*Sicherheitsaspekte bei der Arbeit mit mobiler IT*

# Aufklären und Sensibilisieren

**Mobilität steht für Freiheit, flächendeckende Konnektivität und Flexibilität. In der IT äußert sich das in immer vielfältigeren mobilen Geräten wie Laptops, Handys, Blackberrys oder auch internetfähigen Bordcomputern im Auto. Die Leistungsfähigkeit und Anwendungsvielfalt dieser Geräte steigt enorm. Eine Vielzahl von Schnittstellen, wie WLAN, Bluetooth, UMTS oder USB, gewährleisten optimale Konnektivität. Die Problemstellung erschließt sich von selbst: Jede weitere Anwendung und Schnittstelle bietet Angriffsflächen und offenbart Sicherheitslücken. Für den produktiven, sicheren Einsatz von mobilen Geräten ist es also absolut notwendig, die Technologien zu kennen und bestimmte Regeln zu befolgen, damit der Traum von Freiheit durch Mobilität nicht zum Alptraum wird.**

Mobile Geräte sind zunehmend in der Lage alle Aufgaben zu erledigen, die auch die Büroausstattung mit PC und Telefon leistet. Der Laptop ist bereits als vollwertiger Desktopersatz zu sehen, daher beziehen sich die Ausführungen vor allem auf Smartphones und Co.

## Bauartbedingte „Schwächen"

Mobile Endgeräte sind klein und können somit fast überall genutzt werden. Dieser Vorteil ist von der sicherheitstechnischen Seite gesehen gleichzeitig die größte Schwäche. Sie befinden sich außerhalb des überschaubaren und kontrollierbaren Firmenumfelds und somit auch außerhalb dessen Sicherheitseinrichtungen. Gehen sie verloren oder werden sie gestohlen, ist die Gefahr besonders groß, dass Informationen in falsche Hände gelangen.

Dass dies ein alltägliches Problem ist, zeigen 62.000 Handys, 2.900 Notebooks und 1.300 PDAs die schon im Jahr 2001 binnen eines halben Jahres in London in Taxis liegen gelassen wurden[1]. Selbst die Militärs und Geheimdienste sind vor einem derartigen Verlust nicht geschützt[2].

## Sicherheitsfaktor Mensch

Das größte Sicherheitsrisiko ist wie so oft der Mensch, also der Benutzer der mobilen Geräte. Er erlaubt Familienmitgliedern, aber auch Externen den Zugriff auf die Systeme, vergisst sie im Taxi und installiert sich unbewusst Schadsoftware aus dem Internet oder von USB-Sticks.

In der Vergangenheit waren die meisten Schadprogramme, für das Laptop einmal ausgenommen, relativ harmlos. Getarnt als hilfreiches Programm oder als Display-Theme zur „Verschönerung" wurden nur im schlimmsten Fall Daten gelöscht oder das Gerät unbrauchbar gemacht. Doch mittlerweile findet eine Professionalisierung der Angriffe statt. Anbieter für Abhörsoftware werben mit der unbemerkten Überwachung mobiler Geräte. Sie erlauben das Belauschen von Telefonaten, die Nutzung der Geräte als Wanze oder das Auslesen gespeicherter Daten. Ein verantwortungsbewusster Umgang mit dem mobilen Gerät schützt jedoch gegen die meisten Angriffe.

## Sicherheitsrisiko Schnittstellen

Die Anzahl der verfügbaren Schnittstellen in mobilen Geräten steigt, um jederzeit eine optimale Konnektivität gewährleisten zu können. Dieser Komfortgewinn bringt zusätzliche Gefahren mit sich. Im Folgenden werden exemplarisch die Schwachstellen der meistgenutzten Schnittstellen aufgezeigt.

**GSM**

Statistisch gesehen besitzt heute jeder Deutsche mindestens ein Mobiltelefon. Die meisten Geräte setzen dabei mit GSM auf einen schon über 20 Jahre alten Standard mit einem genauso alten Verschlüsselungsverfahren, das zunehmend nicht mehr als sicher einzustufen ist[3]. Aktuell geht man davon aus, dass innerhalb der nächsten zwei Jahre ein Abhören von GSM für unter 2000 Euro möglich und deshalb auch für „übliche“ Kriminelle interessant wird. Eine Lösung dieser Problematik ist die Nutzung von UMTS, das ein neues sichereres Verschlüsselungsverfahren einsetzt.

**WLAN**

Wireless Local Area Network (WLAN) ermöglicht, zum Beispiel in Form von öffentlichen Hotspots, fast überall einen schnellen Zugriff auf das Internet. Zwar bietet WLAN eine Verschlüsselung der Daten zum Access Point an, doch nicht alle Verschlüsselungen sind sicher (WEP-Verschlüsselung). Auch bei verschlüsselten WLANs kann der Betreiber eines Access Points alle nicht zusätzlich verschlüsselt übertragenen Daten mitschneiden. Dies nutzen Angreifer beispielsweise bei „Rough-Access Points”, die einen kommerziellen und vertrauenswürdigen Access Point vortäuschen, um so an sensible Daten zu kommen. Die Nutzung von VPN- oder SSL-Verbindungen ist deshalb auch bei verschlüsselten WLANs Pflicht.

**Bluetooth**

Bluetooth entwickelt sich zur universellen Schnittstelle für Peripheriegeräte wie Freisprecheinrichtungen oder Mäuse. Mit steigender Verbreitung werden und wurden aber auch Sicherheitslücken in den Implementierungen einzelner Geräte bekannt, die unter Umständen ein Abhören von Gesprächen, aber auch das Auslesen und Aufspielen von Daten erlaubt.

**USB und Firewire**

Neben Funkschnittstellen können auch von Peripherieschnittstellen Gefahren ausgehen. Über Firewire lässt sich ohne Zugriff auf das Betriebssystem der Arbeitsspeicher im laufenden Betrieb auslesen. Mittels präparierter USB-Sticks kann Schadsoftware auf das Rechnersystem aufgespielt oder Daten von der Festplatte auf den Stick kopiert werden. Mit wenigen Handgriffen und Verhaltensweisen kann man diese Gefahr stark einschränken.

**Autoren:**

**Marian Jungbauer** und **Markus Linnemann** sind Mitarbeiter im Bereich Trusted Computing und Awareness am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen.
E-Mail: marian.jungbauer@internet-sicherheit.de, markus.linnemann@internet-sicherheit.de

**Prof. Dr. Norbert Pohlmann** ist Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen
E-Mail: norbert.pohlmann@internet-sicherheit.de
www.internet-sicherheit.de

### Verhaltensregeln für den Umgang mit mobiler IT

- Minimierung der auf dem Gerät gespeicherten sensiblen Informationen
- Einschränkung der Nutzer: Keinen Personen, auch keinen Familienmitgliedern, unbeaufsichtigten Zugriff erlauben, oder/und stark restriktive Benutzerkonten einsetzen.
- Keine sensiblen Transaktion an öffentliche Plätzen und in nicht vertrauenswürdigen Netzwerken (z.B. Öffentlichen WLAN Access Points). Man erledigt seine Bankgeschäfte ja auch nicht am Bahnhof. Es sollte mindestens eine WPA-, besser noch WPA2-Verschlüsselung bei WLAN gewählt werden. Müssen sensible Daten übertragen werden, so ist die Nutzung von VPN- oder SSL-Verbindungen Pflicht.
- Nutzen von Sicherheitsfunktionen wie Geräte-PINs. PINs nie in der Standardeinstellung verwenden.
- Geräte niemals unbeaufsichtigt lassen und falls doch den Zugriff konsequent sperren.
- Nicht verwendete Schnittstellen (Beispiel: Bluetooth) ausschalten, beziehungsweise Kabel trennen.
- Nur Software installieren, die auch wirklich notwendig ist und verwendet wird.

## Grundsätzliche Verhaltensregeln

Trotz steigender Gefahren lässt sich das Risiko eines Angriffs durch eine Kombination aus technischen Schutzmaßnahmen und Verhaltensregeln der Benutzer minimieren. Den hundertprozentigen Schutz gibt es bei Computern ebenso wenig, wie beim Verschließen des Eigenheims, aber man kann es einem Eindringling so schwer wie möglich machen. Schon durch die Einhaltung weniger Verhaltensregeln können Sicherheitsrisiken vermieden werden (Kasten).

Der Grund für ein mögliches Fehlverhalten lässt sich häufig auf eine fehlende Sensibilisierung zurückführen. Besonders Mobiltelefone waren lange Zeit so eingeschränkt, dass die Meinung entstand, dass diese Geräte nicht von Schadsoftware befallen werden können. Eine Meinung, die heute nicht mehr zu halten ist. Umfassende Awareness-Schulungen der Benutzer können hier bei der Fehlervermeidung helfen.

## Technische Schutzmaßnahmen

Wie bei stationären Rechnersystemen muss in Zukunft auch bei mobilen Geräten der Dreisatz: „Virenscanner, Personal Firewall und (falls möglich) automatische Updates“ gelten. Virenscanner und Firewalls gibt es mittlerweile auch für Mobiltelefone und Smartphones. Sie werden aufgrund fehlender Sensibilisierung der Benutzer gegenüber Schwachstellen auf diesen Geräten immer wichtiger.

Neben der Grundausstattung mit Sicherheitsprogrammen lässt sich ein Eindringen über Schwachstellen der Schnittstellen nur durch konsequentes Ausschalten nicht genutzter Schnittstellen erreichen. Dies sorgt nicht nur für eine erhöhte Sicherheit, sondern wirkt sich auch positiv auf die Laufzeit der Geräte aus.

Mindestens genauso wichtig wie die bereits genannten Maßnahmen, die sich vornehmlich gegen Angriffe richten, ist der Schutz wichtiger Daten gegen Verlust oder Diebstahl. Deshalb sollten, sofern möglich, alle Daten auf den Geräten verschlüsselt werden. Aufgrund steigender Leistungsfähigkeit der Geräte ist der mit der Verschlüsselung einhergehende Performanceverlust zu vernachlässigen. Darüber hinaus sind regelmäßige Sicherungen der Daten ebenso notwendig wie bei stationären Systemen.

## Grundsätzliches zur Hardwareauswahl

Mobile Geräte sollten nach Funktion und Sicherheitslevel ausgewählt werden. Für sicherheitskritische Telefonate werden beispielsweise Mobiltelefone angeboten, die keine Schnittstellen anbieten und einen Kryptochip beinhalten, um die Kommunikation abhörsicher zu verschlüsseln. Das Blackberry für den Chef sollte nicht unbedingt mit sicherheitskritischen Daten in Berührung kommen, oder aber aufwändig abgesichert werden. Bei der Hardware gilt es Geräte zu wählen, die keine überflüssigen Funktionen anbieten und für das notwendige Sicherheitsniveau geeignete Maßnahmen bereit halten.

## Ausblick und Forschung

Der Mensch wird immer einer der wichtigsten (Un-)Sicherheitsfaktoren bleiben. Aufklärung und Sensibilisierung im Umgang mit mobilen Geräten ist daher eine absolute Notwendigkeit für Unternehmen.

Die Forschung arbeitet an neuen Konzepten, die mobilen Geräte mit Sicherheitsplattformen und Sicherheitsankern auszustatten. Prozesse können mit diesen Technologien konsequent getrennt werden, ebenso wie sicherheitskritische Daten von allen weiteren Informationen. Die wichtigste Neuerung ist wahrscheinlich, dass die Vertrauenswürdigkeit dieser Geräte überprüfbar gemacht wird und somit nur Geräte kommunizieren miteinander, die sich vorher gegenseitig als sicher eingestuft haben. Diese Technologien werden unter der Begrifflichkeit „Trusted Computing“ zusammengefasst und können die Sicherheit stationärer und mobiler Geräte erhöhen.

Die Freiheit durch mobile Geräte ist also erreichbar, wenn man die aufgezeigten Verhaltensregeln berücksichtigt und mit den technischen Möglichkeiten umzugehen weiß. □

1 http://news.bbc.co.uk/2/hi/uk_news/1518105.stm
2 www.heise.de/newsticker/Laptop-Schwund-beim-FBI–/meldung/85465
3 Rütten, Christiane: Unerwünschte Mithörer – Angriff auf die GSM-Verschlüsselung. www.heise.de/mobil/Angriff-auf-die-GSM-Verschluesselung–/artikel/99949