Jens Heider, Rachid El Khayari

Geht Ihr Smartphone fremd?

Übersicht der Angriffsvektoren für Geräte im Unternehmenseinsatz

Smartphones haben sich längst als praktische Alleskönner durchgesetzt und sind aus dem Unternehmensalltag nicht mehr wegzudenken. Genauso unerlässlich wie das allgegenwärtige Nutzen ihrer vielfältigen Funktionen ist aber auch ihre Absicherung geworden. Der folgende Beitrag stellt die wichtigsten Angriffsvektoren vor, die für eine Unternehmensabsicherung berücksichtigt werden sollten, um die Kontrolle über die genutzten Informationen zu behalten.

1 Einleitung

Der Begriff des Informationszeitalters ist beinahe schon so alt, dass er in Vergessenheit gerät. Dennoch hat heutzutage kaum ein Gut einen höheren Stellenwert als Information. Dies ist auch in einem Unternehmen nicht anders, denn hier manifestiert sich Information in Form der im Unternehmen erzeugten Daten als höchst schützenwertes und sensibles Gut – als Schutzgut.

Da diese Daten an verschiedensten Stellen innerhalb eines Unternehmens erzeugt, verarbeitet, transformiert oder übertragen werden, gestaltet sich die Absicherung dieses Schutzgutes als recht komplex.

Innerhalb dieser Informationsnutzung stellen Smartphones ein weiteres Element dar, an dem Unternehmensdaten vorliegen und zu schützen sind. Für Unternehmen, die den Zugriff auf ihrer Daten und Dienste nun auch durch Smartphones ermöglichen, stellt sich somit die Frage ob und welcher Neubetrachtung dieses Arbeitsgerät hinsichtlich der IT-Sicherheit unterzogen werden muss und wie bisherige Ansätze zum Unternehmensschutz erweitert werden müssen.

Dr. Jens Heider

leitet das Testlabor Mobile Sicherheit am Fraunhofer-Institut für sichere Informationstechnology (SIT) in Darmstadt und untersucht seit 2004 mobile Systeme auf Schwachstellen

E-Mail: jens.heider@sit.fraunhofer.de

Rachid El Khayari

Wissenschaftlicher Mitarbeiter im Testlabor Mobile Sicherheit am Fraunhofer-Institut für sichere Informationstechnology (SIT) mit Schwerpunkt iOS-Sicherheit

E-Mail: rachid.el.khayari@sit.fraunhofer.de

Mit dem Einsatz von Notebooks existiert zwar bereits schon seit längerem ein Vertreter der mobilen Endgeräteklasse innerhalb von Unternehmen. Ein Hauptunterschied liegt sicherlich aber darin, dass Smartphones mehrere grundlegende Merkmale vereinen, die zusammen aus der Sicherheitsperspektive zu betrachten sind. So gelten für die Smartphone-Nutzung im Unternehmen allgemein folgende Risikofaktoren:

- Höheres Verlustrisiko durch Formfaktor und allgegenwärtige Nutzung
- Betrieb und entsperrter Gerätezugang häufig in ungesicherter Umgebung
- Vorwiegend erfolgt Kommunikation über öffentliche Netze, was Geräte/Software-Schnittstellen für Angreifer einfacher erreichbar macht
- Hohes Missbrauchspotential durch umfassenden Zugriff auf Unternehmensinformationen
- Vielfalt an Smartphone-Funktionen und Schnittstellen erzeugt Fehleranfälligkeit durch Software-Komplexität
- Absicherung erschwert durch die Vielzahl von Softwareversionen und Geräte-Herstellern
- Freie Konfigurier- und Erweiterbarkeit erhöht Nutzerverantwortung
- Anspruch als persönliches, vertrauenswürdiges Gerät, was Akzeptanz von Restriktionen reduziert

Die organisatorischen Maßnahmen die für den Desktop-Bereich bereits Anwendung finden bleiben dabei grundsätzlich die selben. Sie müssen im Falle von Smartphones nun das Unternehmen aber in einem wesentlich dynamischeren Umfeld, mit heterogenen Geräten, ohne geschützten Perimeter und gegen eine größere Angriffsfläche absichern.

Um genauer verstehen zu können mit welchen Sicherheitsmaßnahmen den vorhandenen Bedrohungen entgegengewirkt werden kann, betrachten wir im Folgenden allgemeine Angriffsvektoren für Smartphones, die potentiell unabhängig von dessen Betriebssystem zu berücksichtigen sind. Die Angriffsvektoren beschreiben dabei Mittel und Wege, mit deren Hilfe ein Angreifer potentiell sein Ziel erreichen kann. Dabei geht es insbesondere darum

Abb. 1 | Physische und logische Smartphone-Angriffsvektoren

zu differenzieren inwiefern sich diese Angriffsvektoren im Vergleich zu Desktop-Systemen unterscheiden.

Aufgrund der unterschiedlichen Voraussetzungen, die für Angriffe notwendig sein können, werden die Angriffsvektoren auf der logischen und der physischen Ebene getrennt betrachtet. Daran anschließend erfolgt resümierend ein Ausblick, wie auf Entwicklungs- und Nutzerseite den Bedrohungen in Zukunft begegnet werden kann.

2 Logische Angriffsvektoren

Angreifer versuchen erfahrungsgemäß immer zunächst – ähnlich wie der elektrische Strom – den Weg des geringsten Widerstandes zu gehen. Hierfür bieten sich vor allem logische Angriffsvektoren an, da dazu kein physischer Zugriff auf das Zielgerät notwendig ist und somit viele potentielle Opfer effizient gleichzeitig angegriffen werden können. Dennoch bieten diese Angriffsvektoren häufig auch die Möglichkeit ganz gezielt Opfer auszuwählen, bspw. durch das Identifizieren über eine digitale Nutzeridentität oder die direkte Adressierung eines Gerätes.

Angriffsvehikel sind dabei die potentiellen Schwächen in den verschiedenen Software- und Dienst-Schnittstellen, die ein Smartphone auf dieser logischen Ebene anbietet.

2.1 Kommunikationsdienste

Eine sehr grundlegende Rolle für Angriffe spielen sämtliche Kommunikationsdienste, wie etwa E-Mail, SMS, MMS, Instant-Messenger oder etwa VoIP-Dienste, da diese dazu verwendet werden können, um Schadsoftware direkt an das Endgerät zu übertragen oder den Nutzer auf entsprechend präparierte Inhalte im Internet zu lenken.

Lassen sich Angriffe über E-Mails noch etwa serverseitig aus dem Postfach herausfiltern, gestaltet sich das für VoIP-Verbindungen schwieriger. Hier ist es zudem in den meisten Fällen notwendig dynamisch ausgehandelte Ports in der Firewall zu öffnen, um die Funktion des Dienstes zu ermöglichen. Im Falle von dienstspezifischen Schwachstellen kann dies dem Angreifer ermöglichen weiteren Schaden anzurichten.

SMS und MMS gehen zudem vollständig an den Sicherheitsmechanismen eines Unternehmens vorbei und können von der Administration unbemerkt Schadcode auf das Endgerät transportieren (siehe bspw. [3]) oder zur Installation dieser auffordern. Die dabei verwendeten gefälschten vertrauenswürdigen Absenderidentitäten und das gezielte Adressieren von Schlüsselpersonen (sog. Spear Phishing) sind besonders im Unternehmensumfeld als kritische Szenarien zu berücksichtigen.

2.2 Browser

Der Web-Browser ist eine der am meist genutzten Anwendungen auf heutigen Smartphones und bildet das Eingangstor zu den Inhalten des World Wide Web. Diese Inhalte sind heute häufig nicht nur von statischer Natur, vielmehr werden beim Browsen auch auf der Endgeräteseite Daten und Eingaben aktiv verarbeitet. Da für diese Verarbeitung auf den Endgeräten immer komplexe Standards verwendet werden, steigt auch das Risiko für mögliche Schwachstellen, über die ein Angreifer etwa Schadsoftware auf dem Endgerät zur Ausführung bringen kann.

Dabei stellt gerade die Verbindung zwischen Browser und Telefon ein zusätzliches Angriffsziel dar. Durch Schwachstellen im Browser können dann beispielsweise mit der Nutzeridentität der SIM-Karte aus Webseiten heraus kostenpflichtige Anrufe erzeugt (bspw. demonstriert in [1]) und SMS für Dienste versendet werden. Ein Angreifer erhält aber möglicherweise dadurch auch ein Mittel, um Sicherheitsprozesse zur Bestätigung einer Nutzeridentität zu umgehen bzw. zu missbrauchen.

2.3 Baseband Prozessor

Das eigentliche Telefon im Smartphone wird durch den sog. Baseband Prozessor realisiert. Dieser wurde unlängst aus zwei Richtungen als weiterer Angriffspunkt identifiziert. Einmal von außen über die Mobilfunkschnittstelle für Angriffe gegen das Endgerät, und als Trittbrett aus dem Smartphone heraus gegen Basisstationen des Mobilfunknetzes bzw. gegen andere Nutzer. Im ersten Fall richtet sich der Angriff meist gegen die Verfügbarkeit, aber teilweise auch auf den Zugriff auf vertrauliche Daten im Smartphone-Speicher. Im anderen Fall gegen die Verfügbarkeit des Mobilfunkdienstes.

Ausgenutzt werden dabei jeweils Fehler in der proprietären Software des Baseband-Prozessors. Solche Fehler blieben in der Vergangenheit häufig in reinen Funktionstests der Hersteller unbemerkt. Durch die umfangreiche Programmierbarkeit der Smartphones und den stark gesunkenen Preisen der Technik für Basisstationen stehen den Angreifern nun aber mehr Möglichkeiten zur Verfügung, mit Interaktionen außerhalb der geprüften Spezifikation die Anfälligkeit für sicherheitskritische Schwä-

chen aufzuspüren und auszunutzen. Die Tragweite dieser Angriffe wurde in letzter Zeit häufig diskutiert (siehe bspw. [2][3][4]).

2.4 Smartphone Apps

Jede Erweiterung der Funktionalität eines Gerätes birgt prinzipiell die Gefahr, dass durch den daraus resultierenden Anstieg der Komplexität auch die IT-Sicherheit beeinträchtigt wird. Gerade bei Smartphones ergibt sich insbesondere eine mangelnde Transparenz der Anwendungen (Apps) bezüglich potentiell versteckter Funktionen und daraus resultierenden Risiken. Durch die Art der Nutzung und der allgegenwärtigen (unsichtbaren) drahtlosen Kommunikation sowie einer unmittelbaren Verknüpfung mit standardisierten, realen Nutzeridentitäten im Smartphone, stehen einem hohen Angriffspotential lediglich geringe Möglichkeiten des Nutzers gegenüber, eine Manipulation, vor dem Eintreten eines Schadensfalls, festzustellen.

Ebenso geht von installierter Zusatzsoftware die Gefahr aus, dass darin enthaltene Schwachstellen von Angreifern genutzt werden könnten, um unberechtigten Zugriff auf Daten der Anwendung oder auch auf andere Bereiche des Smartphones zu erhalten. Insbesondere als Ergebnis des Preisdrucks im App-Markt, der geringen Hürden für Programmiereinsteiger und der funktionsorientieren Nutzerwahrnehmung, sind gegenwärtig die schlechten Sicherheitseigenschaften einer Vielzahl von Apps nicht verwunderlich.

Hier zeigen sich die Stärken und Schwächen der Sicherheitsmodelle von Smartphone-Betriebssystemen, die Unterstützung der Hersteller zur sicheren Anwendung der Sicherheitskonzepte und der umgebenden App-Ökosysteme.

Der aktuelle ENISA Report [5] bestätigt zudem die Wichtigkeit des Ineinandergreifens des Schutzes durch: Review-Systeme, Reputationsmechanismen, der Isolation von Apps von Betriebssystemkomponenten (sog. Sandboxing), die Beschränkung auf vertrauenswürdige Softwarequellen (sog. walled gardens) und der Möglichkeit aus der Ferne eine Anwendung vom Endgerät entfernen zu können (sog. kill-switch), wenn diese als schädlich entlarvt wurden.

In unseren Praxistests zeigt sich aber gegenwärtig noch, dass der daraus resultierende Schutz dennoch lückenhaft ist und dem Risiko durch technische Weiterentwicklungen, aber für höhere Sicherheitsanforderungen in manchen Punkten auch durch einen Kompromiss zwischen Funktionalität und Sicherheit begegnet werden müssen.

Auch aus datenschutzrechtlicher Perspektive sind viele Apps relevant. Sie haben häufig umfassenden Zugriff auf Gerätekennungen, Standortdaten, E-Mail- und Telefonkontakte, SIM-Kartennummer und weitere personenbezogene Daten und können diese ohne Unterrichtung der Nutzer an Gerätehersteller, Provider oder Anbieter von Analysediensten übermittelt, weshalb der Düsseldorfer Kreis auch die Möglichkeit für eine datenschutzgerechte Smartphone-Nutzung fordert [6].

2.5 Multimedia-Player

Aber nicht nur die Komplexität von zusätzlicher Software erhöhen die Risiken auf Smartphones. Auch die Komplexität der Verarbeitung komprimierter Multimedia-Datenströme (bspw. MP3, MP4, WMA, TIFF, PDF, etc.) hat in der Vergangenheit bereits einige Verwundbarkeiten auch in Smartphones hervorgerufen. Neben der Absicherung vor schädlichen Apps ist die Nutzung dieser beliebten Datenformate auf Unternehmens-Smartphones ein leicht zu übersehender Aspekt bei Sicherheitsrichtlinien.

Die Folgen einer Schwäche bei der Verarbeitung von Multimediadaten zeigt der „JailbreakMe“ iOS Exploit. Dieser nutzte Schwächen bei der Verarbeitung von PDF-Dateien zunächst für ein Entfernen der Betriebssystemrestriktionen (sog. Jailbreak), konnte nach der Veröffentlichung aber auch für Angriffe aus sämtliche Daten und Funktionen ausgenutzt werden [7].

2.6 Fernwartung

Die Fernwartung von Smartphones, als Teil eines sog. Mobile Device Management ist ein wesentliches Sicherheitselement, um in dem dynamischen Umfeld Sicherheitsrichtlinien überprüfen und durchsetzen zu können. Gerade kritische Aspekte wie fehlende Updates, eine unsichere Geräte-Konfiguration oder die Nutzung von Unternehmensdiensten über nicht registrierte Geräte können über Schnittstellen der Fernwartung adressiert werden.

Dennoch ist solch eine Schnittstelle mit Zugriff auf tiefgreifenden Betriebssystemfunktionen auch mit gewissen Risiken verbunden. Bei Schwächen in den Schnittstellen zur entfernten Geräteverwaltung entstehen für Angreifer interessante Möglichkeit in die Geräte einzudringen bzw. Sicherheitseinstellung zu manipulieren. So könnten etwa Kommunikationsverbindungen zum Angreifer umgeleitet oder Software zum Auslesen von Daten und Passwörtern installiert werden. Gerade bei der Smartphone-Nutzung in öffentlichen Netzen liegt eine erhebliche Last auf der Sicherheit der MDM-Protokolle, der eingesetzten Server-Software und ihrer Konfiguration.

Eine entsprechend geprüfte MDM-Softwarelösung begegnet diesem Risiko jedoch mit Schutzmaßnahmen gegen Manipulation und unterstützt durch das Durchsetzen von organisatorischen Maßnahmen die Unternehmenssicherheit mit der zentralen Verwaltung der Geräte. Dennoch sollte immer berücksichtigt werden, dass eine zentrale, einheitliche MDM-Lösung für unterschiedliche Betriebssysteme zwar ein wichtiges Kontrollwerkzeug darstellt, aber das Potential der Absicherungsmöglichkeiten einzelner Geräte, bedingt durch Betriebssystemunterschiede, nicht immer ausgeschöpft wird bzw. vorgegebene Schutzmerkmale nicht für alle Geräte immer sicher umgesetzt werden können.

2.7 Anwender

Letztlich kann auch der Nutzer des Smartphones zum Erfüllungsgehilfe für einen Angreifer werden. Dabei zielt der Angreifer auf die Unwissenheit des Nutzers bezüglich des richtigen Verhaltens bei System- und Warnhinweisen, oder er nutzt Schwächen in der Betriebssystemdarstellung aus, um Nutzer über die eigentlichen Konsequenzen zu täuschen. Ein klares Indiz für den Erfolg dieser Methode ist die Verbreitung von Schadsoftware, die auf das Bestätigen von Warnhinweisen angewiesen ist (z.B. ZeuS-in-the-Mobile (ZitMo), Cabir). Darüber hinaus besteht bei vielen Nutzern ein großes Vertrauen zu ihrem persönlichen Telefon, sodass Angreifer diese vermeintliche Vertrauenswürdigkeit des Gerätes missbrauchen können.

Auch die Delegation von Sicherheitseigenschaften an den Nutzer ist im Falle von Unternehmensendgeräten problematisch, da viele Nutzer die Auswirkungen notwendiger Einstellungen eventuell nicht richtig einschätzen können (z.B. Entscheidungsmög-

lichkeiten bei Sicherheitsdialogen, notwendige Passcode-Komplexität, etc.).

Den Nutzern die Hintergründe für die Sicherheitsmeldungen zu vermitteln und auf die Gefahren aufmerksam zu machen, ist damit ein wichtiger Schritt in der Absicherung von Unternehmens-Smartphones. Denn das Risiko vieler Angriffswege kann durch aufmerksamen und sicherheitsbewussten Einsatz des Smartphones deutlich verringert werden.

3 Physische Angriffsvektoren

Durch das hohe Verlustrisiko von Smartphones und die weit verbreiteten Nahfunkschnittstellen müssen auch physische Angriffsvektoren betrachtet werden, bei denen ein Smartphone in Besitz des Angreifers gelangt ist oder sich dieses zumindest in der näheren Umgebung befindet.

3.1 Drahtlos Schnittstellen

Obwohl drahtlos Schnittstellen (Bluetooth, NFC, WiFi, etc.) zunächst nur die Übertragung von Daten ermöglichen, die zusätzlich auf höheren Ebenen des Übertragungsstandards abgesichert werden, findet bereits beim Empfang der übertragenen Datenpakete eine Verarbeitung statt. Ein üblicher Angriffsvektor ist daher der Versand manipulierter Datenpakete, die Schwächen in der Empfangsverarbeitung ausnutzen. Schafft es ein Angreifer Programmcode auf diese Weise einzuschleusen kann er Zugriff auf Nutzerdaten und Passwörter erlangen.

Wird eine schwache Verschlüsslung verwendet (bspw. WEP) ist es zudem möglich, dass ein Angreifer direkt die Verschlüsselung bricht und in der Folge alle übertragenen Daten mitlesen kann.

Aus Angreifersicht ist jedoch das abfangen übermittelter, unverschlüsselter Daten nach wie vor häufig viel einfacher, als dazu in das Gerät einzubrechen. Er kann sich dabei zu Nutze machen, dass einem Opfer, bei der Auswahl eines verfügbaren öffentlichen WLAN-Zugangs, lediglich dessen (frei wählbarer) Namen angezeigt wird. Betreibt ein Angreifer einen eigenen Hotspot mit passendem Namen (bspw. Free Internet, Telekom, oder Hotel) kann er Opfern einen falschen Zugang vortäuschen und kann direkt die über diesen Hotspot gesendeten und empfangenen Daten der Opfer mitlesen. Da immer noch etliche Anwendungen unverschlüsselte Verbindungen aufbauen erhält der Angreifer so zumindest die ungeschützte Kommunikation (siehe z.B. [8]). Wird zudem vom Nutzer bei der unsicheren Anwendung dasselbe Passwort wie im Unternehmensumfeld verwendet, kann der Angriff auch auf das Unternehmen ausgeweitet werden. Daher stellt diese Angriffsart nicht nur eine Bedrohung bei unsicheren Unternehmensanwendungen dar.

3.2 Speicherkarten

Daten auf externen Speichermedien sind häufig ungeschützt. Im Gegensatz zu Notebooks, bei denen eine Vollverschlüsselung mit Anmeldung vor dem Booten (sog. Pre-Boot-Authentication) zum Standard bei Unternehmens-Notebooks gehört, ist ein entsprechender Schutz bei Smartphones noch selten. Wo vorhanden ist der Schutz häufig durch zu schwache Passwörter für Brute-Force-Angriffe anfällig (siehe bspw. [9] für Angriffe auf BlackBerry Geräte mit SD-Card Verschlüsselung). Die schwachen Passwörter sind dabei häufig dem Eingabemedium geschuldet. Gelangt dann ein Smartphone in den Besitz eines Angreifers, können somit die Daten auf den Speicherkarten häufig recht einfach ausgelesen werden.

Kann ein Angreifer zudem manipulierte Daten auf der Speicherkarte platzieren und dieses unauffällig dem Opfer wieder unterschieben, lassen sich so auch Verwundbarkeit des Smartphones ausnutzen. Zudem können Angreifer das Smartphone auch als Wirt für Infektionen von Unternehmens-PCs verwenden. Der Rat keine unbekannten USB-Stricks oder CDs in Unternehmens-PCs zu verwenden, kann durch das, als vertrauenswürdig geltende, Smartphone vom Angreifer umgangen werden. So können beim Synchronisieren des Smartphones mit dem PC gezielt infizierte Daten und Software auf den PC des Opfers gelangen, durch die im nächsten Schritt auch das Unternehmensnetzwerk attackiert werden kann (siehe bspw. [10]).

3.3 SIM-Karte

Obwohl die SIM-Karte an sich eine hohe Sicherheit gegen Angriffe bietet, können Angreifer mit physischem Zugriff durch Schwächen in der Spezifikation die Kommunikation zwischen der SIM-Karte und dem Smartphone (SIM-Toolkit) manipulieren. Dadurch können, je nach Unternehmensanwendung und Gerätenutzung, gegebenenfalls IT-sicherheitsrelevante Informationen mitgelesen bzw. verändert werden [11].

Kritisch wird dieser Angriff insbesondere dann, wenn es dem Angreifer gelingt, ein derart manipuliertes Gerät unauffällig seinem Opfer wieder unterzuschieben. In der Vorbereitung sind solche Angriffe natürlich recht aufwändig, die eigentliche Manipulation am Gerät kann dann aber meist wie ein Akku-Wechsel – abhängig vom Smartphone-Modell – durch wenige Handgriffe am Gerät durchgeführt werden. Die dabei zusätzlich eingesetzten Bauteile im SIM-Schacht fallen dabei erst auf, wenn SIM oder Akku gewechselt werden müssen, was nicht mehr allzu häufig vorkommt. In sicherheitskritischen Bereichen kann daher eine regelmäßige Kontrolle von Smartphones auf Manipulationen wichtig sein.

3.4 Hardware-Schnittstellen

Auch wenn auf Software-Ebene Sperren ein unberechtigtes Nutzen des Geräts verhindern, so können Angreifer durch vollständiges Zerlegen des Gerätes versuchen diese Sperren zu umgehen. Der Zugriff über dann erreichbare Speicherbusse und Hardware-Schnittstellen (bspw. JTAG) erfordert zwar einen deutlich höheren Aufwand als der Zugriff über Softwareschnittstellen, ermöglicht aber noch häufig einzelne Schutzmechanismen der Nutzerschnittstelle zu umgehen.

Erst eine Absicherung durch eine vollständige Verschlüsselung wirkt diesen Angriffen effektiv entgegen. Dazu muss die Verschlüsselung auf einem externen, starken Nutzergeheimnis beruhen.

3.5 Speicher

Speziell die im Smartphone-Speicher abgelegten Informationen sind bei direktem Zugriff durch Angreifer einem hohen Risiko ausgesetzt. Fehlt eine starke Verschlüsselung können durch Manipulationen von Betriebssystem-Funktionen im Flash-Speicher

häufig Schutzmechanismen umgangen, aber auch Nutzerdaten direkt aus den Speicherbausteinen ausgelesen werden.

3.6 Firmware

Ebenso stellt der Schutz der Integrität der Firmware die Basis für viele Sicherheitsfunktionen im Smartphone dar. Bleibt die Manipulation der Firmware und das Zurücklegen vom Nutzer unbemerkt (sog. Evil Maid Attack), so kann der Angreifer die vollständige Kontrolle aus der Ferne über das Smartphone und die Daten erlangen. Er kann dabei über längere Zeit nicht nur aktuelle Daten abrufen, sondern auch jederzeit Funktionen wie GPS-Ortung, Mikrofon oder Kamera vom Smartphone des Opfers nutzen.

Als kritische Firmware-Manipulation ist dabei auch der sog. Jailbreak bei iOS-Geräten zu zählen, da dieser wichtige Sicherheitsfunktionen in iOS-Geräten abschaltet. Nicht zu Unrecht bieten daher bereits zentrale MDM-Lösungen eine Jailbreak-Erkennung an, um derart manipulierte Geräte von der Nutzung im Unternehmen auszuschließen. Allerdings ist eine Jailbreak-Erkennung auf der Endgeräte-Seite prinzipiell ein Wettlauf mit der Jailbreak-Community und gegenwärtige Erkennungsverfahren sind häufig leicht zu umgehen. Somit können sich nicht nur Mitarbeiter über diese Hürde leicht bewusst hinwegsetzen, auch für Angreifer die einen Evil-Maid-Angriff planen stellt diese Gegenmaßnahme nur ein kleines Hindernis dar.

3.7 USB

Viele der Zugriffe durch physische Manipulationen am Smartphone können aber auch durch die Nutzung hardwarenaher Protokolle über USB realisiert werden, ohne das Smartphone zu öffnen. Diese Schnittstelle bietet fast immer die Möglichkeit die Firmware direkt auszutauschen und mehr oder weniger direkt auf den Flashspeicher zuzugreifen. Beispielsweise ist es bei iOS-Geräten über USB möglich, trotz gesperrter und verschlüsselter Geräte, auf einige Inhalte und Passwörter zuzugreifen [12][13].

Darüber hinaus stellen viele Smartphones weitere logische Schnittstellen für Modem-Funktionen und Datenzugriff über USB bereit, die ein zusätzliches Einfallstor für Angriffe darstellen können. Insbesondere die häufig anzutreffende Möglichkeit USB als Datenverbindung und Ladefunktionalität zu nutzen, kann von Angreifern bei manchen Smartphone-Modelle zu unbemerktem Datenzugriff an fremden manipulierten USB-Ladestationen ausgenutzt werden.

4 Ausblick

An Gegenmaßnahmen für viele der hier aufgezeigten Angriffsvektoren wird seitens der Smartphone-, Betriebssystemhersteller und Drittanbietern bereits weiter gearbeitet. Allerdings zeigt sich nach wie vor verständlicherweise, dass den funktionalen Anforderungen des Consumer-Bereichs Priorität eingeräumt wird und erst nach und nach Funktionen für die Sicherheitsanforderungen des Enterprise-Segments Einzug halten.

Die boomenden App-Märkte und der resultierende Wunsch ein gut gefülltes Smartphone auch im Unternehmen einsetzen zu können wird in Zukunft verstärkt das Kontrollkonzept für Unternehmenssicherheit auf eine harte Probe stellen. Hier werden sich klar die Systeme durchsetzen, die es ermöglichen, trotz der geforderten Erweiterbarkeit, eine Kontrolle der Interaktion mit Unternehmensdiensten auf Endgeräte- und Unternehmensseite durchzusetzen (siehe bspw. BizzTrust [14]).

Neben der Verbesserung der Kontrolle von Anwendungen auf dem Gerät, um Schadsoftware in ihren Möglichkeiten einzudämmen, wird es aber auch vertrauenswürdige Instanzen geben müssen, die mit Hilfe von Standards die Sicherheitseigenschaften von Smartphone-Anwendungen bestätigen. Konsequenterweise wird dies bereits bei der App-Entwicklung ansetzen müssen, da aufgrund der rasanten Update-Zyklen die praktischen Testverfahren nur ein Teil der Sicherheitseigenschaften auf Dauer gewährleisten werden können. Nur mit diesen Maßnahmen wird sich die Smartphone-Nutzung der „Bring-your-own-device"-Mentalität (BYOD) in geregelte und sichere Bahnen lenken lassen. Der gera-

dezu explosionsartigen Verbreitung heterogener Geräte und Anwendungen wird man nur mit Hilfe von übergreifenden Mobile-Device-Management-Lösungen Herr werden, deren Einsatz für alle mobilen Endgeräte mit Zugriff auf Unternehmensressourcen durchgesetzt werden können.

Seitens der Betriebssystemhersteller, der Gerätehersteller, der Lösungsanbieter und Netzbetreiber besteht zudem weiterer Handlungsbedarf in Bezug auf ganzheitliche Lösungsansätze, um die bestehenden Risiken abzuschwächen oder gar zu eliminieren. Hier zeichnet sich ein Trend zur Bildung von Konsortien ab, um diese Herausforderung anzunehmen.

Auch die Wissenschaft ist an dieser Stelle angehalten sich für die Bildung solcher Konsortien einzusetzen und sich an vorhandenen Konsortien zu beteiligen, um kurz-, mittel- und langfristige Lösungen zu erarbeiten. So ist auch ein allgemein enges Zusammenarbeiten von Industrie und Forschung außerhalb solcher Konsortien sinnvoll, um auch neue, zunächst unkonventionell erscheinende Methoden, zu erarbeiten, die ein flexibles Reagieren auf die hochdynamische Entwicklung ermöglichen und damit den Freiraum zu schaffen, um systematischere langfristige Ansätze zu durchdenken.

5 Fazit

Viele Smartphone-Systeme setzen bereits mehr Sicherheitsfunktionalität um, als herkömmliche Desktop-PCs. Allerdings bieten Smartphone durch ihre Nutzungscharakteristik und die Vielzahl der Schnittstellen eine größere Angriffsfläche, wie die Aufzählung der Angriffsvektoren beschreibt. Zudem zeigt sich oft in Praxistests, dass die Grundeinstellungen der Geräte in vielen Fällen nicht für Unternehmen geeignet sind und zum Teil auch noch nicht die Sicherheit bieten, die sie versprechen.

Als erste Maßnahme ist daher beim Smartphone-Einsatz zu klären welche Sicherheitsanforderungen sich aus dem Geschäftsbereich ableiten, welche Daten und welche Dienste auf Smartphones genutzt werden sollen, um daraus entsprechend das Sicherheitskonzept zu erarbeiten und letztlich auch die Endgeräteeinstellungen den Sicherheitsanforderungen anzupassen. Allerdings reicht es meistens nicht, diese Einstellungen nur einmal vorzunehmen. Die Einhaltung der Vorschriften muss auch effizient kontrollierbar bzw. durchsetzbar sein und auch auf der Unternehmensseite muss die Infrastruktur so angepasst werden, dass nur bekannte, kontrollierte Geräte Anschluss finden.

Zudem ist das Wissen um mögliche Angriffe und dessen Verbreitung im Unternehmen sehr wichtig. Durch eine gute Absicherung kann viel für die Sicherheit getan werden. Der Nutzer ist aber ein Faktor, der bei der Absicherung nicht vernachlässigt werden darf. Sowohl im Hinblick auf die sicherheitsbewusste Smartphone-Nutzung, aber natürlich auch im Hinblick auf die Einbeziehung von Wünschen zur produktiven Arbeit. Hier muss ein Kompromiss zwischen Funktionalität und Sicherheit angestrebt werden. Denn werden dem Nutzer zu viele Hürden in den Weg gelegt und versteht er die Gründe dafür nicht, wird er sonst nur aktiv Wege suchen die Hürden zu umgehen, meist mit schlimmeren Folgen für die IT-Sicherheit des Unternehmens.

Aus der Perspektive von Unternehmen ist es aber vor allem wichtig sich bereits der potentiellen Gefahren und Risiken bewusst zu sein. So kann das Unternehmen auf eventuelle, in der Zukunft eintretende, Schadensfälle (bspw. Geräteverlust, Fund manipulierter Geräte, etc.) durch entsprechende Prozesse vorbereitet werden, um im Bedarfsfall zeitnah reagieren zu können (allgemein als Incident Management bekannt). Dies sollte auch Prozesse zur kontinuierlichen Überprüfung der getroffenen Maßnahmen auf ihre Wirksamkeit einschließen, um dynamisch auf sich ändernde Rahmenbedingungen und Erkenntnisse reagieren zu können. Zudem ist es hilfreich auch gemäß des „Think-like-an-alien"-Ansatzes vorzugehen, also dort auf Schwächen zu prüfen, wo man sie zunächst nicht vermutet. Die Sicherheitseigenschaften also stets kritisch zu hinterfragen und zu prüfen, ob die getroffenen Annahmen tatsächlich gelten und durch regelmäßige Überprüfungsroutinen an die aktuelle Bedrohungslage anzupassen.

Für die Einschätzung der Einsatzsicherheit im Unternehmen ist zudem die Geräte-Sicherheit nur der erste Schritt und sollte nicht isoliert betrachtet werden. Auch sichere Produkte müssen häufig erst individuell für die Einsatzumgebung angepasst werden, um Angreifern einen gleichmäßigen Schutz entgegenzusetzten, der nicht an den Integrationspunkten zur Unternehmensinfrastruktur und –Diensten gefährliche Schwächen aufweist.

Für höhere Sicherheitsanforderungen wird jedoch häufig auch ein Kompromiss zwischen Funktionalität und Sicherheit nötig sein. Dennoch ermöglicht ein durch Absicherung in der Funktionalität reduziertes Smartphone immer noch ein produktiveres Arbeiten, als ein Verzicht auf die vielseitigen Helfer.

Literatur

[1] Welt-Online (2008): *iPhone ruft automatisch Abzock-Nummer an, http://bit.ly/v7TUbs*

[2] Weinmann, R.-P. (2011): *All Your Baseband Are Belong To Us,* http://bit.ly/9Ot4A0

[3] Mulliner, C., Golde, N, Seifert, J.-P. (2011): *SMS of Death: from analyzing to attacking mobile phones on a large scale,* http://bit.ly/vd9JGh

[4] Grugq (2010): *Base Jumping – Attacking the GSM baseband and base station,* http://bit.ly/9LaMMd

[5] Dekker, M., Hogben, G. (2011): *Appstore security: 5 lines of defence against malware*, ENISA Report, http://bit.ly/pj2Tb5

[6] Düsseldorfer Kreis (2011): Beschluss – Datenschutzgerechte Smartphone-Nutzung ermöglichen! http://bit.ly/xFDNY3

[7] Bachfeld, D., Mulliner, C. (2010) *Mobile Bedrohungen – Spionageangriffe und Abzocke auf Android und iPhone*, http://bit.ly/uwv3cz

[8] Eikenberg, R., Schmidt, J. (2011): *Die Hotspot-Falle – Gefahren in öffentlichen Funknetzen,* http://bit.ly/uAkLz1

[9] iX-News (2011): *Werkzeug knackt BlackBerry-Passwörter,* http://bit.ly/ocToes

[10] heise-Online (2010): *Erneut Mariposa-Virus auf Vodafone-Smartphones*, http://bit.ly/a0MBXR

[11] heise-Online (2009): *BSI-Kongress: Preis für Beitrag zu Handy-Manipulation*, http://bit.ly/rYAdh2

[12] Heider, J., Boll, M. (2011): *Lost iPhone? Lost Passwords! Practical Consideration of iOS Device Encryption Security,* http://bit.ly/hvUnu9

[13] Heider, J., Boll, M. (2011): *iOS Keychain Weakness FAQ – Further Information on iOS Password Protection* http://bit.ly/o5nq9l

[14] Fraunhofer-Institut SIT (2011): *BizzTrust: Zwei Smartphones in einem*, http://bit.ly/nQYGLD