COMPUTERWOCHE
VOICE OF DIGITAL

Link: https://www.computerwoche.de/a/sicherheitsrisiken-vermeiden,1938307

Handy, PDA & Co.

Sicherheitsrisiken vermeiden

Datum: 24.06.2010
Autor(en): Katharina Friedmann

Viele mobile Nutzer können die Sicherheitsrisiken, die von Handys & Co. ausgehen, überhaupt nicht einschätzen. Erfahren Sie, wo Gefahren lauern und wie Sie sich schützen können.

Das von **Handys**[1], **Smartphones**[2] und PDAs ausgehende Risiko ist auf zwei Faktoren zurückzuführen: Zum einen gehen Nutzer mit den handlichen Mobilgeräten in der Regel nachlässiger um als mit ihren **Notebooks**[3], zum anderen sind Sicherheitsvorkehrungen wie **Verschlüsselung**[4] und **Virenschutz**[5] auf den mobilen Rechenzwergen noch nicht so verbreitet wie etwa auf Laptops. IT-Sicherheitsverantwortliche sind sich dessen offenbar bewusst, wie eine Untersuchung von **Credant Technologies**[6] zeigt. Demnach halten 94 Prozent der 300 befragten **IT-Security**[7]-Verantwortlichen diese Mobilgeräte für ein größeres Sicherheitsrisiko als etwa mobile Speichermedien (88 Prozent) oder **Notebooks**[8] (79 Prozent). Eine 2007 unter anderem von der **National Cyber Security Alliance**[9] (CSIA) initiierte, weltweite Umfrage unter 700 mobilen Anwendern bekräftigt dies. Demzufolge räumten 73 Prozent der Teilnehmer ein, nicht sicher zu sein, wo die mobilen Sicherheitsrisiken liegen, und auch hinsichtlich der Best Practices beim Arbeiten unterwegs nicht im Bild zu sein. Nahezu 30 Prozent gaben zu, mobile Sicherheitsrisiken "kaum jemals" zu berücksichtigen und keine Präventivmaßnahmen zu treffen.

Die COMPUTERWOCHE-Schwesterpublikation "**CSO**[10]" hat die gröbsten "Sicherheitsvergehen" auf Seiten der Nutzer aufgelistet - darunter Fehler, die sich mobile Anwender mit ihren **Notebooks**[11] nicht leisten würden.

1. Auf das Handy-Passwort verzichten

Die grundlegendste **Sicherheitsvorkehrung**[12] und erste Verteidigungslinie für mobile Devices, das **Passwort**[13], ist für mobile Anwender offenbar alles andere als selbstverständlich: Im Rahmen der erwähnten Credant-Erhebung gab jeder zweite (56 Prozent) befragte IT-Security-Verantwortliche zu, bei seinem eigenen Mobilgerät oder **Smartphone**[14] nicht immer ein Kennwort zu verwenden. So werden aus abhandengekommenen Mobilgeräten gefährliche Mobilgeräte. Und weil sie klein und leicht sind, werden **Handys**[15] häufiger verlegt oder gestohlen als Laptops: So wurden etwa nach einer Erhebung von Pointsec (jetzt Check Point) in Chicago allein im Jahr 2005 in einem Zeitraum von sechs Monaten 85.000 Mobiltelefone sowie 21.000 PDAs und Smartphones, in London 63.000 Handys und 5.800 PDAs in Taxis liegen gelassen.

Das Deaktivieren der Passwortabfrage - wie etwa bei Apples iPhone möglich - ist riskant.
Foto: areamobile

Unternehmen investieren Milliarden in Informationssicherheit, riskieren aber Hacking und Sabotage, indem sie den unkontrollierten Zugriff auf mobile Endgeräte zulassen. Abhilfe können Firmen schaffen, indem sie kritische Inhalte auf **abhandengekommenen Handys**[16] mittels Management-Software aus der Ferne sperren oder löschen. Ein proaktiver Ansatz, um Nutzer vor sich selbst schützen: Security-Policies für Mobilgeräte und Applikationen etablieren und durchsetzen. Dazu zählen etwa Richtlinien, die starke Gerätepasswörter zum Entsperren eines brachliegenden Telefons fordern.

2. Das Smartphone als "Kennwort-Reminder" nutzen

Mobiltelefone[17] werden zunehmend als **Minicomputer**[18] genutzt. Entsprechend befinden sich dort mittlerweile alle möglichen Arten von Informationen - beispielsweise **Server**[19]- und andere Passwörter, die offen einsehbar in Lotus Notes oder unter "Kontakte" abgelegt sind. Bei einer globalen Umfrage des auf Mobile Security spezialisierten Anbieters Mformation unter 500 **CIOs**[20] gab mehr als die Hälfte der Befragten an, dass sich technische Produkt- und Vertriebsinformationen sowie Kundendetails auf den (häufig privaten) Handys ihrer Mitarbeiter befinden. Über eine genaue Aufstellung der dort vorgehaltenen Daten verfügten indes nur zwölf Prozent der Unternehmen.

Ein sicherer Aufbewahrungsort für Passwörter ist beispielsweise der "Mobilesitter" des Fraunhofer SIT. Foto: TeleTrusT Deutschland

Noch schlimmer: Meist liegen diese kritischen Firmeninformationen auf ungesicherten Geräten. Laut **McAfees**[21] "Mobile Security Report 2008" nutzen 79 Prozent der mobilen Privatanwender wissentlich ungeschützte Devices, weitere 15 Prozent sind sich über den Sicherheitsstatus ihres Mobilgeräts nicht im Klaren. Um Informationen auch dann schützen zu können, wenn die Nutzer nicht so umsichtig sind, wie sie sein sollten, müssen entsprechende **Security-Policies**[22] auf Mobilgeräten durchgesetzt werden.

3. Mobile Applikationen aus unsicherer Quelle öffnen

Auf Symbian-Handys werden Applikationen bei der Installation auf ein Zertifikat überprüft.
Foto: Nokia

Ohne mobile Anwendungen und Inhalte - von Messaging und E-Mail über Spiele und Geschäftsapplikationen bis hin zu Produktivitätssoftware - ist ein Mobilgerät im Prinzip nicht mehr als ein Telefon. Daher werden ständig neue **Spezialanwendungen**[23] entwickelt - allerdings bei weitem nicht alle gleich gut. Das Herunterladen oder Öffnen einer "schädlichen" oder auch nur schlecht konstruierten Applikation kann viele Probleme hervorrufen.

Auch hier gilt es für Unternehmen, mittels Sicherheitsrichtlinien sicherzustellen, dass ausschließlich autorisierte Applikationen auf die Mobilgeräte ihrer Mitarbeiter geladen werden können.

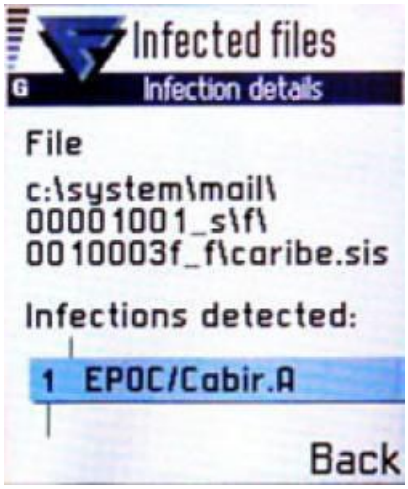
4. Mit dem Handy riskante Websites besuchen

Das Gros der Mobiltelefone ermöglicht den Zugriff aufs **Internet**[24]. Was bedeutet, dass Handy-Nutzer ebenso leicht auf gefährliche **Websites**[25] oder an riskanten Content geraten können wie PC-Anwender. Jeder weiß, welchen Schaden bösartige Web-Seiten auf einem Desktop anrichten können - vom Systemabsturz durch **Malware**[26] bis hin zu unerbetenen Inhalten, die den Rechner zur Schnecke machen. Davon sind mittlerweile auch Mobiltelefone betroffen.

Das Risiko, unangebrachte beziehungsweise unerwünschte Inhalte oder gefälschte Rechnungen zu erhalten sowie **Datenverluste**[27] zu erleiden, macht laut McAfee-Report mittlerweile rund 86 Prozent der Mobilanwender Sorgen. Auch musste sich weltweit immerhin einer von sieben Nutzern schon einmal mit einem mobilen Virus herumschlagen. Um sich gegen solche Gefahren zu wappnen, müssen mobile Privatanwender wie Unternehmen unerbetene Inhalte blockieren und infizierte Mobilgeräte schnell und vollständig bereinigen können.

5. Mobiltelefone mit offenen oder ungesicherten Bluetooth- und WLAN-Verbindungen

Einige der gängigsten mobilen **Viren**[28] und **Würmer**[29] machen sich ungesicherte **Bluetooth**[30]-Verbindungen zunutze, um in Mobilgeräte einzudringen oder sich auf weitere Devices zu verbreiten. So etwa die beiden bekanntesten Schädlinge "**Cabir**[31]" und "**CommWarrior**[32]" samt Varianten. Angriffe auf Mobiltelefone via **WLAN**[33]-Verbindung wiederum wurden bislang noch keine gemeldet, was sich Experteneinschätzungen zufolge allerdings ändern dürfte, sobald mehr Mobilgeräte diese Verbindung nutzen.



Schmuggelt sich via ungesicherte Bluetooth-Verbindungen ins Handy: der Cabir-Virus.

Darüber hinaus können Außenstehende offene ungesicherte Verbindungen kapern, um in das Firmennetz einzudringen, und Schaden an Systemen und Daten anrichten. Eine Möglichkeit, Firmendaten und -Assets vor externen Angriffen dieser Art zu schützen, sind Policies, die den Zugriff auf bestimmte Handy-Funktionen (etwa WLAN oder Bluetooth) nur unter gewissen Umständen zulassen.

Fazit

Mobiltelefone werden für Unternehmen immer wichtiger. Deshalb sollten Anwender mit ihren Handys, Smartphones und PDAs ebenso sorgfältig umgehen wie mit ihren Laptops. Nur so lassen sich die zunehmend mächtigen Rechenzwerge und die dort immer häufiger untergebrachten sensiblen Daten angemessen schützen. Die Einführung entsprechender Sicherheitsrichtlinien beziehungsweise Remote-Management-Unterstützung für alle mobilen Mitarbeiter sind Schritte in die richtige Richtung.

Links im Artikel:

[1] **https://www.computerwoche.de/schwerpunkt/h/Handy.html**

[2] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1870641/**
[3] **https://www.computerwoche.de/schwerpunkt/n/Notebook.html**
[4] **https://www.computerwoche.de/knowledge_center/security/1863721/**
[5] **https://www.computerwoche.de/knowledge_center/security/1878128/**
[6] **http://www.credant.com/**
[7] **https://www.computerwoche.de/schwerpunkt/s/Security.html**
[8] **https://www.computerwoche.de/knowledge_center/notebook_pc/1873788/**
[9] **http://www.csialliance.org/**
[10] **http://www.csoonline.com/**
[11] **https://www.computerwoche.de/knowledge_center/notebook_pc/1880296/**
[12] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1865059/**
[13] **http://de.wikipedia.org/wiki/Passwort**
[14] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1865690/index5.html**
[15] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1870052/**
[16] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1875239/**
[17] **http://de.wikipedia.org/wiki/Handy**
[18] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1865690/**
[19] **https://www.computerwoche.de/schwerpunkt/s/Server.html**
[20] **https://www.computerwoche.de/schwerpunkt/c/CIO.html**
[21] **http://home.mcafee.com/Root/AboutUs.aspx**
[22] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1862868/**
[23] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1872868/**
[24] **https://www.computerwoche.de/schwerpunkt/i/Internet.html**
[25] **https://www.computerwoche.de/knowledge_center/security/1878353/**
[26] **https://www.computerwoche.de/knowledge_center/security/1869500/**
[27] **https://www.computerwoche.de/schwerpunkt/d/datenverlust.html**
[28] **http://de.wikipedia.org/wiki/Computervirus**
[29] **http://de.wikipedia.org/wiki/Computerwurm**
[30] **https://www.computerwoche.de/schwerpunkt/b/bluetooth.html**
[31] **https://www.computerwoche.de/nachrichtenarchiv/553794/**
[32] **https://www.computerwoche.de/nachrichtenarchiv/554310/**
[33] **https://www.computerwoche.de/knowledge_center/security/1878203/**
