WHITE PAPER

Acronis®

Mobile Sicherheit

Die fünf größten Gefahren für die Unternehmenssicherheit durch den Einsatz mobiler Geräte und wie Sie diese lösen können

Der rasant zunehmende Einsatz mobiler Geräte bietet Unternehmen heutzutage zahlreiche Möglichkeiten, um Arbeitsabläufe im Unternehmen zu beschleunigen oder zu verbessern und schafft damit nachhaltige und messbare Mehrwerte. Außendienstmitarbeiter und Führungskräfte, die viel unterwegs sind, Vertriebsmitarbeiter und Projektmanager benötigen alle Zugriff auf Applikationen und Unternehmensdaten von Mobilgeräten aus. Der Einsatz von iPad, iPhone und anderen mobilen Geräten hat großen Unternehmen zweifellos erhebliche Vorteile beschert. Aber diese Vorteile gehen auch mit neuen Sicherheitsrisiken einher, vor denen IT-Abteilungen stets wachsam sein müssen. Unternehmenskritische Daten könnten sonst möglicherweise gefährdet sein.

Zu den Gefahren gehören:

1. Ungesicherter Datentransfer
2. Verlust/Diebstahl von Geräten
3. Offene Wi-Fi-Netzwerke und öffentliche Hotspots
4. Malware und Viren
5. Ungenaue Unternehmensrichtlinien

Durch die zunehmende Integration von Lösungen für Privatanwender auch in die Unternehmensinfrastruktur (BYOD - Bring Your Own Device), sind Lösungen zur Verwaltung mobiler Daten heute wichtiger als je zuvor[1]. In diesem Artikel zeigen wir Ihnen die aktuellsten Bedrohungen für die Sicherheit Ihrer mobilen Geräte auf, sowie Lösungsansätze, um diese Risiken zu reduzieren, die Vorteile durch den Einsatz mobiler Geräte wie iPad und iPhone optimal nutzen zu können und gleichzeitig die IT-Sicherheit gewährleisten und Mitarbeiter zufrieden stellen zu können. Produktivitätssteigerungen und optimierte Arbeitsabläufe gewinnen im heutigen IT-Unternehmensumfeld immer mehr an Bedeutung.

Ungesicherter Datentransfer

Problem:

Durch den zunehmenden Einsatz von iPads® und anderen Tablets ist die effiziente Verwaltung mobiler Daten heute ganz besonders wichtig, da diese Geräte oftmals nur sehr begrenzte eigene Speicherkapazität für die Datenablage bereitstellen. Mitarbeiter entscheiden sich in der Regel für Zwischenlösungen und Synchronisierungsmöglichkeiten, die für Privatanwender konzipiert sind und laut den neuesten Eingaben bei der FTC (Federal Trade Commission) die Standards für eine sichere, verschlüsselte Datenübertragung und -speicherung nicht erfüllen.[2]

Lösung:

Die Verwaltung mobiler Daten ermöglicht den einfachen, sicheren und kontrollierten Zugriff auf Unternehmensdaten von mobilen Geräten aus. Ohne den Einsatz einer professionellen Lösung können Mitarbeiter diese Daten zwar oftmals auf mobilen Geräten abrufen und austauschen, Ihr Unternehmen jedoch ernsthaften Risiken aussetzen. Workarounds wie die Verwendung von Synchronisationsdiensten für Privatanwender zur Ablage von Unternehmensressourcen für den mobilen und offline-Zugriff – bei denen Dateien ungeschützt sind und der Zugriff nicht von der IT verwaltet wird – stellen eine Sicherheitslücke dar und entsprechen nicht den Richtlinien für Unternehmen. Nur durch Lösungen, die garantieren, dass der Datenzugriff sowohl während der Übertragung als auch auf dem Gerät selbst passwortgeschützt und verschlüsselt ist, können unternehmenskritische Daten geschützt und Mitarbeitern ein effizientes Arbeiten auf den neuesten mobilen Geräten ermöglicht werden. Solche Lösungen sind in bestehende Unternehmensumgebungen z.B. in Active Directory schnell integrierbar und können die bereits vorhandene Rechenzentrums-Infrastruktur und Server verwenden, statt zusätzliche Komponenten von Drittanbietern zu benötigen. Diese Funktionen ermöglichen es der IT, die Kontrolle zu behalten und bieten optimale Sicherheit unter Berücksichtigung von Compliance-Anforderungen.

Verlust/Diebstahl von Geräten

Problem:

Die Sicherheitsrisiken für Unternehmen durch verlorene oder gestohlene Geräte sind an sich nichts Neues. Die steigende Anzahl mobil tätiger Mitarbeiter erhöht diese Risiken allerdings zusätzlich. Mangels Integration in die kontrollierte Server-Infrastruktur und Remote Management-Möglichkeiten, können iPads und andere Tablets von der IT großer Unternehmen nicht remote gelöscht oder gesperrt werden, wenn das Gerät in falsche Hände fällt.

Lösung:

Wenn ein Gerät verloren geht, gestohlen oder die Sicherheit gefährdet wird, gibt es Lösungen, die es dem IT-Leiter ermöglichen, Unternehmensdateien remote vom Gerät zu löschen. Werden im Unternehmen iPads verwendet, empfiehlt es sich, eine mobile Sicherheitslösung zu berücksichtigen, die im Unternehmensumfeld bereits bewährt ist und als vertrauenswürdig eingestuft wird und nachweislich bereits erfolgreich bei der Integration von Apple-Geräten mit Windows-Servern implementiert wurde.

Während sich Diebstahl und Verlust von Mitarbeiter-Geräten nicht vollständig vermeiden lassen, bemühen sich sowohl mobile Datenverwaltungs- als auch mobile Gerätemanagement-Lösungen insbesondere darum, die Unternehmens-Ressourcen zu schützen. Die besten Lösungen ermöglichen es der IT auch, speziellen Zugriff auf Grundlage individueller Unternehmens-Strategien zu konfigurieren, wie etwa die Integration in Active Directory® und das Aktivieren oder Deaktivieren der Anwenderrechte zum Öffnen, Drucken oder Versenden einer Datei per E-Mail, sowie vieles mehr.

> *„Sicherheitsexperten sind sich einig, dass die meisten Bedrohungen für mobile Geräte von Menschen verursacht werden, deren Geräte gestohlen werden oder die ihre Geräte verlieren. Statt des Umgangs mit Malware liegt die größte Herausforderung für die mobile Unternehmenssicherheit darin, die Vielzahl an Geräten, die Mitarbeiter in einem Netzwerk anmelden können, bestmöglich zu verwalten.“*
>
> *—eWeek.com, „Dealing with Enterprise Mobile Security,“ 6. Oktober 2010*[3]

Offene W-LAN Netze und öffentliche Hotspots

Problem:

Studien zeigen, dass Endanwender (und somit auch Mitarbeiter) sehr nachlässig mit der Sicherheit ihres Handys umgehen.[4] Einem aktuellen Bericht von Juniper Networks zufolge sind WLAN-Angriffe auf dem Vormarsch, weil Hacker sich über offene Verbindungen einfachen Zugang zu sozialen Netzwerken und E-Mail-Konten verschaffen können.[5] Noch schlimmer ist, dass viele Verbraucher sich immer noch nicht bewusst sind, welche Risiken öffentliche W-LAN-Netze bergen, auch wenn sie als „geschlossene" Hotspots angezeigt werden. Zum Beispiel richtete die in Großbritannien ansässige Tageszeitung „The Guardian" im April letzten Jahres einen falschen W-LAN-Hotspot an einem Flughafen ein und konnte damit ganz einfach Benutzerinformationen wie E-Mail-Passwörter und Kreditkarten-Details erhalten.[6] Im selben Artikel heißt es, dass Unternehmensinformationen auf Smartphones denselben Bedrohungen ausgesetzt sind.

Lösung:

Was kann ein Enterprise Unternehmen tun, um dies zu vermeiden? Man kann es Mitarbeitern nicht verbieten, ihre Smartphones und Tablets in der Öffentlichkeit zu benutzen – das widerspricht ganz dem eigentlichen produktiven Nutzen des Gerätes. Die Verwaltung mobiler Geräte bietet Bereitstellungs- und Management-Tools und die Möglichkeit, Applikationen und E-Mail- / PIM-Lösungen in einem eigenen Containerformat zu verschlüsseln und mit einem Passwort zu versehen. Jedoch ist MDM (Mobile Device Management) nicht in der Lage, Unternehmensdaten zu schützen, die nicht in diesem Format vorliegen. Daher bedarf es einer Lösung, die auf dem Gerät Sicherheit für Unternehmensdaten bietet und Berechtigungen erfordert, damit Ressourcen ebenso wie Gerät und Netzwerk geschützt sind[7].

Malware und Viren

Problem:

Mit dem zunehmenden Einsatz neuer Technologien entstehen auch neue Formen von Schadsoftware. Aktuelle Pressemeldungen über Malware, die als Android®-Applikationen getarnt sind, haben dieses Problem zu einer Priorität der Unternehmens-IT bei Überlegungen für die mobile Sicherheit gemacht.[8] Das iPad ist zwar dank des von Apple® streng überwachten App Stores noch kein primäres Ziel für Trojaner-Apps, ist aber trotzdem nicht völlig gegen Viren immun.[9] Und mit der steigenden Popularität des Gerätes steigt auch die Tendenz, dass es doch zum Ziel böswilliger Angriffe werden könnte.

> *„Wenn Sie ein Android-Handy oder iPhone besitzen, ist die Wahrscheinlichkeit versehentlich Malware herunterzuladen heute 2,5-mal höher als im Januar letzten Jahres,“*
>
> *–TGDaily.com, „Mobile malware explodes in first half of 2011,“ 4. August 2011*[10]

Lösung:

Die Unternehmens-IT kann nicht verhindern, dass Mitarbeiter mobile Applikationen herunterladen, die geschäftskritische Informationen aufspüren und letztendlich auf unternehmenskritische Ressourcen zugreifen könnten. Sie kann Daten jedoch auf Seiten von Servern und Netzwerken schützen, indem diese beim Datentransfer und der Ablage auf dem Gerät eines Mitarbeiters verschlüsselt werden. Lösungen für die Verwaltung mobiler Dateien wurden speziell für die Integration in die bestehende Unternehmens-Infrastruktur entwickelt und bieten diese Funktionen zusammen mit einer zentralen Kontrollfunktion an, die es der Unternehmens-IT ermöglicht, bei Problemen die MFM-App eines Mitarbeiters per Fernzugriff zu löschen.[11]

Unternehmensrichtlinien zur Bekämpfung von Gefahren neuer Technologien

Problem:

Ungenaue Unternehmensrichtlinien im Umgang mit neuen Technologien zur besseren Unterstützung von Mitarbeitern durch Erlauben von Geräten und Lösungen, die für Privatanwender konzipiert sind, werden häufig nicht direkt als Sicherheitsbedrohung wahrgenommen. Doch laut aktuellen Berichten setzen sich Unternehmen enormen Risiken aus, wenn sie keine klar definierten Vorgaben haben[12]. Viele Unternehmen unterstützen die Wünsche ihrer Mitarbeiter bei der Auswahl von Geräten und Applikationen, durch die sie Ihre Produktivität steigern könnten. Doch dieselben Unternehmen verabschieden nur sehr langsam neue Unternehmensrichtlinien zur Abwehr der besonderen Bedrohungen, die durch den Einsatz neuer Technologien in der Arbeitswelt entstehen.

Lösung:

Die Sicherstellung der Integrität von Unternehmensressourcen beginnt mit klar festgelegten Richtlinien und Standards. Während solche Maßnahmen Malware nicht verhindern können, setzen sie jedoch Anforderungen an Mitarbeiter hinsichtlich deren Verantwortung und Haftung fest und machen sie auf Gefahren aufmerksam, was den Zugriff und die Übertragung wichtiger Dateien auf mitarbeitereigenen oder Firmengeräten betrifft. Die Einführung einer einfachen Richtlinie, die die Verteilung unsicherer für Privatanwender konzipierter Applikationen zur Übertragung von Unternehmensdaten — oder das unverschlüsselte Zusenden per E-Mail - verbietet, ist eine einfache aber wesentliche Maßnahme, um Sicherheitsbedrohungen durch die neue Mobilität zu vermeiden. Sichere Lösungen für das mobile Dateimanagement ermöglichen es Unternehmen, ihren mobilen Nutzern den angemessenen Zugriff bereitzustellen. Als zusätzliche Maßnahme empfiehlt es sich für ein Unternehmen, eine Strategie zur Bereitstellung und Verwaltung mobiler Geräte sowie für E-Mail-Sicherheit zu entwickeln und durchzusetzen.

DURCHSETZEN VON RICHTLINIEN FÜR MOBIL ARBEITENDE MITARBEITER

Statement des Journalist Michael Finneran in der Ausgabe der InformationWeek von 7. Mai 2011:

„Ohne gut durchdachte Richtlinien kann man mobile Arbeitskräfte nicht absichern. Und man kann nicht erwarten, dass Menschen sich an Richtlinien halten, die nicht durchgesetzt werden.“ [13]

Fazit

Die Einführung neuer Technologien, zum Nutzen mobiler Mitarbeiter, sind oftmals ein Segen für die Produktivität eines Unternehmens. Damit die Sicherheitsrisiken, die diese Technologien mit sich bringen, nicht kritische Unternehmensdaten gefährden, müssen der IT und den Mitarbeitern Tools zur Verfügung gestellt werden, mit denen diese Sicherheitsprobleme bewältigt werden können, während gleichzeitig der Zugang und die Benutzerfreundlichkeit, die die Mitarbeiter erwarten, gegeben sind.

Tablets und Smartphones werden heute in den verschiedensten Umfeldern eingesetzt - vom Einzelhandel bis hin zum Gesundheitswesen[14] - und der Einsatz wird noch weiter steigen. Es gibt bereits Lösungen, die genau den Bedürfnissen der Mitarbeiter für mobilen Datenzugriff entsprechen und trotzdem die Unternehmensrichtlinien und Kontrolle sicherstellen. Solche Lösungen können leicht in weniger als 10 Minuten auf bestehenden Dateiservern in Unternehmen installiert werden und bieten sofortige Integrationsmöglichkeit der Mobilgeräte, sodass die IT vorhandene Benutzerrichtlinien und Dateiberechtigungen sofort auf das mobile Gerät übertragen kann.[15]

Über Acronis®:

Acronis® ist ein führender Hersteller von Lösungen der nächsten Generation für Datenverfügbarkeit, -zugriff und -sicherheit, mit denen die heutigen komplexen IT-Umgebungen vereinfacht werden. Die Technologie von Acronis ermöglicht Unternehmen jeder Größe, den Anspruch von Anwendern nach Datenzugriff jederzeit und überall zu realisieren. Sie reduziert das Risiko, wertvolle Unternehmensdaten zu verlieren und hilft, Kosten für Verwaltung und Speicherung unter Kontrolle zu halten. Acronis verfügt über bewährte Technologien für Datenmigration und Disaster Recovery für physische, virtuelle sowie Cloud-Umgebungen einerseits und über sichere Lösungen für File-Sharing und Synchronisation andererseits, unabhängig von Typ oder Plattform. Damit ermöglicht Acronis Unternehmen, neue strategische Möglichkeiten der IT wie BYOD und die Einbindung von Macs in Unternehmen zu verwirklichen.

Weitere Informationen stehen unter www.acronis.de zur Verfügung.

Folgen Sie Acronis auf Twitter und Facebook

1. http://www.tmcnet.com/channels/mobile-device-management/articles/215991-employee-use-demands-mobile-device-management.htm
2. http://www.wired.com/threatlevel/2011/05/dropbox-ftc/
3. http://www.eweek.com/c/a/Security/Dealing-With-Enterprise-Mobile-Security-855336/
4. http://www.cnn.com/2011/TECH/mobile/03/28/survey.security.mashable/index.html
5. http://www.webpronews.com/mobile-device-security-threats-at-all-time-high-2011-05
6. http://www.guardian.co.uk/technology/2011/apr/25/wifi-security-flaw-smartphones-risk
7. http://www.grouplogic.com/resource-center/white-papers/enterprise-security-with-mobilecho-form.html
8. http://www.eweek.com/c/a/Security/Android-Most-Targeted-Mobile-Malware-in-Q2-2011-McAfee-128399/
9. http://www.geek.com/articles/mobile/ios-has-10x-more-security-holes-than-android-but-its-still-safer-says-symantec-20110628/
10. http://www.tgdaily.com/security-brief/57684-mobile-malware-explodes-in-first-half-of-2011
11. http://www.networkworld.com/news/2011/052311-grouplogic-mobilecho.html
12. http://www.thesecurityblog.com/2011/06/how-businesses-and-users-can-improve-mobile-security/
13. http://www.informationweek.com/news/mobility/business/229402924
14. http://www.smartgorillas.com/?p=5507
15. http://www.grouplogic.com/enterprise-file-sharing/ipad-file-system/

Für weitere Informationen besuchen Sie http://www.acronis.de

Acronis Germany GmbH
Landsberger Str. 110, 80339 München
Tel. +49 89 613 72 84-0
Fax +49 89 613 72 84-99
info-de@acronis.com
http://www.acronis.de

Händlerstempel