

## Deutsche Anwalt- und Notar-Versicherung

### Presseartikel

## Neue Herausforderungen für die IT-Sicherheit

**MOBIL = RISKANT?**

NEUE HERAUSFORDERUNGEN FÜR DIE IT-SICHERHEIT



Unternehmen rüsten ihre Mitarbeiter zunehmend mit mobilen Kommunikationsgeräten aus. Damit ist es möglich, Dienste über drahtlose Netzwerke oder lokal verfügbare mobile Anwendungen zu nutzen. Auf der anderen Seite sind mobile Endgeräte allerdings auch einer Vielzahl von Gefahren ausgesetzt. Diese reichen vom Verlust oder Diebstahl des Endgerätes bzw. der auf dem Endgerät gespeicherten Informationen, über Manipulationen bis hin zur Bedrohung der Vertraulichkeit und Verfügbarkeit der Kommunikationskanäle. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat deshalb einige grundlegende Empfehlungen zu geeigneten Schutzvorkehrungen für mobile Endgeräte und deren Anwendungen erarbeitet, die wir nachfolgend in Auszügen dokumentieren:

### Prozess der Absicherung

Die Absicherung mobiler Endgeräte kann nur durch die Kombination verschiedener Sicherungsmaßnahmen stattfinden. Diese Maßnahmen finden sich im Lebenszyklus des Endgerätes wieder, der wie folgt eingeteilt wird:

#### 1. Auswahl und Beschaffung der mobilen Endgeräte

Bei der Auswahl müssen neben den funktionalen Anforderungen der Benutzer verschiedene Punkte beachtet werden. Das Gerät muss sich in die bestehende Unternehmenspolicy einbinden lassen, ohne dass große Änderungen nötig sind. Die integrierten Sicherheitsmechanismen des Gerätes und der Betriebssoftware müssen bei den geforderten Anwendungen entsprechenden Schutz bieten. Auf die Vertrauenswürdigkeit der Lieferanten und Hersteller ist zu achten. Insbesondere sollte die Herstellungskette vertraut sein, da bei modernen mobilen Endgeräten neben dem Hardwarehersteller auch Provider Software auf das Gerät aufbringen können.

#### 2. Installation

Die Erstinstallation der Geräte erfordert die Kennzeichnung der Geräte, so dass ein wieder gefundenes Gerät möglichst erkannt werden kann. Es ist zu prüfen, welche Anwendungen bereits auf dem Gerät vorinstalliert sind, insbesondere wenn neben dem Hardware- und Betriebssystemhersteller auch Provider Anwendungen installiert haben. Optional muss das Gerät mit zu der Unternehmenspolicy passenden Schutzmechanismen ausgestattet und in eine Verwaltungsinfrastruktur eingebunden werden. Neben der Geräteinstallation müssen auch die Anwender mit der Bedienung und der Funktion der Sicherheitsmechanismen vertraut gemacht werden.

#### 3. Betrieb

Während des Betriebs ist es nötig, die Software der Geräte mit Sicherheitsupdates zu versorgen. Dazu zählen sowohl die Firmware der Geräte als auch das Betriebssystem mit seinen Treibern und alle Anwendungen. Das dafür zuständige Gerätemanagement muss außerdem melden, wenn nicht vertrauenswürdige Software auf einem mobilen Endgerät installiert worden ist. Weiterhin sollte der Anwender den Verlust seines mobilen Endgerätes melden, auch wenn er das Gerät kurze Zeit später wieder gefunden hat. Anschließend muss die Integrität des Gerätes von vertrauenswürdiger Stelle sichergestellt werden.

#### 4. Außer Betrieb setzen

Nach dem Einsatz eines mobilen Endgerätes muss sichergestellt sein, dass die darauf gespeicherten Daten gelöscht bzw. unbrauchbar gemacht werden. Zudem muss sichergestellt werden, dass das Gerät anschließend keine geschützten Unternehmensressourcen mehr nutzen kann.

Zusätzlich ist es ratsam, Bedrohungs- und Risikoanalysen und Penetrationstests durchzuführen, um konkrete Schwachstellen der Infrastruktur und der eingesetzten Geräte zu finden. Jede Art der Absicherung kann in eine der folgenden drei Phasen eingeteilt werden:

### **1. Präventiver Schutz**

Darunter fallen alle Maßnahmen, die im Vorhinein ohne konkreten Angriff zur Erhöhung der Sicherheit eingeführt werden. Dazu zählen z. B. Schulung der Mitarbeiter, eine Unternehmenspolicy, Installation von Verschlüsselungssoftware, etc.

### **2. Angriffserkennung**

Maßnahmen, die einen stattfindenden Angriff bemerken und melden, wirken als erkennende Maßnahmen. Dazu zählen das Gerätemanagement zur Meldung von Schwachstellen und versuchten Angriffen, die Anzeige verloren gegangener Geräte oder die Analyse von Logfiles.

### **3. Wiederherstellung und Reparatur eines kompromittierten Systems**

Nach erfolgtem Angriff eines Gerätes müssen ebenfalls Maßnahmen eingeleitet werden. Diese meist organisatorischen Maßnahmen stellen die Wirkung des Angriffs und erfolgte Schäden fest und beseitigen diese. Technische Maßnahmen zur Reaktion werden heute nur vereinzelt eingesetzt.

Redaktionsschluss: 09.02.2007

Wir danken AOK Business

(Stand 11/2007)