Mit der Zunahme mobiler Geräte wachsen die Sicherheitsrisiken

# Sicher mobil – Mobile Security?!

*Von Christian Flory, Hans Joachim Giegerich, Christian Schülke und Michael Wiesner*

**Ohne mobile Kommunikation und mobile Endgeräte ließ sich die Unternehmens-IT durch das zwiebelschalenartige Zonenmodell gut schützen. Durch mobile Kommunikation erwachsen der Zwiebel Sprösslinge, die mit herkömmlichen Methoden nicht zu besichern sind.**

*Christian Flory, Projektleiter Hessen-IT, HA Hessen Agentur GmbH*

*Hans Joachim Giegerich, Geschäftsführer Giegerich & Partner GmbH*

*Christian Schülke, Geschäftsführer schuelke.net internet. security.consulting*

*Michael Wiesner, Geschäftsführer Secutrends GmbH*

Sicherheit ist ein Grundbedürfnis eines jeden Menschen. Wenn wir in die Wirtschaft schauen, muss auch hier der Sicherheit ein sehr hoher Stellenwert zugeschrieben werden. Die Sicherheit des Unternehmens hat dabei unterschiedliche Aspekte, zu denen beispielsweise Prozesssicherheit, Vertrags- und Finanzierungssicherheit, Personalsicherheit und die Gebäudesicherheit gehören. Der IT-Sicherheit, die natürlich auch die Aspekte der mobilen IT-Sicherheit beinhaltet, kommt dabei eine Schlüsselfunktion zu, da Informationstechnologien heute sehr viele Prozesse eines Unternehmens unterstützen und ein ganzheitliches IT-Sicherheitskonzept alle Aspekte der Unternehmenssicherheit berücksichtigen muss.

Erinnern Sie sich noch an die Vision, die Bill Gates anlässlich der Comdex 1994 in Las Vegas für das Jahr 2005 mit Hilfe eines Videos vortrug? „Information at your fingertips" war seinerzeit das Schlagwort – jede benötigte Information jederzeit und überall zur Verfügung haben, quasi mit einem Fingerschnippen. Vieles ist seit dieser Zeit Realität geworden, zum Beispiel der PDA in der Jackentasche, der Zugriff auf das geballte Wissen des Internets und vieles mehr. Aus dem PDA wurde schließlich das Smartphone, was die ständige und aktuelle Verfügbarkeit von E-Mail, Kalender, Kontakten sowie Dokumente aller Art mit sich brachte.

Unabhängig von der Frage, ob nun ein Smartphone oder ein Notebook das mobile Endgerät der Wahl ist, stellt sich bei nüchterner Betrachtung unweigerlich die Frage, wie sicher das Ganze ist. Denn durch die Übertragung geschäftsrelevanter Informationen sind mehr oder weniger unbemerkt auch wichtige Unternehmenswerte, so genannte Assets, auf die mobilen Endgeräte gewandert.

Was ändert sich de facto, wenn Unternehmensdaten mobil werden? Diese Daten befinden sich in erster Linie nicht mehr im geschlossenen Firmennetzwerk, sondern sind irgendwo auf dem Globus unterwegs. Dadurch können interne Sicherheitsmaßnahmen nicht greifen, was eine gesonderte Absicherung der mobilen Endgeräte notwendig macht.

**Assets – Bestimmen Sie für sich selbst, welche Werte Sie auf ihren mobilen Endgeräten mit sich tragen:**

– Kunden- und Vertriebsdaten
– Angebotskalkulationen
– Forschungsergebnisse
– persönliche Kontakte und Kontaktdaten
– interne Buchhaltungsdaten
– sonstige Firmengeheimnisse

Versuchen Sie zu Ihrer eigenen Sicherheit, möglichst wenige Assets mobil bei sich zu tragen.

Abgesehen vom möglichen Diebstahl oder sonstigen Verlust der Endgeräte, ändert sich das Bedrohungspotential bei mehr Mobilität der Daten nur unmerklich, während sich zugleich die Angriffsfläche rapide vergrößert, wie auch Studien des Jericho-Forums zeigen. Vieles verdient allerdings eine neue Betrachtung und Bewertung. Ist also der Einsatz von mobilen Endgeräten geplant, sind zunächst einmal CIO (Chief Information Officer), CCO (Chief Compliance Officer) und CSO (Chief Security Officer) gefragt. Denn eigentlich banale Gepflogenheiten – beispielsweise die Selbstverständlichkeit, Außenstehenden keine Einblicke in Unternehmensinterna zu gewähren – werden plötzlich zu einer Herausforderung.

**Das Risiko „Spionage via Shoulder Surfing" droht an vielen Orten.**

Leider gibt es Menschen, die nicht nur die Langeweile in der Bahn, im Flugzeug oder an anderen öffentlichen Orten zum Shoulder Surfing treibt, indem sie mobil Arbeitenden über die Schulter blicken. Ob die so gewonnenen Informationen der Belustigung des nächsten Stammtisches dienen oder finstereren Zwecken, sei dahin gestellt. Ein weiteres beliebtes Alltagsszenario: Gar allzu menschliche Bedürfnisse treiben den Teilnehmer eines Meetings – hier wählen wir exemplarisch einen Vertriebsmitarbeiter in Verhandlungen mit dem Einkauf eines Unternehmens – aufs stille Örtchen. Nun ist es ein Leichtes, mit Hilfe eines geeignet manipulierten USB-Sticks beiläufig wesentliche Informationen vom Notebook der betroffenen Person abzuziehen. Die notwendige Software findet sich zuhauf genau dort, wo wir auch alles andere gerne nachlesen: im Internet.

Der Verlust mobiler Endgeräte, sei es durch Diebstahl oder einfaches Vergessen, stellt eine nicht zu unterschätzende Gefahr dar. Die Tatsache, dass Hersteller Mechanismen zur Wiederbeschaffung verlorener Notebooks implementieren und Geschäftsmodelle florieren, die sich mit der Wiederbeschaffung der Geräte und insbesondere der darauf befindlichen Daten befassen, spricht eine deutliche Sprache. Gleiches gilt für den Zugriffschutz für mobile Daten, denn die Verwertung gestohlener Daten aller Art ist quasi salonfähig geworden. Hier hat sich eine Schattenwirtschaft entwickelt, deren Umsatzvolumen wesentlich höher ist als gemeinhin angenommen. Übrigens kostet der Verlust eines Notebooks nach einer Studie des US-amerikanischen Ponemon Instituts im Schnitt 50.000 US-Dollar.

„Papa, darf ich mal auf Deinem Notebook spielen?“ Die Frage ist so putzig, dass viele Väter nicht widerstehen können. Seitdem sich die Erkenntnis durchgesetzt hat, dass selbst seriöse Webseiten honoriger Unternehmen zur Virenschleuder werden können, ist in dieser Diskussion endgültig kein Auge mehr zuzudrücken. In diesem Sinne kurz und bündig: Nicht erweichen lassen! Ein Firmenrechner ist ein Firmenrechner! So sei an dieser Stelle auch der Hinweis nicht vergessen, dass genau jenes Endgerät sicherlich über einen VPN-Tunnel ins Unternehmen verfügt und somit quasi als mobiles Einfallstor in die Unternehmens-IT dienen kann.

**Mit USB-Sticks werden häufig Unternehmensdaten gefischt.**

Der Markt mobiler Endgeräte ist dabei noch deutlich vielfältiger, als die bisherigen Ausführungen vermuten lassen. Wenn wir als mobiles Endgerät all das definieren, was wenigstens üblicherweise zur Erfassung zum Transport oder auch zur Verarbeitung von Daten dienen kann, beinhaltet dies neben den angesprochenen intelligenten Telefonen, den Smartphones, und Notebooks natürlich auch die weit verbreiteten USB-Sticks sowie Digitalkameras und andere mobile Speichermedien. Gerade USB-Sticks sind eine gern genommene Quelle, um Daten zu fischen, die jemand anderem gehören. Hand aufs Herz: Machen Sie sich immer die notwendigen Gedanken, welchen USB-Stick Sie gerade weitergeben oder in Ihren eigenen Rechner stecken?

Nicht immer sind mobile Endgeräte und Datenspeicher, die der Anwender nutzt, auf den ersten Blick als solche zu erkennen. Dazu zählen zum Beispiel mobile Erfassungsgeräte für RFID-Transponder, die sogar personenbezogene Daten enthalten können und somit besonderen Vorsichtsverpflichtungen unterliegen. Ebenso MP3-Player, digitale Bilderrahmen oder auch via Bluetooth oder IrDA (Infrared Data Association) angeschlossene Drucker oder Smartcards. Werden diese Geräte benutzt, so sind sie in die Sicherheitsinfrastruktur mit einzubeziehen und entsprechend abzusichern.

Ohne technisch ins Detail zu gehen, wird anhand der besprochenen Beispiele klar, dass diese mobilen Geräte unterschiedliche Schnittstellen und hiermit auch unterschiedliche Schwachstellen aufweisen. Dadurch werden eine dedizierte Betrachtung und Absicherung je nach Gerätetyp notwendig. Wer wertvolle Unternehmensdaten unverschlüsselt auf USB-Sticks mit sich herumträgt, handelt grob fahrlässig. Sind darunter sogar

**Bedrohungen**

– Datendiebstahl oder Manipulation durch Schadsoftware
– Kompromittierung durch offene Schnittstellen (WLAN, Bluetooth)
– Ausspähen von Daten durch „Shoulder Surfing“
– Diebstahl oder sonstiger Verlust
– Nutzung ungeschützter oder unverschlüsselter Netze (WLAN)
– Nutzung vermeintlich sicherer Netze (GSM)
– Nutzung von unkontrollierbaren Anwendungen (mobiler Code)

personenbezogene Daten oder Personaldaten, ist ein Konflikt mit dem Gesetz in Form des Bundesdatenschutzgesetzes gegeben.

Mithin stellt sich die Frage: Wie sind die durch mobile Endgeräte vielfältiger gewordenen Kommunikationsbeziehungen einerseits sowie die vielfältiger gewordenen Endgeräte an sich andererseits so weit zu schützen, dass man damit ruhigen Gewissens weiter arbeiten kann? Die Antwort könnte lauten: Im Prinzip ist das möglich, aber...! Der Einwand bezieht sich auf den Komfort, die Geräteauswahl – nicht jedes mobile Endgerät unterstützt Sicherheitsmechanismen –, die Organisation mobiler Kommunikation im Unternehmen und letztlich die Eigenorganisation des Benutzers mobiler Endgeräte.

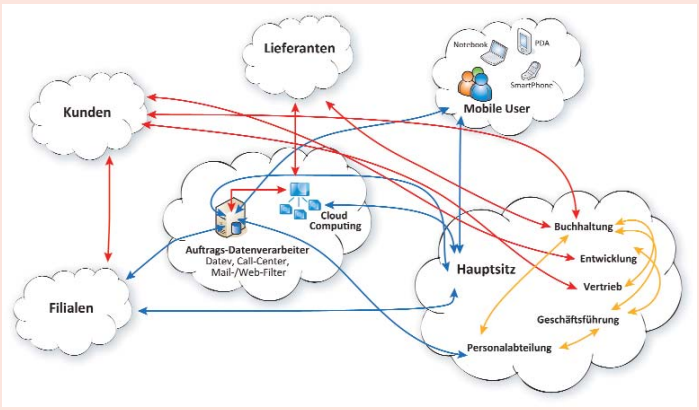
**Mobile Kommunikation durchlöchert das Zonenmodell der Unternehmens-IT.**

War die Unternehmens-IT ohne mobile Kommunikation und mobile Endgeräte durch ein zwiebelschalenartiges Modell, das so genannte Zonenmodell, noch gut zu schützen, erwachsen der Zwiebel durch mobile Kommunikation plötzlich Sprösslinge, die mit herkömmlichen Methoden einfach nicht mehr zu besichern sind. Gemäß den Vorstellungen des Jericho-Forums ist daher jedes Endgerät für sich zu besichern, ebenso die Kommunikation zwischen diesen Endgeräten und dem Rest der Welt. Konkret bedeutet das, dass ein geeignetes Schutzkonzept den sicheren Datenzugang – starke Authentifizierung und geeignete Autorisierungsmechanismen –, die Datenhaltung – die Verschlüsselung – sowie den verschlüsselten Datentransport technisch wie organisatorisch gewährleisten muss.

### Vielfältige Kommunikationsbeziehungen – Daten sind vielfach unterwegs

Werden diese Anforderungen erfüllt, kommt das nächste Dilemma. Je nach Region oder Land, in dem sich ein Nutzer mit seinen mobilen End-

**Beziehungsstruktur der elektronischen Unternehmenskommunikation**




Quelle: schuelke.netinternet.security.consulting

geräten aufhalte, erfüllt er wahlweise die Anforderungen von Datenschutz und Compliance auf diese Weise – oder er kommt genau deswegen mit dem Gesetz in Konflikt. Einige Staaten erlauben keine Verschlüsselung von Daten ohne einen staatlichen Zugang zu diesen (Lawfull Interception). Exemplarisch ist hier der Konflikt zwischen den Vereinigten Arabischen Emiraten (VAE) und Research in Motion (RIM), dem kanadischen Hersteller der Blackberry-Smartphones, zu nennen. RIM konnte ein Verbot der Blackberry-Nutzung in den VAE nur verhindern, indem sich das Unternehmen mit der Regierung über nicht weiter veröffentlichte Zugriffsmöglichkeiten auf die verschlüsselten Daten geeinigt hat. Hinzu kommen nach wie vor vorhandene Exportbeschränkungen, beispielsweise die der US-Regierung für besonders starke Verschlüsselungsalgorithmen.

Es existiert eine Vielzahl von Kommunikationsbeziehungen und Notwendigkeiten der Datenhaltung. Entwickelt man das Modell des Jericho-Forums zu einem Beziehungsmodell weiter, in dem klar wird, welche Daten überhaupt auf welchen Endgeräten zu sehen sein werden bzw. gespeichert werden dürfen, erhält man mit der Minimierung dieser Bedürfnisse ein Maß an Datenreduktion bzw. nachgelagert die Reduktion des Sicherheitsproblems. Diese scheinbare Binsenweisheit gewinnt im Zeitalter mobiler Kommunikation enorm an Bedeutung.

**Je kleiner die mobilen Geräte sind, desto geringer sind Sicherheitsangebote, beispielsweise zur Verschlüsselung und zur Authentifizierung.**

Dabei variiert die Tauglichkeit verschiedener Gerätetypen im Hinblick auf das angedachte Sicherheitssystem stark. Während Windows- oder MacOS-basierte Notebooks, Laptops und Tablet-PCs durch vielseitig wählbare Softwarelösungen glänzen, schrumpft die Auswahl geeigneter Lösungen mit sinkender Gerätegröße. Schon bei Smartphones trennt sich die Spreu vom Weizen. Businessorientierte Smartphones erfahren hier in der Regel eine bessere Unterstützung als die Geräte für das Consumer-Umfeld. Im Businessbereich gibt es daher eigens für hochsichere Anwendungsum-

**Sicherungsmöglichkeiten mobiler Endgeräte**

- Physische Absicherung: Mobile Geräte wie Laptops, Smartphones, USB-Sticks, externe Festplatten usw. möglichst nicht unbeaufsichtigt liegen lassen; bei Abwesenheit Zugang sichern durch Sperrung und falls möglich physisch sichern durch Schlösser
- Alle nicht benötigten Konnektivitäten abschalten (Bluetooth, W-LAN, Infrarot, USB-Ports usw.)
- Sichtschutz vor unliebsamen Beobachtern, beispielsweise durch spezielle Filterfolie beim Laptop-Display
- Zugangsschutz zu den Geräten, zum Beispiel mit Login und Passwort oder biometrischen Verfahren
- Verschlüsselung der auf dem mobilen Endgerät abgelegten Daten mit Standards wie AES, 3DES und Blowfish/Twofish
- Eventuell GPS-Locator zum Wiederfinden im Verlustfall
- Darüber hinaus Absicherung wie bei nicht mobiler IT beispielsweise durch Datensicherung, Schutz vor Viren und anderer Malware sowie vor Netzattacken

gebungen entwickelte Geräte und Systeme. Der Markt bietet inzwischen ebenfalls mobile Datenträger mit mehr oder weniger starken Verschlüsselungs- und Authentisierungsmechanismen. Wo solche nicht vorhanden sind, empfiehlt sich eine Software, die den Datenträger oder Teile davon verschlüsseln kann. Diese Datenträger sind dann jedoch nicht mehr mit jedem PC benutzbar. Vollends dünn wird das Angebot für denjenigen, der Verschlüsselung und Authentifizierung beispielsweise bei Digitalkameras sucht. Sofern diese geschäftlichen Zwecken dienen, sind wertvolle Bilddaten also möglichst schnell auf Medien zu transferieren, die leichter zu sichern sind.

Diese Beispiele zeigen nur einen kleinen Ausschnitt der besonderen Sicherheitsanforderungen, die bei mobilen Endgeräten zu beachten sind. Ein geeignetes Sicherheitskonzept ist also bereits in der Planungsphase für den Einsatz dieser Geräteklasse notwendig und sollte im Rahmen des Informationssicherheitsmanagementsystems (ISMS) entwickelt, implementiert und gesteuert werden. Nur so ist ein ganzheitlicher Schutz des Assets Information möglich – ob im Unternehmen oder immer und überall „at your fingertips".

**Hessen-IT bietet Unternehmen Beratung an.**

Die Aktionslinie Hessen-IT des Hessischen Wirtschaftsministeriums informiert Unternehmen zu allen wichtigen Fragen des Einsatzes von Informations- und Kommunikationstechnologien und natürlich auch zu IT-Sicherheitsaspekten. Der Projektträger der Aktionslinie, die HA Hessen Agentur GmbH, hat verschiedene Leitfäden herausgebracht, die sich mit dem Thema IT-Sicherheit beschäftigen, genauso wie eine interaktive Lern-CD. Zu den Maßnahmen gehört auch die Durchführung von Veranstaltungen und Workshops. Im Rahmen der Aktivitäten von Hessen-IT ist darüber hinaus eine Expertengruppe hessischer IT-Sicherheitsanbieter sehr aktiv, aus deren Arbeit dieser Artikel entstanden ist. ■

**Weiterführende Links zum Thema**

- Aktionslinie Hessen-IT: http://www.hessen-it.de
- Mobile Device Management (Wikipedia-Artikel): http://de.wikipedia.org/wiki/Mobile_Device_Management
- Information at your fingertips: http://www.mr-gadget.de/future-tech/2009-05-20/zurueck-in-die-zukunft-die-vision-von-bill-gates-aus-dem-jahr-1994
- Verlorene Notebooks: http://www.pressetext.de/news/091203005/lost-laptop-online-detektive-bringen-verlorene-notebooks-zurueck/
- Kosten für verlorene Notebooks: http://www.cio.de/knowledgecenter/security/883698/
- Securing Mobile Devices: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Securing-Mobile-Devices.aspx
- Jericho Forum: http://www.opengroup.org/jericho/