Mobile Security

Risiken erkennen, Massnahmen ableiten

Foto: Kigoo-Images @ pixelio.de

Mobile Endgeräte sind aus dem heutigen Berufsleben nicht mehr wegzudenken. Vor allem Smartphones und Tablet PCs sind zu unverzichtbaren Arbeitsmitteln geworden. Das Telefonieren ist nicht mehr Hauptsache, sondern das Verwalten von Adressen und Terminen, Standard-Office-Anwendungen, Kommunikation über Email bis hin zu sicherheitskritischen Applikationen, beispielsweise für den Zugang zum Firmennetzwerk, Speicherung von Passwörtern, (Kunden-)Datenbanken, gehören zum Leistungsumfang aktueller Geräte.

Autor: Andreas Wisler

Durch diese vielen Nutzungsmöglichkeiten verdrängen diese Geräte vermehrt Notebooks in den mobilen Bereichen. Damit erhöht sich aber auch das Sicherheitsrisiko für das Unternehmen. So werden grosse Mengen an teilweise vertraulichen Daten aus dem Firmennetzwerk kopiert und unterwegs bearbeitet. Diese Geräte sind aber in der Regel nicht automatisch in die Firmen-IT-Infrastruktur eingebunden und können so nicht zentral verwaltet werden. Daher ist es wichtig, dass dem Schutz des mobilen Gerätes Rechnung getragen wird. Es ist essentiell, dass sich die Benutzer, aber auch das IT-Sicherheitsteam im Unternehmen bei der Anschaffung, dem Betrieb, wie aber auch bei der Entsorgung mit den Risiken und möglichen Massnahmen auseinandersetzen. Mangelhafte Schutzmassnahmen können im Falle eines Verlustes einschneidende Konsequenzen nach sich ziehen.

Bedürfnisse können

Bei der Beschaffung ist es wichtig, einen Anforderungskatalog zu erstellen, der die Sicherheitsmechanismen, den Bedienkomfort, die vorhandenen Schnittstellen, die Handhabung der zentralen Administration sowie Authentifizierungsmöglichkeiten beinhaltet. Aus administrativen Gründen empfiehlt es sich, nur auf einen Gerätetypen zu setzen. Da nicht alles mit technischen Möglichkeiten gelöst werden kann, gehören verbindliche Richtlinien an die Benutzung der mobilen Geräte dazu.

Die potentiellen Gefährdungen lassen sich darin unterscheiden, ob der Angreifer im Besitz des Gerätes ist oder nicht. Hat er das Gerät in Besitz, kann er die enthaltenen Daten entwenden oder die Software manipulieren. So ist es auch denkbar, dass der Angreifer das Gerät unbemerkt entwendet, die Software manipuliert und dem Besitzer wieder unterschiebt. So bleibt der Angriff unbemerkt, da nur wenige Minuten genügen, die Manipulationen vorzunehmen. Ist der Angreifer nicht im Besitz des mobilen Gerätes, so kann er die Kommunikationswege nutzen, um das Gerät zu stören oder gar zu kompromittieren. Es werden aktive Angriffe und passive unterschieden. Aktive beeinflussen den Datenverkehr direkt. Passive hingegen werden durch Abhören und Beobachtung der Kommunikationskanäle durchgeführt und sind daher nur sehr schwer zu entdecken.

Beim Betrieb der mobilen Geräte gilt es die vorhandenen Sicherheitsfunktionen

Zum Autor

Andreas Wisler (Tel.: 052 320 91 20), Dipl. Ing. FH, CISSP, ISO 27001 Lead Auditor, ist Geschäftsführer der GO OUT Production GmbH, welche sich mit ganzheitlichen und produktneutralen IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Regelmässig veröffentlicht er einen informativen Newsletter zu aktuellen Sicherheitsthemen, der kostenlos und unverbindlich auf www.gosecurity.ch (Infonews) heruntergeladen werden kann. Im Rahmen des Swiss Security Days ist er für die Schulungen an der Klubschule Winterthur zuständig.

zu nutzen und wo immer möglich zentral vorzugeben (etwa via Exchange Server). Dazu gehören der Zugriffsschutz durch ein Passwort, das automatische Sperren nach einer bestimmten Inaktivitätszeit, die Verschlüsselung des Datenspeichers und Sicherheitsvorgaben an den Internetbrowser. Auch bei diesen Geräten gelten die Mindestanforderungen von acht bis zehn Zeichen an das Passwort. Kennt das Gerät keine Verschlüsselung, sollte ein passendes Verschlüsselungsprodukt evaluiert werden. Mindestens die Daten müssen vor fremden Zugriff geschützt werden. Weiter gilt es, wie bereits bei Servern und PCs bekannt, das Betriebssystem und die installierten Applikationen regelmässig zu aktualisieren. Dazu müssen die mobilen Geräte im vorhandenen Patch-Konzept berücksichtigt werden. Nicht vergessen werden darf die Kommunikation zur eigenen Firma. Diese muss immer über einen verschlüsselten Weg erfolgen, etwa HTTPS oder VPN. Alle nicht benötigten Schnittstellen sind zu deaktivieren, idealerweise wiederum zentral vorgegeben. Dazu gehören unter anderem Bluetooth und Infrarot.

Schutz nach Zwischenfall

Besteht der Verdacht auf eine Manipulation des Geräts, sollten umgehend alle Passwörter und Zugänge geändert oder gesperrt werden. Je nach Schweregrad sollte eine umfassende Sicherheitsüberprüfung des attackierten Gerätes durchgeführt werden. Vor der Wiederinbetriebnahme müssen alle Daten gelöscht werden (Betriebssystem neu aufspielen und das Gerät in den Auslieferungszustand bringen).

Früher oder später wird jedes Gerät ersetzt. Daher ist es wichtig, bereits im Vorfeld auf das Ende des Lebenszyklus vorbereitet zu sein. Besonderes Augenmerk gilt hierbei der Löschung der Daten. Diese sollten unwiederbringlich zerstört werden.
Wird die Daten-Sicherheit durchgängig berücksichtigt, ist bei der Beschaffung, dem Betrieb und bei der Entsorgung immer sichergestellt, dass die Daten vor fremden Zugriff geschützt sind. ◆

IT-Security Forum #9

Am 4. November 2011 fand in Winterthur das IT-Security Forum #9 statt. Fünf Fachbeiträge zur technischen und organisatorischen IT-Sicherheit zeigten ein aktuelles Bild auf. Auch die mobile Sicherheit beschäftige die Referenten in zwei Beiträgen: «wird die mobile Security in Unternehmen vernachlässigt?» sowie «von der Device fokussierten hin zur Information fokussierten Sicherheit». Weitere Informationen und die Anmeldung sind unter www.itsecurityforum.ch abrufbar.