via de infraroodpoort, een cradle, docking station of tijdens PDA-synchronisaties met een PC. En ook via Bluetooth en Wi-Fi-verbindingen kunnen virussen zich verspreiden. Zelfs het surfen naar een verdachte WAP-site met WML-scripts kan een mobieltje besmetten.

De nieuwe generatie mobiele telefoons en PDA's gebruiken onder meer EPOC, PalmOS, Windows CE, Microsoft-smartphone en Symbian als besturingssystemen. 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 of PDA dat beschrijfbaar is met het risico dat er zich een virus of *Trojan horse* nestelt. Een ander heikel punt is de Java Virtual Machine die ervoor zorgt dat het toestel Java-programma's aankan. Virussen kunnen gebruik maken van de Java Virtual Machine en zodoende kwaadaardige taken uitvoeren.

Virussen

De laatste maanden komen we in de praktijk meer en meer schadelijke Windows CE/Pocket PC-virussen en andere ongewenste saboterende verschijnselen tegen. Het Trojaanse paard *WinCE.Brador.a* (kortweg Brador) brengt handcomputers in gevaar. Dit programma installeert het bestand *svchost.exe* in de Autorun-map van Windows. De eerstvolgende keer dat het apparaat wordt aangezet, treedt Brador in werking. Via Brador is een buitenstaander in staat om de volledige macht over een mobiel toestel over te nemen.

Wie echter denkt dat alleen mobieltjes en handcomputers op basis van Windows-systemen gevaar lopen, heeft het mis. *Liberty Crack* richt zich op het EPOC-besturingssysteem voor Psion PDA's. Dit *Trojaanse paard* doet zich voor als een gratis versie van *Gambit Studios Liberty Gameboy emulator.* Eenmaal geïnstalleerd kan Liberty Crack alle programma's op de zakcomputer verwijderen. Ook het besturingssysteem PalmOS van Palm wordt getroffen door virussen. Zo is er het virus *Phage.936* dat alle programma's in een Palm PDA beschadigt. Het zeer kleine programmaatje is in staat zichzelf te repliceren en gebruikt de infraroodpoort om binnen te komen. Na besmetting zullen alle programma in de Palm weigeren. Na het opstarten

Ronald Eygendaal *is werkzaam als Senior Risk & Fraud-manager en heeft meer dan 12 jaar ervaring in beveiliging, fraudeonderzoeken en informatiebeveiliging in het bijzonder. Hij 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). (ronaldeygendaal@protectioncompany.com)*

van een programma verschijnt enkel een grijs scherm. Een besmette Palm kan worden *gereanimeerd* door de beschadigde programma's te verwijderen en ze weer helemaal opnieuw te installeren.
Een ander voorbeeld is de *Cabir*-worm. Deze heeft het gemunt op telefoons en PDA's op basis van het Symbian-besturingssysteem. De worm verplaatst zich door gebruik te maken van de Bluetooth-functionaliteit. De worm doet zich voor als een nuttig programma namelijk *Caribe Security Manager*. In het Symbian Installer System-bestand zit echter de worm verstopt. Als het ontvangen bestand eenmaal is geaccepteerd, installeert het virus zich in de *apps*-directory. De worm wordt actief na het in- en uitschakelen van de telefoon en vertoont zich met de melding *Caribe* op het display van de telefoon of PDA. Na het actief worden van de worm zal deze zich proberen te verplaatsten door poorten te scannen die binnen het bereik van Bluetooth liggen. De worm is vrij onschadelijk, maar vertraagt wel de telefoon.
Het succesvolle Symbian OS, dat onder andere wordt gebruikt in Nokia en Sony Ericsson en mobiele telefoons van Fujitsu, is zo open dat alle Application Programming Interfaces (API's) eenvoudig zijn te benaderen. Ook kunnen er programma's op de achtergrond draaien. Dit alles zorg voor een goede voedingsbodem voor virussen en kwaadaardige code.
Alhoewel Microsofts smartphone geen scripttaal en geen Intel x86-code begrijpt, zijn het vooral de downloads van ringtones en Java-games die een kwaadaardige werking kunnen hebben. Net als in Symbian OS kunnen er in de smartphone programma's op de achtergrond draaien. Ook biedt de smartphone de mogelijkheid vanuit het OS het telefoonboek aan te spreken. Deze functie is ideaal voor virussen om zich te verplaatsen. De smartphone ondersteunt Outlook-, IMAP- en POP3/SMTP-e-mailfunctionaliteit. Al deze functies maken de smartphone kwetsbaar voor virussen. Merken zoals palmOne, Motorola, iPAQ en Mitac hebben toestellen gebaseerd op de Microsoft-smartphone in het assortiment.

Bluetooth

Een andere bedreiging voor de mobiele telefoon is Bluetooth. Veel mobiele telefoon van zowel de huidige als de nieuwe generatie zijn hiermee uitgerust. Bluetooth is draadloze netwerktechnologie bedoeld voor draadloze verbindingen op zeer kort afstand tussen verschillende apparaten. Vooral mobiele telefoon van merken zoals Nokia en Sony Ericsson zijn uitgerust met Bluetooth. Er zijn veel toepassingen denkbaar zoals een draadloze verbinding tussen een mobiele telefoon en een headset.
Bluetooth kent de nodige beveiligingsproblemen en vooral *Bluesnarfing* zou een bedreiging vormen. Bluesnarfing is een geavanceerdere vorm van *Bluejacking*. Bij Bluejacking sturen onbekenden een tekst naar een Bluetooth-apparaat en kijken hoe de ontvanger verbaast om zich heen kijkt. Bij Bluesnarfing kunnen onbekenden de gegevens in een Bluetooth-apparaat lezen zonder dat de eigenaar van het apparaat dit weet. De onbekende heeft dus toegang tot de telefoonlijst, de agenda, wachtwoorden, pincodes en ander informatie.
Als kwaadwillenden een *Bleubug attack* succesvol uitvoeren op de met Bluetooth uitgeruste mobiele telefoon, kunnen ze het toestel misbruiken. De kwaadwillende kan bijvoorbeeld SMS'jes versturen, GPRS-verbindingen opzetten en zelfs een telefoongesprek beginnen. Dit alles op kosten van een ander. Het is dus van belang om voorzicht om te gaan met Bluetooth.

Wie denkt dat alleen mobieltjes en handcomputers op basis van Windows-systemen gevaar lopen, heeft het mis.

Ringtones

De zeer populaire ringtones voor de mobiele telefoon kunnen ook een gevaar zijn. Zoals bekend wordt een ringtone tegen betaling verstuurd naar de mobiele telefoon. Vaak gebeurt dit tegen een geringe financiële vergoeding. Er zijn echter dubieuze ringtonen in omloop. Zo is er een ringtone welke gelijk na het downloaden in de telefoon het toestel zeer hard laat trillen. De ringtone zelf geeft verder geen geluid. Voor het downloaden van deze dubieuze ringtone wordt wel geld in rekening gebracht. Gelukkig kan men uitsluitend besmet worden door middel het downloaden van desbetreffende ringtone en de ringtone richt verder ook niet echt schade aan. Behalve dan schade in de portemonnee.

Fraude

In alle gevallen die we nu lieten zien, moeten virusprogrammeurs en hackers geavanceerde technieken gebruiken om de mobiele telefoon onder controle te krijgen. Een stuk eenvoudiger wordt het als de mobiele telefoon ergens onbeheerd ligt, zoals op het bureau of op de koffietafel in de kantine. Bij zowel diefstal als het tijdelijke onbeheerd achterlaten van de telefoon kan de eigenaar slachtoffer worden van fraude. Een listige praktijk is de doorschakelfraude, ook wel *ster21-fraude* genoemd. Hoe werkt een doorschakelfraude?
Onbekenden schakelen een mobiele telefoon door naar een buitenlands of een 0900-nummer. Vervolgens kiest men het telefoonnummer van de mobiele telefoon. Als gevolg van de doorschakeling zal deze oproep niet uitkomen op de mobiele telefoon maar worden doorgezet naar het dure, doorgeschakelde nummer. Vervolgens wordt de mobiele telefoon uit de doorschakelfunctie gehaald. Hierdoor wordt de mobiele telefoon weer gewoon bereikbaar. Echter, de verbinding tussen het telefoonnummer van de mobiele telefoon en het nummer waar naar is doorgeschakeld, staat gewoon open.
Diegene die het telefoonnummer van de mobiele telefoon aankiest, betaalt de standaardkosten voor de oproepen naar een mobiele telefoon. De eigenaar van de

mobiele telefoon betaalt de kosten voor het gesprek naar het doorgeschakelde nummer. Het hierboven beschreven scenario kan per mobiel telefoonnummer ongeveer 5 tot 6 keer worden gedaan. Op de rekening manifesteert dit zich als overlappende gesprekken.
Het vervelende van deze vorm van fraude is dat de gebruiker van de mobiele telefoon hiervan niets hoeft te merken, hij kan immers zijn toestel gewoon gebruiken. Zelfs het uitschakelen van de mobiele telefoon biedt geen solaas. Deze doorgeschakelde verbinding blijft gewoon intact tot dat de feitelijke oproeper, dus de fraudeur, de verbinding verbreekt.

Bij Bluesnarfing kunnen onbekenden de gegevens in een Bluetooth-apparaat lezen zonder dat de eigenaar van het apparaat dit weet.

leiding van het toestel, maar ook op de speciale website van de politie staat hoe YUNU moeten worden ingesteld.
Elke mobiele telefoon is voorzien van een uniek vijftiencijferig chassisnummer, het IMEI-nummer. IMEI is de afkorting van *International Mobile Equipment Identification* en is beschreven in een internationale ETSI-standaard waar fabrikanten van mobiele telefoon zich aan moeten houden. Het IMEI-nummer van de desbetreffende mobiele telefoon kan zichtbaar gemaakt worden door *#06# in te toetsen op de telefoon. Het IMEI-nummer staat ook vermeld in de documentatie en op de doos waarin het toestel bij aankoop wordt geleverd. De IMEI kan worden gebruikt om een mobiele telefoon uniek te identificeren. Het nummer kan van groot belang zijn bij de opsporing van het toestel na een diefstal. Maar ook de fraudedetectiesystemen die in gebruik zijn bij aanbieders van telecomdiensten werken deels op basis van de IMEI. Het is mogelijk om op basis van een IMEI, ongeacht het telefoonnummer van de SIM-kaart, verbinding te maken met de mobiele telefoon.
Als een mobiele telefoon gestolen is, weet de dief de YUNU niet en daardoor wordt de gestolen telefoon waardeloos. Wanneer de dief een andere SIM-kaart in het toestel doet, zal het toestel niet werken. Immers uitsluitend de juiste combinatie YUNU/SIM-kaart werkt. Wanneer de dief de originele SIM-kaart in het toestel stopt kan hij er nog niets mee want hij weet de YUNU niet.
Wanneer de gedupeerde de IMEI aan de politie heeft doorgegeven, kan de politie het gestolen toestel bombarderen met SMS-berichten. Op basis van een IMEI is het immers mogelijk om verbinding te maken met een toestel. Door dit SMS-bombardement wordt de gestolen mobiele telefoon waardeloos voor iemand anders. Kortom, zowel YUNU als IMEI zijn belangrijk voor de beveiliging van een mobiele telefoon. ■

Beveiliging

Straatroof en diefstal van mobiele telefoons is de laatste tijd enorm toegenomen. Volgens het *Meldpunt gestolen gsm telefoons* worden in Nederland maandelijks 20.000 mobiele telefoons gestolen. Ontvreemding kan pijnlijke gevolgen hebben als het gaat om een telefoon met diverse kantoorfaciliteiten. Gevoelige bedrijfsgegevens kunnen immers op straat komen te liggen. Een goede manier om de mobiele telefoon goed te beveiligen, is door gebruik te maken van de speciale beveiligingscode *Your Unique Number* (YUNU). YUNU is dus wat anders dan de pincode die moet worden ingevoerd bij het aanzetten van de mobiele telefoon. YUNU zorgt ervoor dat de mobiele telefoon uitsluitend werkt met de eigen SIM-kaart. Het instellen van de YUNU is heel eenvoudig maar zeer doeltreffend. Hoe de YUNU ingesteld moet worden, is afhankelijk van het merk mobiele telefoon. Er zijn mobieltjes zonder YUNU in de handel, maar de meeste zichzelf respecterende merken hebben deze mogelijkheid. Informatie over de YUNU staat ongetwijfeld in de hand-

SMS-oplichting

Wie denkt dat het ontvangen van SMS-berichten niets kost, kan bedrogen uitkomen. De *lok-SMS* is een van de bekendste oplichtingtrucs. Via een lok-SMS worden mensen opgeroepen om naar een betaalnummer te bellen. Dit betaalnummer blijkt in werkelijkheid een nummer te zijn waar men niets aan heeft, maar wel wordt men voor enkele tientallen euro's enkele minuten aan de lijn gehouden. Een ander voorbeeld van oplichting met SMS. In de centra van de binnensteden spreken collectanten passanten aan met het verhaal geld in te zamelen voor een goed doel. Diegenen die geld willen schenken, moeten een SMS-bericht versturen waarna 80 eurocent van het beltegoed als gift wordt afgeschreven. Daarnaast maken de deelnemers kans op een prijs ter waarde van enkele tienduizend euro's. Na een SMS-bericht verstuurd te hebben, blijven de gulle schenkers ongevraagde berichten op hun telefoon ontvangen. Per ontvangen bericht wordt 80 eurocent in rekening gebracht. De ontvangers hebben geen mogelijkheid om de berichtenstroom te stoppen. Alleen de verzender van die berichten, die vermoedelijk tevens het geld ontvangt, kan een einde maken aan de SMS-terreur.