IBM Global Technology Services (GTS)
Thought Leadership White Paper

Januar 2012

Sicherheit mobiler Endgeräte von Endbenutzern im Unternehmen

Mit durchsetzbaren Richtlinien für die mobile Sicherheit und Best Practices den Schutz von Unternehmensdaten verbessern

IBM

Kurzübersicht

Mit mobilen Endgeräten, einschließlich Smartphones und Tablets, können immer mehr Mitarbeiter „jederzeit und überall“ arbeiten. Die Sicherheit von Unternehmensdaten stellt insbesondere bei mobilen Endgeräten, die leicht verloren gehen oder gestohlen werden können, ein Problem dar. Das Sicherheitsrisiko wird durch die immer stärkere Nutzung mobiler Endgeräte von Mitarbeitern in vielen Unternehmen noch weiter verschärft. Erfahrungsgemäß gehen Mitarbeiter bei der Nutzung mobiler Endgeräte für geschäftliche Zwecke gerne den Weg des geringsten Widerstands, was zu Sicherheitsproblemen führen kann. Klar dokumentierte und durchsetzbare Richtlinien für die mobile Sicherheit sind unumgänglich, wenn das Risiko eines Datenverlusts reduziert werden soll.

In diesem White Paper werden die Sicherheitsrisiken beim Einsatz mobiler Endgeräte, mit denen auf Unternehmensdaten zugegriffen wird, beschrieben. Ferner werden Konzepte für die Risikominderung vorgestellt, die unter anderem Authentifizierung, Datenverschlüsselung, Schutz vor Malware und Viren sowie Netzwerksicherheit umfassen.

Management verschiedener Endgeräte und Plattformen

Früher haben Unternehmen Mobilitätslösungen häufig auf einer einzigen mobilen Plattform standardisiert, beispielsweise auf BlackBerry-Smartphones, die aus Kostengründen nur einer bestimmten Anzahl Mitarbeitern bereitgestellt wurden. Heute haben immer mehr Mitarbeiter ein eigenes mobiles Endgerät und möchten dieses auch für geschäftliche Zwecke nutzen. Da die Endgeräte, die Mitarbeiter für ihre Arbeit nutzen, so unterschiedlich sind, steht die IT-Organisation vor großen Herausforderungen und die Unternehmensdaten sind einem Sicherheitsrisiko ausgesetzt. Viele mobile Endgeräte und Plattformen sind nur für den privaten Gebrauch konzipiert und lassen folglich Sicherheitsstandards für den Umgang mit Unternehmensdaten vermissen. Beim Thema mobile Sicherheit sind folgende Aspekte zu berücksichtigen:

- Zugriffskontrolle, ggf. einschließlich Kenncodesperren
- Datenschutz, z. B. Verschlüsselung
- Schutz vor Malware

Zugriffskontrolle

Mobile Endgeräte können verloren gehen oder gestohlen werden. Wenn eine Authentifizierung z. B. mit Kenncodesperre erforderlich ist, können unbefugte Benutzer nicht so einfach auf das Gerät zugreifen. Leider erschweren die meisten Konzepte die Bedienung für den Besitzer des Geräts und führen so schnell zu Unzufriedenheit, insbesondere wenn es sich um das eigene Gerät handelt. Derzeit gibt es nur wenige leistungsfähige Lösungen, um den Zugriff auf private und geschäftliche Daten ausreichend voneinander zu trennen, auch wenn dies wahrscheinlich ein Schwerpunktbereich für einige Anbieter ist.

Neben numerischen und alphanumerischen Kennwörtern als Standardlösung gibt es weitere Sicherheitsoptionen wie z. B. Biometrie (Fingerabdruck- oder Spracherkennung), Smart Cards, Token oder digitale Zertifikate. Für eine Mehrfaktorauthentifizierung können sogar zwei oder mehr dieser Optionen erforderlich sein.

Vermeidung des Verlusts von Unternehmensdaten

In seiner sechsten jährlichen Studie stellte das Ponemon Institute fest, dass die Kosten für Unternehmen im Falle einer Datenschutzverletzung auf durchschnittlich 7,2 Millionen US-Dollar angestiegen sind. Im Durchschnitt beliefen sich die Kosten eines Unternehmens auf 214 US-Dollar pro betroffenem Datensatz – ein deutlicher Anstieg gegenüber den 204 US-Dollar noch im Jahr 2009.[1] Die Studie basiert auf den tatsächlichen Erfahrungen mit Datenschutzverletzungen bei 51 US-amerikanischen Unternehmen aus 15 verschiedenen Branchen. Wenn man das auf Unternehmen weltweit hochrechnet, sind die jährlichen Kosten durch verlorene oder gestohlene Daten enorm und werden vermutlich noch weiter steigen, da mobile Endgeräte immer kleiner werden und deshalb auch eher einmal im Taxi oder Restaurant vergessen werden.

Hinzu kommen noch die vorsätzlichen Angriffe. Im Rahmen der Studie des Ponemon Institute wurden böswillige Angriffe als Hauptursache von 31 % aller in der Studie berücksichtigten Datenschutzverletzungen identifiziert, gegenüber 24 % im Jahr 2009 und 12 % im Jahr 2008.[2] Das „Bereinigen“ oder Löschen aller Daten vom mobilen Endgerät nach einer bestimmten Anzahl an Anmeldeversuchen mit ungültigem Kennwort kann dazu beitragen, das Risiko eines physischen Angriffs zu reduzieren. Wenn ein Endgerät verloren geht oder gestohlen wird, sollten vom jeweiligen Endbenutzer oder dem Administrator die Daten auf dem mobilen Endgerät über Fernzugriff gelöscht werden.

Durch die Verschlüsselung von Daten auf mobilen Endgeräten kann ein höheres Sicherheitsniveau erreicht werden. Dabei bietet die hardwarebasierte Verschlüsselung, eine der am häufigsten eingesetzten Methoden, Vorteile gegenüber der Softwareverschlüsselung, da die Funktionalität in das Endgerät integriert ist und damit die Leistung verbessert werden kann.

Browser und virtualisierte Anwendungen können eine Alternative zur Datenspeicherung auf mobilen Endgeräten bieten. In diesem Fall werden sehr wenige oder keine Daten auf dem Endgerät gespeichert. Stattdessen werden die Daten bei Bedarf abgerufen und angezeigt, wodurch das Risiko eines Datenverlusts sinkt. Allerdings ist dafür Netzwerkzugriff erforderlich, d. h., Benutzer können weder offline noch ohne Netzwerkverbindung auf Daten zugreifen. Darüber hinaus kann die Leistung geringer sein als bei einem nativen Rich Client, der auf lokale Daten auf dem mobilen Endgerät zugreift. Außerdem kann es für die Endbenutzer zu längeren Antwortzeiten kommen.

Bekämpfung neuer Viren

Die Bedrohung für PCs durch Malware gehört schon zum Alltag. Im Bereich der mobilen Endgeräte ist dieses Problem noch weniger verbreitet, nimmt aber mit steigender Beliebtheit dieser Geräte zu. Benutzer können ihre Endgeräte durch einen Besuch auf einer infizierten Website, Erhalt einer SMS oder Installation einer Anwendung unwissentlich infizieren. Selbst Anwendungen aus „vorab genehmigten" Online-Stores (wie Apple App Store oder Google Marketplace) können infiziert sein. Für die Inhaber der Stores für Anwendungen ist es praktisch unmöglich, bei allen Anwendungen umfassende Codeüberprüfungen durchzuführen. Bei der Bekämpfung dieser Risiken kommt Sicherheitssoftware, die mit den derzeit für PCs verfügbaren Lösungen vergleichbar ist, immer mehr zum Einsatz. Die Software wird auf dem mobilen Endgerät ausgeführt, sucht dort nach Malware und Viren und wird regelmäßig aktualisiert, wenn neue Sicherheitsrisiken bekannt werden.

Festlegung von Sicherheitsrichtlinien

Es ist extrem schwierig zu verhindern, dass Mitarbeiter ihre eigenen mobilen Endgeräte für Geschäftszwecke nutzen. IT-Experten können diesem Trend zuvorkommen, indem sie Richtlinien und Verfahren festlegen, in denen bestimmt wird, auf welche Inhalte von diesen Endgeräten aus zugegriffen werden kann, wie der Zugriff erfolgt und wie das Unternehmen bei einem Verlust oder Diebstahl eines Endgeräts verfährt, auf dem sich geschäftliche Informationen befinden. Auf diese Weise können die Mitarbeiter nach wie vor unterwegs, zuhause oder an einem Kundenstandort produktiv arbeiten und das Unternehmen reduziert das Risiko, dass Unbefugte Zugriff auf die Daten erhalten. Nachstehend ist ein Beispiel für Sicherheitsrichtlinien für mobile Endgeräte aufgeführt, die Sie als Ausgangsbasis verwenden können. Es eignet sich für private Endgeräte von Mitarbeitern und für solche, die vom Unternehmen bereitgestellt werden:

- Alphanumerisches Kennwort mit acht Zeichen für das mobile Endgerät
  - Ablauf alle 90 Tage
  - Sperre des Geräts nach 15 Minuten
  - Die Aufforderung zur Kennworteingabe auf dem Endgerät sollte nach jedem nicht erfolgreichen Anmeldeversuch in immer längeren Abständen erfolgen, um Schutz vor Brute-Force-Anmeldeversuchen zu bieten
- Bereinigung des Endgeräts
  - Über Fernzugriff (durch den Administrator), falls das Endgerät verloren geht oder gestohlen wird
  - Nach 10 Anmeldeversuchen mit ungültigem Kennwort, um Schutz vor Brute-Force-Anmeldeversuchen zu bieten
- Verschlüsselung von ruhenden Daten für Mitarbeiter mit Zugriff auf wertvolle oder sensible Daten
  - Mindestens 128-Bit-Verschlüsselung gemäß Advanced Encryption Standard (AES)
  - Schutz für die entsprechenden Verschlüsselungsschlüssel, die so ausgetauscht oder gespeichert werden, dass sie weder im Dateisystem noch bei der Übertragung problemlos in lesbarer Form abgerufen werden können
  - Verfahren zur Wiedergabe des Verschlüsselungsstatus eines bestimmten Endgeräts ausgehend von Nutzen, Anwendung von Richtlinien etc.

- Bluetooth-Konfiguration, die sicherstellt, dass das Gerät für andere unsichtbar ist und nur mit bereits bekannten, d. h. bereits gekoppelten, Endgeräten funktioniert, die diese Features unterstützen
- Regelung, dass Fernzugriff zur Datensynchronisation oder auf die Unternehmensinfrastruktur über ein genehmigtes Gateway für den Fernzugriff erfolgt und die erforderliche Sicherheitsauthentifizierung unterstützt wird
- Lokale Synchronisation unter Verwendung von direkten Universal Serial Bus- (USB), Infrarot-, Bluetooth-, Wireless Local Area Network- (WLAN), Local Area Network- (LAN) oder mobilen Verbindungen
- Virenschutzprogramm auf allen Endgeräten mit Verbindung zum Unternehmensnetzwerk
- Firewallprogramm auf dem mobilen Endgerät

Die Gesamtlösung heißt: Implementierung von Sicherheitsrichtlinien

Nachdem Sie die gewünschten Richtlinien definiert haben, helfen Ihnen Sicherheitslösungen für mobile Endgeräte, diese Richtlinien umzusetzen. Eine Mobile Device Management-Lösung (MDM) ist eine wichtige Voraussetzung dafür. Die bekannten Messaging-Lösungen wie IBM Lotus Domino oder Microsoft® Exchange verfügen zwar über grundlegende Funktionen für das Gerätemanagement, innovative MDM-Lösungen bieten jedoch normalerweise ein umfassenderes Konzept. Dazu zählen unter anderem Self-Service-Funktionen wie Geräteregistrierung, Datenlöschung über Fernzugriff oder Onlinehilfe und das Management mobiler Anwendungen oder die Kostenkontrolle von Sprach- und Datenkommunikation. Darüber hinaus können mit einigen MDM-Lösungen geschäftliche und private Daten voneinander getrennt werden und es ist keine generelle Kennwortsperre für den Zugriff auf das ganze Endgerät nötig, nur für den geschäftlich genutzten Bereich. Sie bieten zudem Funktionen zur Bereinigung von Unternehmensdaten über Fernzugriff, wenn der Mitarbeiter das Unternehmen verlässt. Die persönlichen Daten des Mitarbeiters bleiben dabei erhalten.

Software für die mobile Sicherheit bietet Schutz vor Malware und Viren für mobile Endgeräte. In Kombination mit MDM kann der Sicherheitsstatus des Endgeräts bestimmt werden, bevor eine Verbindung zum Netzwerk hergestellt wird. Falls das Gerät die Sicherheitsprüfung nicht besteht, kann der Benutzer entsprechend benachrichtigt und das Gerät von anderen getrennt werden, um die Risiken für das Unternehmensnetzwerk zu reduzieren.

Für weitere Informationen

Wenn Sie mehr über IBM Enterprise Services – Managed Mobility Services erfahren möchten, wenden Sie sich bitte an Ihren IBM Vertriebsbeauftragten oder IBM Business Partner oder besuchen Sie die folgende Website: **ibm.com**/services/mobility

Finanzierungslösungen von IBM Global Financing ermöglichen ein effektives Cash-Management, sorgen dafür, dass Sie technologisch immer auf dem neuesten Stand sind, optimieren die Gesamtbetriebskosten und verbessern den Return on Investment (ROI). Mit unseren Global Asset Recovery Services können Sie durch neue Lösungen mit mehr Energieeffizienz einen Beitrag zum Schutz unserer Umwelt leisten. Weitere Informationen zu IBM Global Financing finden Sie unter: **ibm.com**/financing

IBM leistet keine rechtliche Beratung oder Beratung bei Fragen der Buchführung und Rechnungsprüfung. IBM gewährleistet und garantiert nicht, dass seine Produkte oder sonstigen Leistungen die Einhaltung bestimmter Rechtsvorschriften sicherstellen. Der Kunde ist für die Einhaltung anwendbarer Sicherheitsvorschriften und sonstiger Vorschriften des nationalen und internationalen Rechts verantwortlich.

[1] „2010 Annual Study: U.S. Cost of a Data Breach“, Ponemon Institute, LLC, März 2011.

[2] „2010 Annual Study: U.S. Cost of a Data Breach“, Ponemon Institute, LLC, März 2011.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustrasse 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter: **ibm.com**

IBM, das IBM Logo, ibm.com und Lotus Domino sind Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein.

Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter **ibm.com**/legal/copytrade.shtml

Microsoft ist eine Marke der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein.

Vertragsbedingungen und Preise erhalten Sie bei den IBM Geschäftsstellen und/oder den IBM Business Partnern.

Die Produktinformationen geben den derzeitigen Stand wieder. Gegenstand und Umfang der Leistungen bestimmen sich ausschließlich nach den jeweiligen Verträgen.

Diese Veröffentlichung dient nur der allgemeinen Information. Die in dieser Veröffentlichung enthaltenen Informationen können jederzeit ohne vorherige Ankündigung geändert werden. Aktuelle Informationen zu IBM Produkten und Services erhalten Sie bei der zuständigen IBM Verkaufsstelle oder dem zuständigen Reseller.

Diese Veröffentlichung enthält Internetadressen von anderen Unternehmen als IBM. IBM übernimmt keinerlei Verantwortung für die auf diesen Websites enthaltenen Informationen.

Bei abgebildeten Geräten kann es sich um Entwicklungsmodelle handeln.

© Copyright IBM Corporation 2012

Bitte der Wiederverwertung zuführen

AZW03001-DEDE-02