IT Audit

Mobile Benutzer – Wertschöpfung oder Bedrohung für das Unternehmen?

Zunehmend fordern Mitarbeiter mobile Lösungen zur Arbeitserleichterung, während Unternehmen, Organisationen oder Behörden sich erhoffen, mittels Einsatz von mobilen Geräten eine Wertschöpfung zu erzielen. Die Vorteile für Mitarbeiter sind dabei, dass sie jederzeit und überall Zugriff auf alle Unternehmensdaten haben.

Die meisten größeren deutschen Unternehmen haben schon irgendeine Form von mobilen Lösungen für ihre Mitarbeiter im Einsatz. Unternehmen, die dies bisher nicht haben, äußern Sicherheitsbedenken als größtes Hindernis. Der Artikel gibt Aufschluss über die Bedrohungen beim Einsatz von mobilen Geräten und soll Verantwortlichen im Einzelfall helfen, zwischen Gefahren und Nutzen abwägen zu können. Da die Betrachtung generisch ist, kann sie von Unternehmen genutzt werden, um die individuelle Situation zu abstrahieren.

Ausgangssituation

Wird die Integration von mobilen Geräten ins Unternehmensnetzwerk betrachtet, können mehrere Teilaspekte diskutiert werden. Dazu zählen der Benutzer, die mobilen Geräte, die Zugangsebene und das Unternehmensnetzwerk.

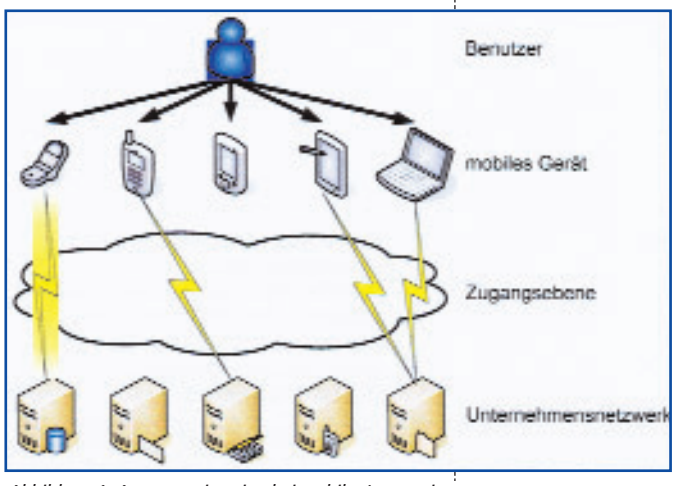

Abbildung 1: Ausgangssituation bei mobiler Integration

Benutzer

Wichtig ist, dass die individuellen Bedürfnisse der einzelnen Mitarbeiter nach Kommunikation durch eine benutzerfreundliche Lösung erfüllt werden. Als Konsequenz werden Unternehmen je nach Anwendungsgebiet mehrere mobile Gerätetypen im Einsatz haben. Sicherheit wird dabei seitens des Benutzers als zweitrangig eingestuft. Erfüllt eine Lösung nicht seine Bedürfnisse, wird sie nicht eingesetzt oder der Benutzer sucht eigene Lösungen oder Erweiterungen, ohne dabei Rücksicht auf die Sicherheit zu nehmen oder diese mit der IT des Unternehmens abzustimmen.

Mobile Geräte

Die mobilen Geräte stellen dem Benutzer, unabhängig von dessen Aufenthaltsort, Telekommunikations- bzw. Datendienste zur Verfügung. Diese Geräte sind klassifizierbar nach dem Grad der Mobilität, den vorhanden Ressourcen der Geräte und den beschränkten Ein- und Ausgabemöglichkeiten. Für den mobilen Unternehmenseinsatz sind besonders Notebooks und Handhelds wie Mobiltelefone, Smartphones und PDAs von Bedeutung.

Für die Ermittlung des Schutzbedarfs von mobilen Geräten ist es notwendig, sich über die vorhandenen oder übermittelten Daten wie beispielsweise E-Mails, Dateien wie Geschäftsberichte ein Bild zu machen. Die Daten können sich alternativ auf dem mobilen Gerät befinden oder durch den Zugriff des Benutzers auf das Unternehmensnetzwerk gewonnen werden. Viele mobile Geräte bieten auch die Möglichkeit, als portables Speichermedium genutzt zu werden. Der Speicherort der Daten kann sich entweder ständig auf dem Gerät in einem internen Speicherbereich oder nur zeitweise auf einer entfernbaren Speicherkarte befinden.

Ein modernes mobiles Gerät verfügt über eine Vielzahl von unterschiedlichen Schnittstellen. Dazu gehören Anbindungen an Mobilfunkprovider über GSM, GPRS und UMTS. Außerdem sind inzwischen einige Geräte mit WLAN- und LAN-Anschlüssen ausgestattet. Schon bald werden auch die mobilen Geräte mit einem oder mehreren der WiMAX-Standards ausgestattet sein. Im **Personal-Area-Network** (PAN)-Umfeld gibt es eine Vielzahl von Verbindungsmöglichkeiten. Darunter fallen Bluetooth, Infrarotschnittstelle. Außerdem werden eine oder mehrere USB-Schnittstellen oder serielle Kabelverbindungen zur Verfügung gestellt [1].

Zugang zum Unternehmensnetzwerk

Es gibt verschiedenste Szenarien für den mobilen Zugriff auf ein Unternehmensnetzwerk. Allgemein können wir davon ausgehen, dass der Zugriff von mobilen Endgeräten auf das Unternehmensnetzwerk im Prinzip über ein oder mehrere ungesicherte Netzwerke realisiert wird. Dies können fremde Unternehmensnetzwerke sein, öffentliche Internet-Zugangspunkte in Cafés oder Flughafenlounges. Der Zugriff kann über WLAN oder Bluetooth erfolgen sowie direkt paket- oder leitungsvermittelt über die Infrastruktur eines Mobilfunkbetreibers; auch eine Einwahl über eine Telefonleitung ist möglich.

Unternehmensnetzwerk

Grund für den Einsatz von mobilen Geräten ist die eine gewünschte Wertschöpfung durch Nutzung der Daten und Anwendungen des Unternehmens von überall. Diese Daten und Anwendungen sind aber auch wertvoll für einen Angreifer und müssen daher im mobilen Umfeld besonders sorgfältig geschützt werden. Etliche Server stellen im Unternehmen Dienste zur Verfügung, die auch mobil genutzt werden sollen. Dazu gehören E-Mail-Server, Datenbanken, Customer Relation Systeme, Groupware-Lösungen und Dateiserver. Das Unternehmensnetzwerk muss ggf. mit zusätzlichen Servern, wie etwa einer Middleware für mo-

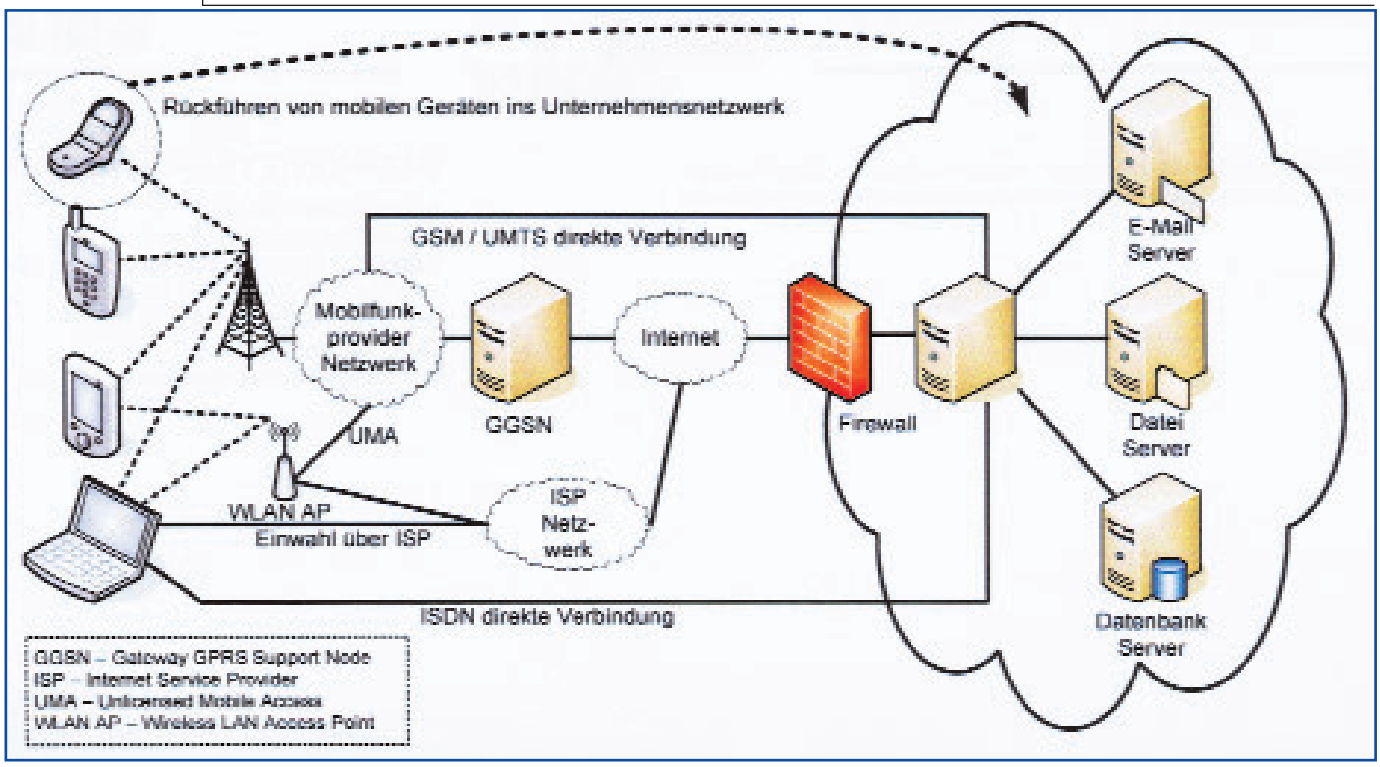

Abbildung 2: Beispiele für Szenarien der Zugangsebene

bile Geräte, angepasst werden, um den Zugriff von außen auf die Unternehmens-Server zu ermöglichen. Der Zugang zum Unternehmen erfolgt über Firewall-Systeme und VPN-Lösungen. Unternehmensnetzwerke sind bisher in der Regel gegen Bedrohungen von außen durch ihre Firewall- und vielleicht Intrusion Detection-Systeme geschützt.

oder gestohlen; oder können – wie vom BSI veröffentlicht – auch in Besprechungen genutzt werden, um einen Raum abzuhören, entweder mit dem Wissen des Besitzers oder durch manipulierte Geräte.
Bei diesen Geräten kommt es zwecks Spionage sogar zur Manipulation von Geräte-Hard- oder Software. Dabei wird z.B. direkt die Platine des Gerätes angezapft, als Strom

Bedrohungen für den mobilen Einsatz

Benutzer
Allgemein sind „Social Engineering"-Techniken, wie sie beispielsweise beim Phishing eingesetzt werden, sehr erfolgreich. Somit ist der legitime Benutzer im Unternehmen eine ernstzunehmende Bedrohung für die IT – entweder aus Naivität oder Unachtsamkeit bieten sie große Angriffsflächen. So kann es in Zügen und an anderen öffentlichen Plätzen einem Benutzer passieren, dass ein Angreifer Informationen direkt von seinem Bildschirm abliest. Darüber hinaus ist auch die persönliche soziale Interaktion zum Beispiel beim Bier in der Kneipe geeignet, um an Informationen über ein Unternehmen zu gelangen.

Mobile Geräte
Mobile Engeräte bieten eine besonders große Angriffsfläche, da der Benutzer sie ständig bei sich hat. Bedrohungsszenarien sind vielfältig: Geräte werden liegen gelassen oder sogar Datenlieferant. Besonders bei Anwendungen in einem Hochsicherheitsumfeld, wo Daten und Informationen den höchsten Sicherheitsanforderungen unterliegen, muss die Frage nach der Vertrauenswürdigkeit der Hersteller und Bezugsquelle der verwendeten Hardware gestellt werden.

Mobile Geräte sind ständig im Wandel und mit jeder Generation unterstützen die Geräte mehr Anwendungen und Dienste. Früher waren sie reine Hardwareimplementierungen, die wenig Platz für Angriffe geboten haben, heute bieten sie flexible Softwareplattformen, die mit **Software Developing Kits** (SDKs) ausgeliefert werden. Diese Flexibilität verstärkt die Gefahr vor Angriffen mit Software und das bei gleichzeitigem steigendem Schutzbedarf für die zunehmende Quantität und Qualität der Daten auf den mobilen Geräten.

Seit Anfang 2006 gibt es ein kommerzielles Produkt namens FlexiSpy für Symbian- Telefone, um hinter Personen herzuspionieren. Vermarktet wird dies als eine Art „Privatdetektiv" für den eigenen Lebenspartner. Der Anwender installiert die Software auf dem Gerät von dem Partner und vergibt dabei eine nur ihm bekannte Tastenkombination für den Zugriff auf die Software. Diese Anwendung versteckt sich danach vollständig vor dem legitimen Benutzer. Die Software sammelt alle Verbindungsdaten sowie Nachrichten und schickt sie an Server der Firma FlexiSpy auf die der Anwender dann Zugriff hat. Es bedarf keiner großen Phantasie, dass in einem Spionage-Umfeld ähnliche Lösungen, verborgen vor der Öffentlichkeit, auch auf anderen Systemen eingesetzt werden. In den ersten fünf Monaten des Jahres 2006 hat sich nach F-Secure die Anzahl der mobilen Schadsoftware auf 200 verdoppelt.

Daneben ergeben sich ernstzunehmende Bedrohungen durch Softwarefehler. So sind die Betriebssysteme von mobilen Geräten, aufgrund der ähnlichen Rechnerarchitektur wie bei Arbeitsplatzrechnern, ebenfalls anfällig für „buffer overflow"-Angriffe.
Der Zugriff mit unautorisierter unternehmensfremder Hardware, sollte unterbunden werden, da es nicht möglich ist diese Geräte verlässlich zu überprüfen und Aussagen über den Systemzustand zu treffen.

Firmengeheimnisse könnten über Hard- oder Software-Keylogger oder andere Schadsoftware in falsche Hände kommen.

Zugangsebene

Die Betrachtung der Zugangsebene ist aufgrund der vielen denkbaren Szenarien für einen Zugriff auf das Unternehmensnetzwerk recht umfangreich und würde den Rahmen dieses Artikels sprengen. Insgesamt haben unsere Untersuchungen gezeigt, dass die Zugangsebene, egal ob GSM, GPRS, UMTS, ISDN, WLAN oder Bluetooth verwendet wird, sich nicht als sicher einstufen lässt.

Unternehmensnetzwerk

In diesem Artikel werden nur die durch die Integration von mobilen Geräten zusätzlich entstehenden Bedrohungen für das Unternehmensnetzwerk betrachtet. Für die zusätzliche Bedrohung durch mobile Geräte sind zwei Angriffsszenarien denkbar.

Zum einen kann das mobile Gerät einen entfernten unerlaubten Zugriff auf das Unternehmensnetzwerk aufbauen oder es wird durch den Benutzer ein manipuliertes Gerät zurück in das Unternehmen gebracht und lokal verbunden. In beiden Fällen kann ein durch Schadsoftware verseuchtes Gerät versuchen, andere Rechner anzugreifen oder Informationen aus dem Unternehmen unerlaubt zu versenden. Gestohlene oder gefundene Geräte können missbraucht werden, um auf Unternehmensdaten zuzugreifen. Außerdem können die mobilen Geräte, begünstigt durch ihre diversen Schnittstellen, auch an Hintertüren vorbei, die Unternehmens-Firewall aufreißen. Damit können gezielt Daten aus dem Unternehmen geschleust und Angriffe auf ein anderes System im Unternehmen durchgeführt werden.

Fazit

Die Ausgangssituation stellt sich als sehr komplexe Herausforderung für die IT der Unternehmen dar. Es existiert eine Reihe von handfesten Bedrohungen für die Daten und Ressourcen der Unternehmen. Mit der Einführung der mobilen Geräte muss das hoffentlich schon bestehende Sicherheitskonzept des Unternehmens angepasst werden. Dazu müssen Gegenmaßnahmen für die individuell zutreffenden hier vorgestellten Bedrohungen erarbeitet werden. Abhängig vom Schutzbedarf der Daten müssen z.B. weitere Sicherheits-Tools wie Firewall, Virenscanner und Verschlüsselungssoftware für bestehende mobile Lösungen verwendet werden, um das Gerät gegen vorliegende Gefahren zu härten. Außerdem sind z.B. die Verwendung von VPN-Technologie und die Minimierung der auf dem Gerät installierten Software wichtig. Jedoch ergeben sich weiterhin einige zusätzliche Probleme durch den Einsatz von gehärteten Geräten. Mobiles Arbeiten kann die Produktivität und die Wertschöpfung steigern. Jedoch führt dies auch zu einem erhöhten Management- und Sicherheitsaufwand für die IT eines Unternehmens. Dies kann bei schlechter Planung schnell dazu führen, dass die erhoffte Wertschöpfung durch die Integration der Geräte ausbleibt. Die Ausgaben für solche Sicherheits-Tools und der Wartungsaufwand können die Kosten für die mobilen Geräte in die Höhe treiben. Außerdem fordern sie Einbußen beim Komfort für den Benutzer (eingeschränkte Funktionalität) und bei der Performance des Gerätes. Des Weiteren lässt sich mit den gehärteten Geräten kein solides Sicherheitskonzept für Hochsicherheitsanwendungen erreichen [2]. In diesem Bereich kann bis heute keine sichere Integration realisiert werden.

Dipl.-Inform. (FH) Malte Hesse, malte.hesse@internet-sicherheit und
Prof. Dr. Norbert Pohlmann, norbert.pohlmann@informatik.fh-gelsenkirchen.de
Institut für Internet-Sicherheit, Fachhochschule Gelsenkirchen, Neidenburger Str. 43, 45877 Gelsenkirchen, www.internet-sicherheit.de

Literatur

[1] M. Hesse: „Sichere Integration mobiler Nutzer in bestehende Unternehmensnetzwerke“, Diplomarbeit, Institut für Internet-Sicherheit, FH-Gelsenkirchen 2006
[2] M. Hesse, N. Pohlmann: „Location Based Security - Ansätze für ein Stufenkonzept“, in "DACH Mobility 2006", Hrsg.: Patrick Horster, syssec Verlag, 2006