Viren infizieren auch PDA

Viren infizieren auch PDA

Mobilität ist gefragt: nicht nur für Unternehmen, sondern auch für Privatanwender gehören Kleincomputer (PDA[1]), Notebooks und Handys mit Internetzugang fast schon zur Standardausstattung. Mit der schnellen Verbreitung, dem technischen Fortschritt und der höheren Leistungsfähigkeit von mobilen Geräten steigt gleichzeitig auch die Gefahr von Hacker- und Virenattacken. Viele Anwender sind sich nicht bewusst, dass – genau wie herkömmliche Computerplattformen – auch mobile Geräte mit Internetzugang von aussen angreifbar sind. Und das, obwohl weltweit täglich etwa 10 bis 15 neue Viren und Würmer entdeckt werden, die auch vor Handhelds[2] nicht Halt machen.

Eric Chien

Die steigende Zahl verkaufter PDA zeigt, dass digitale Assistenten auf dem Vormarsch sind: Laut der Analyse von IDC[3] [1] wurden im Jahre 2001 weltweit 14,6 Mio. Handhelds verkauft; 2002 soll die Zahl auf 16,5 Mio. steigen und für 2006 sagt IDC sogar den Verkauf von rund 31,6 Mio. PDA voraus.

Der Einsatz von PDA und ähnlichen mobilen Geräten – vor allem mit einem direkten Zugang zum Internet – öffnet einen neuen Infektionskanal für Viren, Würmer und Trojanische Pferde. Es ist deshalb wichtig, durch richtige Vorsorge die Sicherheitslücke rechtzeitig zu schliessen.

Die mit Abstand führende Plattform für Handheld-Computer ist das Palm-Betriebssystem PalmOS. IDC erwartet, dass es von diesem Produkt im Jahr 2003 mehr als 18,9 Mio. Einheiten geben wird. Neben dem Palm-Betriebssystem zählen WindowsCE (eingesetzt von Casio und Compaq) und EPOC (eingesetzt beispielsweise von Psion) wohl zu den am häufigsten eingesetzten Betriebssystemen.

Wie funktioniert PalmOS ?

PalmOS verwendet kein herkömmliches Dateisystem. Das System ist soweit abgewandelt und optimiert worden, dass es zum einen für das Zusammenspiel mit Primärgeräten wie zum Beispiel dem PC geeignet ist und zum anderen den begrenzten Speicherplatz des Palm bestmöglich nutzt. Daten werden in Speicherblöcken – den so genannten Records oder Datensätzen – gespeichert. Zusammengehörige Datensätze werden zu Datenbanken gruppiert, die beispielsweise Sammlungen von Adressbucheinträgen oder Terminplaner sein können.

Eine Datenbank im PalmOS entspricht in etwa einer herkömmlichen Datei. Der Unterschied besteht darin, dass PalmOS Daten in vielfältige Records unterteilt, anstatt sie in einem zusammenhängenden Block abzulegen. Bei einer Modifizierung solcher Datenbanken finden die Veränderungen nur im Speicher statt, im Gegensatz zur traditionellen Desktop-Methode, bei der die Daten temporär im Random Access Memory (RAM) abgelegt werden, bevor sie auf die Festplatte geschrieben werden. Die spezielle Art der Datenspeicherung im PalmOS schafft Platz für Anwendungsdatenbanken (mit ausführbarem Code), die auf verschiedene Weise (z.B. via Kabel, Infrarot oder auch Speicherkarte) auf den PDA übertragen werden können.

Infektionswege

Obgleich jede Methode, mit der ein ausführbarer Code auf das Palm-Gerät gebracht wird, eine Eintrittsmöglichkeit für einen schädlichen Code darstellt, wird in Zukunft der Internetzugang die herausragendste Bedrohung darstellen. Nachfolgend sind drei mögliche Methoden bzw. Transportwege beschrieben, wie ein bösartiger Code übertragen werden kann.

HotSync

Die grundlegende Methode, Anwendungen auf den Palm zu transferieren, ist die HotSync-Funktion. Sie wird in erster Linie dazu verwendet, Daten auf dem PDA mit Daten auf dem PC abzugleichen, Daten auf dem PC zu aktualisieren oder neue Anwendungen vom PC aus auf dem PDA zu installieren.

Gegenwärtig ist HotSync die wohl einfachste und auch häufigste Methode, einen schädlichen Code einzuführen. Nachdem der Benutzer beispielsweise ein neues Programm aus dem Internet auf seinen PC heruntergeladen hat, kann er es mittels der HotSync-Funktion vom PC auf seinen Palm übertragen. Das neue Programm ist startbereit, egal ob es sich um ein Schachspiel oder einen Virus handelt, der wahllos E-Mails zu allen gespeicherten Kontaktadressen verschickt.

IrDA

Der Palm enthält Übertragungseinrichtungen, die mit Infrarot (IR) arbeiten. Diese Einrichtungen entsprechen den Bestimmungen der *Infrared Data Associations*[4] (IrDA). Die Mehrheit der Programme benutzt den Palm-Exchange-Manager, der eine einfache Schnittstelle für PalmOS-Anwendungen zur Verfügung stellt. Hierüber können Daten von einem entfernten Gerät mit Standard-Protokollen gesendet und empfangen werden. Auf diesem Übertragungsweg kann der Palm auch mit einem schädlichen Code in Berührung kommen.

Derzeit geben die Geräte noch eine Mitteilung an den Benutzer heraus, wenn Daten eintreffen. Diese Message-Funktion kann jedoch ausgeschaltet werden, wozu ein spezieller Code auf dem Empfangsgerät nötig ist. Via Infrarot können dann schädliche Programme mit anderen infizierten Geräten kommunizieren und Informationen oder Codes austauschen, ohne dass der Benutzer etwas davon merkt.

Netzwerkzugang

Spezielle für den Palm erhältliche Modem-Hardware oder kabellose Modems bieten Zugang zu vielen Standard-Internetprotokollen. Im Allgemeinen steht ein eingeschränktes Web-Browsing sowie ein E-Mail-Zugang (mit der Möglichkeit, Dateien an das E-Mail anzuhängen) zur Verfügung. So kann der Benutzer E-Mails mit Palm-Anwendungen im Anhang erhalten, abspeichern und ausführen. Solche Anwendungen können einen schädlichen Code enthalten.

Darüber hinaus erlaubt es die Net Library den PalmOS-Anwendungen, Verbindungen mit beliebigen Maschinen im Internet herzustellen und Daten von und zu diesen Maschinen mit Hilfe der Standard-TCP/IP-Protokolle zu transferieren. Neben der Eintrittspforte über die E-Mail-Funktion des Palm oder den Web-Browser kann ein bösartiger Code mit-

hörende Server-Ports öffnen, um einen ferngesteuerten Zugang zu ermöglichen, vertrauliche Daten zu verschicken oder einen zusätzlichen schädlichen Code zu erhalten. Ein Netzwerkzugang ist daher geradezu eine Einladung für sich schnell verbreitende Viren.

Programmierbarkeit

Während die oben beschriebenen Wege die Türen zum Palm-Gerät darstellen, ist die Rechnerarchitektur der Schlüssel, um sich unberechtigt Zugang auf das Gerät zu verschaffen.

Viele der Anwendungen, die auf PalmOS laufen, sind programmierbar. Über Standardschnittstellen für die Anwendungsprogrammierung können Programme auf verschiedenen Geräten miteinander interagieren. So können sich Anwendungen beispielsweise gegenseitig Ausführungscodes zusenden und sich anweisen, eine Aktion auszuführen oder Daten zu modifizieren: Ein schädliches Programm kann z.B. einen Ausführungscode senden, um alle E-Mail-Adressen aus der Adressliste abzufragen. Danach kann durch einen weiteren Ausführungscode die E-Mail-Anwendung angewiesen werden, E-Mails mit dem schädlichen Programm selbst als Anhang zu versenden. All diese Funktionen können ohne Eingriff des Benutzers ausgeführt werden und ohne sein Wissen ablaufen. Diese Programmierbarkeit bedeutet eine hohe Anfälligkeit für sehr einfache E-Mail-basierte Viren wie beispielsweise W97M/Melissa und VBS/Love Letter.

Dateisystem

Über die Datei-Funktionen im PalmOS kann der Benutzer – wie bei einer herkömmlichen PC-Datei – Dateien lesen, schreiben, suchen oder verändern. Solche Funktionen sind alles, was ein Virus braucht, um sich zu verbreiten. Viren können sich an andere Anwendungsdatenbanken auf dem Gerät anhängen, wobei sie den Einsprungpunkt[5] des Programms ändern, um sicherzustellen, dass sie zukünftig ausgeführt und ständig vervielfältigt werden.

Der Palm verfügt über keinerlei eingebaute Zugangskontrollen zu Datenbanken und Records. System-Datenbanken können genauso einfach verändert werden wie Benutzer-Datenbanken. Ein schädlicher Code kann damit nicht nur Systemdateien modifizieren, sondern diese auch zerstören.

Bibliotheken

PalmOS wird mit vielen Bibliotheken inklusive der Net Library vertrieben, die es PalmOS-Anwendungen erlaubt, eine Verbindung mit jeder anderen Maschine im Internet herzustellen.

Die Bibliothek für IR-Funktionen stellt eine direkte Schnittstelle für die IR-Übertragung dar. Solche Bibliotheken machen es leicht, einen äusserst gefährlichen Code zu programmieren. Selbst ohne tiefere Kenntnisse der IR-Übertragung könnte ein Programmierer einen Agenten schaffen, der eingehende IR-Datenübertragungen überwacht. Hierdurch könnten bösartige Programme mit anderen infizierten Geräten kommunizieren.

Die Net Library bietet Programmierern ausserdem die Möglichkeit, Programme mit sogenannten Berkley Sockets zu erstellen. Diese Programme reichen von kleinen SMTP[6]-Engines, die für E-Mail-Funktionalität auf Geräten ohne eigenen Mail-Client sorgen, bis zu Servern, die am Netzwerk auf eintreffende Kommandos «lauschen», um Hackern so den Fernzugriff zu gewähren.

Zunehmende Bedrohung für PDA

Obwohl es möglich ist, Viren, Würmer und Trojaner für das PalmOS zu programmieren, ist ihre Ausbreitung aus verschiedenen Gründen eingeschränkt.

So hält der Palm zwar den grössten Marktanteil an PDA, doch ist die Zahl der PDA-Benutzer deutlich geringer als jene der PC-Benutzer. Zudem gibt es noch verschwindend wenige PDA-Benutzer mit Internetanschluss. Eine schädliche PalmOS-Anwendung kann sich daher nicht annähernd so schnell verbreiten wie beispielsweise ein Windows-Virus.

Ein weiterer Grund für die Einschränkung der Ausbreitung liegt darin, dass die Art des Datenaustauschs bei PDA immer noch asymmetrisch ist. Das bedeutet, dass Palm-Besitzer Anwendungen und Daten von wenigen Primärquellen herunterladen. Erst durch einen symmetrischen Datenaustausch, bei dem zahlreiche PDA-Benutzer Informationen mit vielen anderen PDA-Benutzern austauschen, steigt das Risiko der Virenausbreitung drastisch an, wie am Beispiel der Makroviren (z.B. Melissa) zu beobachten war.

Trotz allem bleibt zu bedenken, dass PDA durch die sinkenden Preise allmählich zu Standardgeräten in Unternehmen werden und damit die Virenbedrohung deutlich ansteigt. Werden erst E-Mails via Palm abgerufen und Dokumente oder ausführbare Anhänge mit dem PDA ausgetauscht, steigt die Gefahr, dass ein bösartiger Code unbemerkt ausgeführt wird. Ist ein ausführbarer Code erst einmal im Umlauf, dann sind den Möglichkeiten des Missbrauchs keine Grenzen gesetzt. Palms sind leicht zu infizieren und begünstigen E-Mail-Viren durch ihre simple Programmierbarkeit. Der einzige sinnvolle Schutz bietet eine vernünftige Antivirensoftware für PDA, die inzwischen von vielen Herstellen angeboten wird.

Les virus peuvent également infecter les PDA

La mobilité est de mise: non seulement pour les entreprises mais aussi pour les particuliers, les petits ordinateurs (PDA), notebooks et téléphones mobiles à accès Internet font déjà presque partie de l'équipement standard. Mais tandis que les appareils mobiles connaissent une rapide diffusion et que leur technologie progresse en même temps que leurs performances, le danger d'attaques par les hackers et virus augmente. De nombreux utilisateurs ne sont pas conscients du fait que – au même titre que les plates-formes traditionnelles – les appareils mobiles à accès Internet sont exposés aux attaques de l'extérieur. Et ce, bien que l'on détecte chaque jour dans le monde 10 à 15 nouveaux virus et vers qui n'épargnent pas non plus les handhelds.

Referenz

[1] *IDC*: Sync or Swim: The Worldwide Smart Handheld Devices Market Forecast and Analysis, 2002-2006. April, 2002, Framingham, MA 01701 USA

Adresse des Autors

Eric Chien, Bachelor Molekular-Genetik und Elektrotechnik der University of California, Los Angeles, und Leiter des europäischen Virenforschungslabors von Symantec (Symantec Security Response), Dublin, Irland

[1] PDA: Personal Digital Assistent

[2] Handhelds: Computer im Westentaschenformat. Sie verfügen über Büro-Funktionen wie Kalender, Adress- oder Notizbuch und erlauben die digitale Kommunikation (z.B. für E-Mail). Die meisten Handhelds verfügen über ein kleines Keyboard oder einen mit einer Schrifterkennung (Stift) ausgestatteten Touchscreen. Handflächengrosse Stiftcomputer werden auch als PalmPC oder PDA bezeichnet.

[3] IDC ist ein weltweit führendes Unternehmen für Technologieinformationen, Branchenanalysen und Marktforschungsdaten und bietet Entwicklern, Herstellern und Benutzern von Informationstechnologie strategische Beratungsleistungen (www.idc.com).

[4] IrDA: www.irda.org

[5] Die meisten Viren kopieren sich an den Programmanfang und werden so beim nächsten Programmstart zuerst ausgeführt.

[6] SMTP: Simple Mail Transfer Protocol