

Mobile Geräte sicher eingesetzt

Security und Datenschutz gewinnen in Unternehmen dank Smartphones und Tablets ganz neue Bedeutung. Gefordert ist ob vieler neuer Risiken ein detailliertes Einsatzkonzept.

VON CHRISTOPH AUMAYER

Mobile Devices – bis vor wenigen Jahren noch einfache kabellose Telefone mit stark eingeschränktem Funktionsumfang – bieten heute als Smartphones, Personal Digital Assistance (PDA) oder als Tablet-PCs umfangreiche und ausgereifte Funktionen, wodurch sich eine Vielzahl neuer Einsatzmöglichkeiten ergibt. Neben klassischen Eigenschaften im Consumer-Bereich bieten solche Geräte heute einen grossen Umfang professioneller Merkmale, was sie für einen Einsatz im Business-Umfeld interessant machen. So verwenden Mitarbeiter ihre Mobile Devices vermehrt als mobile Arbeitsplätze, wodurch die Geräte unweigerlich mit sensitiven Daten in Berührung kommen. Daraus ergeben sich neue Herausforderungen hinsichtlich Sicherheit und Datenschutz, mit denen sich Unternehmen heute konfrontiert sehen.

Problemstellung

Die bereits grosse und im hohen zweistelligen Prozentbereich weiter wachsende Verbreitung mobiler Devices – Gartner spricht von weltweit mehr als 1,8 Milliarden Smartphones und mit Web-Browsern ausgestattete Mobile Devices ab 2013, in der Schweiz wurden laut Weissbuch 2010 alleine im vergangenen Jahr 1,5 Millionen neue Smartphones verkauft –, das breite Spektrum unterschiedlicher Geräte, sowie deren vielseitige Verwendungsmöglichkeiten führt zu einigen Zielkonflikten:

► Die Vielzahl existierender, auf unterschiedlichen Soft- und Hardware-Plattformen basierenden Mobile Devices (iOS, Android, Windows Phone 7, BlackBerry, Symbian, etc.) bieten unterschiedliche, teilweise noch unausgereifte Funktionen und Sicherheitsmechanismen (mehr dazu im folgenden Schwerpunkt-Artikel ab Seite 38). Dies kann die Durchsetzung unternehmensweit gültiger Compliance-Anforderungen und Sicherheits-

Vorgaben erschweren, die sich auch auf betriebliche Aspekte wie das zentrale Management und die Provisionierung beziehungsweise Konfiguration der Geräte auswirken.

► Seitens des Managements und der Mitarbeiter besteht in der Regel die Erwartung, dass die Integration mobiler Gadgets in die Unternehmensinfrastruktur vorangetrieben wird und entsprechende Devices zur Verfügung gestellt werden. Die IT als klassisches Cost Center muss in ihrer Rolle als Business-Enabler einen Weg finden, einerseits die Wünsche des Managements zu erfüllen, andererseits aber auch den internen Vorgaben und Weisungen zu entsprechen.

► Aufgrund des stetig steigenden Bedarfs an neuen Geräten und dem grossen Konkurrenzdruck, dem die Hersteller vermehrt ausgesetzt sind, nimmt die «Time to Market» neuer Geräte kontinuierlich ab. Dies wiederum kann die Unternehmen vor die Herausforderung stellen, neue Geräteklassen und -modelle binnen kürzester Zeit für den Einsatz im Geschäftsumfeld fit zu machen – was sich mit der Markteinführung von Apples iPad einmal mehr eindrücklich gezeigt hat.

► Die jederzeitige und ortsungebundene Verwendung von Mobile Devices führt im

Endeffekt dazu, dass die ansonsten durch umfangreiche Massnahmen geschützten Unternehmensressourcen an vielen Stellen – nämlich auf den Smartphones der Mitarbeiter – angreifbar werden. Deshalb muss der Schutz dieser Geräte erhöhten Anforderungen genügen und mindestens so gut geplant und umgesetzt werden wie bei anderen Clients.

► Oft werden Mobile Devices neben der geschäftlichen Nutzung auch privat gebraucht, oder befinden sich gar im privaten Besitz. Dadurch existiert ein Rollenkonflikt, da derselbe Benutzer an einem einzelnen Gerät sowohl seine private, wie auch seine geschäftliche Rolle einnimmt und dadurch unterschiedliche, teilweise kontroverse Interessen vertritt.

Je nach Einsatzzweck und Integrationsgrad mobiler Geräte, sowie der an sie gestellten Anforderungen, müssen die unternehmensspezifischen Problemstellungen identifiziert und mit geeigneten Massnahmen eliminiert werden.

Sicherheitsaspekte

Aufgrund der bereits erwähnten und einer Vielzahl weiterer Problemstellungen können Mobile Devices, wenn sie nicht entsprechend geschützt sind, auf unterschiedliche Weise missbraucht werden. Dabei steht in erster Linie der Datendiebstahl respektive die Wirtschaftsspionage im Vordergrund. Weitere Angriffsvektoren sind jedoch der Identitätsmissbrauch, Zugriff auf die Unternehmensinfrastruktur oder der einfache Missbrauch der Telefonfunktionen, was beispielsweise die Kompromittierung von Zwei-Faktor-Authentifizierungslösungen basierend auf mTAN miteinschliesst. Um einen umfassenden Schutz zu gewährleisten, müssen deshalb unterschiedliche Aspekte berücksichtigt werden:

► **Datensicherheit:** Schutz der Daten, die auf dem Mobile Device permanent oder temporär gespeichert sind. Dabei muss der Schutz

IN KÜRZE

- Die rasant wachsende Verbreitung von Mobile Devices, auch im Geschäftsumfeld, bringt einige neue Herausforderungen und Risiken für IT-Abteilungen.
- Dabei stehen die Sicherheit der Daten, der Kommunikation, der Plattformen und der Schutz vor Missbrauch im Zentrum.
- Es bedarf deshalb unbedingt eines Einsatzkonzeptes.

sets, das heisst unabhängig vom aktuellen Zustand des Gerätes (ein- oder ausgeschaltet) gewährleistet sein. Ebenso gilt es, neben dem internen Speicher auch allfällige externe Speichererweiterungen (z.B. SD-Karten) zu berücksichtigen.

► **Kommunikationssicherheit:** Schutz jeder Datenverbindung, unabhängig von der gewählten Übertragungstechnologie (UMTS, WLAN, Bluetooth etc.), sowie der verfügbaren Schnittstellen (USB etc.).

► **Sicherheit der Unternehmensinfrastruktur:** Schutz vor unberechtigtem Zugriff auf die Unternehmensinfrastruktur über die Schnittstellen und Verbindungen, die durch die Mobile Devices etabliert sind.

► **Platformsicherheit:** Schutz des Gerätes und seines Betriebssystems, sowie jeglicher installierter Software vor Angriffen aller Art. Besonders hervorzuheben sind hierbei mutwillige Modifikationen des Betriebssystems durch den Benutzer (beispielsweise Jailbreaking), sowie Gefahren ausgehend von einer sehr hohen Anzahl verfügbarer Dritthersteller-Applikationen (Apps) verschiedenster offizieller und inoffizieller Quellen (App Stores). Ebenso können standardmässig vom Hersteller installierte Software-Komponenten wie Browser, E-Mail, SMS/MMS, Multimedia-Player sowie Synchronisationsdienste Ziele von Angriffen sein.

► **Missbrauch des Gerätes:** Schutz des Gerätes vor unberechtigter Verwendung der Gerätefunktionen wie beispielsweise des Telefonmoduls durch Malware. Im Fokus stehen dabei sogenannte Dialer-Programme, die ohne Wissen des Benutzers kostenintensive Mehrwert-Dienste abrufen. Gefahren lauern zusätzlich durch in Dritthersteller-Applikationen integrierte Werbebanner, die über die Internetschnittstelle ebenso kostenintensive Services beziehen und abbuchen.

Organisatorische Lösungsansätze

Da Mobile Devices in der Regel überall zum Einsatz kommen, also auch in potentiell unsicheren Umgebungen, müssen sie ebenso wie andere portable Geräte umfassend geschützt werden. Um diesen Schutz zu gewährleisten, ist eine Verankerung der Mobile Devices in der Sicherheitsorganisation eines Unternehmens mindestens so wichtig, wie die technische Implementierung von Sicherheitsmassnahmen, auf die in den kommenden Schwerpunkt-Artikeln – zum Beispiel in der Marktübersicht über Mobile-Device-Management-Lösungen (ab S. 40) – genauer eingegangen wird. Aus organisatorischer Sicht ist das Augenmerk insbesondere auf folgende Aspekte zu legen:

► **Zentrales Device Management:** Die Unternehmensinfrastruktur wird üblicherweise

von zentraler Stelle verwaltet. Dies gilt sinn- gemäss auch für das Management von Mobile Devices. Erschwerend dabei wirkt der Um- stand, dass in der Regel eine grosse Zahl verschiedener Geräte mit unterschiedlichem Funktionsumfang parallel im Einsatz steht. Darüber hinaus befinden sich unter Umstän- den viele der mobilen Geräte in Privatbesitz, weshalb eine zentrale Verwaltung und Kon- trolle aus Sicht der Besitzer stets im Verdacht steht, in deren Privatsphäre einzugreifen. Wie geht man damit um?

► **Device Lifecycle Management:** Das De- vice Lifecycle Management umfasst die Koor- dination des gesamten Lebenszyklus von Mo- bile Devices, das heisst von der Beschaffung und Inventarisierung, über die Provisionierung und Bereitstellung, die Aktualisierung und Reparatur, bis hin zur Entsorgung der Geräte, und ist damit ein wichtiges Thema. Dazu gehört auch die Planung von Massnah- men, falls Geräte verloren gehen oder ge- stohlen werden.

► **Data Lifecycle Management:** Auch der Umgang mit Unternehmensdaten auf Mobile Devices muss geplant und koordiniert werden. Dies umfasst neben dem Speichern die- ser Daten auf den Geräten auch eine allfällige Synchronisierung mit anderen Geräten, das Sichern gegen Datenverlust (Backup), sowie das unwiderrufliche Löschen von lokal ge- speicherten Informationen.

► **Compliance-Vorgaben und Security-Gui- delines:** Mobile Geräte unterliegen, wie die gesamte Infrastruktur einer Unternehmung, gewissen Compliance-Vorgaben und Security-Richtlinien. Die Etablierung und das Er- zwingen von gerätespezifischen Security-Po- lices, gepaart mit der Bewusstseinsförderung beim Endbenutzer hinsichtlich realer Gef- ahren im Umgang mit Mobile Devices (Stich- wort «User-Awareness»), unterstützt eine Unternehmung in der Einhaltung entspre- chender Vorgaben.

Ohne Einsatzkonzept geht es nicht

Mobile Devices wie iPhones oder iPads komplett aus dem eigenen Unternehmen zu ver- bannen, ist heute ein Ding der Unmöglichkeit. Sie einfach so und ohne weitere Massnahmen in die Firma zu integrieren, birgt auf der an- deren Seite jedoch grosse Risiken. Es bedarf deshalb unbedingt eines Einsatzkonzeptes, in dem alle Aspekte angemessen berücksichtigt und darauf mit entsprechenden konzeptio- nellen Ansätzen und technischen Lösungen reagiert wird.

CHRISTOPH AUMAYER IST LEITER DES FACHBEREICHS SECURITY SERVICES BEI DER IN&OUT AG.

