FOKUS: SECURITY

Risiko Smartphone

Mit der Flut selbst mitgebrachter Smartphones und Tablets treten ganz neue Sicherheitsprobleme auf. Dabei stellt sich heraus: Es sind weniger Viren, die den Security-Verantwortlichen Sorgen bereiten, sondern die Schussligkeit der Anwender.

→ VON JENS STARK

Ohnmächtig muss die IT zusehen, wie ein Mitarbeiter nach dem anderen sein privates Smartphone oder Tablet ins Unternehmen mitbringt und an die IT-Infrastruktur ankoppelt. Da meist der Chef der Erste ist, der den Modetrend «Bring Your Own Device» verinnerlicht, bleibt den Security- und IT-Verantwortlichen nur übrig, die Faust im Sack zu machen. Denn verbieten lässt sich die Lawine bekanntlich schon längst nicht mehr. Um die Anzahl schlafloser Nächte zumindest zu reduzieren, sollten sich die IT-Verantwortlichen einmal vor Augen führen, wo die Gefahren in Sachen Smartphone-Security tatsächlich lauern. Dabei stellt sich dann schnell heraus, dass das höchste Risiko nicht in klassischer Malware wie Viren, Trojanern und infizierten Websites zu suchen ist, sondern vielmehr bei etwas ganz Banalem: dem Verlust des Smartphones.

Wenn selbst der Prototyp der nächsten iPhone-Generation von einem Apple-Mitarbeiter auf dem Tresen einer Bar im Silicon Valley «verloren gehen» kann – wie vor gut einem Jahr geschehen –, kann man sich gut vorstellen, dass die mobilen Begleiter ganz normaler Anwender noch viel öfter während einer feuchtfröhlichen Stunde im Pub, bei der Personenkontrolle am Flughafen oder auf dem Rücksitz eines Taxis unbemerkt zurückbleiben.

HÖCHSTES RISIKO: VERGESSLICHKEIT

Die EU-Organisation Enisa (European Network and Information Security Agency) geht davon aus, dass rund zwei Prozent der Smartphones verloren oder gestohlen werden. Das Problem dabei: Die Geräte enthalten mittlerweile höchst heikle Informationen. Zum einen sind dies wichtige private Daten wie Adressen, Fotos und Kreditkarteninfos, zum anderen immer mehr Geschäftsinformationen wie etwa die Firmen-E-Mails samt brisanten Attachments. Die Enisa bewertet daher die Datenweitergabe durch den Verlust respektive den Diebstahl von Smartphones als höchstes Risiko in Sachen mobiler Security (vgl. Tabelle rechts). Erst an vierter Stelle rangieren klassische Gefahren wie Phishing- oder Spyware-Angriffe.

«Wo es viele Freiheiten gibt, ist auch viel Missbrauch möglich»

Andrej Massaro, Sophos Schweiz

Schweizer Security-Experten schätzen das Gefahrenpotenzial ganz ähnlich ein. So teilt René Eberhard, CEO des unter anderem auf mobile Sicherheit spezialisierten IT-Security-Dienstleisters Keyon, grundsätzlich die Einschätzung der Enisa. Er geht sogar davon

BILD: FOTOLIA.COM/DRUBIG-PHOTO

«Angriffe auf Smartphones werden derzeit noch als zu wenig relevant eingestuft – ein Fehler»

René Eberhard, Keyon

«Innerhalb eines Jahres haben sich die Angriffe auf mobile Plattformen mehr als verdoppelt»

Candid Wüest, Symantec

aus, dass die Bedrohungen zunehmen, und moniert, dass «aktuell Angriffe auf Smartphones als noch zu wenig relevant eingestuft werden».

Auch Candid Wüest, Virenjäger bei Symantec Schweiz, findet es wenig verwunderlich, dass Verlust und Datenlecks ganz oben auf der Risikoliste stehen. Allerdings nehme auch die Bedrohung durch Malware zu: «Innerhalb eines Jahres haben sich die Angriffe auf mobile Plattformen mehr als verdoppelt», berichtet Wüest. «Wir konnten erstmals beobachten, dass Schadcode tatsächlich Schaden angerichtet hat, also damit Geld oder Daten gestohlen wurden.» Eine weitere Gefahr besteht laut dem Virenexperten darin, dass Anwender Schadcode über ihre mobilen Geräte in das interne Netzwerk einschleusen und damit weitere Firmensysteme infizieren.

Ein Problem, an das derzeit übrigens kaum jemand denkt, sind die vielfältigen Spionagemöglichkeiten durch die Benutzer, wie Andrej Massaro, neuer Country-Manager von Sophos in der Schweiz, zu Protokoll gibt: «Die Foto- und Scan-Funktionen moderner Handys führen zu einem enormen Spionagepotenzial», betont er. Böswillige Mitarbeiter bräuchten heute nicht mehr im Geheimen eine CD zu brennen, sie müssten nur das Handy zücken und die Dokumente abfotografieren.

WAHL DER RICHTIGEN PLATTFORM

Immer wieder wird im Zusammenhang mit den mobilen Plattformen auch die Frage aufgeworfen, welche der derzeit erhältlichen Betriebssysteme in Bezug auf die genannten Sicherheitsrisiken zu bevorzugen seien. Hier ist sich die von Computerworld befragte Expertenrunde einig, dass Googles Android-Betriebssystem die meisten Unsicherheiten aufweise. «Android ist heute die offenste Plattform und daher auch diejenige mit der grössten Angriffsfläche», so Keyon-CEO René Eberhard. Apples iOS stufen die Experten als vergleichsweise sicherer ein.

Wenn er eine Empfehlung abgeben müsste, würde sich Sophos-Schweiz-Chef Andrej Massaro für den BlackBerry von Research In Motion (RIM) aussprechen. Dies sei vor allem wegen der integrierten Verschlüsselung der Daten und dem hauseigenen Server für Unternehmen das sicherste System. Ganz sicher könne man sich aber auch hier nicht sein: «Es gibt Stimmen, die behaupten, dass der kanadische Betreiber RIM-Daten an gewisse Geheimdienste weitergeben muss.» Ansonsten plädiert auch Massaro für iOS statt Android. Letzteres lasse einfach zu viele Freiheiten «und wo es viele Freiheiten gibt, ist auch viel Missbrauch möglich», so sein Fazit.

VERGESST DAS BETRIEBSSYSTEM

Die Diskussion um die sicherste Plattform ist jedoch im Grunde genommen müssig. Zumindest im BYOD-Zeitalter wählen die Anwender die Plattform nicht nach Sicherheitskriterien aus, sondern danach, was in Sachen Smartphone und Tablet-PC gerade angesagt ist. Dieser Meinung ist auch Symantec-Virenjäger Wüest: «Der private Nutzer bringt sein eigenes Gerät in die Firma mit. Damit sind Fragen zum Betriebssystem obsolet, denn der Administrator wird im Ernstfall hierauf keinen Einfluss nehmen können.» Zudem verweist er auf die schnelle Entwicklung der Branche: «Niemand wird heute mit Gewissheit vorhersagen können, welches Gerät und Betriebssystem auf den Smartphones in zwei oder fünf Jahren populär sein wird.»

Einer Ansicht, der René Eberhard nur zustimmen kann: «Die hohen Produktezyklen bei Hardware und Software sowie kaum vorhandene Roadmaps der Hersteller, erlauben keine strategische und langfristige Planung der Sicherheit», meint der Keyon-CEO. Die Konsequenz: «Sicherheitstechnische Überlegungen müssen unabhängig von der Plattform gemacht werden.» Deshalb müssten künftig hauptsächlich die Daten geschützt werden und nicht mehr die Plattformen als solche, postuliert Eberhard. Auch Wüest rät den Entscheidern, «die Informationen und Identitäten der Firma zu schützen und zu managen, unabhängig von der Infrastruktur». Schliesslich würden heutzutage Daten dynamisch verschoben, und zwar sowohl auf mobile Geräte als auch auf physische wie virtuelle Server und in die Cloud. «Ein informationszentrischer Ansatz hilft, die wichtigen Dokumente in jeder dieser Umgebungen ihrem Wert entsprechend zu schützen», führt Wüest aus.

REMOTE WIPE WIRKUNGSLOS

Ein mobiles Devicemanagement, wie es viele Unternehmen heute als Sicherheitsmassnahme betreiben, reiche dann nicht mehr aus, argumentiert Andrej Massaro. Künftig werde mobile Security direkt auf dem Gerät ein Thema, also die konsequente Verschlüsselung der Daten, die Bekämpfung von Malware und die Kontrolle der genutzten Apps.

Eines der Verfahren, die heute bereits angewendet werden, ist das Löschen von Daten aus der Ferne. Die meisten Security-Anbieter bieten heute sogenannte Remote Wipes an. Geht das Smartphone verloren, lassen sich die Daten vom Besitzer löschen. Doch hundertprozentig sicher ist auch dieses Verfahren nicht. «Ein Remote Wipe ist wenig effektiv», gibt Keyon-CEO Eberhard zu bedenken. «Ein einfaches Entfernen der SIM-Karte oder ein Faraday-Käfig, der die Verbindung kappt, machen diese Massnahme wirkungslos», sagt er. Umso wichtiger wird es in Zukunft sein, dass die Daten auf den mobilen Geräten von vornherein für fremde Augen unlesbar – sprich verschlüsselt – sind. ←

Platz	Grund	Risiko	Beschreibung der Gefahr
1	Geräteverlust/-diebstahl	Hoch	Freier Zugang auf ungeschützten Speicher
2	Unachtsamkeit	Hoch	Der User gibt unabsichtlich Daten von seinem Smartphone preis
3	Altgeräte ausser Betrieb	Hoch	Das Smartphone wurde nicht ordnungsgemäss ausgemustert, die Daten bleiben für jeden lesbar
4	Phishing	Mittel	Abgreifen von Kreditkartennummern, Passwörtern und anderen heiklen Daten durch gefälschte Apps, E-Mails, SMS etc.
5	Spyware	Mittel	Installierte Spyware sammelt unentdeckt persönliche Daten
6	Network Spoofing	Mittel	Smartphones verbinden sich über «gefälschte» Access-Punkte (Wi-Fi, GSM); die Kommunikation wird dort von den Angreifern kontrolliert und für Attacken (z. B. Phishing) ausgenutzt
7	Überwachungsangriff	Mittel	Gezieltes Abhören eines ganz bestimmten Smartphone-Besitzers
8	Dialerware	Mittel	Malware nutzt Premium-Dienste oder -Nummern zum Abzocken
9	Financial Malware	Mittel	Spezielle Malware, die Bank-/Kreditkartendaten etc. abgreift
10	Netzwerk-Engpass	Leicht	Kein Netz aufgrund von Überlastung

Die Top-10-Risiken für Smartphones laut www.enisa.europa.eu