Lagebild zur Bedrohung
der Unternehmenssicherheit durch Smartphones & Co.

Mit Sicherheit mobil

Die Verbreitung von mobilen Geräten und die Nutzung des Mobilfunknetzes als Internetzugang schreiten sehr schnell voran. Laut Gartner werden 2013 mehr als die Hälfte der Internetnutzer auch mit mobilen Geräten über Mobilfunknetze ins Internet gehen. Um auf die technischen Fortschritte von Smartphones und Tablet-PCs zu reagieren, ist es zwingend notwendig, die einst für Laptops definierten Sicherheitsrichtlinien anzupassen und gegebenenfalls neue zu erstellen. Folgender Beitrag beschreibt, welche Gefahren aktuell von Smartphones und Tablet-PCs ausgehen, welche Lösungsansätze die Basis für ein hohes Sicherheitsniveau bilden und welche Probleme es bei der Realisierung gibt.

Das Jahr neigt sich dem Ende entgegen und neben Cloud Computing war es vor allem der Bereich Mobile Security, der in der IT-Sicherheitsbranche viel diskutiert wurde. Die Vorteile von mobilen Geräten wie zum Beispiel Smartphones und Tablet-PCs sind bestechend. Das Internet mit seinen Diensten ist über die vielfältigen Kommunikationsschnittstellen (WLAN, UMTS, LTE etc.) stets verfügbar. Sehr leistungsstarke Endgeräte sind fast immer und überall nutzbar sowie einfach und schnell über Touchscreens zu bedienen. Sie vereinen Handy, Computer, Navigationssystem und MP3-Player in einem multifunktionalen, mobilen Gerät.

Die Nutzung mobiler Endgeräte erlaubt es den Unternehmen, vorhandene oder neue Geschäftsprozesse zu optimieren beziehungsweise zu etablieren, und ermöglicht zudem die Realisierung neuer Geschäftsszenarien. Dieser Mehrwert steht aber in direkter Konkurrenz zu den Gefahren, die eine Integration von Tablets und Smartphones in ein Unternehmen mit sich bringt. IT-Verantwortliche müssen wissen, welche Bedrohungen von diesen innovativen Computern im Hosentaschenformat ausgehen und welche Strategien ergriffen werden müssen, um diese Geräte sicher in die Unternehmensinfrastruktur einbinden zu können.

Mobilfunkverbindungen

Verfolgt man die Nachrichten über Angriffe auf Mobilfunkverbindungen, scheint es, dass sämtliche Verbindungsmöglichkeiten potentiell geknackt sind. Haben das Auslesen von Adressbüchern per Bluetooth und das Stehlen von Identitäten in einem manipulierten WLAN gestern noch für Schlagzeilen gesorgt, sind es heute die Möglichkeiten, Gespräche abzuhören und SMS mitzulesen, die für Furore sorgen. Um an die gewünschten Informationen zu kommen, können die Protokolle direkt angegriffen (GSM, Bluetooth) oder beispielsweise die Datenübertragung per UMTS-Standard gestört werden, wodurch ein Rückfall auf veraltete, unsichere Standards (GPRS) erzwungen wird. Musste früher noch Hardware im vierstelligen Eurobereich angeschafft werden, um Mobilfunkgespräche unerlaubt abzuhören, so sind mittlerweile die notwendigen Angriffskomponenten schon für unter 100 Euro zu erwerben und die Software, die benötigt wird, ist Open Source.

Falsche oder manipulierte Hotspots, sogenannte Rouge Access Points, sind zwar nicht mehr im aktuellen Gespräch, werden aber trotzdem noch für das Abgreifen von Daten verwendet. Dabei hat der Angreifer von Anfang an Zugriff auf sämtliche Daten, da die komplette Kommunikation über sein Netzwerk läuft. Je nach verwendeter Technik kann er sogar die Verbindung mit dem manipulierten Netzwerk erzwingen. Selbst verschlüsselte Kanäle sind für den „man in the middle" keine unüberwindbare Hürde. Somit können stark besuchte Orte, wie beispielsweise Flughäfen, an denen Anwender „nur mal eben E-Mails checken" wollen, zu einer wahren Fundgrube von sensiblen Informationen werden.

App-Gefahren

Ein Herausstellungsmerkmal, aber auch gleichzeitig die Achillesverse der Smartphones, sind ihre Apps! Viele dieser Applikationen übermitteln vertrauliche Daten, eindeutige Gerätekennungen, Aufenthaltsorte oder sogar ganze Adressbücher, zum Teil ohne dass es dem Anwender bewusst ist. Dazu kommt, dass Funktionalität und Design beim Erstellen der Apps Vorrang gegenüber der Sicherheit haben, sodass manche Apps zu einem massiven Sicherheitsproblem führen können. Dies sind nur die ungewollten Sicherheitsrisiken. Was ist mit bewusst entwickelter Schadsoftware, deren Ziel die Kontrolle über das fremde Gerät ist? Das Sicherheitsunternehmen Dasient stellte nach der Untersuchung von 10.000 Android-Apps fest, dass etwa acht Prozent der Apps mit Malware verseucht waren. Die wachsende Anzahl an Quellen, die beschreiben, wie Schadsoftware in die verschiedenen Stores und Markets eingeschleust wird, zeigt, dass Malware für Smartphone und Co. keine fiktive Bedrohung mehr ist, sondern Realität.

Fremdkontrolle

Hat der Angreifer Zugriff auf ein fremdes Gerät erlangt, wachsen seine Möglichkeiten, Schaden anzurichten, enorm. Er ist nun in der Lage, die Position des Gerätes zu verfolgen und damit ein Bewegungsprofil des Besitzers zu erstellen, kann E-Mails, Anrufe, SMS, Dokumente und andere Daten auslesen, hohe Kosten durch Anrufe und SMS verursachen oder auch direkt Gespräche und Nachrichten abhören beziehungsweise mitlesen. Auch kann das Smartphone als Wanze verwendet werden, die neben Sprache auch Bilder oder Videos mit hoher Auflösung an den Angreifer sendet. Durch die wachsenden internen Speicher im Gigabyte-Bereich können die Daten sogar erst zwischengespeichert und dann bei Bedarf oder dann, wenn eine ausreichende Verbindung besteht, übermittelt werden. Des Weiteren ist auch der Weg in das Firmennetz durch den Zugriff auf das Smartphone möglich. Ausgelesene Zugangsdaten können genutzt werden, um die vom Unternehmen eingerichteten Schutzbarrieren, welche vor Fremdzugriffen schützen sollen, zu umgehen. Dabei wird der Angreifer direkt auf VPN- oder Remote-Zugänge zurückgreifen oder die E-Mails bequem durch das firmeneigene Webinterface lesen.

Verlustängste

Neben dem Angriff aus der Ferne besteht auch die folgenschwere Möglichkeit, Informationen eines entsorgten, gefundenen oder geklauten Gerätes auszulesen, um an wertvolle Daten und Dienste zu gelangen. Ständig wechselnde unsichere Umgebungen (Flughäfen, Bahnhöfen, Cafés) erhöhen die Wahrscheinlichkeit des unabsichtlichen Verlustes und des gezielten Diebstahls! Dabei erlaubt eine forensische Analyse des Smartphones auch Zugriff auf bereits gelöschte Daten. War das Auslesen von Handys noch mit dem kostspieligen Kauf von Flasherboxen und anderer Hardware für jedes einzelnen Modell verbunden, so gibt es mittlerweile teilweise kostenlose Software, die nur noch auf ein Betriebssystem beschränkt ist und nicht mehr auf das Modell. Somit kann der Verlust eines Gerätes zu einer massiven Sicherheitsbedrohung werden. Aber auch ein wiedergefundenes oder als Werbegeschenk in das Unternehmen geschicktes Gerät ist eine potenzielle Gefahr. Wer weiß, ob der ehrliche Finder oder edle Spender das Gerät nicht kompromittiert hat, um an sensible Informationen zu gelangen?

Lösungsansätze und ihre Probleme

Leider treten bei den meisten Lösungsansätze im Bereich der IT-Sicherheit schon bei der Realisierung Komplikationen auf, bevor das eigentliche Problem in Angriff genommen werden kann. Es fängt bereits mit der Anschaffung des richtigen Gerätemodells an. Soll ein einheitliches Rollout vom Unternehmen bestimmt werden, welches zwar die Homogenität der Geräte bewahrt, aber wahrscheinlich die Akzeptanz der Anwender vermindert, die dann doch wieder ihr eigenes Gerät nutzen, oder soll doch besser die Bring-Your-Own-Device-Strategie (BYOD) verfolgt werden, bei der der Anwender sein Arbeitsgerät selbst bestimmen darf, aber so die Heterogenität der Geräte unausweichlich ist und ein erhöhter administrativer Aufwand in Kauf genommen werden muss? Diese Frage lässt sich nicht allgemein beantworten und ist von Unternehmenspolitik und -philosophie abhängig. Beide Strategien sind zudem von der Update-/Sicherheitspolitik der Hersteller abhängig. Es gibt derzeit drastische Unterschiede in der Verfügbarkeit von Betriebssystemupdates bei den Herstellern. Auch ist für den Anwender nicht immer einfach ersichtlich, wie lange ein Gerät noch unterstützt wird.

Mobile Device Management System

Ein ganzheitliches Mobile Device Management System erlaubt weitreichende Eingriffe für IT-Administratoren, um die Integration von Smartphones in die Unternehmensstrukturen zu verwalten. Das Gerät erhält dabei eine Identität, um automatisierte, regelkonforme und identitätsbezogene Prozesse zu ermöglichen. Beim Verlust eines Gerätes könnten im Folgenden automatisch sämtliche mit der gleichgestellten Identität verbundenen Rechte und Zugänge entzogen werden, so dass eventuell unerlaubt ausgelesene Zugangsdaten keinen Nutzen mehr für den Angreifer haben. Auch könnte der Verstoß gegen Security-Richtlinien, etwa das Abschalten des Virenschutzes, mit Hilfe eines solchen Systems unterbunden werden. Die Basis für jedes MDMS ist die Integrität des Betriebssystems, welche weder durch die gewollte Manipulation des Anwenders noch durch die Kompromittierung durch Malware beeinträchtigt werden darf. Es bedarf demnach einer Technik, die die Unversehrtheit, also die Integrität des Gerätes prüft.

Trusted Smartphones

Aktuell sind die meisten Sicherheitslösungen für Smartphones nur aufgesetzte Erweiterungen und keine vollständig integrierten Sicherheitslösungen. Es ist von den Herstellern einfach nicht vorgesehen, dass Sicherheitslösungen auf Betriebssystem-ebene und auf der Hardwareebene ansetzen.

Da wir bei mobilen Geräten mit einer Zunahme von „mobile Malware" zu rechnen

haben, muss auch der Trend bei diesen Geräten in Richtung sicherer Betriebssysteme gehen, die auf einer nicht manipulierbaren Sicherheitsplattform aufbauen. Selbst das Anzapfen von Geräteplatinen durch zusätzliche Hardware wäre durch die Verwendung einer solchen Plattform, zumindest in der Theorie, feststellbar. Da der Sicherheitsplattform ein Secure-Boot-Vorgang zugrunde liegt kann auch der Systemzustand auf Hardwareebene erfasst werden. Anhand dieses Zustandes kann dann entschieden werden, ob dem Smartphone der Zugang zum Firmennetz gewährt wird oder ob es weitere Sicherheitsprozesse durchlaufen muss, bis es den notwendigen Sicherheitszustand vorweisen kann.
Natürlich hat auch diese Technik ihre Grenzen. In der Praxis wird es immer Manipulationsmöglichkeiten für einen Angreifer geben, wenn dieser physikalischen Zugriff auf ein Gerät hat. Jedoch lässt sich der Aufwand für den Angreifer durch eine vernünftige Sicherheitsplattform erhöhen und der mögliche Aktionsradius in Bezug auf den Zugriff auf Daten lässt sich minimieren. Wie bereits am Anfang erwähnt, ist leider für kleine mobile Geräte – abgesehen von Notebooks – bisher kein Sicherheitsmodul verfügbar, und auch die Entwicklung von sicheren Betriebssystemen für diese Geräte hat gerade erst begonnen.

Virtuelle sichere Umgebungen

Unternehmen haben oft das Problem, dass sich auf den Smartphones von Mitarbeitern, unabhängig davon, ob es Dienst- oder Privatgeräte sind, geschäftliche und private Daten des Besitzers vermischen. In der Virtualisierung sieht man hier eine Möglichkeit, dies zu ändern. Es gibt in der Forschung aktuell zwei Ansätze, dieser Problematik zu begegnen. Der erste Ansatz ist die Virtualisierung des gesamten Systems eines Smartphones. So befinden sich auf dem Smartphone ein virtuelle sichere Umgebung für den privaten und ein weitere virtuelle sichere Umgebung für den dienstlichen Gebrauch. Der andere Ansatz lagert bestimmte Funktionen des Betriebssystems in einzelne sogenannte Compartments aus, die zwar voneinander isoliert sind, aber über einen Sicherheitskern kommunizieren können. Für beide Ansätze muss das Betriebssystem aber so weit modifiziert werden, dass aktuell noch kein praktischer Einsatz möglich ist. Durch die Verwendung von virtuellen sicheren Umgebungen kann die Integrität eines Smartphones sichergestellt werden. Apps laufen isoliert und so kann auch Schadsoftware nur in abgesteckten nicht kritischen Bereichen aktiv werden und keinen nennenswerten Schaden anrichten.

Diese verschiedenen Lösungsansätze zeigen, dass die Forschung und die Industrie Möglichkeiten besitzen, das Sicherheitsniveau von Smartphones zu erhöhen. Es ist nun an der Zeit, dass die Hersteller reagieren und notwendige Anpassungen ermöglichen beziehungsweise umsetzen.

Der Anwender

Bei einer Übersicht über die Bedrohung von IT-Geräten sollte das biologische System vor dem Gerät nicht vernachlässigt werden. Erfahrungen aus dem PC-Bereich haben gezeigt, dass der Anwender ein nicht zu unterschätzender Faktor für die IT-Sicherheit ist. Neben dem „normalen" Anwender hat in den letzten Jahren eine neue „Art" ihren Einzug in die Unternehmen genommen. Es sind die Digital Natives, also junge Mitarbeiter, die gerne immer online und erreichbar sein wollen, die nun mehr und mehr in die Unternehmen drängen. Die hohe Kommunikationsfreudigkeit, ob in sozialen Netzen oder Mikro-Blogging-Diensten, bedarf einer anwenderangepassten Übermittlung von Verhaltensregeln für das Erlangen einer Sicherheitskompetenz. Dabei ist zu beachten, dass es nicht ausreicht, die bekannten Spielregeln von Laptops und Desktops-PCs auf Smartphones zu übertragen. Auch wenn die sozialen Netze am Arbeitsplatz gesperrt sind, können beispielsweise per Smartphone sensible Information an Dritte weitergegeben werden.

Vielen Anwender ist zudem auch nicht bewusst, wie einfach die Einsicht in oder das Erlangen von vertraulichen Informationen in öffentlichen Bereichen, beispielsweise im Flugzeug, im Zug oder im Cafe, sein kann. Es reicht zum Teil schon, wenn der Interessierte einen Blick über die Schulter wagt. Ganz davon abgesehen, dass einige Personen dazu neigen, ganz ohne Aufforderung, während eines Telefonats, sensible Informationen im Zugabteil oder an der Kasse im Supermarkt in die Welt herauszuschreien.

Fazit

Der Aufwand, welcher für die mobile Sicherheit getrieben wird, sollte immer dem eigentlichen Schutzbedarf angemessen sein. Daher muss betrachtet werden, welche Daten überhaupt schützenswert sind, wie hoch ein möglicher Schaden wäre und wie wahrscheinlich dessen Eintreten überhaupt ist. Jedoch haben derzeit Daten, die bei Verlust eine beachtliche Bedrohung für das Unternehmen bedeuten, auf mobilen Geräten nichts zu suchen, da aktuelle Sicherheitslösungen noch keinen hinreichenden Schutz bieten. Wieder einmal scheint es, dass bei der Umsetzung einer technischen Revolution zuletzt an die IT-Sicherheit gedacht wurde. Die momentane Entwicklung zeigt, dass wir uns mit Consumer-Geräten beschäftigen, denen gewisse Business-Features aufgesetzt wurden, die aber leider noch weit von einem vollwertigen Business-Einsatz entfernt sind. Die Herausforderung im Bereich der mobilen Sicherheit ist, eine passende Nutzung und angemessene Schutzmechanismen für mobile Geräte zu finden, die die Risiken kalkulierbar werden lassen. ■

Oliver M. Achten, Projektleiter der Forschungsbereiche Mobile Security und Cloud Computing des Institut für Internet-Sicherheit.

Prof. Dr. (TU NN) Norbert Pohlmann, Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit an der Fachhochschule Gelsenkirchen (www.internet-sicherheit.de).