Beispielrichtlinie zur mobilen Sicherheit

Anwenden der Richtlinie

Die Absicherung privat und zu Unternehmenszwecken genutzter Mobilgeräte, wie etwa Smartphones oder Tablets, stellt für IT-Abteilungen eine echte Herausforderung dar. Die Beispiel-Richtlinie kann Unternehmen als Leitfaden bei der Implementierung bzw. Aktualisierung ihrer Sicherheitsrichtlinie für Mobilgeräte dienen.

Sie können die Richtlinie ganz nach Ihren Wünschen an die Anforderungen im Unternehmen anpassen. Es handelt sich bei dem Beispiel nicht um eine umfassende Richtlinie, sondern vielmehr um eine Basisvorlage, die Sie beliebig erweitern können.

Hintergrundinformationen

Ein zentrales Problem besteht darin, dass User Mobilgeräte nicht als Bedrohung der Computer- und Datensicherheit wahrnehmen. So lassen sie beim Einsatz von Mobilgeräten häufig nicht die gleiche Vorsicht walten, wie beim Einsatz anderer Geräte, wie etwa Desktops.

Problematisch ist ferner die Tatsache, dass User beim Verwenden ihrer eigenen Geräte oft auf ihre eigenen Rechte pochen und Datenschutzbestimmungen im Unternehmen missachten.

Die Richtlinie ermöglicht Unternehmen, Mobilgeräte zu überwachen, und sollte in die vorhandenen Richtlinien im Unternehmen zum Schutz von Daten und der Nutzung von Computern eingegliedert werden.

Beispielrichtlinie

1. Einleitung

Mobilgeräte, wie etwa Smartphones und Tablets, spielen mitunter eine wichtige Rolle bei der Erreichung von Unternehmenszielen.

Sie bergen jedoch auch beträchtliche Sicherheitsrisiken: Werden keine hinreichenden Vorsichtsmaßnahmen getroffen, können sich Unbefugte über Mobilgeräte unter Umständen Zugriff auf die IT-Infrastruktur Ihres Unternehmens verschaffen. Datenverluste und Systeminfektionen sind häufig die Folge.

<Unternehmen X> möchte Informationen schützen, Kunden absichern und sein geistiges Eigentum und seinen Ruf bewahren. In diesem Dokument finden Sie Praxistipps sowie die Voraussetzungen für den sicheren Umgang mit Mobilgeräten.

2. Wirkungsbereich

1. Alle Mobilgeräte (im Besitz von <Unternehmen X> oder der Mitarbeiter), die auf Unternehmensnetzwerke, -daten und -systeme zugreifen können. Von der IT-Abteilung verwaltete Laptops im Unternehmen sind hiervon ausgenommen. Zu solchen Geräten zählen auch Smartphones und Tablets.

2. Ausnahmen: Wenn eine Unternehmensanforderung von dieser Richtlinie ausgenommen werden soll (zu teuer, zu komplex, beeinflusst andere Unternehmensanforderungen negativ), muss eine durch das Sicherheitsmanagement autorisierte Risikobewertung vorgenommen werden.

3. Richtlinien

3.1 Technische Anforderungen

1. Die Geräte müssen unter folgenden Betriebssystemen laufen: Android 2.2 oder höher, IOS 4.x oder höher. <Sie können die Betriebssysteme an Ihre Wünsche anpassen>.
2. Benutzerkennwörter zu den Geräten dürfen nur in verschlüsselten Kennwortspeichern aufbewahrt werden.
3. User müssen ein sicheres Kennwort für die Geräte konfigurieren, das den Anforderungen der Kennwortrichtlinie von <Unternehmen X> genügt. Das Kennwort darf nicht für andere Anwendungen im Unternehmen verwendet werden.
4. Nur Geräte, die von der IT-Abteilung verwaltet werden, dürfen direkt mit dem Unternehmensnetzwerk verbunden werden.

3.2 Pflichten der User

1. User dürfen nur unternehmensrelevante Daten auf die Mobilgeräte laden.
2. Abhanden gekommene oder gestohlene Geräte müssen der IT-Abteilung von <Unternehmen X> umgehend gemeldet werden.
3. Vermutet ein User, dass ein unbefugter Zugriff über Mobilgeräte auf Unternehmensdaten erfolgt ist, muss er dies der IT-Abteilung in Einklang mit Melderichtlinien in <Unternehmen X> mitteilen.
4. Der Einsatz von Geräten mit Jailbreak oder Software/Firmware zum Zugriff auf eigentlich nicht für den User vorgesehene Funktionen ist nicht gestattet.
5. User dürfen keine Raubkopien oder illegalen Inhalte auf die Geräte laden.
6. Sämtliche installierten Anwendungen müssen offiziellen, vom Entwickler des jeweiligen Betriebssystems autorisierten Quellen entstammen. Es darf kein Code von fragwürdigen Quellen installiert werden. Die IT-Abteilung von <Unternehmen X> kann Ihnen im Zweifel mitteilen, ob eine Anwendung vertrauenswürdig ist.
7. Die Geräte sind mit den aktuellen Patches des Herstellers oder Netzwerks auszustatten. Sie sollten mindestens einmal pro Woche überprüfen, ob neue Patches vorhanden sind, und mindestens einmal im Monat Patches installieren.
8. Die Geräte dürfen nicht an Computer angeschlossen werden, die nicht über aktuellen, aktivierten Malwareschutz verfügen und gegen Unternehmensrichtlinien verstoßen.
9. Geräte müssen in Einklang mit den Compliance-Standards von <Unternehmen X> verschlüsselt werden.
10. Bei der Verknüpfung von privaten und professionellen E-Mail-Konten ist stets Vorsicht geboten. Unternehmensdaten dürfen nur über die Unternehmens-E-Mail-Adresse versendet werden. Hegt ein User den Verdacht, dass Unternehmensdaten über ein persönliches E-Mail-Konto (im E-Mail-Text oder als Attachment) verschickt wurden, so muss er die IT-Abteilung von <Unternehmen X> umgehend darüber in Kenntnis setzen.
11. (Trifft nicht auf alle Unternehmen zu.) User dürfen keine Geräteinhalte (wie etwa Mediendateien) auf Unternehmenscomputern sichern oder synchronisieren, sofern dies nicht zu Unternehmenszwecken erfolgt.

* Bei einem Jailbreak werden werksseitig installierte Sperren deaktiviert. So kann auf das Betriebssystem zugegriffen werden: Der gesamte Funktionsumfang wird freigeschaltet und nicht zulässige Software kann installiert werden.