

# Sicherheit beim Mobile Computing

Dipl.-Ing. Dr. Gerhard Klett

25.08.2010

Schöne ständig neue Welt der Datenverarbeitung. Computer sind endlich so klein und handlich, dass sie permanent mitgeführt werden können. Ihre Kommunikationsfähigkeiten verbinden sie an jedem Ort der Welt mit zahlreichen Informationsressourcen im globalen Internet und im Netzwerk des eigenen Unternehmens. „Always online“ ist Alltag und keine Fiktion mehr.

Informations- und Kommunikationstechnologien wachsen zusammen. Wir erleben diese Konvergenz in Form immer leistungsfähigerer Smartphones oder Netbooks, die mit ihren multitasking fähigen Betriebssystemen und Kommunikationsmöglichkeiten die Abarbeitung komplexer Applikationen („Apps“) gestatten.

In dieser digitalen Lebenswelt begegnen wir Vernetzungsformen mit Bezeichnungen Wireless LAN (*WLAN*), Bluetooth oder ZigBee. Objekte mit aufgeklebten oder implantierten Mikrochips mit RFID(*Radio Frequency Identification*)-Transpondern werden in Netzwerke eingebunden, bilden ein kommunikationsfähiges Netzwerk in unserer Einkaufsstüte, vernetzen sich mit Navigationssystemen und verbinden sich ohne Weiteres mit weiter reichenden, anderen Netzwerken. Neue Anwendungen für Logistik, Warenwirtschaft oder für das tägliche Leben entstehen.

Aber wie sieht es mit dem Schutz sensibler Daten bei so zahlreichen Kommunikationsmöglichkeiten aus?

Pauschal gesagt entstehen mit dem Mobile Computing auch neue Möglichkeiten für den Datenmissbrauch – gewissermaßen die Kehrseite der Medaille.

Mobile Computing bedeutet

- Mobilität von Diensten und Applikationen wie z. B. E-Mail, Instant Messaging, Filetransfer etc., die von jedem Ort der Welt aus benutzt werden können;
- Mobilität der Endgeräte. Die Geräte müssen bequem portabel und von einer stationären Stromversorgung unabhängig sein;
- Mobilität der Netzanbindung. Die Verbindung mit dem Unternehmensnetz soll über drahtlose Netze mit vielen Zugriffspunkten oder Mobilfunknetzen von überall auf der Welt sicher möglich sein.

Und nicht zuletzt bedeutet Mobile Computing auch die Verwendung von mobiler Peripherie wie Speicherkarten, USB-Sticks und Headsets, um nur einige aufzuführen.

Betrachten wir nun zwei der wichtigsten Sicherheitsprobleme und geeignete Sicherheitsmaßnahmen zu deren Minimierung:

- 1.) Verlust des mobilen Endgerätes oder mobiler Speicher durch Verlieren oder durch Diebstahl.  
Mobile Endgeräte sollen uns überall begleiten, dabei möglichst klein, leicht und „schick“ sein. Sie sind milieuwechselnde Geräte und in Zügen, Flugzeugen, Wartesälen, Abflughallen, Mietwagen, Hotelbars, Umkleidekabinen von Saunen etc. anzutreffen. Sie sind Accessoires eines „Lifestyles“. Das Hauptproblem ist damit vorbestimmt: die Gefahr, das Gerät zu verlieren oder gestohlen zu bekommen.

Schutz: Zur Verminderung des Diebstahlrisikos sowie zur Verhinderung von Datenverlusten und unberechtigter Einsichtnahme gibt es eine Menge erprobter Maßnahmen. Hier eine Auswahl:

Das Gerät muss durch ein nichttriviales Passwort vor einer unberechtigten Inbetriebnahme geschützt sein. Auf keinen Fall dürfen die Initialpasswörter der Hersteller einfach weiterverwendet werden. Sie sind bekannt und im Internet veröffentlicht. Wenn die Policy des Unternehmens es gestattet, sensible Daten auf mobilen Geräten und Speichern abzulegen, müssen diese mit einem evaluierten Verfahren verschlüsselt werden.

Unterdrücken des „Besitzerstolzes“: Geräte nicht herumzeigen oder offen an der Kleidung tragen: mobile Endgeräte sind unternehmenseigene Arbeitsgeräte und keine Modeaccessoires.

Geräte nicht offen sichtbar im Mietwagen (sondern im Kofferraum) oder im Hotelzimmer liegen lassen: Wenn sie nicht mitgeführt werden, müssen sie sicher in einem abgeschlossenen Behältnis aufbewahrt werden.

Administration der mobilen Geräte und Anlegen eines Gerätepasses durch eine zentrale Stelle im Unternehmen: Im Gerätepass sind mindestens die Seriennummern, Hardware-/Software-Ausstattung, Patch- und Update Level sowie die Zugriffsberechtigungen auf unternehmenseigene Ressourcen zu verzeichnen.

Ansprechstelle im Unternehmen für Hilferufe von unterwegs einrichten: Hier ist auch der Verlust des Gerätes zu melden. Bei dieser Stelle muss ein Prozess für die nötigen Aktionen wie das Sperren von Netzzugängen, Beschaffung von Ersatzgeräten usw. vorhanden sein.

Regelmäßiges Anfertigen von Sicherungskopien der Daten auf einem stationären Rechner oder auf nichtflüchtigen Speicherkarten.

## 2.) Verwendung öffentlicher Netze zum Datenaustausch

Bei der drahtlosen Kommunikation ist das Übertragungsmedium die Luft, weswegen man bei der Schnittstelle zum Netzwerk auch von einer „Luftschnittstelle“ spricht, die mit speziellen Antennen über weite Entfernungen (mehrere Kilometer) sehr leicht abzuhören und aktiv zu beeinflussen ist. Schutz gegen Abhören und Manipulation bietet die konsequente Verwendung von überprüften Virtual Private Networks („VPN“) und die Aktivierung von vorhandenen Schutzmechanismen wie mindestens WPA2 bei WLAN mit einem vielstelligen (z.B. 16 Stellen) zufällig erzeugten Initialschlüssel.

Die Globalität, die einen wesentlichen Faktor unserer heutigen Geschäftswelt darstellt und auch den Mittelstand erfasst hat, erfordert immer mehr Reisen zu entfernten Niederlassungen der Unternehmen. Effiziente Geschäftsprozesse erfordern Erreichbarkeit und Interaktion auch außerhalb des Büros. Stationäre Datenverarbeitung von einem festen Ort aus ist dabei eine nicht akzeptable Einschränkung. Datenverarbeitung von verschiedenen Orten dieser Welt (*Mobile Computing*) ist heute ein Muss, welches mit vielen gravierenden Sicherheitsrisiken verbunden ist, von denen zwei im vorliegenden Artikel kurz diskutiert wurden.