WissenHeute Jg. 59 10/2006

Das Thema im Überblick

Computerviren und -würmer treten zunehmend auch in Mobilfunkdiensten und -netzen auf und werden zu einer nicht zu unterschätzenden Bedrohung für eine sichere Übertragung auch aus und in Unternehmensnetze. Ein Beispiel dafür ist der Computerwurm CommWarrior, der sich seit März 2005 über einen Mobilfunkdienst verbreiten kann. Neben Antivirenprogrammen ist insbesondere ein ausgeprägtes Sicherheitsbewusstsein bei den Anwendern notwendig, um ein hohes Sicherheitsniveau zu erreichen. Deshalb sollten Schutzmaßnahmen beispielsweise im Umgang mit Bluetooth, unbekannter Software, zweifelhaften Internetseiten oder E-Mails sowie WLAN- und Infrarot-Schnittstellen getroffen und beachtet werden.

Mobile Security – Schutzmaßnahmen für Mobilfunkendgeräte

Mobile Endgeräte sind heute für unterschiedliche Anwendungen erhältlich. Beispielsweise besitzt ein Notebook viele Schnittstellen, die neben dem Anschluss der Tastatur und einem weiteren Display auch Anschlüsse an verschiedene Mobilfunknetze, das Festnetz und insbesondere an Unternehmensnetze ermöglichen. Deshalb kommt der Sicherheit, der mobile Security, eine herausragende Bedeutung zu. So hat die Bedrohung durch Computerviren und Spams in den letzten Jahren deutlich zugenommen. Seit Ende 2004 sind in der Fachwelt auch die ersten Viren und/oder Würmer für Mobilfunkendgeräte bekannt. Bisher sind die einzelnen Handy-Viren zwar noch sehr einfach und können sich nur im begrenzten Umfang verbreiten. Ein wirkungsvoller Schutz kann aber nur unter Mitwirkung aller Beteiligten erzielt werden.

Der Autor

Dipl.-Ing. Stefanus Römer studierte an der RWTH Aachen Allgemeine Elektrotechnik und ist seit 1994 im Konzern Deutsche Telekom im Produktmanagement tätig. Seit April 2001 arbeitet er als Produktmanager bei T-Mobile, wo er insbesondere für mobile Intranet-Access-Lösungen und Schutzmaßnahmen für Handy-Viren zuständig ist.

Ausgangslage

Die ersten Computerviren für Mobilfunkendgeräte sind in der Fachwelt seit Ende 2004 bekannt (Tabelle), wovon aber nur wenige im Umlauf sind. Bei den meisten handelt es sich lediglich um Fallstudien (Proof of Concept[1]). Im März 2005 trat unter der Bezeichnung CommWarrior zum ersten Mal ein Computerwurm auf, der Mobilfunkendgeräte mit offenen Betriebssystemen[2], z. B. Smartphones oder Personal Digital Assistants (PDAs) befiel und sich mittels Multimedia Messaging Service (MMS) sowie über Bluetooth[3] selbstständig verbreitete. Schädliche Computerprogramme (Malware) wie Viren, Würmer oder Trojaner[4] sind aus der PC-Welt schon seit vielen Jahren bekannt und jeder Anwender ist

1 Einige Begriffe sind in einem Glossar auf Seite 563 erklärt.

2 **Offenes Betriebssystem:** Engl. Open Source, eine Software, deren Quellcode frei zugänglich ist.

3 Nahbereichsfunkstandard, IEEE 802.15.1; siehe hierzu den Beitrag „Bluetooth – ein neuer Funkstandard", Unterrichtsblätter, Nr. 6/2000, S. 276 ff.

4 Siehe hierzu den Beitrag „Computerviren – Vom Ärgernis zur ernsten Bedrohung", WissenHeute, Nr. 8/2004, S. 420 ff.

Tabelle Auswahl bekannter Viren und Würmer für Mobilfunkendgeräte

Datum	Virus	Plattform	Aktivität
15.06.2004	Cabir	Symbian Series 60	Weiterverbreitung nur über Bluetooth, fester Dateiname caribe.sis
17.07.2004	Duts	Windows Pocket PC	Proof of Concept, infizierte Dateien auf Endgerät, keine automatische Weiterleitung
06.08.2004	Brador	Windows Pocket PC Mobile 2003 (Windows CE 4.2)	Proof of Concept; manuelle Verbreitung über E-Mails, Backdoor-Trojaner ermöglicht dem Hacker volle Kontrolle über das infizierte Endgerät
19.11.2004	Skulls	Symbian Series 60, Series 80	Trojaner; ersetzt alle Anwendungs-Icons durch Totenköpfe und deaktiviert die Verknüpfung zu den ursprünglichen Anwendungen, sodass nur telefonieren möglich ist; keine selbstständige Verbreitung
01.02.2005	Gavno (Locknut.A)	Symbian Series 60	Trojaner, der vorgibt, ein Patch für das Betriebssystem zu sein und der Teile des Betriebssystems überschreibt und somit das Endgerät unbrauchbar macht
07.03.2005	CommWarrior	Symbian Series 60	Trojaner, Phone Reset (auf spezielles Datum hin), versendet sich über MMS und Bluetooth; dabei benutzt die Variante C zufällige Dateinamen

sich der damit verbundenen Gefahren bewusst. Computerviren im Mobilfunk sind in der Öffentlichkeit aber noch weitgehend unbekannt. Mit der zunehmenden Verbreitung von Smartphones und PDAs sowie der steigenden Nutzung leistungsstarker mobiler Datendienste wie MMS, General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) oder High Speed Data Packet Access (HSDPA) werden sich die Bedrohungslage und damit auch das Problembewusstsein aber nachhaltig verändern.

Smartphones und PDAs haben sich inzwischen zu leistungsstarken Computern entwickelt, deren Rechenleistung und Speicherkapazität von mehreren hundert Megabyte mit den PC-Standards vor fünf Jahren durchaus vergleichbar sind. Über immer breitbandigere mobile Datendienste können diese Endgeräte nahezu überall mit dem Internet oder einem Unternehmensnetz verbunden werden. Dadurch entstehen weitere Gefahren für die einzelnen Unternehmensnetze. Weil auch immer mehr sensible Daten auf diesen Endgeräten gespeichert werden können, ergibt sich ein zusätzliches Risiko, beispielsweise durch deren Verlust oder eventuellen Diebstahl.

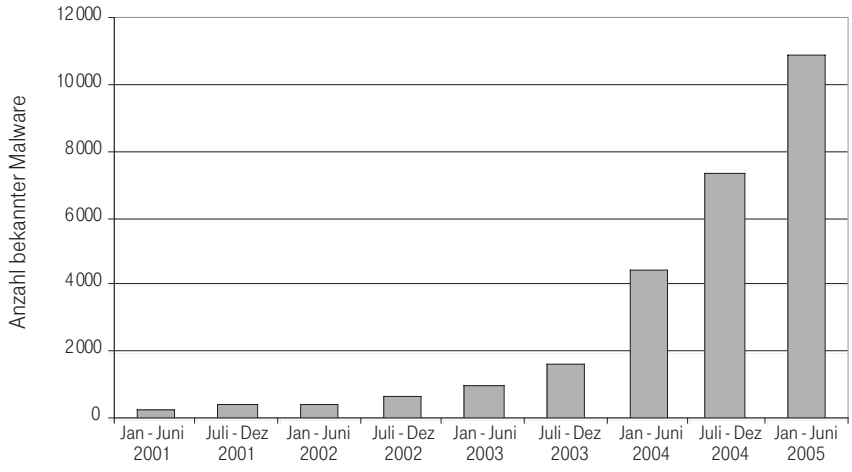
Nach der Studie eines Herstellers von Antiviren-Software[5] wurden bereits im ersten Halbjahr 2005 knapp 11 000 verschiedene Viren, Würmer oder Trojaner registriert (Bild 1). Dies ist eine Zunahme von ungefähr 175 Prozent innerhalb eines Jahres. Gleichzeitig ist zu erkennen, dass sich der Schwerpunkt der Hacker mehr und mehr in den kriminellen Bereich verlagert. Ging es in der Vergangenheit überwiegend um Motive wie Selbstbestätigung oder Experimentierfreude, so stehen heute eindeutig finanzielle Absichten im Vordergrund. Es geht beispielsweise um das Ausspähen sensibler Daten, die Erschleichung von Diensten oder um die Nutzung von Bezahldiensten (z. B. 0190-Nummern) ohne Einwilligung des Geschädigten. Betrachtet man die Faktoren, die diese Entwicklung ermöglicht haben, so stößt man auf drei Voraussetzungen:

- Vormachtstellung eines einzigen offenen Betriebssystems im PC-Umfeld
- hohe Verbreitung von PCs
- starke Nutzung von Breitband-Internet

Im Mobilfunkbereich sind diese Voraussetzungen für eine große Verbreitung von Malware zurzeit noch nicht erfüllt. Eine klare Vorherrschaft eines Betriebssystems ist nicht erkennbar; PDAs mit Microsoft Windows Mobile und Smartphones mit Symbian-Betriebssystem sind ungefähr zu gleichen Anteilen verbreitet. Zusammen machen PDAs und Smartphones noch immer den

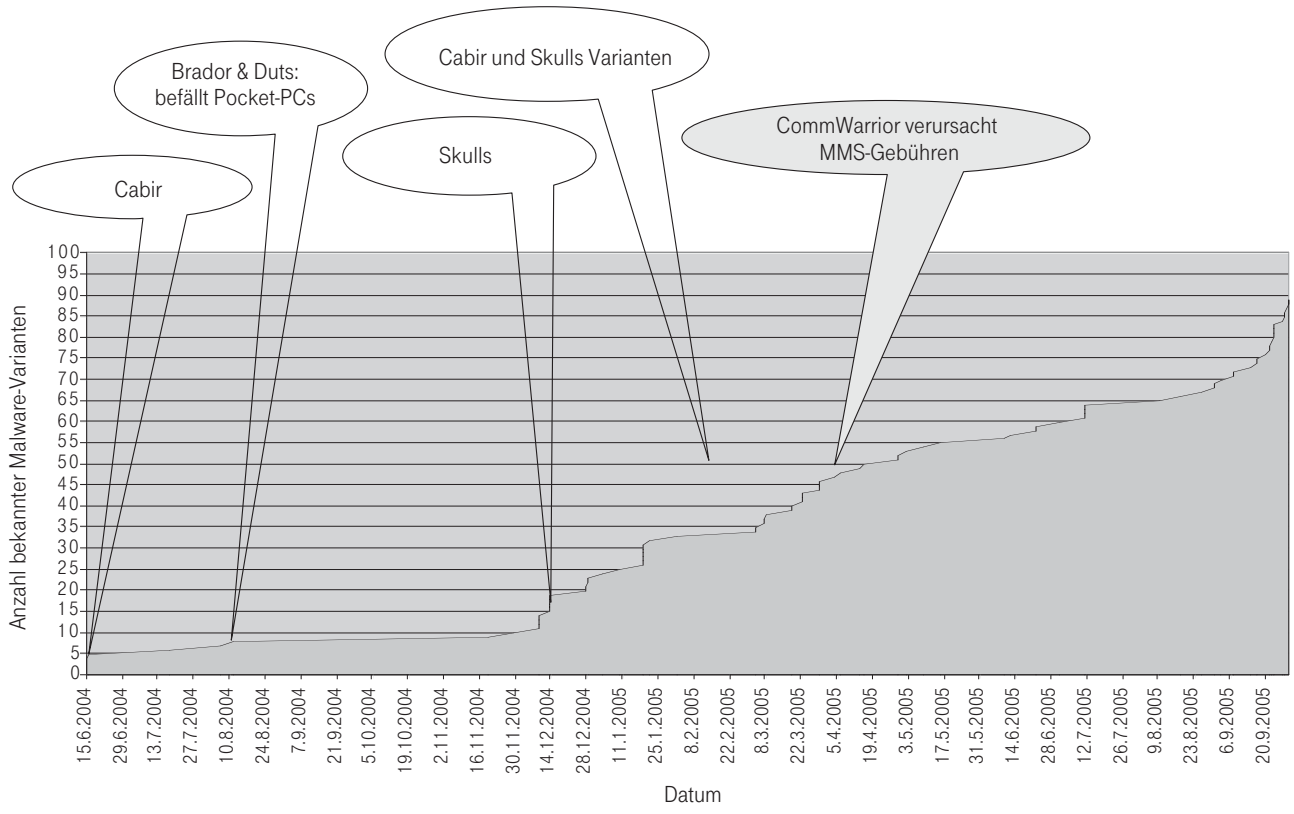
[5] Symantec Internet Security Report, September 2005.

Bild 1 Bedrohung durch Viren, Würmer und Trojaner im PC-Bereich



Quelle: Symantec Internet Security Report, September 2005

Bild 2 **Bedrohung von Mobilfunkgeräten durch Viren, Würmer und Trojaner**



MMS Multimedia Messaging Service

Quelle: F-Secure 2005

kleineren Teil aller im Einsatz befindlichen Mobilfunkendgeräte aus. Dabei steht die Entwicklung der mobilen Datenkommunikation erst am Anfang. Vergleicht man die aktuelle Zahl der bekannten Malware-Varianten für Mobilfunkendgeräte (Bild 2) mit den Zahlen aus der PC-Welt (s. Bild 1), so kann vermutet werden, dass die Entwicklung im Mobilfunkbereich ungefähr fünf Jahre hinter der Entwicklung im PC-Bereich zurückliegt.

Bild 3: Blackberry, Anwendungsbeispiel Navigation

Leistungsumfang PDAs und Smartphones

Personal Digital Assistants sind kleine Taschencomputer, die ursprünglich für die Verwaltung persönlicher Informationen (Personal Information Management = PIM) wie zum Beispiel Kontakte, Termine oder Notizen entwickelt wurden. Sie verfügen über ein größeres Display als Smartphones und sind in der Regel mit einer Tastatur und/oder einer Schrifteingabe ausgestattet. In der zweiten Entwicklungsstufe wurden diese Endgeräte mit einem vollwertigen Mobilfunkteil ergänzt. Damit können zusätzliche Anwendungen wie E-Mail, Online-Adressbuch, Browsing, Messaging und Sprachübertragung genutzt werden. Typische Vertreter dieser Produkte sind der Blackberry (Bild 3) oder die MDA-Familie (Mobile Digital Assistant = MDA) von T-Mobile (Bild 4). Überwiegend verwendetes Betriebssystem sind neben EPOC (Symbian) und Research in Motion (RIM) das Microsoft Windows Mobile oder das Microsoft Pocket-PC. Als Smartphones werden Mobiltelefone be-

Bild 4: MDA compact, Anwendungsbeispiel Mailfunktion

Bild 5: Nokia 6280, Anwendungsbeispiel mobiler Zugriff auf das Internet

zeichnet, die zusätzlich zur Sprachanwendung ähnliche Funktionen wie ein PDA aufweisen. Sie verfügen beispielsweise über einen integrierten Organizer. Darüber hinaus ist es möglich, weitere Anwendungen zu installieren. Smartphones sind somit – analog zur Integration eines Funkmodems in den PDA – Mobiltelefone mit integrierten PDA-Funktionen. (Ein typischer Vertreter dieser Endgeräteteklasse ist das Web'n'Walk-Produkt Nokia 6280 von T-Mobile, Bild 5.)

Das im Smartphone-Segment mit knapp 90 Prozent Marktanteil am weitesten verbreitete Betriebssystem heißt Symbian OS. Es handelt sich hierbei um eine Weiterentwicklung des aus dem PDA-Bereich bekannten und bewährten EPOC-Betriebssystems, dessen erste Version bereits 1981 veröffentlicht wurde. Alle namhaften Hersteller von Mobiltelefonen gehören inzwischen zum Kreis der Symbian-Lizenznehmer und bieten Endgeräte auf der Grundlage dieses ausgereiften Systems an. Über einen geringeren Marktanteil im Smartphone-Bereich verfügen Betriebssysteme wie Microsoft Mobile Edition, Linux, Palm oder das Java-basierte SavajeOS.

Die Übergänge zwischen einem Smartphone und einem kombinierten PDA sind fließend. Es lässt sich feststellen, dass beim Smartphone die Nutzung als Telefon deutlich im Vordergrund steht und es sich hierfür besser eignet als ein PDA. Allerdings verfügt ein Smartphone meist über ein kleineres Display und oft steht nur eine Telefontastatur zur Verfügung, sodass das Eintippen von Texten noch mühsamer ist als bei einem PDA.

Smartphones und PDAs erreichen heute die Leistungsfähigkeit älterer Notebooks. Prozessoren bieten schon jetzt eine 400-MHz-Taktfrequenz und einen Arbeitsspeicher von mehreren hundert Megabyte als Standard. Günstige Flash ROMs[6] ermöglichen zusätzlichen Speicherplatz ohne die Stoßempfindlichkeit von Festplatten. Damit eignen sich diese Endgeräte für Anwendungen, die zuvor nur in der PC-Welt bekannt waren. Die Auflösung auf dem Display von etwa 600 x 400 Pixel schränkt jedoch die Verwendung von vorhandenen Internet- oder Intranet-Inhalten ein.

Zum Standardfunktionsumfang heutiger Smartphones und PDAs gehören unter anderem Dienste und Anwendungen wie

- Short Message Service (SMS),
- MMS,
- E-Mail,
- Web-Browsing und
- GPRS, UMTS sowie HSDPA.

Hinzu kommen Schnittstellen für Nahbereichstechniken wie

- Wireless Local Area Network (WLAN),
- Bluetooth,
- IrDa[7] und
- Universal Serial Bus (USB).

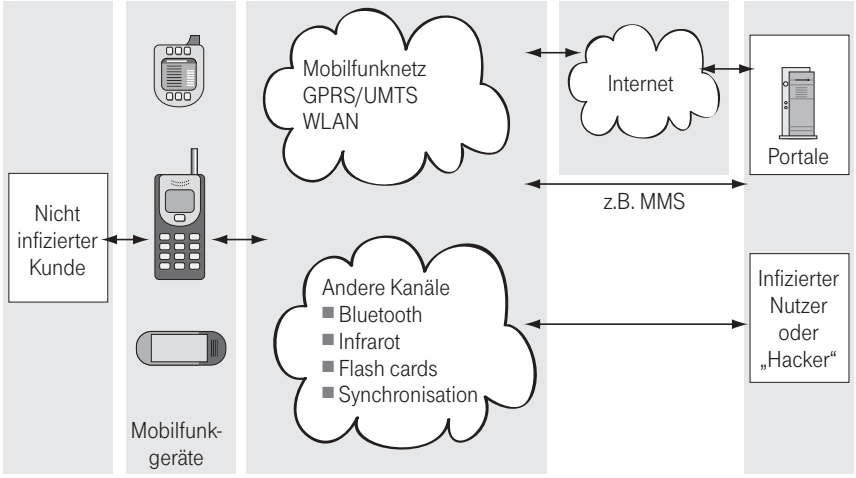
Zudem können große Datenmengen und Anwendungen leicht über externe Speicherkarten ein- und ausgelesen werden.

Aufgrund des leistungsstarken und reichhaltigen Funktionsumfangs, der offenen Betriebssysteme sowie der zunehmenden Vernetzung über nahezu alle Kommunikationsmöglichkeiten sind Smartphones und PDAs Ziele für Angriffe jedweder Art. Handy-Viren können sich über alle genannten Dienste und Schnittstellen verbreiten und in das Endgerät eindringen. Ohne ein Problembewusstsein der Benutzer, wie es im PC-Bereich bereits vorhanden ist, wird einer ungehinderten Verbreitung von Handy-Viren nur schwer zu begegnen sein.

Bedrohungsanalyse

Die Bedrohung beispielsweise durch Malware betrifft sämtliche Beteiligte der Wertschöpfungskette (Bild 6) im Mobilfunk:

Bild 6 Beteiligte der Verbreitungswege für Handy-Viren



GPRS General Packet Radio Service
MMS Multimedia Messaging Service
UMTS Universal Mobile Telecommunications System
WLAN Wireless Local Area Network

6 **Flash ROM:** Von engl. Flash (Blitz) und Read Only Memory; ein nicht flüchtiger Speicher, der sich sowohl lesen als auch beschreiben lässt. Die Datenspeicherung und -löschung erfolgen blockweise, also im Gegensatz zu anderen Speicherlösungen nicht Byte für Byte. Durchsetzung einer Sicherheitspolitik.

7 **IrDa:** Abk. Infrared Data Association; Protokollarchitektur für die optische Infrarot-Datenübertragung im Kurzstreckenbereich (z. B. bei Notebooks).

- **Bedrohung für den Kunden**
  Unerwartete Kosten; Belästigung, Ausspähen, Verändern oder Löschen sensibler Daten, eingeschränkte Nutzbarkeit des Endgerätes oder Mobilfunkdienstes, Beschädigung des persönlichen Rufs bei der Weitergabe von Malware.
- **Bedrohung für den Mobilfunkbetreiber**
  Image-Schaden, Umsatzeinbuße, Verschlechterung der Dienstqualität und erhöhte Kosten im Service.
- **Bedrohung für den Endgerätehersteller**
  Image-Schaden; Umsatzverlust.
- **Bedrohung für den Software-Entwickler oder Anwendungs-Provider**
  Misstrauen der Kunden gegenüber neuen Anwendungen.

Die Hauptmissbrauchsfälle sind:

- Unberechtigte Nutzung von Telefondiensten (SMS, MMS) und Datenverbindungen (GPRS, UMTS; HSDPA)
- Verletzung von Datenintegrität oder Ausspähen sensibler Daten
- Zugriff auf kritische Ressourcen der SIM-Karte[8] (z. B. Deaktivierung durch mehrfache Falscheingabe von PIN/PUK[9])
- Missbrauch von Zugriffrechten und Erschleichung von kostenpflichtigen Diensten
- Mithören von empfangenen oder gesendeten Daten
- Weitergabe von Malware
- Einschränkung der Nutzung

Die bis heute bekannten Malware-Varianten beschränken sich überwiegend auf das Betriebssystem Symbian Series 60; Microsoft-Betriebssysteme sind jedoch grundsätzlich mindestens ebenso gefährdet. Die sehr kurzen Produktlebenszyklen verschärfen die Situation zusätzlich, weil hierdurch Sicherheitslücken im Betriebssystem wahrscheinlicher werden. Handy-Viren können grundsätzlich über alle Medien verbreitet werden, die von Maleware gezielt ausgenutzt werden können. Hierzu zählen unter anderem

- Nahbereichstechniken wie Bluetooth, IrDA oder WLAN,
- Nachrichtendienste wie MMS, Instant Messaging oder E-Mail,
- Internetverbindungen (z. B. Web Download) oder
- externe Speicherkarten.

Da die derzeit bekannten Handy-Viren wie z. B. Cabir oder CommWarrior zur Verbreitung meist die Bluethooth-Schnittstelle nutzen, wird im Folgenden hierauf besonders eingegangen.

Die Bluetooth-Übertragungstechnik ist inzwischen sehr verbreitet, ohne dass den Nutzern immer das damit verbundene Sicherheitsrisiko[10] bewusst ist. Bluetooth ist eine Technik zur kabellosen Vernetzung mehrerer Kundengeräte im Nahbereich bis etwa 10 m Abstand um einen Master. Überall, wo bisher im unmittelbaren Nahbereich Kabel notwendig waren, kann heute Bluetooth zum Einsatz kommen, beispielsweise für Verbindungen wie

- Handy-zu-PC,
- Freisprecheinrichtung (Headset-zu-Handy),
- PDA- oder Notebook-zu-PC,
- Handy-zu-Handy,
- PC-zu-Drucker,
- Digitalkamera-zu-PC,
- Handy im Auto oder
- HiFi-zu-Multimedia-PC.

Ein häufiger Anwendungsfall ist der Einsatz von Bluetooth für Freisprecheinrichtungen (Headset). Auch bei Spiele- und Musikanwendungen wird Bluetooth immer beliebter.

Verwendete Abkürzungen

GPRS	General Packet Radio Service
HSDPA	High Speed Data Packet Access
IrDA	Infrared Data Association
MDA	Mobile Digital Assistant
MMS	Multimedia Messaging Service
PDA	Personal Digital Assistant
PIM	Personal Information Management
PIN	Personal Identification Number
PUK	Personal Unblocking Key
RIM	Research in Motion
ROM	Read Only Memory
SIM	Subscriber Identity Module
SMS	Short Message Service
UMTS	Universal Telecommunications System
USB	Universal Serial Bus
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

Vielen Anwendern ist jedoch nicht immer bewusst, dass eine dauerhaft aktive Bluetooth-Schnittstelle die Gefahr eines Viren-Befalls oder des Auslesens persönlicher

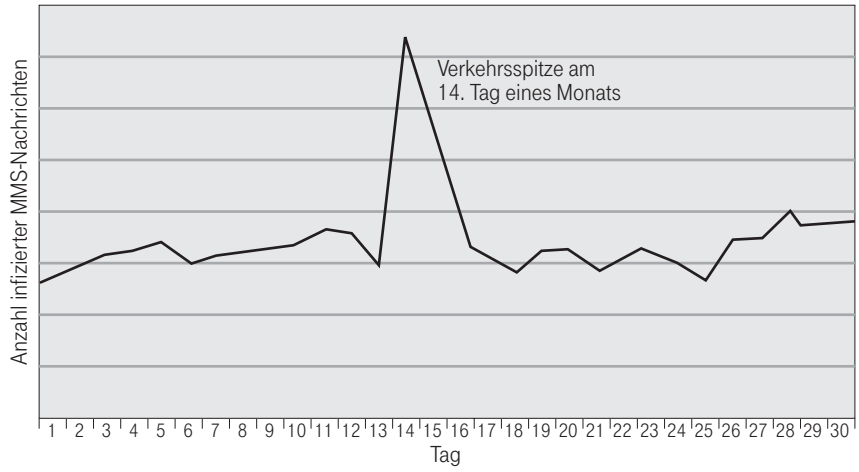
[8] **SIM-Karte:** Abk. Subscriber Identity Module; Chipkarte, die in Mobilfunktelefonen benutzt wird und für deren Betrieb zwingend erforderlich ist. Sie ordnet dem Mobiltelefon eine Rufnummer und einen Mobilfunkbetreiber zu.

[9] **PUK:** Abk. Personal Unblocking Key, persönlicher Entsperrcode; im Mobilfunksystem ein achtstelliger Sicherheitsschlüssel zum Entsperren einer durch Falscheingabe der Personal Identification Number (PIN) gesperrten SIM-Karte.

[10] Siehe hierzu den Beitrag „Sicherheitsaspekte beim Bluetooth-Standard“, WissenHeute, Nr.8/2006, S. 425 ff.

Bild 7 **Benutzerabfragen nach Eingang einer infizierten Nachricht**

Bild 8 Typisches monatliches Verkehrsaufkommen bei CommWarrior



MMS Multimedia Messaging Service

Daten mit sich bringt. Die Sorglosigkeit der Anwender wird bereits von Werbeagenturen ausgenutzt, die an stark frequentierten zentralen Plätzen Bluetooth-Sender für Werbeeinspielungen aufstellen. Erste Erfahrungen mit dieser „neuen" Werbemethode haben gezeigt, dass sehr viele Handy-Besitzer ständig ihre Bluetooth-Schnittstelle aktiviert halten und ein bedenklich hoher Anteil die unbekannten Werbeeinspielungen akzeptiert und auf ihr Endgerät lädt. Bei ersten Feldversuchen im September letzten Jahres wurden innerhalb von 18 Tagen insgesamt 26 205 Passanten mit einer offenen Bluetooth-Schnittstelle gezählt; davon akzeptierten fast fünf Prozent die Werbeeinspielung.

Kasten Texte infizierter MMS-Nachrichten

- Norton AntiVirus released now for mobile, install it!
- Dr. Web New Dr. Web antivirus for Symbian OS. Try it!
- MatrixRemover Matrix has you. Remove matrix!
- 3DGame 3DGame from me. It is FREE !
- MS-DOS MS-DOS emulator for SymbvianOS. Nokia series 60 only. Try it!
- PocketPCemu PocketPC *REAL* emulator for Symbvian OS! Nokia only.
- Nokia ringtoner Nokia RingtoneManager for all models.
- Security update #12 Significant security update. See www.symbian.com
- Display driver Real True Color mobile display driver!
- Audio driver Live3D driver with polyphonic virtual speakers!
- Symbian security update See security news at www.symbian.com
- SymbianOS update OS service pack #1 from Symbian inc.
- Happy Birthday! Happy Birthday! It is present for you!
- Free SEX! Free *SEX* software for you!
- Virtual SEX Virtual SEX mobile engine from Russian hackers!
- Porno images Porno images collection with nice viewer!
- Internet Accelerator Internet accelerator, SSL security update #7.
- WWW Cracker Helps to *CRACK* WWW sites like hotmail.com
- Internet Cracker It is *EASY* to *CRACK* provider accounts!
- PowerSave Inspector Save you battery and *MONEY*!
- 3DNow! 3DNow!(tm) mobile emulator for *GAMES*.
- Desktop manager Official Symbian desctop manager.
- CheckDisk *FREE* CheckDisk for SymbianOS released!MobiComm

Beispiel CommWarrior

Der MMS-Wurm CommWarrior trat zum ersten Mal im März 2005 auf und war der erste Wurm, der sich über einen Mobilfunkdienst verbreiten konnte. Von dem MMS-Wurm CommWarrior sind inzwischen verschiedene Varianten bekannt. Allen Varianten ist gemeinsam, dass sie sich per Bluetooth oder MMS verbreiten und vor der Installation ausdrücklich vom Benutzer bestätigt werden müssen (Bild 7). Eine schädigende Funktion enthält Commwarrior nicht, er versucht lediglich weitere Handys zu infizieren. Dazu versendet er im Abstand von etwa 31 Minuten eine Nachricht mit Anhang an sämtliche Kontakte, die er im Adressbuch findet. Nach der Installation laufen alle Varianten vom Nutzer unbemerkt im Hintergrund. Dabei wählen sie in den Kontakten zufällige Mobilfunkrufnummern aus und verschicken sich selbst als Anhang von MMS-Mitteilungen an die entsprechenden Empfänger. Um eine weite Verbreitung des CommWarriors zu verhindern, werden derart infizierte MMS-Nachrichten jedoch von den meisten Mobilfunknetzen abgewiesen. Der Kunde erhält dann die Fehlermeldung „message sending failed!".

Wenn andere Handys in der näheren Umgebung mittels Bluetooth erreichbar sind, versucht der CommWarrior, eine Verbindung zu diesen herzustellen und sich selber an diese Endgeräte zu übertragen.

Für die Herstellung einer Bluetooth-Verbindung muss üblicherweise beim empfangenden Handy der Aufbau der Verbindung vom Nutzer akzeptiert werden. Daher sollte ein Anwender darauf achten, dass er keine Bluetooth-Verbindung von unbekannten Nutzern akzeptiert. Problematisch wird es, wenn der Wurm dauernd mittels Bluetooth verschickt wird, weil das „Opfer" in diesem Falle so lange mit Anfragen „bombardiert" wird, bis es entweder die Installation akzeptiert oder die Bluetooth-Verbindung deaktiviert.

Auf neu infizierten Endgeräten wird der CommWarrior stets am vierzehnten Tag eines Monats zum ersten Mal aktiv. Daher ergibt sich für Mobilfunknetzbetreiber im Verkehrsablauf mit den infizierten MMS-Nachrichten jeweils am vierzehnten Tag eines Monats eine typische Verkehrspitze (Bild 8). Infizierte MMS-Nachrichten enthalten Texte wie sie im Kasten beispielhaft aufgeführt sind.

Schutzmaßnahmen

Unstrittig ist, dass sich die Bedrohungslage im Mobilfunkbereich weiter verschärfen wird. Unklar ist jedoch, ab wann die Bedrohung zu einem ernsten Problem werden kann. Zwar ist bis heute mit dem MMS-Wurm CommWarrior nur ein einziger Malware-Typ bekannt geworden, der sich in begrenzten Rahmen selbstständig verbreitet. Die Bedrohungen durch Viren und Spams werden in der Fachwelt dennoch ernst genommen. Bereits heute haben beispielsweise Kunden von T-Mobile die Möglichkeit, über T-Zones einen Antiviren-Client für Smartphones oder ihren PDA zu beziehen.

Um allerdings ein möglichst hohes Sicherheitsniveau zu erzielen, reichen isolierte Einzelmaßnahmen auf Dauer nicht aus. Vielmehr ist ein Maßnahmenbündel unter Einbeziehung sämtlicher Beteiligten einschließlich der Kunden, Hersteller, Mobilfunkbetreiber und Softwareentwickler notwendig.

An vorderster Stelle steht der Anwender: Beim Empfang einer Nachricht, z. B. über Bluetooth, und vor jeder Software-Installation, wird er um Zustimmung gefragt. Wie im PC-Bereich, muss er sich der zunehmenden Bedrohung bewusst sein und folgende Grundregeln beachten:

- Niemals neue Software unbekannter Herkunft installieren. Selbst wenn, wie im Falle des CommWarriors, die Absenderadresse bekannt ist, sagt dies nichts über die tatsächliche Herkunft der Software aus. Im Zweifel sollte beim vermeintlichen Absender nachgefragt werden, ob die Software tatsächlich unbedenklich ist.
- Niemals Software von einer zweifelhaften Internetseite herunterladen.
- Die Bluetooth-, WLAN- oder IrDa-Schnittstelle nur dann aktivieren, wenn sie auch tatsächlich benötigt wird und sobald wie möglich deaktivieren, wenn sie nicht mehr benötigt wird.
- Bluetooth-, WLAN- oder IrDa-Schnittstelle so konfigurieren, dass diese für andere Personen unsichtbar ist.
- Keine Bluetooth-, WLAN- oder IrDa-Verbindungen von unbekannten Gegenstellen akzeptieren.
- Eine WLAN-Verschlüsselung (z. B. WEP[11] oder WPA[12]) nutzen.
- Den Zugang zum Endgerät mit einem Kennwort schützen.
- Eine Verschlüsselungssoftware zum Speichern sensibler Daten auf dem Endgerät nutzen.

Glossar

Malware
Kunstwort, das aus dem englischen malicious und Software zusammengesetzt ist und eine Sammelbezeichnung für Viren, Würmer und Trojaner ist.

Virus
Ein Virus ist ein Computerprogramm, das sich durch Anhängen und/oder Modifizieren an andere Objekte vervielfältigt. Man unterscheidet:

- Makro-Virus, der sich mit Dokumenten verbindet und sich durch E-Mails verbreitet.
- Datei-Virus, der sich mit Programmen verbindet und durch Programmaufruf gestartet wird.
- Boot-Virus, der den Boot-Sektor einer Festplatte oder Diskette modifiziert; er ist heute nahezu „ausgestorben".

Wurm
Ein Wurm ist ein Computerprogramm, das sich selbstständig vervielfältig, indem es sich an andere Systeme sendet.

Netzwerk-Wurm
Netzwerk Würmer verbinden sich sehr schnell direkt über das Netzwerk (z. B. Internet).

E-Mail-Wurm
Verbreitet sich über Anhänge von E-Mails.

Trojaner
Ein Trojaner (von „Trojanisches Pferd") ist ein Programm mit versteckter Funktion. Ein Trojaner kann beispielsweise unbemerkt sämtliche Aktionen des Benutzers protokollieren und an einen entfernten Server senden oder er kann Daten auslesen, manipulieren oder löschen.

Proof of Concept
Fallstudie, die beispielhaft mögliche Angriffsmechanismen belegen soll.

Wild
Eine Malware ist „in the wild", wenn sie sich selbstständig verbreitet und Geräte außerhalb einer Laborumgebung befällt.

[11] **WEP:** Abk. Wired Equivalent Privacy; im Standard IEEE 802.11 spezifizierter Verschlüsselungsdienst, der die Vertraulichkeit der übertragenen Daten gewährleisten soll.

[12] **WAP:** Abk. Wi-Fi Protected Access; Vorgriff auf den offiziellen Sicherheitsstandard IEEE 802.11i; entwickelt von der Industrievereinigung WiFi Alliance.

Darüber hinaus sind die Hersteller in der Pflicht, Mobilfunkendgeräte mit einer Sicherheitsarchitektur (Security Framework) auszustatten, die unter anderem folgende Grundanforderungen erfüllt:

- Installation von Software nur mit Zustimmung des Benutzers.
- Unterstützung von Zertifikaten, die den Ursprung einer neuen Software eindeutig authentisieren.
- Schutz kritischer Systemressourcen (z. B. SIM-Karte, Adressbuch oder Nachrichtenversand) vor dem Zugriff durch nicht zertifizierte Anwendungen.
- Unterstützung von Möglichkeiten zur nachträglichen Aktualisierung des Betriebssystems.

Die Softwareentwickler stehen in der Verantwortung, ihre Software zertifizieren zu lassen, um es dem Anwender zu ermöglichen, den Ursprung der Software vor einer Installation zweifelsfrei erkennen zu können.

Die Mobilfunkbetreiber sind gefordert, eine grundlegende Sicherheitsarchitektur bei ihren Lieferanten einzufordern und ihren Kunden Endgeräte mit einem hohen Sicherheitsniveau bereitzustellen. Als kundenorientierter Dienstleister werden die Mobilfunkbetreiber darüber hinaus bestrebt sein, ihre Kunden maximal zu unterstützen und einer massiven Verbreitung von Malware über ihre Mobilfunknetze entgegenzutreten. Hierzu zählen die Bereitstellung von leistungsstarker Antiviren-Software sowie eine kompetente Hilfestellung über Customer Care und Internet. Schon jetzt stellt beispielsweise T-Mobile über T-Zones (http://pfw.t-zones.de/) unter dem Menüpunkt „Downloads“ eine Antiviren-Software für verschiedene Smartphones zum direkten Download bereit (Smartphone-Typ auswählen und Suchbegriff „Antivirus“ eingeben).

Zusammenfassung

Die Bedrohung durch schädliche Computerprogramme (Malware) für Mobilfunkgeräte wird in den kommenden Jahren weiter zunehmen. Das Bedrohungspotenzial ist jedoch heute noch gering, weil die Voraussetzungen für eine massenhafte Verbreitung von Malware noch nicht erfüllt sind. Mobilfunkbetreiber und Endgerätehersteller arbeiten aber bereits gemeinsam an Maßnahmen, um dieser Entwicklung entgegenzuwirken. Um ein hohes Sicherheitsniveau zu erzielen, sind die Mitwirkung der Kunden und deren Problembewusstsein von entscheidender Bedeutung.

(He)