



■ Sicherheit von PDA und Smartphone Informationsbroschüre für Entscheider

Erstellt von der Projektgruppe „Mobile Security“
des Kompetenzbereiches Sicherheit

Stand: Februar 2007

1. Einleitung

Mobile Endgeräte lassen sich aus dem heutigen Berufsleben nicht mehr wegdenken. PDAs (Personal Digital Assistant) und Smartphones (PDA mit Mobilfunktion) werden je nach Leistungsumfang zum Telefonieren, für die Verwaltung von Adressen und Terminen, für Standard-Office-Anwendungen, zur Kommunikation über E-Mail als auch für sicherheitskritische Applikationen (Zugang zum Firmennetz, Buchhaltung, Kundendatenbanken) benutzt.

Durch die Vielzahl von Nutzungsmöglichkeiten dieser Geräte und die immer stärkere „Ersetzung“ von Notebooks im mobilen Bereich erhöht sich auch das Sicherheitsrisiko für das Unternehmen: Große Mengen vertraulicher Daten (E-Mails, Zugangsdaten, Kundendaten, Buchhaltungsdaten usw.) werden aus dem Unternehmensnetz kopiert und unterwegs bearbeitet. Die Geräte sind bei ihrem Einsatz nicht automatisch in die Firmen-IT-Infrastruktur eingebunden. Daher profitieren sie nicht immer von einer sicheren zentralen Authentisierung und Autorisierung. Im Unternehmensnetzwerk vorhandene Sicherheitsmechanismen wie z. B. eine Firewall greifen nicht mehr. Vielmehr ist das Gerät bei der Gewährung von Zugriffsrechten auf sich gestellt.

Sowohl die Mitarbeiter, die die mobilen Geräte nutzen, als auch das IT-Sicherheitsteam im Unternehmen müssen sich daher bei der Anschaffung, dem Betrieb als auch bei der Entsorgung mit den Sicherheitsrisiken auseinandersetzen und entsprechende Maßnahmen ergreifen.

Mangelhafte Schutzmaßnahmen können einschneidende Konsequenzen für den wirtschaftlichen Fortbestand von Unternehmungen haben. Im Einzelfall führen sie sogar zur persönlichen Haftung der Unternehmensleitung.

Die vorliegende Broschüre richtet sich an Entscheider, die Beschaffung, Nutzung, Administration und den Betrieb von PDAs und Smartphones verantworten. Sie gibt einen schnellen Überblick über notwendige Maßnahmen, um das Sicherheitsrisiko auf ein beherrschbares Maß zu reduzieren.

2. Beschaffung und Einführung

Schreiben Sie schon während des Beschaffungs- und Einführungsprozess der Geräte das Thema Sicherheit groß. Grundsätzlich haben Sie die Möglichkeit bestimmte Gerätetypen kontrolliert einzuführen oder/und auch Privatgeräte für den Einsatz im Unternehmen zu zulassen. Unabhängig davon, für welches Modell Sie sich entscheiden, bedenken Sie, dass Mitarbeiter „ihren“ PDA bzw. Smartphone viel stärker noch als den PC als persönliches Arbeitsmittel ansehen. Damit öffnen diese Geräte eine empfindliche Lücke in ihre IT-Infrastruktur.

Security Checkliste

- Erstellen Sie einen Anforderungskatalog, der mindestens folgende Themen beleuchtet: Sicherheitsmechanismen, Bedienkomfort, Schnittstellen, Hardware- und Software-Anforderungen, zentrales Management, Authentifizierungsmöglichkeiten und Kosten.
- Beschränken Sie sich grundsätzlich auf wenige Gerätetypen, um Sicherheitsmechanismen zu vereinfachen.
- PDAs und Smartphones werden meist mit einem nur unzureichenden Set an Sicherheitsfunktionen ausgeliefert. Diese Bordmittel reichen häufig nicht aus, um Ihre Geräte gut genug zu schützen. Ergänzende Sicherheitsanwendungen sind am Markt verfügbar. Sie sollten aber mit Ihrer IT-Infrastruktur kompatibel sein.
- Definieren und implementieren Sie verbindliche Richtlinien für die sichere Verwendung der Geräte. Achten Sie darauf, dass die Geschäftsführung das Sicherheitskonzept unterstützt.
- Führen Sie für Ihre Geräte möglichst eine zentrale Administration ein.
- Achten Sie auf einen leistungsfähigen Konfigurationsschutz aller mobilen Endgeräte.
- Prüfen Sie, ob Ihr bestehender Versicherungsschutz auch den Verlust und/oder Missbrauch dieser Geräte abdeckt.

3. Betrieb

Die folgende Checkliste gibt Empfehlungen für generelle Sicherheitsmaßnahmen (I) sowie für den Umgang mit wichtigen Bedrohungsszenarien. (II-V).

Security Checkliste

I. Generelle Sicherheitsmaßnahmen

- Sensibilisieren Sie alle Geräthenutzer regelmäßig für den sicheren Umgang mit PDAs und Smartphones.
- Konfigurieren Sie wichtige Sicherheitsfunktionen (Zugriffsschutz, automatische Sperre, Verschlüsselung, Internetbrowser) vor und dokumentieren Sie diese verständlich für die Benutzer.
- Etablieren Sie frühzeitig verbindliche Richtlinien zur sicheren Nutzung und Speicherung von Daten und Programmen.
- Verwenden Sie eine Mindestlänge von 8 Zeichen für Passworte und nutzen Sie Groß- und Kleinschreibung sowie Sonderzeichen.
- Schützen Sie grundsätzlich auch zusätzliche Speicherkarten mit einem Passwort.
- Binden Sie das Gerät über ein Virtual Private Network (VPN) in das Authentifizierungssystem Ihres Unternehmens ein.
- Bietet das Gerät werksseitig keine Verschlüsselungsfunktion, so sollte dringend ein Verschlüsselungsprodukt eingesetzt werden.
- Legen Sie ein Bestandsverzeichnis aller Geräte an und dokumentieren Sie beispielsweise die Benutzer-ID, die Gerätenummer, sowie Besonderheiten der Gerätekonfiguration.
- Aktualisieren Sie regelmäßig das Betriebssystem und Sicherheitsanwendungen mit den neuesten Updates.

II. Geräteverlust und unautorisierte Zugriff auf das Gerät

Vorbeugende Maßnahmen

- Sorgen Sie für die automatische Verschlüsselung aller Speichermedien des Geräts.
- Bringen Sie einen Hinweis an, aus dem hervorgeht, an wen sich ein ehrlicher Finder wenden kann. Nutzen Sie hierfür gegebenenfalls eine neutrale Adresse.

Rückwirkende Maßnahmen

- Nutzen Sie automatische Löschemechanismen, die notfalls bei Verlust aktiviert werden können.
- Sperren Sie verlorene und/oder entwendete Geräte per Fernzugriff.

III. Datenverlust

Vorbeugende Maßnahmen

- Stellen Sie Softwarelösungen bereit, die dem Nutzer helfen regelmäßig Sicherungskopien in einer sicheren Unternehmensumgebung zu erstellen.
- Nutzen Sie abgesicherte, möglichst verschlüsselte Synchronisationsmechanismen zwischen mobilen und stationären Geräten.

Rückwirkende Maßnahmen

- Nutzen Sie Data-Recovery Leistungen des Geräteherstellers oder eines dafür spezialisierten Dienstleisters.

IV. Defekte Geräte

Vorbeugende Maßnahmen

- (siehe vorbeugende Maßnahmen unter Punkt III)

Rückwirkende Maßnahmen

- Denken Sie daran, vor dem Einschicken defekter Geräte zum Hersteller alle Daten - sofern möglich - zu sichern und zu löschen bzw. zu verschlüsseln.

V. Missbrauch bei der Datenübertragung und Angriff auf die Funkschnittstelle

Vorbeugende Maßnahmen

- Aktivieren Sie Funkschnittstellen wie zum Beispiel Bluetooth und Infrarot nur bei Bedarf.
- Ermöglichen Sie Zugriffe auf das Unternehmensnetzwerk ausschließlich über ein VPN.
- Nutzen Sie stets aktuelle Virensoftware und Firewall.

Rückwirkende Maßnahmen

- Ändern Sie umgehend alle kompromittierten und bedrohten Passworte.
- Führen Sie eine umfassende Sicherheitsüberprüfung der attackierten Geräte durch.

VI. Unautorisierter Zugriff auf das Unternehmensnetzwerk

Vorbeugende Maßnahmen

- Verschlüsseln Sie Ihre Informationen auf Datei- oder Verzeichnisebene oder nutzen Sie eine automatische Verschlüsselung des gesamten Speichermediums.
- Legen Sie keine Passwörter oder andere Schlüssel im Klartext auf dem Speichermedium ab und schalten Sie die automatische Speicherung von Passwörtern grundsätzlich aus.
- Nutzen Sie weitere Schutzmechanismen wie Firewalls und Intrusion-Detection-Systeme.

Rückwirkende Maßnahmen

- (siehe rückwirkende Maßnahmen unter Punkt V)

4. Entsorgung

Wie alle Datenträger müssen auch PDAs und Smartphones am Ende ihres Lebenszyklus geregelt entsorgt werden. Besondere Aufmerksamkeit gilt hierbei vor allem dem Umgang mit den Speichermedien.

Security Checkliste

Datenlöschung

- Organisieren Sie die Rücknahme der zu entsorgenden Geräte durch eine zentrale Annahmestelle und führen Sie dort die Datenlöschungen durch.
- Nutzen Sie spezielle Software um Daten unwiederbringlich zu löschen.
- Nutzen Sie z.B. einen Schredder, um Speicherkarten mechanisch zu zerstören.
- Als Alternative zur Zerstörung oder Löschung von Speichermedien bietet sich die vollständige Verschlüsselung aller Daten an.

Entsorgung der Geräte

- Achten Sie darauf, dass Geräte entweder beim Hersteller oder einem autorisierten Dienstleister entsorgt werden.

5. Weiterführende Informationen

IT-Sicherheit allgemein

- Bundesministerium für Sicherheit in der Informationstechnik:
<http://www.bsi.bund.de/gshb/index.htm>
- Kompass der Sicherheitsstandards, BITKOM, DIN, 2006
http://www.bitkom.org/de/publikationen/38337_40496.aspx
- Matrix der Haftungsrisiken, BITKOM, 2005
http://www.bitkom.org/de/publikationen/38337_31034.aspx
- Bundesministerium für Wirtschaft und Technologie:
<http://www.itsmig.de/portal/index.php>

Mobile Datensicherheit

- Mobile Endgeräte und mobile Applikationen:
Sicherheitsgefährdungen und Schutzmaßnahmen, Bundesamt
für Sicherheit in der Informationstechnik 2006
<http://www.bsi.bund.de/literat/doc/mobile/index.htm>

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.000 Unternehmen, davon 800 Direktmitglieder mit etwa 120 Milliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikationsdiensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmenbedingungen, eine Modernisierung des Bildungssystems und eine innovationsorientierte Wirtschaftspolitik ein.

Ihr Ansprechpartner:

Lutz Neugebauer
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 242
Fax: 030/27 576 - 409
l.neugebauer@bitkom.org
www.bitkom.org

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel.: 030/27 576 - 0
Fax: 030/27 576 - 400

bitkom@bitkom.org
www.bitkom.org