

"Der Fokus der Angreifer liegt zur Zeit ganz klar auf Android"

DANIEL AJ SOKOLOV, 22. September 2011 17:00

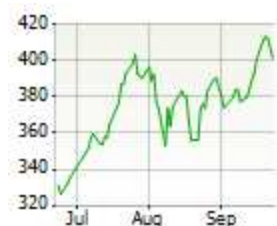


"Das schwächste Glied in der Kette wird angegriffen: Der User"

APPLE

USD 401,82

-2,50% ↓



GOOGLE

USD 520,66

-3,44% ↓



Smartphones sind beliebt - bei Kriminellen - Größte Schwachstelle ist der User

Im Juni 2004 tauchte die erste Schadsoftware für Mobiltelefone auf. Der vermutlich in Frankreich entwickelte "Cabir" verbreitete sich über Bluetooth auf Geräte mit Symbian-Betriebssystem. Der von Cabir angerichtete Schaden hielt sich in Grenzen, im Wesentlichen war der Schädling nur darauf bedacht, sich selbst weiterzuverbreiten.

Probleme

Dennoch stellte er die Hersteller von Virenschutz-Software vor Probleme. Deren Ingenieure waren darauf spezialisiert, Code für x86-CPU und vor allem Windows-Systeme zu analysieren. Mit Befehlen für ARM-Prozessoren und Symbian mussten sie sich erst vertraut machen. Heute hat sich das Bild gewandelt. Leistungsfähigkeit und Verbreitung von Smartphones sind enorm gestiegen. Auch die Nutzung hat sich geändert. So werden etwa mit dem Handy immer häufiger Einkäufe und Bankgeschäfte erledigt.

Entsprechend attraktiv sind Smartphones für Kriminelle geworden. Über 5.000 Mobil-Schädlinge sind inzwischen

bekannt, Tendenz steigend. Gegenüber dem täglichen (!) Zuwachs von 45.000 bösartigen Programmen für herkömmliche Computer ist das zwar wenig, doch kann ein gekapertes Handy eine ungeahnte Hebelwirkung für organisierte Verbrecher und Cracker im Staatsauftrag entfalten.

Geheimdienste, Polizei, Steuerfahnder, ...

Letztere suchen vor allem Informationen (Geheimdienste, Polizei, Steuerfahnder) oder wollen (zer)stören (Armee). Erstere sind vorrangig an Geld interessiert. Der Weg vom Eindringen in ein System zum Geld ist bei Handys häufig kürzer, als bei herkömmlichen Computern. Denn die meisten Handys können "Mehrwertdienste" nutzen oder exotische Auslandsdestinationen anrufen (wo der Inhaber eines Gateways Ausschüttungen abzweigen kann). Mit der zunehmenden Verbreitung von E-Banking und Online-Shopping am Handy, m-payment und mobilen Zahlungsverfahren wie NFC vervielfachen sich die Betrugsvarianten.

TAN für E-Banking-Transaktionen

Immer häufiger werden die TAN für E-Banking-Transaktionen per SMS auf Handys übertragen. Dies soll Trojanern auf dem Computer des Kunden die Arbeit erschweren. Ist aber auch dessen Handy infiziert, haben die Verbrecher relativ leichtes Spiel.

Die Doppel-Infektion ist dabei einfacher, als vielfach angenommen. Einerseits werden Handys immer häufiger mit herkömmlichen Computern verbunden, sei es über USB oder Bluetooth. Das Handy mag als Modem, Fotoapparat oder MP3-Player dienen oder auch nur ein Software-Update benötigen, die Verbindung mit dem PC drängt sich auf. Ist eines der beiden Geräte von einem Schädling befallen, ist der Weg zur Infektion des anderen nicht weit.

Bei vielen Android-Geräten kann Software auch über einen gekoppelten Google-Account aufgespielt werden, eine Bestätigung am Handy ist gar nicht mehr erforderlich. Sind also Google-Account oder der PC gehackt,

gelangt man relativ einfach aufs Handy.

Wlan

Andererseits haben immer mehr Smartphones auch WLAN mit an Bord. Dies ist für unerwünscht Neugierige sehr attraktiv. Einen WLAN-Zugangspunkt mit dem selben oder einem ähnlichen Namen wie ein bekannter, unverdächtiger Hotspot ist schnell eingerichtet - und schon kann Datenverkehr mitgelesen und beeinflusst werden.

Abhilfe würde die konsequente Verschlüsselung der Datenübertragung sorgen. Doch häufig wird das von Websites, Mail-Servern und anderen Diensten nicht standardmäßig aktiviert oder gar nicht unterstützt. Zudem sind die Zertifikate, die die Identität der Gegenstelle bestätigen sollen, nicht mehr unbedingt vertrauenswürdig. Bei potenziell unsicheren WLAN-Hotspots kann ein VPN (Virtual Private Network) schützen. Dabei wird der gesamte Datenverkehr verschlüsselt und über einen Server geleitet - und erst dort gelangen die Informationen unverschlüsselt ins Internet. Der Betreiber eines WLAN-Hotspots kann also nicht mitlesen oder beeinflussen.

"Privatkunden scheuen diese Kosten in der Regel."

"Der Haken an der Sache ist, dass ein VPN-Dienst Geld kosten, sofern er nicht bereits im Firmennetz verfügbar ist", meinte Sicherheitsberater Klaus Darilion von der Wiener Firma IPcom, "Privatkunden scheuen diese Kosten in der Regel." Zwar gibt es auch einige gebührenfreie VPN-Angebote, aber deren Qualität schwankt. Und das Vertrauensproblem wird lediglich vom Hotspot zum VPN-Betreiber verlagert.

Ein manipuliertes Mobiltelefon mit WLAN-Funktion kann außerdem in einem zuvor sicheren Netz Angreifern Tür und Tor öffnen. Somit muss sich ein Cracker nicht mehr durch die Firewall eines Ministeriums oder einer Bank quälen. Er infiziert Mobiltelefone der Mitarbeiter und wartet bis eines dieser Geräte in dem Betrieb über WLAN online geht und dabei von innen einen Port öffnet.

Wettrennen

Zudem können Handys Informationen liefern, die der Computer am Schreibtisch oder der Laptop nur selten haben: Wer wann wo mit wem was kommuniziert. Geodaten, SMS, E-Mail, Fotos, soziale Netzwerke und Aufzeichnungen von Telefonaten oder sogar nur in der Umgebung des Handys geführte Gespräche sind sehr attraktiv für Informations-Diebe.

Also hat das Wettrennen der Hacker mit den Viren-Bekämpfern längst begonnen. Der österreichische Anti-Viren-Spezialist Ikarus wird noch im September einen kostenlosen Virenschanner für Android-Handys herausbringen. Für Businesskunden gibt es schon länger die Möglichkeit, den mobilen Datenverkehr unabhängig von Netzbetreiber oder Betriebssystem verschlüsselt über einen Proxy zu leiten (VPN) und zusätzlich von Ikarus auf Gefahren durchsuchen zu lassen.

"Der Primärfokus der Angreifer liegt zur Zeit ganz klar auf Android"

Mit Applikationen am Handy selbst startet Ikarus bewusst mit Googles Android. "Der Primärfokus der Angreifer liegt zur Zeit ganz klar auf Android", erläuterte Ikarus-CEO Joe Pichlmayr gegenüber dem WebStandard, "Insbesondere günstigere Prepaid-Modelle sind beliebte Ziele. Bei täglich (!) 500.000 neuen Android Telefonen ist der Markt für Angreifer einfach zu 'verlockend'."

Symbian tritt aufgrund rückläufiger Marktanteile langsam in den Hintergrund. Microsofts Windows Phone hat (im Unterschied zu den PC-Betriebssystemen) einen viel zu geringen Marktanteil. Und Apples iOS profitiert in dieser Hinsicht vom geschlossenen System. Die Zahl der jailbreaKed (und damit bereits gehackten) iPhones ist relativ gering und die Kontrolle der im App Store verfügbaren Software relativ rigide. Zumindest für Wirtschaftskriminelle sind Android-Ziele attraktiver.

Zero-Day-Exploits

Handy-Betriebssysteme sind meist deutlich sicherer gestaltet, als es frühe PC-Betriebssysteme waren. Dennoch musste Cabir im Jahr 2004 keine Zero-Day-Exploits und ungewöhnliche Systemzustände ausnutzen. Der Wurm suchte einfach nach anderen Bluetooth-Geräten, die sich freimütig zu erkennen gaben, und bat diese um die gefällige Erlaubnis sich hinüberzukopieren. Der Nutzer des Zielgerätes musste seine

Zustimmung erteilen. Solange er sie verweigerte, war sein Handy sicher.

Dieses Bild hat sich bis heute kaum geändert. Die größte Schwachstelle in Sicherheitsbelangen ist und bleibt der Mensch. Zwar können auch Schwachstellen in der Software für Attacken ausgenutzt werden, aber wozu der Aufwand, wenn es auch einfach geht...

"Das schwächste Glied in der Kette wird angegriffen: Der User"

"Das schwächste Glied in der Kette wird angegriffen: Der User", so Pichlmayr, "Das kann so genanntes Social Engineering sein mit einer guten Phishing-Lüge." Auch vom PC bekannte Ansätze, wo Malware als "Flash-Player-Update" oder neuer Video-Codec untergejubelt wird, sind bekannt. "Das Handy-Betriebssystem selbst würde ein derartige Installation nicht zulassen", betont der Virenbekämpfer, "Es ist immer der User, der dem Angriffs-Tool alle erforderlichen Rechte einräumt."

Schlag nach bei Cabir.

Beliebt ist auch die Verfälschung legitimer Programme. 99 neue Angry Bird Levels können Freude bereiten - besonders Jenem, der ein bisschen Zusatzcode eingeschleust hat. Und natürlich gibt es auch in der Handy-Software selbst Schwachstellen, die ausgenutzt werden. iPhone-Inhaber genießen hier den Vorteil relativ schneller Updates durch Apple - wenn sie die Aktualisierungen auch einspielen. Aus Bequemlichkeit, Angst vor Datenverlust oder dem drohenden Verlust eines erfolgreichen Jailbreaks wird das aber von Manchen unterlassen.

Updates

Wer ein Android-Handy verwendet muss auf sein Update oft erschreckend lange warten. Denn die Hersteller reagieren unterschiedlich schnell. Häufig weisen Geräte, die von Netzbetreibern in Umlauf gebracht werden, speziell angepasste Software auf. Dann muss ein Update erst die Qualitätssicherung des Netzbetreibers durchlaufen. Dies verzögert die Schließung bereits bekannter Sicherheitslücken weiter, für ältere Modelle wird der Aufwand bisweilen ganz unterlassen. Hier haben Google und seine Partner noch Aufholbedarf.

Am Teuersten ist guter Rat aber, wenn der Telefonapparat selbst abhanden kommt. Beim Fall in die Badewanne oder Toilette sind vielleicht die Daten weg. Beim Liegenlassen oder einem Diebstahl geraten sie aber in falsche Hände, was weitaus schwerer wiegen kann. Selbstredend gibt es dafür schon eine Menge Apps. Sie ermöglichen das Löschen der Daten aus Ferne und/oder die (ungefähre) Lokalisierung des verschwundenen Objekts. "Das hilft aber höchstens bei Dieben, die das Handy selbst verkaufen wollen. Bei Spionage ist das nutzlos", weist Darilion auf, "Die Täter deaktivieren die Netzverbindung oder nehmen einfach den Akku raus. Oder sie ziehen schnell ein Speicherabbild und legen das Handy zurück." Dann ahnt das Opfer vielleicht nicht einmal etwas von dem erfolgten Datendiebstahl. (Daniel AJ Sokolov, derStandard.at, 25.9.2011)

Links

Ikarus

© derStandard.at GmbH 2011 -

Alle Rechte vorbehalten. Nutzung ausschließlich für den privaten Eigenbedarf.

Eine Weiterverwendung und Reproduktion über den persönlichen Gebrauch hinaus ist nicht gestattet.