Der Spion in der Tasche

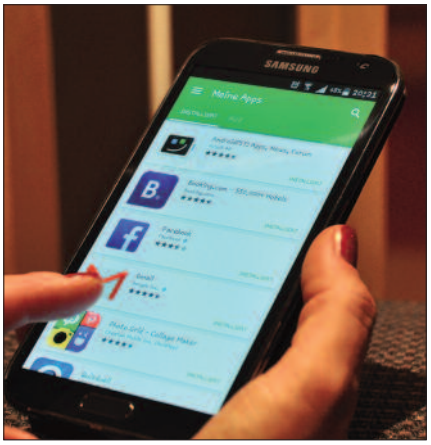
Apps ermöglichen einen schnellen Zugriff auf Anwendungen auf mobilen Geräten. Doch viele Apps enthalten Schadcodes, die Zugriff auf Geräte und Manipulation von Daten ermöglichen.

Mit der Nutzung von Smartphones und Tablets steigt die Zahl der Anbieter von Applikationen (Apps) für mobile Geräte. Laut dem Marktforschungsinstitut *Gartner (www.gartner.com)* wurden 2013 weltweit mehr als 102 Milliarden Apps aus App-Stores heruntergeladen. Immer mehr Menschen greifen über mobile Geräte auf das Internet zu. Diese Entwicklung wird durch ein steigendes Angebot an Online-Speichermöglichkeiten und günstige Tarife begünstigt. Laut dem Jahresbericht der Rundfunk und *Telekom Regulierungs-GmbH (RTR)* wurden 2013 von Kunden österreichischer Mobilfunknetze 110.000 Terabyte an Daten – Up- und Downloadvolumen – verbraucht. Der Datenverbrauch wird mit der Verbreitung der LTE-Technologie und der Zunahme an datenbasierten Anwendungen auf mobilen Endgeräten weiter steigen.

Mobile Geräte, die ständig eingeschaltet sind, sind Angriffsziele für Kriminelle. Während bei der Benützung von PCs mittlerweile ein Sicherheitsbewusstsein für Schutzmaßnahmen (Virenschutz, Firewall u. a.) gegeben ist, lässt dieses bei mobilen Geräten noch auf sich warten. Allein der Verlust oder Diebstahl eines Smartphones kann weitreichende Folgen haben, wenn die darauf gespeicherten Daten ausgelesen und verwertet werden können.

Angriffe auf mobile Geräte erfolgen häufig durch Schadsoftware. Diese muss nicht immer erkennbar sein. Eine Applikation aus einer vertrauenswürdigen Quelle (z. B. *Google-Play)* kann genauso zu einem Datenverlust oder Datendiebstahl führen.

Apps sind unabhängig von Betriebssystem und Hersteller kritisch, da sie an den Hersteller Nutzerinformationen übermitteln. Speziell bei Android-Apps besteht die Gefahr einer Infektion durch Schadsoftware, da nur unzureichende Kontrollmechanismen zu ihrer Überprüfung eingesetzt werden. Dazu zählt die Überprüfung einer App, bevor diese im App-Store zur Verfügung gestellt wird. Entgegen anderen Plattformen erfolgt unter *Google-Play* keine



Apps für mobile Geräte sollte man nur aus sicheren Quellen beziehen.

wirkungsvolle Überprüfung auf die Bösartigkeit von Anwendungen. Abgesehen von einem Hinweis beim Installationsvorgang, bei dem die App bestimmte Berechtigungen fordert, gibt es für den Benutzer keine Information über mögliche Risiken. Nutzer können bösartige Apps zumeist nicht erkennen.

Eine harmlos wirkende Spiele-App kann kostenpflichtige Anrufe tätigen oder SMS an Premium-Dienste versenden. Eine Phishing-App, die als Sicherheitszertifikat getarnt ist, kann eingehende SMS auf mTANs prüfen und sie unbemerkt an Unbefugte weiterleiten. Werden der App Berechtigungen zum Nachladen von Programmteilen und zum selbstständigen Aufbau einer Internetverbindung erteilt, kann die Anwendung automatisch Programm-Updates durchführen und Programm-Codes nachladen.

Berechtigungen für Apps. Viele Apps verlangen unverhältnismäßig mehr Rechte, als für deren Funktionalität notwendig ist. Ein Beispiel von vielen Taschenlampen-Apps für Android ist die vom Entwickler *Golden-Shores Technologies,* die über 1,2 Millionen-Mal von *Google-Play* heruntergeladen worden ist. Wenn man dieser App die entsprechenden Rechte gewährt, kann sie den Standort des Gerätes bestimmen, auf gespeicherte Daten zugreifen, Bilder und Videos aufnehmen und die Anrufer-ID sowie die Nummer eines verbundenen Gesprä-

ches ermitteln. Vor der Installation einer App aus *Google-Play* wird dem Benutzer eine Liste mit Berechtigungen angezeigt, bevor mit dem Button „Installieren“ bestätigt wird.

Sollte nicht klar sein, warum beispielsweise eine Spiele-App auf persönliche Informationen und den Standort zugreifen will, sollte sie dazu nicht berechtigt werden. Auf dem Smartphone lassen sich die Berechtigungen bereits installierter Apps unter den Einstellungen aufrufen und in einigen Betriebssystemversionen auch nachträglich ändern, entweder unter „Einstellungen“ und „Apps“ oder „Anwendungsmanager“ und „App-Name“.

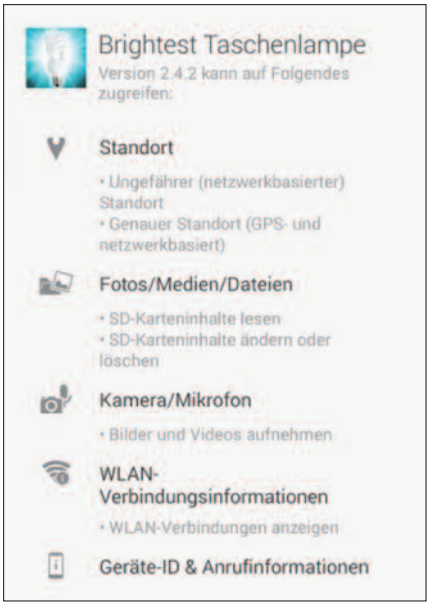
Aufforderung per SMS. Nicht nur in den offiziellen App-Stores lauert die Gefahr von Schadprogrammen. Oft erfolgt die Aufforderung zur Installation einer angeblichen Sicherheits-App per SMS. Der Nutzer wird per Link zu einem Server im Internet geleitet, wo die bösartige Anwendung hinterlegt ist. Sobald die Anwendung installiert wird, ergeben sich viele Einsatzmöglichkeiten für den Angreifer.

Damit die Malware vorerst unerkannt bleibt, erfolgt das Nachladen von bösartigen Programmcodes erst zu einem späteren Zeitpunkt. Die Anwendung erkennt anhand der Gerätesensoren den besten Zeitpunkt, um aktiv zu werden, beispielsweise zur Nachtzeit. Für das Schadprogramm und den Angreifer ergibt sich der Vorteil, dass die Geräteleistung voll zur Verfügung steht, während der Eigentümer schläft. Dies bildet eine geeignete Voraussetzung zur Errichtung eines mobilen Botnets. Dabei werden weltweit massenweise Smartphones infiziert, die relativ einfach durch den Botnet-Besitzer gesteuert werden können.

Im Gegensatz zu privat genutzten PCs sind Smartphones meist dauerhaft mit dem Internet verbunden und können von den Botnet-Betreibern benutzt werden, wann immer sie wollen. Ein solches Schadprogramm war unter anderem als *Android.B.Master* bekannt. Kriminelle konnten damit einen Umsatz von mehreren Millionen Dollar er-

FOTO: BERNHARD ELBE

Viele Smartphone-Besitzer nutzen oft bedenkenlos frei zugängliche WLAN-Netzwerke und Hotspots, ohne entsprechende Sicherheitsvorkehrungen anzuwenden.



Berechtigungen einer Taschenlampen-App für Android.

zielen, indem infizierte Smartphones ohne Zutun des Besitzers kostenpflichtige Premium-Dienste kontaktierten. Dem Einfallsreichtum von Kriminellen sind dabei keine Grenzen gesetzt.

Eines von vielen Beispielen war die Zusendung von E-Mails und SMS, die augenscheinlich von einem großen Paketzusteller stammten. In der Nachricht war der angebliche Liefer- und Zustellstatus eines Pakets unter Zusatz eines Internet-Links angeführt. Sobald dieser aufgerufen wurde, erfolgte die Installation des Schadprogramms, das eigenständig Premiumdienste in Anspruch nahm. Zusätzlich wurden die Kontaktdaten des Telefons ausgelesen und automatisch SMS-Nachrichten mit beigefügtem Web-Link an diese Kontakte verschickt. Als Zusatzfunktion verfügte diese Variante über die Möglichkeit der Sperre eines infizierten Mobilgerätes, um für die Freigabe „Lösegeld“ zu fordern.

Phishing. Die steigende Nutzung von Bankgeschäften (Mobile-Banking) mit Smartphones und die Einführung neuer Sicherheitsvorkehrungen sowie geänderte TAN-Verfahren zogen neue Formen von Phishing-Attacken nach sich. Dabei wurden PCs von Internetnutzern mit einem Trojaner infiziert, der Banking-Websites manipulierte und die Nutzer zur Eingabe des Handy-Modells und der dazu gehörenden Rufnummer aufforderte. Viele Nutzer ließen sich mit dem Vorwand der erhöhten Absicherung des mTAN-Verfahrens täuschen. Es folgte eine SMS-Mitteilung mit einem Web-Link zu einem angeblichen Sicherheits-Zertifikat. Sobald der Benutzer dieses aufrief, wurde ein Trojaner auf dem mobilen Gerät installiert. 2012 wurde in Europa allein mit dem Smartphone-Trojaner „Eurograbber“ ein Schaden von 36 Millionen Euro verursacht, mehr als 30.000 Bankkunden waren betroffen.

Eine aktuelle Variante einer „Sicherheits-App“ für Android-Systeme, die für Phishing-Angiffe verwendet wird, erkennt anhand der Geräte- und Benutzerdaten den Länder-Standort und verwendet das passende Logo einer Bank des jeweiligen Landes. Wenn sie bei der Installation umfangreiche Zugriffsrechte auf verschiedene Telefonfunktionen fordert, sollten Anwender misstrauisch werden. Die App zielt nicht nur auf das Auslesen von SMS und von mobilen TANs ab, sie ermöglicht einem Angreifer auch das Abhören der Smartphone-Umgebung. Sobald eine derartige Anwendung auf dem Gerät ausgeführt wird, befindet sich das Gerät mehr oder weniger „in fremder Hand“.

Passwort-Verlust. Viele Smartphone-Besitzer nutzen ohne entsprechende Sicherheitsvorkehrungen frei zugängliche WLAN-Netzwerke und Hotspots, ohne sich Gedanken zu machen, wer eigentlich diesen Zugang zur Verfügung stellt oder im Netzwerk mitlesen kann. Allzu leicht lassen sich Zugangs-

FOTOS: BUNDESKRIMINALAMT, KASPERSKY

SMARTPHONES

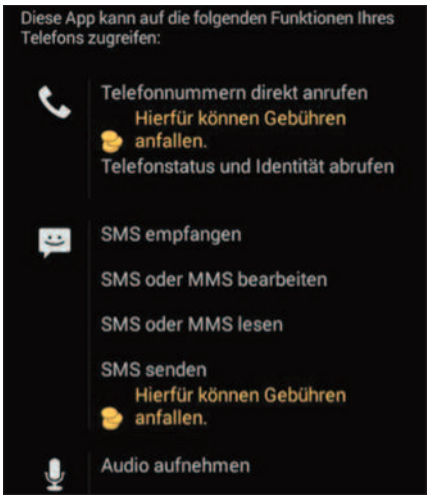
Sicherheitstipps

- Vorsicht bei der Nutzung öffentlicher WLAN-Hotspots.
- Smartphone nie unbeaufsichtigt lassen oder fremden Personen anvertrauen.
- Anti-Viren-Programme (Viren-Scanner) für Smartphones nutzen.
- Betriebssystem und Anwendungen regelmäßig updaten.
- Nur Apps aus sicheren Quellen beziehen.
- Werden für die Installation von Apps mehr Berechtigungen eingefordert, als für deren Funktion erforderlich ist, sollte diese Anwendung nicht installiert werden.
- Nicht benötigte Zusatzdienste (WLAN, GPS, Bluetooth) deaktivieren.
- Vorsicht bei E-Mails oder SMS, die dem Anschein nach von einer Bank oder von Online-Zahlungsdiensten stammen und zum Download einer Datei auffordern oder die Installation von Security-Anwendungen (z. B. „Sicherheitszertifikat“) anregen. Dahinter stecken oftmals Schadprogramme, die unbemerkt Zugangsdaten und mTANs für Online-Banking ausspionieren.

daten für soziale Netzwerke, E-Mail-Konten und andere Anwendungen auslesen. Kritisch wird es, wenn ein einziges Passwort für alle Benutzerkonten und Online-Accounts verwendet wird. Derart erworbene Zugangsdaten werden in Internet-Foren gehandelt.

„Datenhehler“ verkaufen oft nur die Rohdaten, also den gesamten aufgezeichneten Datenverkehr, wobei die „Abnehmer“ nach verwertbaren Daten wie Zugangsdaten suchen müssen. Eine Folge davon sind Bettelbriefe: Internetbetrüger melden sich mit den erworbenen Zugangsdaten unter einem fremden *Facebook*-Konto an und schicken den dort gespeicherten Kontakten eine Nachricht, indem eine fingierte Notlage vorgetäuscht und um Zusendung von Geld ersucht wird.

Den Betroffenen und Opfern ist dabei nicht bewusst, dass die Zugangsdaten schon während eines Auslands-Aufenthalts durch Nutzung eines ungesicherten WLAN-Zugangs im Restaurant oder im Hotel ausgelesen wurden. Gelangen auch die Zugangsdaten des Kontos, mit dem das Smartphone verknüpft ist, in falsche Hände, kann auf das Gerät via Internet zugegriffen werden. Gelingt die Anmeldung unter einem fremden Benutzerkonto, sind alle damit verknüpften Mobilgeräte ersichtlich, der Standort abrufbar, Kalendereinträge, Dateien, Kontaktdaten und Mail-Nachrichten zugänglich sowie die Installation von Apps per Mausklick und das Löschen von Dateien möglich. Die Analyse von Smartphone-Malware ist oft schwierig, da verschiedene Ermittlungsschritte erforderlich sind, wobei die Verhältnismäßigkeit und der Zeit- und Personalaufwand eine Rolle spielen. Zudem hat sich in der Praxis gezeigt, dass technische Ermittlungsmaßnahmen allein wenig zielführend sind. Im ersten Angriff muss die bösartige Anwendung identifiziert werden. Abhängig von der Software-Plattform, sind verschiedene Untersuchungsschritte erforderlich. Dies reicht von der Aufzeichnung des Datenverkehrs im Live-Betrieb bis hin zur Analyse des Programmcodes und kann einige Tage bis Wochen in Anspruch nehmen, bis verwertbare Ergebnisse vorliegen.



App für Phishing-Angiffe: Die Schadsoftware verlangt umfangreiche Zugriffsrechte auf Telefonfunktionen.

Erschwerend kommt hinzu, dass Cyber-Kriminelle flexibel und rasch agieren, indem weltweit verschiedene Websites und Server nur kurze Zeit verwendet werden und bereits nach wenigen Stunden nicht mehr online sind. Durch dieses Vorgehen wird die Sicherung von Beweismitteln zusätzlich erschwert. Eine effektive Ermittlungsarbeit ist nur durch das Zusammenwirken verschiedener Ermittlungsbereiche und Abteilungen sowie internationale Kooperation möglich. *Horst Reisner*

FOTO: BUNDESKRIMINALAMT