Mobile Transaktionen – Einfallstor für **Cyber-Kriminelle**

Von Klaus Jetter

Bildquelle: H+S_pixelio.de

Nur etwa fünf Prozent der weltweit genutzten Smartphones und Tablets sind mit einer Sicherheitssoftware geschützt. In dem Maße, wie die mobilen Endgeräte für das Online-Banking oder Bezahltransaktionen zum Einsatz kommen, gewinnen sie für die Malware-Branche an Attraktivität. Auch die mobile TAN gewährt deshalb keine abschließende Sicherheit – ist aber der Papierversion dennoch bei Weitem vorzuziehen. Red.

2013 sollen in Deutschland rund 28 Millionen Smartphones über den Ladentisch gehen. Das prognostiziert der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (Bitkom). Damit werden die kleinen Helfer Ende dieses Jahres 80 Prozent aller hierzulande verkauften Handys und 96 Prozent des Mobiltelefon-Gesamtumsatzes ausmachen. Doch der Hype um die Rechner im Miniformat bringt auch neue Gefahrenquellen mit sich. Denn die meist unzureichend geschützten Geräte öffnen Cyber-Kriminellen Tür und Tor, um an das Geld und die Daten ihrer Besitzer zu kommen.

Immer neue Wirtschaftsbereiche und Geschäftsfelder rücken in den Fokus der inzwischen professionell organisierten Schadsoftware-Branche. Hatten es die Hacker bislang vor allem auf Systeme und Daten privater Internetnutzer und großer Unternehmen abgesehen, geraten laut Bitkom nun zunehmend mittelständische Unternehmen und Smartphone-Nutzer ins Visier.

Malware-Branche setzt auf die Masse

Im Fokus der Cyber-Verbrecher steht vor allem das Betriebssystem Android, auf dem mittlerweile das Gros der weltweit verkauften Smartphones basiert. Nach Angaben der Marktforschungsfirma IDC entfiel auf Android im ersten Quartal 2013 ein weltweiter Marktanteil von 75 Prozent. Zum Vergleich: Im selben Zeitraum des Vorjahres lag dieser bei 59,1 Prozent. Der Anteil der Angriffe auf dieses Betriebssystem erhöhte sich laut F-Secure von 66,7 Prozent im Jahr 2011 auf 79 Prozent im Jahr 2012. Alleine im vierten Quartal 2012 entdeckten die Sicherheitsexperten 96 neue Gruppen und Varianten von Android-Malware. Damit hat sich die Zahl der Bedrohungen gegenüber dem vorhergehenden Quartal verdoppelt – und ein Ende dieser Entwicklung ist nicht abzusehen.

Zum Autor

Klaus Jetter ist Geschäftsführer D/A/CH & CCE der F-Secure GmbH, München.

Attacken auf Betriebssysteme mit geringen Nutzerzahlen nahmen hingegen ab: So sank die Zahl der Angriffe auf Mobilsysteme, die Symbian nutzen, von 62,5 Prozent im Jahr 2010 auf 19 Prozent in 2012. Erstaunlich niedrig ist mit 0,7 Prozent auch die Zahl der Malware-Übergriffe, die auf Apples Betriebssystem iOS abzielen. Und das, obwohl iOS IDC zufolge im ersten Quartal 2013 einen weltweiten Marktanteil von 17,3 Prozent hatte.

Ein Grund dafür ist die Geschäftspolitik von Apple. Sie verlangt, dass sich App-Entwickler bei dem Unternehmen registrieren und unter anderem ein Geheimhaltungsabkommen unterzeichnen sowie einen Mitgliedsbeitrag entrichten. Damit finden sich im Apple-Store nur geprüfte und speziell für iOS erstellte Apps, deren Entwickler leicht zu ermitteln sind. Android ist dagegen für alle Entwickler zugänglich. Dabei spielt es keine Rolle, ob sie über den Google Play Store oder andere Portale legale Anwendungen oder Malware anbieten.

Viel genutzt, aber selten geschützt

Das Infizieren der Smartphones mit Viren und Co. ist für die Cyber-Kriminellen noch aus einem anderen Grund eine leichte Übung: Nach Schätzungen von Experten ist gerade einmal auf fünf Prozent der weltweit im Einsatz befindlichen Smart-

phones und Tablets eine Sicherheitssoftware installiert.

Dabei kommen Mobiltelefone zunehmend als „mobile Geldbörse" oder für die Verifizierung zum Einsatz, etwa wenn der Nutzer die Anmeldedaten seines E-Mail-Accounts vergessen hat. Viele Smartphone-Besitzer wickeln zudem Bankgeschäfte oder Einkäufe mit ihrem Mobilgerät ab.

Dieses Einfallstor lässt die Malware-Branche nicht ungenutzt. So entdeckten Sicherheitsexperten erst letztes Jahr die erste mobile Schadsoftware mit Drive-by-Download. Bei dieser Methode lädt der Anwender beim Besuch einer präparierten Webseite unwissentlich unerwünschte Schadsoftware auf sein Gerät herunter. Diese nutzt dann beispielsweise Sicherheitslücken eines Browsers aus, etwa um das Gerät unter die Kontrolle des Angreifers zu bringen.

Papier ist nicht die bessere Alternative

Bei all den Bedrohungen stellt sich die Frage, ob der Einsatz eines Mobiltelefons für Vorgänge wie Online-Banking sinnvoll ist. Sind die TAN-Listen auf Papier möglicherweise doch vertrauenswürdiger? Diese Frage lässt sich mit einem klaren „Nein" beantworten. Gerade das TAN-Verfahren auf Grundlage von Papierlisten hat sich als potenzielle Gefahrenquelle erwiesen. Fachleuten aus der Cyber-Crime-Szene gelang es innerhalb kurzer Zeit, die Algorithmen zur Erstellung dieser TANs zu ermitteln.

Das m-TAN-Verfahren, das bei einer Online-Transaktion eine einzelne TAN für diesen Vorgang generiert und per Mobilfunk bereitstellt, ist deutlich sicherer. Dennoch lässt sich auch dieses Verfahren mit Hilfe von Trojanern aushebeln: Sie stehlen die Log-in-Daten, loggen sich in das System der Bank ein und beantragen eine mobile TAN für eine Überweisung. Anschließend gibt die Schadsoftware automatisch die Transaktionsnummer ein und überweist Geld auf ein Konto des Angreifers. Solche Trojaner sind in der Lage, nicht nur stationäre und mobile Rechner auszuspähen, sondern auch Smartphones.

Sicherheitssoftware hilft

Ein Beispiel für diese Malware-Gattung weist der Mobile Threat Report von F-Secure erstmals im vierten Quartal 2012 mit Zitmo.A (Zeus für mobile Android) aus. Dabei handelt es sich um eine mobile Variante des Carberp-Trojaners. Er ist benannt nach der russischen Carberp-Bande, die vor allem im Bankenumfeld aktiv ist. Die Schadsoftware arbeitet ähnlich wie Zitmo und Spitmo (Spy-Eye for mobile) und entwendet genau nach dem oben beschriebenen Vorgehen m-TANs, um Geld von Anwenderkonten auf die Bank-Accounts der Online-Ganoven zu transferieren.

Die gute Nachricht: Bankkunden können sich mit Sicherheitssoftware für Mobilgeräte gezielt gegen solche Attacken schützen. So bietet beispielsweise das Schweizer Telekommunikationsunternehmen Swisscom seit geraumer Zeit ein komplettes Sicherheitspaket für Smartphones und Tablets an, um im mobilen Umfeld eine Sicherheitsbarriere aufzubauen. Es basiert auf dem Home-User-Produkt F-Secure-Mobile-Security und ermöglicht es Swisscom-Vertragskunden, diesen Dienst über ihren mobilen Zugang zu nutzen. Bei Verlust oder Diebstahl des Geräts, bei Infektionen durch mobile Schadprogramme oder bei Spionage-Angriffen sichert die Lösung die vertraulichen und persönlichen Daten ab.

Die gängigsten Malware-Formen auf einen Blick

Virus: Programm-Code, der sich mit Hilfe eines Wirtsprogramms weiterverbreitet. Programm-Viren kopieren sich in eine ausführbare Datei, Daten-Viren befallen reine Datendateien, Bootsektor-Viren Festplatten und Disketten (sehr selten geworden).

Wurm: Computerprogramm, das sich eigenständig in einem Netzwerk verteilen kann. Durch den Verbrauch von Systemressourcen sollen Anwendungen beeinträchtigt oder lahmgelegt werden. Ein Wurm benötigt keinen Wirt, sondern verbreitet sich selbstständig weiter. Beispiel: Bluetooth-Würmer befallen Smartphones und andere mobile Endgeräte über eine drahtlose Bluetooth-Verbindung und verschicken sich selbst in Form von Informationen oder als Programm.

Trojaner: Programm ohne Replikationsmechanismus, das vordergründig Vertrauen erweckt, aber eine verborgene Schadfunktion enthält. Es gewährt dem Hacker Zugriff auf sämtliche Computer-Funktionen. So kann er Programme starten, Dateien kopieren und löschen oder alle Tastaturanschläge mit protokollieren. Trojanern sind typischerweise auf bestimmte Aufgaben spezialisiert wie Passwörter stehlen, Schadprogramme aus dem Internet laden oder Informationen über das infizierte System an die Hacker senden.

Phishing: Begriff aus „password" und „fishing". Gezielte Manipulation von Menschen, um mit Hilfe gefälschter E-Mails oder Webseitensuchen vertrauenswürdige Nutzer-Daten zu erhalten. Typische Beispiele sind Benutzernamen, Passwörter, Kreditkartennummern oder Bankdaten. Bei Phishing werden weder das Betriebssystem noch andere Bereiche des PCs manipuliert.