Dezember 2011 / Januar 2012
Deutschland € 14,90 Österreich € 16,40 Schweiz SFR 29,80
www.TecChannel.de

TECCHANNEL COMPACT

IT EXPERTS INSIDE

Ratgeber Smartphones & Tablets

iPhone, iPad & Android

iTuning

- iCloud richtig einsetzen
- Drucken mit iPad und iPhone

Apps für iOS & Android

- Unverzichtbare Pflicht-Apps
- Die besten Office-Apps im Vergleich

Sicherheit

- Smartphones und Tablets absichern
- Mobile Geräte sperren und fernlöschen

ISBN 419-5-9149-1490-4

Editorial

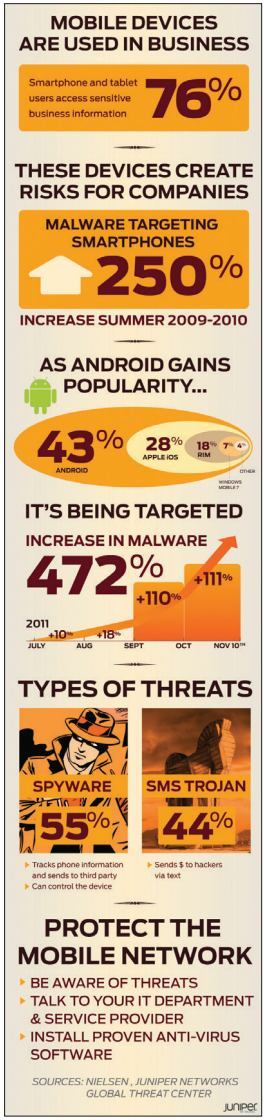
Sicher sind Sie nicht sicher!

„Smartphone-Anbieter müssen auf einem umkämpften Markt bestehen, der permanenten Änderungen unterworfen ist. Auf der Sicherheit der Smartphones oder der Applikationen liegt daher nicht immer die höchste Priorität.“ Dieser Satz stammt aus dem im November 2011 veröffentlichten „Überblickspapier Smartphones“ des BSI (www.tecchannel.de/2038283). In dem zwölf Seiten starken ePaper sind viele Gefahren aufgelistet, die man schon von PCs her kennt, die aber bei Smartphones besonders brisant sind. Phishing, Lauschangriff, Dialer, Trojaner(-Apps) – das komplette Portfolio an kriminellen Aktivitäten erlebt auf den mobilen Geräten eine Renaissance. Abgesehen von den telefonspezifischen Eigenschaften trifft die Problematik auch auf Tablet-PCs zu, denn die basieren auf den gleichen Betriebssystemen.

Für die Unternehmen heißt das: Für Datendiebstahl sind nicht mehr nur PCs und Notebooks das Angriffsziel. Die komplette heimische „IT-Infrastruktur“ der Mitarbeiter mit iPhone, iPad und iPod Touch ist ein viel leichter zu erreichendes Ziel. Dort sind die auf allen Geräten synchronisierten Unternehmensdaten viel einfacher zu holen. Auch andere Plattformen wie BlackBerry und besonders Android sind nicht sicher. Auch ohne Cloud sind Smartphones und Tablets alles andere als Sicherheitsfestungen.

Neben den Sicherheitsaspekten von mobilen Geräten im Speziellen ist deshalb auch der Einsatz von privater Hardware im Unternehmen mit seinen Folgen ein Schwerpunkt dieser Compact-Ausgabe. Wir geben Empfehlungen für die IT-Abteilung und zeigen, wie Endanwender selbst ihre Geräte im privaten wie beruflichen Einsatz sicherer machen. Bei aller Sicherheit kommt aber auch nicht zu kurz, mit welchen Apps Sie produktiver arbeiten und wie Sie mehr aus den Geräten herausholen.

Michael Eckert
Chefredakteur TecChannel



Auf einen Blick: Der Anstieg von mobiler Malware (Quelle: www.globalthreatcenter.com/?p=2492)

Inhalt

	Editorial	**3**
1	**Sicherheit**	**8**
1.1	**Studie: Attacken auf Firmen-IT über Smartphones und Tablets**	**8**
1.1.1	Zahl der Bedrohungen für mobile Endgeräte verdoppelt sich	8
1.1.2	Die Schwachstellen des Jahres	9
1.1.3	Klassische Spam- und Phishing-Attacken gehen zurück	10
1.1.4	Traditionelle Schwachstellen immer noch da	11
1.2	**Smartphones: Malware-Gefahr wächst**	**12**
1.2.1	Mobile Banking ist das Hauptziel der Angreifer	12
1.2.2	Sicherheitssoftware bald unverzichtbar wie auf PCs	13
1.3	**Angriffsziel Tablets: Die Attacken kommen**	**15**
1.3.1	USB-Ports sperren	16
1.3.2	Rootkit Tidserv befällt Windows-Rechner	16
1.3.3	Handel mit Verbrecher-Werkzeug	17
1.3.4	Gefahr mobiler Angriffe wächst	18
1.4	**Private Smartphones und Tablets sicher einbinden**	**19**
1.4.1	Welche Plattformen?	19
1.4.2	Verwaltung tut not	19
1.4.3	Self-Service-Portale entlasten die IT-Abteilung	20
1.4.4	Welche Anwendungen eignen sich?	20
1.5	**Sicherheitsrisiken von Smartphones, Tablets und Handys minimieren**	**22**
1.5.1	Smartphone-Verlust mit fatalen Folgen	22
1.5.2	Kinderkrankheiten in Sachen Sicherheit	22
1.5.3	Smartphones sind lohnende Angriffsziele	23
1.5.4	Mobile Endgeräte ungefährlicher machen	23
1.5.5	Sicherheitsaspekte bei Endgeräteauswahl beachten	23
1.5.6	Smartphones auf Sicherheitsrichtlinien prüfen	23
1.5.7	Vier Faktoren für den sicheren Betrieb	24
1.5.8	Sicherheit ist die Summe vieler Einzelaspekte	26
1.5.9	Checkliste	26
1.6	**Mobile Geräte wirkungsvoll gegen Missbrauch absichern**	**27**
1.6.1	Keine Sicherheitskonzepte	28
1.6.2	Mobile Geräte und soziale Netze	28
1.6.3	Safety first und sicher geht vor stylish	29
1.6.4	Any time, any place, any device	30
1.6.5	Applikationen als Service	31
1.6.6	Gut schlafen mit VPN	32
1.6.7	Firmendaten nie lokal speichern	32
1.6.8	Sperrung via Fernwartung	34
1.6.9	Zum Glück gezwungen	34
1.6.10	Itil als Basis	35
1.6.11	Attraktivität des Unternehmens	35
1.7	**Verwalten, Sichern, Sperren: Notfallplan für verlorene Smartphones**	**37**
1.7.1	Zehntausende von Notebooks und Smartphones „verschwinden“	37
1.7.2	Sicherheitsfunktionen des Smartphones nutzen	38

1.7.3	Apple setzt auf iCloud – Microsoft auf Windows Live	39
1.7.4	Kopplung mit Exchange oder Google Apps	40
1.7.5	Geschlossene, aber sichere Welt: BlackBerry	40
1.7.6	Virtualisierung: Privates und Geschäftliches auf einem Smartphone	41
1.7.7	Tools von Drittanbietern	41
1.7.8	Mit Firewall und Virenschutz	43
1.7.9	Verfahren für den Schutz mobiler Geräte	43
1.7.10	Der ganz große Ansatz: Mobile Device Management	44
1.7.11	Fazit	45
1.8	**Sicherheitsratgeber: Smartphones fernlöschen, orten und sperren**	**46**
1.8.1	Fernlöschen mit Exchange	46
1.8.2	Apps für Android	47
1.8.3	iCloud als MobileMe-Nachfolger	48
1.8.4	Windows Mobile, Android und Symbian – kostenloser Diebstahlschutz von F-Secure	49
1.8.5	Lookout für Android, BlackBerry und Windows Mobile	50
1.8.6	BlackBerry Protect	52
1.8.7	Diebstahlschutz mit Windows Phone 7	52
1.8.8	Fazit	53
1.9	**iOS, BlackBerry, Android und Windows im Sicherheits-Check**	**54**
1.9.1	Bedrohungslage	54
1.9.2	Hacker-Angriffe auf iPhone, Android und Windows	55
1.9.3	Drive-by-Download	56
1.9.4	Direkter Angriff auf Netzwerkebene	56
1.9.5	„Einschmuggeln“ von Schadsoftware	57
1.9.6	Diebstahl und Verlust mobiler Geräte	58
1.9.7	Unterstützung von Sicherheits-Policies in Mobilgeräten	60
1.9.8	Die Sicherheit von iPhone, iPad und Android aktualisieren	61
1.9.9	Fazit	62
2	**Apple iOS**	**63**
2.1	**Ratgeber: Das iPad im professionellen Einsatz**	**63**
2.1.1	iPhone-Apps auf dem iPad nutzen	63
2.1.2	iPad-Internetzugang per iPhone	64
2.1.3	iPad/iPad 2 und Exchange	66
2.1.4	Outlook Web App per Browser	67
2.1.5	Apps für Terminverwaltung und Kalender	68
2.1.6	iPad und SharePoint 2010	69
2.1.7	Apps für Admins	70
2.1.8	Datensicherung und Wiederherstellung	71
2.1.9	Datensicherung verschlüsseln	73
2.2	**Nützliche App-Grundausstattung für das iPhone**	**74**
2.2.1	Diese Apps gehören auf jedes iPhone	74
2.2.2	Boxcar	75
2.2.3	Reeder	76
2.2.4	IM+	77
2.2.5	wetter.info	77
2.2.6	iCab Mobile	78
2.2.7	Flashlight	79
2.2.8	Instapaper	79
2.2.9	Mein iPhone suchen / Find my iPhone	81
2.3	**Nützliche App-Grundausstattung für das iPad**	**82**
2.3.1	iCab Mobile	82

2.3.2	ReaddleDocs for iPad	83
2.3.3	IM+	84
2.3.4	Dropbox	85
2.3.5	TeamViewer HD	86
2.3.6	Night Stand HD	87
2.3.7	Mein iPhone suchen / Find my iPhone	87
2.3.8	Reeder for iPad	88
2.3.9	Tagesschau	89
2.3.10	Taschenrechner HD für iPad	91
2.4	**Workshop: Drucken mit iPhone und iPad**	**92**
2.4.1	Drucken mit iPhone und iPad – AirPrint offiziell nutzen	92
2.4.2	AirPrint für alle Drucker nutzen	93
2.4.3	Drucken mit Apps	94
2.5	**Praxis-Workshop: Apple iCloud richtig einsetzen und Probleme vermeiden**	**95**
2.5.1	iCloud einsetzen	96
2.5.2	Kalender, Mail und Kontakte – Zusatztool notwendig	97
2.5.3	Synchronisation konfigurieren	98
2.5.4	iCloud-E-Mails – Anbindung an Outlook und Co.	99
2.5.5	iCloud-E-Mail-Konto manuell einbinden	99
2.5.6	iPhone suchen, sperren und fernlöschen	100
2.5.7	Fotostream	102
2.5.8	Fazit	102
2.6	**Fotos in der iCloud löschen**	**103**
2.7	**Workshop: Apple iPad sicher betreiben**	**105**
2.7.1	Sicherheit mit Bordmitteln erhöhen: Code-Sperre aktivieren	105
2.7.2	Optionen der Code-Sperre	106
2.7.3	iPad mit Exchange und Office 365 betreiben	107
2.7.4	Nicht nur Admins können iPads löschen	109
2.7.5	Apps auf dem iPad sperren	110
2.7.6	Achtung bei der Installation von Apps und Ortungsdienste	110
2.7.7	Vorsicht mit iCloud und anderen Webdiensten	111
2.7.8	Sicherheitslücken beachten	112
2.7.9	Persönliche Daten vom iPad löschen	113
2.8	**Office-Suiten für Apple iPad im Vergleich**	**114**
2.8.1	Byte Squared Office^2 HD	114
2.8.2	DataViz Documents To Go Premium	115
2.8.3	Quickoffice Pro HD	116
2.8.4	Apple Pages, Numbers und Keynote	117
2.8.5	Fazit	118
3	**Google Android**	**119**
3.1	**Android 4.0 Ice Cream Sandwich im Überblick**	**119**
3.1.1	Nutzeroberfläche neu, Multitasking verbessert	119
3.1.2	Bessere App-Übersicht, neue Widget-Funktionen	120
3.1.3	Schneller reagieren	121
3.1.4	Datenverbrauch kontrollieren	122
3.2	**Nützliche App-Grundausstattung für Android-Smartphones**	**123**
3.2.1	Astro File Manager	124
3.2.2	Documents To Go	124
3.2.3	Dropbox	125
3.2.4	MultiTask Manager	126

1 Sicherheit

Die zunehmende Nutzung von Smartphones und Tablet-PCs im geschäftlichen Umfeld zwingt die IT-Sicherheitsverantwortlichen zur Anpassung ihrer bisherigen Security-Strategien. Von den mobilen Kommunikationsgeräten geht ein erhebliches Gefährdungspotential aus, weil die Nutzer häufig viel zu sorglos sind. Durch umfassende Sicherheits-Policies und ein zielgerichtetes Sicherheitsmanagement können IT-Abteilungen die Risiken minimieren.

1.1 Studie: Attacken auf Firmen-IT über Smartphones und Tablets

Das X-Force-Team von IBM (www.ibm.com/services/us/iss/xforce/) sorgt sich intern um die Sicherheit der weltweit verstreuten hauseignen Kunden. Um hier gegenzusteuern, analysiert das Team aktuelle Angriffstechniken und entwickelt Verteidigungsstrategien gegen Bedrohungen. Die Ergebnisse des nun vorgelegten Berichts speisen sich aus Untersuchungen zu öffentlich bekannten Sicherheitsvorfällen sowie aus der Beobachtung und Analyse von täglich durchschnittlich zwölf Milliarden Vorfällen seit Anfang 2011.

1.1.1 Zahl der Bedrohungen für mobile Endgeräte verdoppelt sich

Die zunehmende Verbreitung von Smartphones und Tablet-PCs sowie die Tatsache, dass sich Mitarbeiter vermehrt mit ihren privaten Geräten in Firmennetze einloggen („Bring Your Own Device“), führen dem Report zufolge zu „neuen Risiken“. Hacker sind gerade dabei, die mobilen Endgeräte als mögliche Einfallstore in die Unternehmens-IT zu entdecken. Mobiltelefoninfektionen lassen sich leicht monetarisieren, schreibt IBM. So setzen die Malware-Versender beispielsweise Premium-SMS-Services auf, die den Nutzern SMS-Texte an eine bestimmte Nummer in Rechnung stellen. Die Malware sorgt dann dafür, dass Textnachrichten von infizierten Handys an diese Premium-Nummern geschickt werden.

Immer mehr Schadsoftware sammelt dem Report zufolge persönliche Informationen der Handynutzer, um diese für Phishing-Attacken oder Identitätsdiebstähle zu nutzen. Zudem spioniert die Schadsoftware auch die Kommunikation der Opfer aus oder verfolgt via GPS den Aufenthaltsort einer Person.

Zwar gibt es bislang nur wenig Berichte über konkrete Viren- und Malware-Attacken auf mobile Endgeräte, allerdings wird diese Zahl nach übereinstimmender Meinung von Sicherheitsexperten in Zukunft sicher zunehmen.