EGIZ E-Government Innovationszentrum

www.egiz.gv.at
E-Mail: post@egiz.gv.at
Telefon: ++43 (316) 873 5514
Fax: ++43 (316) 873 5520
Inffeldgasse 16a / 8010 Graz / Austria

Bedrohungsanalyse und Sicherheitsanforderungen für M-Government Applikationen

Angriffspotentiale und Schutzfunktionen

Version 2.0, 01.07.2011

Thomas Zefferer – thomas.zefferer@egiz.gv.at

Peter Teufl – peter.teufl@egiz.gv.at

Zusammenfassung: Smartphones spielen in immer mehr Bereichen des täglichen Lebens eine zunehmend wichtige Rolle. Aufgrund der umfangreichen Funktionalität moderner Smartphones können diese Geräte in zahlreichen Anwendungsgebieten verwendet werden. So kommen Smartphones bereits in diversen Unternehmen zur Anwendung um Mitarbeitern einen einfachen externen Zugriff auf zentrale Unternehmensinfrastrukturen zu gewährleisten. Eine verstärkte Verwendung von Smartphones ist zukünftig auch in den Bereichen E-Government bzw. M-Government zu erwarten.

Die zahlreichen neuen Möglichkeiten, die Smartphones bieten, bringen jedoch auch eine Reihe neuer Gefahren mit sich. So ergeben sich durch die Integration von Smartphones in bestehende Unternehmens- oder M-Government-Infrastrukturen neue Möglichkeiten für Angriffe. Andererseits können Smartphones auch selbst dazu verwendet werden die Sicherheit dieser Infrastrukturen zu kompromittieren.

Der geplante Einsatz von Smartphones bedarf daher einer detaillierten Sicherheitsanalyse, in der mögliche Bedrohungen identifiziert und geeignete Gegenmaßnahmen erarbeitet werden. Dieses Dokument enthält eine plattformunabhängige Sicherheitsanalyse einer Smartphone-basierten Infrastruktur, die als Grundlage für detaillierte Analysen spezieller Systeme herangezogen werden kann. Ziel ist es, bestehende Assets Smartphone-basierter Infrastrukturen zu identifizieren und entsprechende Bedrohungsszenarien zu skizzieren. Dabei wird speziell auf zwei Szenarien eingegangen. Einerseits werden Unternehmens- und Behördeninfrastrukturen betrachtet, in denen Smartphones für einen externen Zugriff auf interne Services verwendet werden. Andererseits wird der Fokus auch auf mögliche M-Government Infrastrukturen gelegt, welche Smartphone-basierte Dienste für Bürgerinnen und Bürger zur Verfügung stellen. Basierend auf den identifizierten Bedrohungsszenarien werden schließlich Schutz- und Sicherheitsfunktionen von Smartphone-Infrastrukturen diskutiert und analysiert.

Inhaltsverzeichnis

Abbildungsverzeichnis

Revision History

Version	Datum	Autor(en)	
0.1	09.03.2011	Peter Teufl	Initialversion
0.2	11.03.2011	Thomas Zefferer	Kommentare, Restrukturierung
0.3	19.03.2011	Thomas Zefferer	Überarbeitung
1.0	31.03.2011	Thomas Zefferer	Finalisierung Analyse möglicher Angriffe
1.1	20.06.2011	Thomas Zefferer	Schutzfunktionen
1.2	30.06.2011	Peter Teufl	Schutzfunktionen Checklists
2.0	01.07.2011	Thomas Zefferer	Finalisierung Gesamtdokument

Abschnitt I: Allgemeiner Überblick

1 Motivation und Definitionen

Diese Dokument stellt eine allgemeine Methode zur Durchführung von Sicherheitsanalysen Smartphone-basierter Infrastrukturen dar. Ziel dieses Dokuments ist es, eine plattformunabhängige Basis für die Durchführung von Sicherheitsanalysen verschiedenster spezifischer Infrastrukturen zu schaffen. In diesem Dokument werden daher ausschließlich plattformübergreifende und allgemein gültige Überlegungen angestellt. Für die Analyse konkreter Infrastrukturen ist in jedem Fall eine Berücksichtigung plattformspezifischer Merkmale nötig.

Im Rahmen dieses Dokuments werden regelmäßig die beiden Begriffe „Smartphone-Plattform“ und „Smartphone-Infrastruktur“ verwendet. Als „Smartphone-Infrastruktur“ wird ein komplexes System bestehend aus einer zentralen IT-Infrastruktur und dezentralen mobilen Geräten wie Smartphones, die über vordefinierte Kanäle auf Daten und Services der zentralen Infrastruktur zugreifen können, bezeichnet. Der Begriff „Smartphone-Plattform“ beschreibt hingegen das mobile Gerät selbst und umfasst dessen Hardware, Betriebssystem und die auf dem Gerät betriebene Software.

Smartphone-Infrastrukturen finden sich bis jetzt hauptsächlich in Unternehmen, sind aber prinzipiell auch für Behörden und den M-Government Bereich denkbar. Während der generelle Aufbau einer Smartphone-Infrastruktur in Unternehmen und im M-Government vergleichbar ist, gibt es in einigen Detailfragen doch signifikante Unterschiede. In Unternehmensinfrastrukturen werden Smartphones üblicherweise verwendet, um Mitarbeiterinnen und Mitarbeitern auch außerhalb des Unternehmens Zugriff auf Dienste und Daten des Unternehmens zu ermöglichen. Im Rahmen von M-Government Diensten greifen in der Regel Bürgerinnen und Bürger mit ihren Smartphones auf diverse von einer Behörde zur Verfügung gestellte Dienste zu[1]. In beiden Fällen bringt der Einsatz von Smartphones aufgrund der umfangreichen Funktionalität dieser Geräte zahlreiche Vorteile, aber auch Sicherheitsrisiken mit sich. Dieses Dokument versucht Einblick in beide Szenarien zu verschaffen und dabei Besonderheiten von Smartphone-basierten M-Government Infrastrukturen und Lösungen speziell hervorzuheben.

Generelles Ziel dieses Dokuments ist es, plattformunabhängige und allgemein gültige Sicherheitsaspekte von Smartphone-Infrastrukturen zu analysieren. Dazu werden zunächst Assets – sicherheitsrelevante und schützenswerte Komponenten – definiert. Für die einzelnen Assets werden daraufhin verschiedene Bedrohungsszenarien skizziert. Aufbauend auf die in diesem Dokument gezeigten Bedrohungsszenarien können in weiterer Folge diverse in Smartphone-Infrastrukturen zur Verfügung stehende Schutzfunktionen, die diesen Bedrohungen entgegenwirken können, diskutiert und analysiert werden.

[1] Denkbar wäre auch ein Szenario, in dem Mitarbeiterinnen und Mitarbeiter einer Behörde über Smartphones auf interne Dienste zugreifen. Dieses Szenario würde jenem eines Unternehmens entsprechen, welches seinen Mitarbeiterinnen und Mitarbeitern einen externen Smartphone-basierten Zugang zu internen Diensten ermöglicht. Die Behörde würde dabei die Rolle des Unternehmens übernehmen.

2 Komponenten einer Smartphone-Infrastruktur

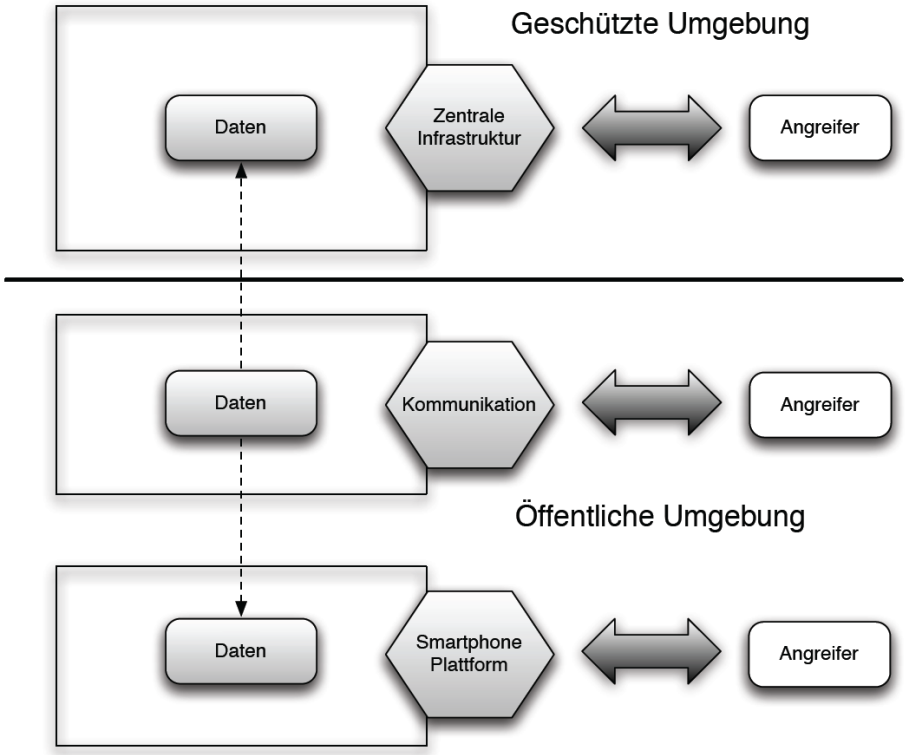

Abbildung 1 – Hauptkomponenten einer Smartphone-Infrastruktur

Abbildung 1 zeigt den Aufbau einer typischen Smartphone-Infrastruktur. Die prinzipielle Struktur ist sowohl bei Smartphone-basierten M-Government Anwendungen als auch bei Smartphone-basierten Unternehmensinfrastrukturen gleich. Die gesamte Infrastruktur lässt sich grundsätzlich in zwei Umgebungen unterteilen.

- **Geschützte Umgebung:** Die geschützte Umgebung umfasst alle Komponenten eines Unternehmens oder einer Behörde, die sich innerhalb einer geschützten (meist zentralen) Infrastruktur befinden. Zum Schutz dieser Infrastruktur und ihrer Komponenten kommen sowohl organisatorische als auch technische Maßnahmen zum Einsatz.

  - **Technische Maßnahmen:** Technische Maßnahmen umfassen physische Vorkehrungen wie Gebäudeschutz, Schließsysteme oder Wachpersonal. Daneben kommen üblicherweise auch IT-Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection Systeme, Netzwerktrennung oder Methoden der sicheren Benutzerauthentifizierung zur Anwendung.

  - **Organisatorische Maßnahmen**: Zu den organisatorischen Maßnahmen zum Schutz sicherer Infrastrukturen gehören allgemeine Verhaltensregeln (Policies), eine entsprechende Schulung des Personals, aber auch Vorschriften in Bezug auf Sicherheitsfunktionen wie zum Beispiel die Vorgabe von Mindestlängen für Passwörter.

- **Öffentliche Umgebung**: In dieser Umgebung können üblicherweise viele der oben genannten technischen und organisatorischen Maßnahmen, die in einer geschützten Umgebung zur Anwendung kommen, nicht mehr verwendet werden. Aufgrund seiner inhärenten Mobilität kann beispielsweise ein Smartphone an nahezu jedem beliebigen Ort eingesetzt werden und ist somit eindeutig der öffentlichen Umgebung zuzuordnen. Für Sicherheitsüberlegungen relevant ist darüber hinaus auch die

Tatsache, dass Smartphones meist sowohl im geschäftlichen als auch im privaten Umfeld verwendet werden. Neben dem Smartphone selbst umfasst die öffentliche Umgebung auch jene Kommunikationswege, die vom Smartphone für die Kommunikation mit Diensten der zentralen Infrastruktur verwendet werden. Diese Kommunikation erfolgt im Allgemeinen über öffentliche Kommunikationspfade wie dem Internet.

Neben dieser Unterteilung in geschützte und öffentliche Umgebungen können für Smartphone-Infrastrukturen außerdem die folgenden drei Hauptbereiche identifiziert werden.

- **Zentrale Infrastruktur:** Die zentrale Infrastruktur befindet sich in der geschützten Umgebung und enthält unter anderem die folgenden Komponenten, die für die Sicherheit des Gesamtsystems im Zusammenhang mit Smartphones von Bedeutung sind.

    - **Daten:** Dabei handelt es sich um alle kritischen Daten eines Unternehmens oder einer Behörde, die für einen Angreifer von Interesse sein könnten. Der Begriff bezieht sich dabei nicht nur auf elektronische Daten, sondern umfasst generell alle Medien, die für die Übertragung oder Speicherung von Daten verwendet werden können. Beispiele dafür sind etwa Dokumente in Papierform oder aufgezeichnete Gespräche, die kritische Informationen beinhalten.

    - **Dienste:** Dienste erlauben den Zugriff auf zentral verfügbare Daten und können sowohl für die interne als auch für eine öffentliche Verwendung zur Verfügung stehen.

    - **Zentrale Zugriffspunkte:** Unabhängig von der jeweiligen Smartphone-Plattform muss für den Zugriff von Smartphones auf interne Services in der Regel ein zentraler Zugriffspunkt bereitgestellt werden, der die Kommunikation zwischen den vorhandenen internen Diensten und Smartphones ermöglicht. Dabei kann es sich beispielsweise um einen VPN Endpunkt, Webserver, oder ähnliches handeln.

- **Kommunikation**: Die Austausch von Daten zwischen der zentralen Infrastruktur und dem Smartphone erfolgt im Allgemeinen über öffentliche Netzwerke wie dem Internet. Bei der speziell bei Unternehmen beliebten Blackberry Architektur kann die Kommunikation auch über dedizierte Kommunikationskanäle erfolgen. Generell können zur Kommunikation sehr unterschiedliche Technologien auf allen Schichten des OSI Referenzmodells zur Anwendung kommen. Auf den hardwarenahen Schichten sind dies zum Beispiel Wireless LANs oder Mobilfunknetzwerke wie GSM oder UMTS. Da diesen Netzwerken grundsätzlich nicht vertraut werden kann, werden auf höheren Abstraktionsschichten oft VPN Protokolle wie IPSEC, L2TP, PPTP oder SSL eingesetzt, die einen sicheren Transport von Daten über unsichere Netzwerke gewährleisten. Der Kommunikationsbereich einer Smartphone-Infrastruktur wird der öffentlichen Umgebung zugeordnet.

- **Smartphone-Plattform:** Die Smartphone-Plattform selbst wird aufgrund deren Mobilität ebenfalls der öffentlichen Umgebung zugeordnet. Für die Smartphone-Plattform können unter anderem die folgenden sicherheitsrelevanten Komponenten identifiziert werden.

    - **Daten:** Die am Smartphone verarbeiteten Daten stehen typischerweise in engem Zusammenhang mit den Daten der zentralen Infrastruktur. Das Smartphone kann beispielsweise für den externen Zugriff auf eine Teilmenge

dieser Daten verwendet werden. Das Smartphone kann aber auch für das Sammeln neuer Daten verwendet werden, die dann über definierte Kommunikationskanäle und Dienste zu den in der zentralen Infrastruktur gespeicherten Daten hinzugefügt werden. Im Rahmen von M-Government Anwendungen können häufig auch vertrauliche und private Daten der Benutzerin oder des Benutzers auf dem Smartphone gespeichert sein.

- **Betriebssystem:** Das Betriebssystem (Operating System) ist das Kernelement eines Smartphones. Es stellt sämtliche Funktionen zur Verfügung, die für den Zugriff auf Daten, das Herstellen von Kommunikationspfaden und das Verwenden von Applikationen benötigt werden.

- **Kommunikationsschnittstellen:** Um Zugriff auf das Internet und auf interne und externe zentrale Services zu bekommen, verwendet ein Smartphone unterschiedliche Kommunikationstechnologien wie zum Beispiel Bluetooth, WLAN, UMTS oder GSM. Über diese Technologien kann ein Zugriff auf Netzwerke hergestellt werden, welche die Kommunikation zwischen Smartphone und zentralem Zugriffspunkt erlauben.

- **Applikationen:** Bei modernen Smartphones gleichen Applikationen in Funktionsumfang und Komplexität zunehmend jenen von Desktop PCs. Dabei gibt es sowohl systemeigene bzw. vorinstallierte Applikationen, als auch Anwendungen, die dem Smartphone über externe Quellen hinzugefügt werden können.

- **Sensoren:** Moderne Smartphones sind in der Regel mit einer Vielzahl von Sensoren ausgestattet. Diese erlauben die Ermittlung diverser Umgebungsparameter und ermöglichen so die Implementierung kontextbezogener Applikationen für Smartphone-Plattformen.

In allen oben genannten Umgebungen und Bereichen spielen Daten eine zentrale Rolle. Wie in Abbildung 1 angedeutet, befinden sich Daten sowohl in der geschützten als auch in der öffentlichen Umgebung. Daten werden in der zentralen Infrastruktur und auf der Smartphone-Plattform gespeichert und verarbeitet, sowie über diverse Kommunikationskanäle übertragen. Ein Angreifer kann theoretisch in allen drei Bereichen versuchen unerlaubten Zugriff auf diese Daten zu erlangen. Entsprechende Bedrohungsszenarien müssen daher in allen Umgebungen und Bereichen berücksichtigt werden.

3 Assets einer Smartphone-Infrastruktur

Im Rahmen dieses Dokuments werden Daten als Kern-Asset betrachtet. Ziel von Angriffen gegen Smartphone-Infrastrukturen ist es meist, Zugriff auf geheime, vertrauliche, private, oder sicherheitskritische Daten zu erlangen[2]. Der Schutz dieser Daten hat demzufolge für Betreiber von Smartphone-Infrastrukturen höchste Priorität. In Unternehmensinfrastrukturen wird es sich bei diesen Daten zumeist um vertrauliche interne Informationen des Unternehmens handeln, die für dieses einen gewissen Wert darstellen. Bei M-Government Infrastrukturen wird hingegen hauptsächlich der Schutz persönlicher Daten von Bürgerinnen und Bürgern von besonderer Wichtigkeit sein. In jedem Fall spielen Daten eine zentrale Rolle

[2] Prinzipiell existieren neben dem unerlaubten Zugriff auf Daten der Smartphone-Infrastruktur auch noch andere Motive für Angriffe. Ein Smartphone, das unter Kontrolle eines Angreifers ist, könnte beispielsweise zum Versenden von Spam missbraucht werden. Aus Sicht eines Betreibers einer Smartphone-basierten M-Government Infrastruktur stellt jedoch der Schutz der personenbezogenen und vertraulichen Daten in der Regel die höchste Priorität dar.

und können daher als übergeordnetes Kern-Asset betrachtet werden, mit dem jedoch weitere untergeordnete Assets in direkter Beziehung stehen.

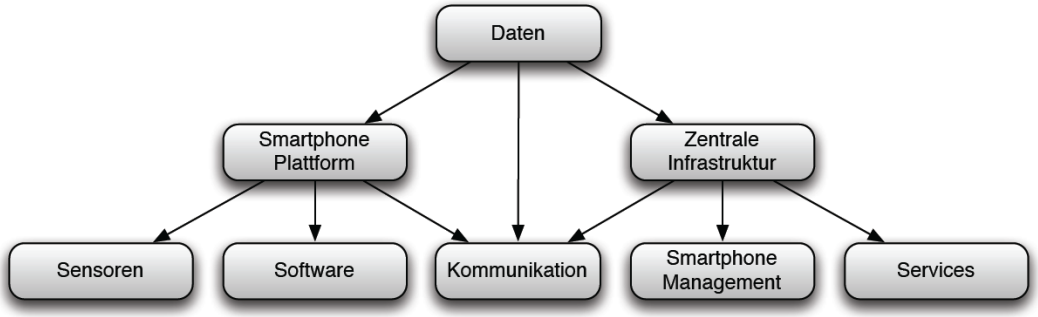

Abbildung 2 – Relevante Komponenten zum Schutz des Kern-Assets „Daten“

Abbildung 2 zeigt, dass zum Schutz des Kern-Assets „Daten“ eine Vielzahl an Komponenten und Faktoren berücksichtigt werden muss. Wie im vorangegangenen Abschnitt erwähnt, müssen Daten prinzipiell in allen drei Hauptbereichen von Smartphone-Infrastrukturen vor unerlaubtem Zugriff durch Angreifer geschützt werden. Das bedeutet, dass Daten sowohl in der zentralen Infrastruktur, als auf der Smartphone-Plattform und während der Kommunikation zwischen zentraler Infrastruktur und Smartphone-Plattform geschützt werden müssen. Während ein entsprechender Schutz in der geschützten Umgebung der zentralen Infrastruktur vergleichsweise einfach zu gewährleisten ist, stellt die Sicherstellung eines adäquaten Schutzes in der öffentlichen Umgebung eine verhältnismäßig größere Herausforderung dar.

Die drei Hauptbereiche lassen sich wie in Abbildung 2 dargestellt in weitere Subkomponenten unterteilen. Für den Bereich „Smartphone“ sind beispielsweise sowohl verfügbare Sensoren, als auch die auf dem Gerät betriebene Software für den Schutz des Kern-Assets „Daten“ von Relevanz. Die in Abbildung 2 gezeigte Hierarchie kann beliebig verfeinert werden um spezielle Aspekte des Gesamtsystems herauszustreichen. Beispielsweise kann auf die Gefahren, die ein in das Smartphone integrierter Kompass mit sich bringt detailliert eingegangen werden, indem das Asset Sensoren weiter differenziert wird.

Die in Abbildung 2 dargestellte Hierarchie soll die Vielzahl an Assets andeuten, die im Zuge einer Sicherheitsüberprüfung einer Smartphone-Infrastruktur berücksichtigt werden muss. Jedes einzelne Asset stellt ein potentielles Angriffsziel dar und muss durch geeignete Maßnahmen entsprechend geschützt werden. Allerdings sind nicht alle Komponenten für alle Smartphone-basierten Infrastrukturen gleich relevant. Beispielsweise kommt der Komponente „Smartphone Management“ in M-Government Lösungen eine vergleichsweise geringe Bedeutung zu[3] während diese in Unternehmensinfrastrukturen eine zentrale Rolle spielen kann. Verschiedene Bedrohungsszenarien der einzelnen Komponenten werden in Abschnitt II dieses Dokuments näher erläutert.

4 Sicherheitsrelevante Aspekte von Smartphones

Die Risiken der mobilen Verwendung von Computern sind hinlänglich bekannt. Mit Laptops, Netbooks und Tablet-PCs gibt es bereits seit längerer Zeit Geräte, die aufgrund ihrer mobilen Verwendbarkeit ein leichteres Ziel für Angriffe sind. Viele der auf diesen Geräten auftretenden Gefahren sind bekannt und können üblicherweise mit organisatorischen und technischen Maßnahmen ausreichend entschärft werden.

[3] Details zu dieser Komponente werden in den nachfolgenden Abschnitten noch näher erläutert.

Obwohl auch Smartphones zur Klasse der mobile Geräte gehören, gilt es bei ihrer Verwendung im Rahmen komplexer Infrastrukturen und Diensten neue Aspekte zu beachten, die sowohl die Verstärkung bereits bekannter Gefahren, als auch das Auftreten neuer Gefahren betreffen. Im Folgenden werden einige Aspekte von Smartphones beleuchtet, die eine sichere Verwendung dieser Geräte erschweren und Angreifern neue Möglichkeiten eröffnen.

- **Umgebung und Verwendung:** Aufgrund der Größe von herkömmlichen Mobiltelefonen und Smartphones ist eine Verwendung dieser Geräte auch in Umgebungen möglich, die für Laptops nicht oder nur eingeschränkt geeignet sind. Aufgrund dieser neuen Umgebungen und der vielfältigen Technologien, die moderne Smartphones unterstützen, ergeben sich sowohl für den geschäftlichen als auch den privaten Bereich laufend neue Anwendungsgebiete. Diese reichen von herkömmlicher Datenverarbeitung, über die Verwendung des Smartphones als Navigationsgerät an Land und auf Wasser, bis hin zum Einsatz von Augmented Reality Anwendungen.

- **Vermischung von privater und geschäftlicher Verwendung:** Ein wichtiger Punkt in Bezug auf die Sicherheit von kritischen Daten auf einem Smartphone ist die Vermischung von privaten und geschäftlichen Bereichen. Diese Überschneidung findet sich zwar prinzipiell auch bei Laptops, geht bei Smartphones aber üblicherweise noch viel tiefer. Smartphones, die beispielsweise von Unternehmen an Mitarbeiterinnen und Mitarbeiter weitergegeben werden, werden in der Regel sowohl privat als auch geschäftlich verwendet. Da das Smartphone im privaten Bereich im Rahmen von Urlauben, sportlichen Aktivitäten oder Lokalaufenthalten in anderen Umgebungen und für andere Zwecke wie Spiele, Multimediaanwendungen oder Navigation verwendet wird, ergeben sich hier neue Bedrohungen, die bei Laptops und bei herkömmlichen Mobiltelefonen aufgrund der eingeschränkten Funktionalität nicht auftreten. Die Problematik betrifft auch Smartphone-basierte M-Government Lösungen. Durch die private Verwendung von Smartphones steigt die Gefahr einer Infizierung des Geräts mit Schadsoftware. Diese kann wiederum die Sicherheit der durch eine M-Government Applikation verarbeiteten Daten kompromittieren.

- **Verwendung neuer Technologien:** Aufgrund der umfassenden technologischen Fortschritte bieten Smartphones heutzutage Features, die vor einigen Jahren nur auf normalen PCs vorhanden waren. Dazu gehören unter anderem hohe Rechenleistungen für Berechnungen und visuelle Darstellungen, hohe Speicherdichten bei RAMs und Flash-Speichern, sowie Breitbandverbindungen zum Internet. Zusätzlich werden Technologien integriert, die bisher typischerweise nur in peripheren oder dedizierten Geräten vorhanden waren. Dazu gehören beispielsweise:

    - Permanente Internetverbindung
    - Positionsbestimmung via GPS, Mobilfunkzellen und WLAN
    - Kameras für das Aufnehmen von HD Videos und Fotos
    - Beschleunigungssensoren, Kompass und Trägheitssensoren um die aktuelle Lage des Smartphones im Raum zu bestimmen
    - Vielfältige Kommunikationsmöglichkeiten über Mobilfunkstandards (UMTS, GSM, LTE), WLAN Standards, Bluetooth oder NFC
    - Umfangreiche Softwareangebote

- **Kombination unterschiedlicher Technologien:** Eine Kombination der herkömmlichen Telefonfunktion mit den oben genannten Technologien aus dem PC-Bereich oder mit Neuentwicklungen wie NFC ergibt zahlreiche neue Möglichkeiten aber auch Bedrohungen. Beispielsweise erlaubt es die permanente Internetverbindung in Kombination mit der Möglichkeit einer exakten Positionsbestimmung, Bewegungen von Benutzerinnen und Benutzern bis auf den Meter genau zu verfolgen. Außerdem können nun direkte Angriffe auf das Telefon und die über dieses Gerät kommunizierten Daten wie Telefongespräche oder Textnachrichten durchgeführt werden.

- **Hoch entwickelte Betriebssysteme:** Um all diese Technologien verwenden zu können und Benutzerinnen und Benutzern eine benutzerfreundliche Oberfläche zu bieten, muss ein hochentwickeltes Betriebssystem verwendet werden. Bisher waren Mobiltelefonbetriebssysteme einfach aufgebaut und implementierten nur ein Mindestmaß an Funktionalität. Aktuelle Smartphones verwenden hingegen höher entwickelte Betriebssysteme, die sehr oft auf PC-Systemen basieren. So basiert beispielsweise das Android Betriebssystem auf Linux, oder Apples iOS auf OS X. Aufgrund der Komplexität und Ähnlichkeit zu herkömmlichen Betriebssystemen und der Unterstützung der zuvor genannten Technologien ergeben sich einerseits Angriffe, die bisher nur von PC Systemen bekannt waren, und außerdem neue Angriffsszenarien, die erst aufgrund der neuen Technologien möglich wurden.

- **Sensoren:** Die unterschiedlichen in aktuellen Smartphones integrierten Sensoren generieren laufend neue Daten, die stark in die Privatsphäre eines Benutzers eingreifen und private Informationen wie Positionsdaten, Telefongespräche, visuelle Daten der Kamera oder akustische Daten des Mikrophons aufzeichnen. Da diese Daten sowohl im privaten als auch im geschäftlichen Bereich für einen Angreifer von Bedeutung sein können, ergeben sich auch hier potentiell neue Bedrohungen.

5 Angriffsarten

Im Zuge der in diesem Dokument angestellten Überlegungen wird von einem Angreifer ausgegangen, der Zugriff auf kritische Daten der Smartphone-Infrastruktur erlangen möchte. Im Rahmen einer Unternehmensinfrastruktur kann es sich dabei beispielsweise um vertrauliche Daten des Unternehmens handeln, die in den zentralen Systemen der Infrastruktur gespeichert sind. Bei M-Government Diensten werden in der Regel persönliche Daten von Bürgerinnen und Bürgern, die beispielsweise dezentral auf Smartphones hinterlegt sind, für Angreifer von besonderem Interesse sein. Um welche Daten es sich konkret handelt und ob diese ausgelesen, gelöscht oder verändert werden, ist dabei sekundär und hängt lediglich von der Art des Angriffs und den Zielen des Angreifers ab.

Prinzipiell steht einem Angreifer in Smartphone-basierten Infrastrukturen eine Vielzahl an Möglichkeiten zur Verfügung. Diese Methoden reichen vom Ausnützen von Sicherheitslücken in diversen Komponenten, über das Erlangen von physischem Zugriff auf sensible Daten (z.B. durch visuelles oder akustisches Aufzeichnen von Dokumente oder Gesprächen), bis hin zu sozialen Angriffen, die direkt auf das Personal und dessen soziales Umfeld abzielen.

Generell hängt die Erfolgswahrscheinlichkeit neben den vorhanden Schwachstellen auch vom betriebenen Aufwand ab. Ein Angreifer mit ausreichenden Ressourcen wird auch bei kleinen Schwachstellen in der Lage sein diese auszunützen und einen erfolgreichen Angriff durchführen können.

Im Rahmen von Angriffen auf Smartphone-Infrastrukturen können Smartphones prinzipiell zwei verschiedene Rollen einnehmen:

- **Angriffe auf das Smartphone:** In diesem Fall ist das Smartphone selbst Ziel eines Angriffs. Dieser Angriff kann es auf die Daten des Smartphones abgesehen haben, oder das Smartphone nutzen, um Zugriff auf weitere Daten, die in zentralen Komponenten gespeichert sind, zu erlangen.

- **Angriffe vom Smartphone:** Aufgrund der umfassenden Funktionalität moderner Smartphones können diese Geräte auch selbst für Angriffe auf zentrale Komponenten von Unternehmen oder Behörden verwendet werden. Folgende Szenarien sind dabei prinzipiell denkbar:

    - **Spionage:** Sensoren wie Kamera und Mikrophon ermöglichen es einem Angreifer unerlaubt Gespräche aufzuzeichnen oder kritische Daten zu fotografieren. Aufgrund ihrer Mobilität und Kommunikationsmöglichkeiten können Smartphones sehr leicht an kritischen Stellen positioniert werden und aufgezeichnete Daten an Dritte weiterleiten.

    - **Angriffe auf das Netzwerk:** Smartphones mit entsprechender Software können verwendet werden, um Daten über Netzwerke zu sammeln. Bei schlechter Absicherung eines WLANs kann das Smartphone dazu benutzt werden weitere Informationen über das dahinterliegende Netzwerk zu sammeln und diese Informationen für weitere Angriffe zu nutzen.

6 Gegenmaßnahmen

Im Gegensatz zur Flexibilität und Adaptionsfähigkeit eines Angreifers sind Gegenmaßnahmen bisher eher statischer Natur. Dabei kann im Prinzip zwischen zwei Kategorien unterschieden werden:

- **Technische Maßnahmen:** Dabei handelt es sich um Maßnahmen, die mit Hilfe technischer Vorkehrungen Angriffe verhindern. Dies kann von physischen Maßnahmen wie einem gesicherten Schließsystem für Türen, bis hin zu der Anwendung asymmetrischer kryptographischer Verfahren für das Verschlüsseln sicherheitskritischer Daten reichen.

- **Organisatorische Maßnahmen:** Hierbei handelt es sich um Maßnahmen, die nicht durch technische Vorkehrungen umgesetzt werden können. Vielmehr werden diese Maßnahmen durch Vorschriften, Hinweise, o.ä. definiert und müssen von den betroffenen Personen umgesetzt werden. Ein Beispiel für eine derartige Maßnahme wäre eine Vorschrift, die es Benutzerinnen und Benutzern verbietet das Smartphone in bestimmten Bereichen einzusetzen oder unbeaufsichtigt liegen zu lassen. Während derartige Maßnahmen in Unternehmen relativ einfach umzusetzen sind, ist dies im Rahmen von M-Government Diensten schwerer möglich. Im Fall von M-Government sind Smartphones im alleinigen Besitz der Bürgerin oder des Bürgers. Die Behörde hat daher diesbezüglich wenig Handhabe und kann die Bürgerin oder den Bürger nicht zwingen entsprechende über Policies definierte Sicherheitsvorschriften einzuhalten.

Prinzipiell sind zur Wahrung der Sicherheit technische Maßnahmen besser geeignet, da sie ihre Sicherheitsfunktion ohne aktives Zutun einer Person immer gleich erfüllen. Die Wirksamkeit organisatorischer Maßnahmen hängt hingegen von vielen Komponenten ab. So ist für viele dieser Maßnahmen eine entsprechende Schulung von Benutzerinnen und Benutzern eine wichtige Voraussetzung. Ein weiteres relevantes Kriterium ist die Tatsache,

dass organisatorische Maßnahmen in der Regel das aktive Mitwirken von Personen voraussetzen. In Anbetracht dieser Umstände muss die Komplexität solcher Maßnahmen gering gehalten werden, da sonst deren Durchführung zu kompliziert und eine entsprechende Schulung zu aufwändig wird.

Sowohl bei technischen als auch bei organisatorischen Maßnahmen können Schwachstellen auftreten, die die Funktion der jeweiligen Sicherheitsmaßnahme einschränken, aufheben, oder es Angreifern ermöglichen sie zu umgehen. Beispiele für solche Schwachstellen sind:

- **Fehler in der Sicherheitsfunktion:** Ein unsicherer Verschlüsselungsalgorithmus oder eine fehlerhafte organisatorische Richtlinie kann beispielsweise die eingesetzte Maßnahme unwirksam machen.

- **Fehlende Sicherheitsfunktion:** Beispielsweise könnte die Datenverschlüsselung auf einem mobilen Gerät, auf dem kritische Daten gespeichert sind, deaktiviert sein.

- **Falsche Anwendung:** Beispielsweise könnte die Verwendung einer zu einfachen Passwort Policy für kritische Daten die eingesetzte Maßnahme unwirksam machen.

- **Umgehen von Sicherheitsfunktionen**: Das sichere Schließsystem einer Tür kann zum Beispiel leicht umgangen werden, falls eine zweite nicht verschlossene Tür zur Verfügung steht.

- **Deaktivieren einer Sicherheitsfunktion**: Das entfernte Löschen der Daten eines gestohlenen Smartphones lässt sich zum Beispiel durch das Entfernen der SIM Karte verhindern.

Schwachstellen jeglicher Art können von Angreifern erkannt und ausgenützt werden. Der Aufwand und die Wahrscheinlichkeit für das erfolgreiche Erkennen und Ausnützen von Schwachstellen hängen dabei prinzipiell von deren Art ab. Je mehr finanzielle oder personelle Ressourcen einem Angreifer zur Verfügung stehen, desto wahrscheinlicher ist es, dass Schwachstellen gefunden und ausgenutzt werden können. Die Bereitschaft Ressourcen zur Verfügung zu stellen hängt wiederum sehr stark davon ab, wie wertvoll das Ziel für den Angreifer ist. Ein aktuelles Beispiel verdeutlicht dies: Für den Angriff auf iranische Atomanlagen wurde unter dem Einsatz von beträchtlichen Ressourcen der Computerwurm Stuxnet entwickelt, der gezielt SCADA[4] Systeme der Firma Siemens angriff und so erheblichen Schaden an iranischen Uran-Anreicherungsanlagen anrichtete. Analysen zeigten, dass es sich bei Stuxnet um hochqualitative Schadsoftware handelte, für deren Erstellung erhebliche Ressourcen notwendig gewesen sein mussten.

7 Methodologie

Ziel dieses Dokuments ist es, ein Werkzeug zur systematischen Evaluierung möglicher Bedrohungen von Smartphone-Infrastrukturen zu schaffen. Dabei werden sowohl Smartphone-basierte Unternehmensinfrastrukturen, als auch Smartphone-basierte M-Government Dienste betrachtet. Das Dokument identifiziert zunächst vorhandene Assets und zeigt mögliche Bedrohungsszenarien auf. Dabei wird versucht, potentielle Probleme unabhängig von System und Plattform zu identifizieren. Für weitere spezifische Analysen bestimmter Plattformen kann dieses Dokument dadurch flexibel als gemeinsame Grundlage verwendet werden.

Das Dokument ist wie folgt strukturiert. Nachdem in Abschnitt I ein allgemeiner Überblick über Möglichkeiten und Herausforderungen von Smartphone-Infrastrukturen gegeben wurde,

[4] SCADA: Supervisory Control and Data Aquisition

werden in Abschnitt II verschiedene Assets definiert und für diese Assets mögliche Bedrohungen identifiziert. Die Auflistung der einzelnen Assets folgt dabei prinzipiell der in Abbildung 2 dargestellten Hierarchie. Aufbauend auf diesem Dokument können dann in weiterer Folge diverse Schutzfunkionen zur Abwehr der gezeigten Bedrohungsszenarien identifiziert und evaluiert werden. Verschiedene Sicherheits- und Schutzfunktionen, mit denen den identifizierten Gefahren begegnet werden kann, werden in Abschnitt III vorgestellt. Neben einer Beschreibung der einzelnen Schutzfunktionen wird für jede Funktion zudem eine Checkliste angegeben, über die diese Schutzfunktion auf einer speziellen Smartphone-Plattform evaluiert werden kann.

Abschnitt II: Assets und Bedrohungen

In diesem Abschnitt werden die einzelnen Assets von Smartphone-Infrastrukturen identifiziert und mögliche Bedrohungen und Angriffsszenarien skizziert. Anhand der in Abbildung 2 dargestellten Asset-Hierarchie werden ausgehend vom Kern-Asset „Daten“ sämtliche Komponenten, die zum Schutz der Smartphone-Infrastruktur gegen Angriffe von außen von Relevanz sind, eingehend analysiert.

Die Relevanz der einzelnen Komponenten hängt in einzelnen Fällen auch vom jeweiligen Anwendungsszenario ab. Für Smartphone-basierte Unternehmensinfrastrukturen sind teilweise andere Komponenten und Assets relevant als für Smartphone-basierte M-Government Lösungen. Auf diesbezügliche Spezifika wird bei der Beschreibung der einzelnen Komponenten gesondert eingegangen.

1 Daten

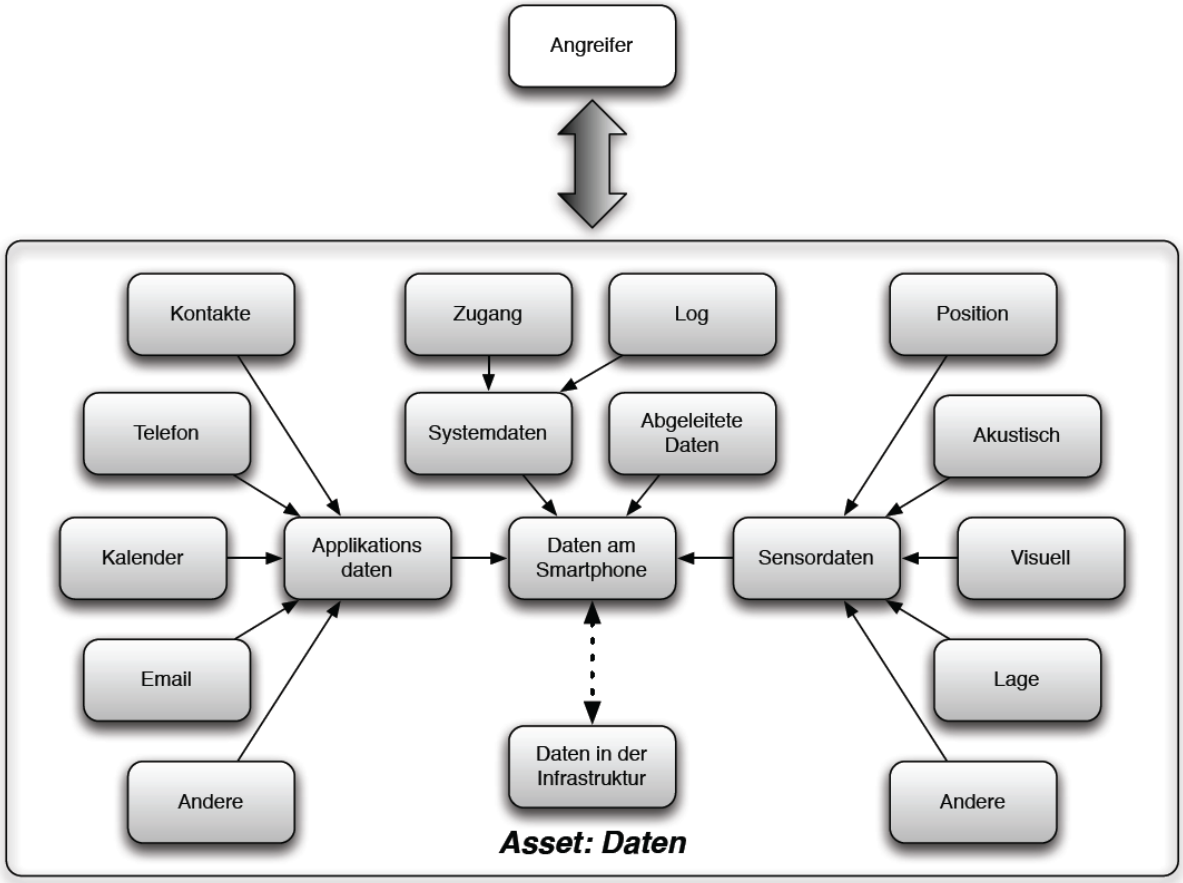

Abbildung 3 – Differenzierte Betrachtung des Kern-Assets „Daten“

Daten sind das Kern-Asset jeder Smartphone-Infrastruktur. Der Schutz dieser Daten, die in der Smartphone-Infrastruktur erstellt, gespeichert, verarbeitet und verbreitet werden, ist daher von höchster Priorität. Abbildung 3 zeigt eine differenziertere Darstellung des Kern-Assets „Daten“, wobei der Fokus auf jene Daten gelegt wird, die auf der Smartphone-Plattform selbst gespeichert oder verarbeitet werden. Grund dafür ist die Tatsache, dass sich Daten am Smartphone üblicherweise in der öffentlichen Umgebung einer Smartphone-Infrastruktur befinden, während Daten in der zentralen Infrastruktur bereits durch die geschützte Umgebung weniger anfällig für diverse Angriffe von außen sind. Die Daten am Smartphone stehen jedoch natürlich oft in engem Zusammenhang mit den Daten, die in der

zentralen Infrastruktur verwaltet werden. Für einen Schutz aller Daten ist daher ein umfassender Schutz der gesamten Smartphone-Infrastruktur unbedingt notwendig.

Wie in Abbildung 3 dargestellt, kann bei Daten am Smartphone prinzipiell zwischen Applikationsdaten, Sensordaten, Systemdaten und abgeleiteten Daten unterschieden werden. Diesen Hauptkategorien können wiederum unterschiedliche Arten von Daten zugeordnet werden. Im Folgenden werden die verschiedenen auf einem Smartphone verfügbaren Daten als Assets (A) identifiziert und diesen mögliche Bedrohungen (B) und Angriffsszenarien zugeordnet.

A1	***Daten:*** Daten sind das Kern-Asset jeder Smartphone-Infrastruktur. Aufgrund der Vielfältigkeit der in einer Smartphone-Infrastruktur vorkommenden Daten wird zwischen folgenden Kategorien unterschieden: • Daten, die sich nur am Smartphone befinden, wie zum Beispiel persönliche Daten der Benutzerin oder des Benutzers, Eingaben der Benutzerin oder des Benutzers, Daten der Smartphone-Sensoren, Systemdaten, etc. • Daten, die lokal am Smartphone gespeichert werden und eine Untermenge der Daten in der zentralen Infrastruktur darstellen. Dazu gehören u.a. Emails oder Daten, die über interne Services der Infrastruktur dem Smartphone zur Verfügung gestellt werden. Diese Daten spielen vor allem in Smartphone-basierten Unternehmensinfrastrukturen eine wichtige Rolle. • Daten, die gerade über einen Kommunikationskanal zwischen Smartphone und zentraler Infrastruktur transferiert werden. • Daten, die zum Beispiel im Zuge eines Prozessablaufs temporär verwendet werden. • Daten, die sich ausschließlich in der zentralen Infrastruktur befinden.
B1	***Zugriff auf Daten:*** Ein Angreifer erhält unberechtigten Zugriff auf Daten der Smartphone-Infrastruktur. Mit Zugriff wird hier die Möglichkeit des Auslesens, Änderns oder Hinzufügens von Daten bezeichnet.

A1.1	***Applikationsdaten:*** Dabei handelt es sich um Daten, die von Applikationen abgerufen oder erstellt werden. Der Begriff umfasst Daten von beliebigen Applikationen, unabhängig davon, ob diese für den Zugriff auf Unternehmensdaten oder im Rahmen der Verwendung des Smartphones für M-Government Applikationen eine Rolle spielen. Aufgrund des breiten Spektrums an Applikationsdaten werden einige spezielle Applikationsdaten im Folgenden noch exemplarisch als eigene Assets definiert.
B1.1	***Zugriff auf Applikationsdaten:*** Applikationsdaten von M-Government Applikationen oder von Applikationen, die in einem Unternehmen verwendet werden, können für einen Angreifer von direktem Interesse sein oder als Basis für weitere Angriffe dienen.

A1.1.1	***Kontakte:*** Diese Daten lassen Rückschlüsse auf das geschäftliche und private soziale Umfeld der Benutzerin oder des Benutzers zu.
B1.1.1	***Zugriff auf Kontaktdaten:*** Ein Angreifer kann Informationen über das soziale Umfeld der Benutzerin oder des Benutzers erhalten. Dadurch können Kontaktdaten von anderen Personen extrahiert werden, die unter Umständen für weitere Angriffe verwendet werden können. Ein Angreifer mit Hintergrundwissen über soziale Beziehungen kann dieses Wissen ausnutzen, um andere Personen im Namen einer Benutzerin oder eines Benutzers zu kontaktieren und somit Zugriff auf weitere Informationen und Dienste zu erhalten. Beispiele für derartige Informationen sind: • Private oder geschäftliche Beziehungen • Telefonnummern • Emailadressen

A1.1.2	***Telefondaten:*** Dieser Begriff umfasst Daten, die mit der Telefonfunktionalität des Smartphones im Zusammenhang stehen. Dazu gehören unter anderem: • SMS-Nachrichten • MMS-Nachrichten • Anruflisten • Gesprächsdaten von Telefongesprächen
B1.1.2	***Zugriff auf Telefondaten:*** Ein Angreifer kann Zugriff auf Informationen in SMS oder MMS Nachrichten erhalten. Zusätzlich können anhand von Anruflisten Rückschlüsse über häufige Kontakte zu anderen Personen gezogen werden. Hierbei muss beachtet werden, dass Anruflisten im Allgemeinen getrennt von Kontaktdaten behandelt werden. Daher bewirkt das Löschen der Kontaktdaten typischerweise nicht das automatische Löschen der Anruflisten. Es können in diesem Fall zwar keine Namen mehr ausgelesen werden, die Telefonnummern der Kontakte in den Anruflisten stehen jedoch weiterhin zur Verfügung.

A1.1.3	***Kalender:*** Hierbei handelt es sich um die Daten, die in Terminkalendern am Smartphone gespeichert werden.
B1.1.3	***Zugriff auf Kalenderdaten:*** Ein Angreifer kann Informationen über den voraussichtlichen Aufenthaltsort von Benutzerinnen und Benutzern zu einem bestimmten Zeitpunkt erhalten. Zusätzlich können aus Kalenderdaten Informationen über das soziale Netzwerk des Benutzers extrahiert werden.

A1.1.4	***Email:*** Dieses Asset umfasst alle Emails von Benutzerinnen und Benutzern, die für eine mobile Verwendung zur Verfügung stehen. Typischerweise wird ein Großteil der Kommunikation in einem Unternehmen via Emails durchgeführt.

	Daher kann davon ausgegangen werden, dass Emails kritische Informationen unterschiedlicher Natur enthalten und Rückschlüsse auf wichtige interne Zusammenhänge zulassen. Es handelt sich daher um ein sehr kritisches Asset innerhalb einer Unternehmensinfrastruktur. Für M-Government Infrastrukturen ist dieses Asset dann von Bedeutung, wenn im Rahmen von M-Government Diensten kritische Daten per Email übertragen werden.
B1.1.4.a	***Zugriff auf kritische Daten in Emails:*** Ein Angreifer kann Zugriff auf kritische Informationen, Dokumente oder andere Daten erhalten, die per Email versendet werden. Beispiele für solche Daten sind: • *Persönliche Daten:* Die umfasst jene Daten, die im Rahmen von M-Government Anwendungen verarbeitet oder übertragen werden. • *Finanzielle Daten eines Unternehmens*: Dazu gehören Bilanzen, Auftragsverrechnung, o.ä. • *Personaldaten*: Dies umfasst Adressdaten (und somit auch private Daten), Funktionen im Unternehmen, Gehaltslisten, etc. • *Daten über Aufträge*: Als Beispiel können hier finanzielle Details, Angebote oder Details zu aktuellen Vergaben genannt werden. • *Daten über Kunden oder Geschäftspartner*: Dazu gehören finanzielle Beziehungen, Aufträge, o.ä. • *Detaillierte Informationen über Produkte*: Die umfasst unter anderem Source Codes oder interne Details, die aufgrund der Wettbewerbssituation nicht nach außen gelangen sollten. • *Daten über geplante kurzfristige und langfristige Entwicklungen im Unternehmen*: Dazu gehören Strategiepapiere, Personalpläne, Aufträge oder auch Kundenbeziehungen.
B1.1.4.b	***Zugriff auf Zugangsdaten:*** Ein Angreifer kann Zugriff auf etwaige Zugangsdaten (z.B. zu webbasierten M-Government Anwendungen) erhalten, die per Email versendet wurden: • *Benutzernamen/Passwörter*: Oft werden Benutzernamen und Passwörter von diversen Zugängen per Email versendet. Dies gilt sowohl für automatische Nachrichten von Konten, bei denen das Passwort vergessen wurde und die zurücksetzt werden sollen, als auch für das Weiterleiten von Zugangsdaten im Rahmen der Systemwartung. • *Rücksetzen von Konten*: Viele Dienste erlauben es, ein Konto über Informationen, die per Email versendet werden, zurückzusetzen. Dabei kann prinzipiell zwischen zwei Verfahren unterschieden werden:

	° *Senden von Passwörtern im Klartext*: In diesem Fall wird das Passwort eines Kontos im Klartext an die Email Empfängerin oder den Email Empfänger übermittelt. Dabei können mehrere Probleme auftreten: 1. Wird ein Email mit solchen Informationen archiviert, kann ein Angreifer unter Umständen das Passwort auslesen und somit Zugang zu dem Konto erhalten. 2. Da von Benutzerinnen und Benutzern oft dieselben Passwörter für mehrere Konten verwendet werden, kann ein Angreifer dadurch auch Zugriff zu anderen Konten der Benutzerin oder des Benutzers enthalten. Aufgrund der Mehrfachverwendung steht zumindest der Zugriff auf andere Konten offen. Darüber hinaus kann der Angreifer ein durch ihn zurückgesetztes Konto mit einem korrekten Passwort versehen, sodass Benutzerinnen oder Benutzer keinen Verdacht schöpfen. ° *Senden von Informationen*: Vielfach werden URLs gesendet, die einmalig zum Zurücksetzen eines Kontos verwendet werden können. Hat ein Angreifer Zugang zu einem Email Konto, kann er sich solche Rücksetz-Emails zusenden lassen, um damit Zugang zu anderen Konten zu erhalten. Hierbei müssen jedoch die Passwörter geändert werden, was unter Umständen Aufmerksamkeit erregt. Diese Aufmerksamkeit kann der Angreifer umgehen indem er das attackierte Mailkonto nach Klartextpasswörtern durchsucht.
B1.1.4.c	***Kommunikationsnetzwerk einer Person:*** Ähnlich wie bei Kontaktdaten können durch Daten in Emails Informationen über das soziale Netzwerk von Benutzerinnen und Benutzern extrahiert werden. Dies umfasst sowohl private Aspekte wie Urlaub, Freizeit oder Freunde, als auch geschäftliche Angelegenheiten. Im Unterschied zu den Kontaktdaten befinden sich in Emails darüber hinaus noch eine Vielzahl weiterer Details, die einem Angreifer eine viel genauere Analyse der sozialen Beziehung von Benutzerinnen und Benutzern ermöglichen.
B1.1.4.d	***Funktion einer Person im Unternehmen:*** Ein Angreifer kann anhand der Sender, Empfänger und Textinhalte feststellen, welche Aufgaben und Funktionen die Person inne hat und wie sie in die Unternehmenshierarchie eingeordnet ist.

A1.1.5	***Daten sozialer Netzwerke:*** Smartphones bieten Benutzerinnen und Benutzern diverse Möglichkeiten um über eigene Applikationen mit sozialen Netzwerken zu kommunizieren. Diese Applikationen haben daher prinzipiell Zugriff auf

	sämtliche Informationen, die in diesem sozialen Netzwerk über die Benutzerin oder den Benutzer gespeichert sind.
B1.1.5	***Zugriff auf Daten sozialer Netzwerke:*** Ein Angreifer kann über Applikationen zum Zugriff auf soziale Netzwerke verschiedenste persönliche Daten von Benutzerinnen und Benutzern extrahieren und so auf das soziales Umfeld rückschließen.

A1.1.6	***Navigationsdaten:*** Auf Smartphones sind in der Regel Navigationsdaten gespeichert. Dies beinhaltet beispielsweise eine Liste von Orten, die die Benutzerin oder der Benutzer unter Verwendung von Navigationssoftware aufgesucht hat, oder die die Benutzerin oder der Benutzer regelmäßig aufsucht.
B1.1.6	***Zugriff auf Navigationsdaten:*** Durch einen Zugriff auf Navigationsdaten kann ein Angreifer Rückschlüsse auf bereits besuchte oder regelmäßig aufgesuchte Aufenthaltsorte von Benutzerinnen und Benutzern ziehen.

A1.2	**Systemdaten*:*** Dabei handelt es sich um Daten, die vom System des Smartphones erstellt und für dessen Funktionalität benötigt werden. Beispiele dafür sind: • Logdateien, die für das Protokollieren von Ereignissen verwendet werden. Dazu gehören beispielsweise Listen aufgerufener Websites oder gestarteter Programme. Die verfügbaren Systemdaten hängen stark von der jeweiligen Smartphone-Plattform ab und können weite Bereiche abdecken. • Buffer, die Tastatureingaben oder andere Daten zwischenspeichern, um zum Beispiel eine Autokorrekturfunktion für Wörter anzubieten, die nicht in den mitgelieferten Wörterbüchern enthalten sind. • Schlüsselspeicher, die Zugangsdaten wie Benutzernamen und Passwörter speichern und von Applikationen für das automatische Einloggen bei verschiedenen Services verwendet werden.
B1.2.a	***Zugriff auf Zugangsdaten:*** Kann ein Angreifer auf diese Daten zugreifen, können diese unter Umständen für das Einloggen bei gespeicherten Services (z.B. M-Government Dienste) verwendet werden. Ein aktuelles Beispiel für diese Bedrohung ist ein bekannter Angriff auf Apples iOS[5].
B1.2.b	***Zugriff auf Logs:*** Diese Daten müssen unbedingt berücksichtigt werden, da sie unter Umständen einem Angreifer Seitenkanäle zu Informationen eröffnen, zu denen er sonst nicht direkt Zugriff hätte. Über Log-Daten erhält der Angreifer möglicherweise Zugriff auf Debug-Meldungen von Applikationen, die kritische Daten enthalten. M-Government Applikationen am Smartphone könnten

5 http://www.pcworld.com/businesscenter/article/219245/iphone_attack_reveals_passwords_in_six_minutes.html

	beispielsweise benutzerbezogene Daten in Log-Dateien schreiben, auf die ein Angreifer dann Zugriff hätte.

A1.3	***Abgeleitete Daten:*** Auch über abgeleitete Daten ist es möglich über Seitenkanäle Informationen zu sicherheitskritischen Daten zu erhalten. Da die Existenz möglicher Seitenkanäle von sehr vielen Faktoren abhängt, sollen hier nur einige Beispiele für mögliche Seitenkanäle auf Smartphone-Plattformen gegeben werden: • *Aufgerufene Websites*: Hat ein Angreifer keinen direkten Zugriff auf den Netzwerkverkehr des Smartphones, so gibt es unter Umständen Log-Dateien, die diese Daten enthalten. • *Positionen*: Ähnlich zum Verlauf besuchter Websites speichern diverse Navigationsapplikationen einen Verlauf besuchter Lokationen. Über diese Daten sind Rückschlüsse auf vergangene Aufenthaltsorte von Benutzerinnen und Benutzern möglich.
B1.3	***Zugriff auf abgeleitete Daten:*** Kann ein Angreifer keinen direkten Zugriff auf die gewünschten Daten erhalten, so ist es ihm vielleicht möglich, indirekt über Seitenkanäle die gewünschten Informationen zu erhalten. Wenn ein Angreifer beispielsweise keinen direkten Zugriff auf die aktuelle Position der Benutzerin oder des Benutzers hat, kann er unter Umständen durch Auslesen der eindeutigen Identifikationsnummer der aktuellen Mobilfunkzelle und Abfragen von externen Datenbanken die Position feststellen.

A1.4	***Sensordaten:*** Moderne Smartphones sind mit einer Vielzahl an Sensoren ausgestattet, die unter anderem die Aufzeichnung visueller und akustischer Daten oder eine exakte Positions- und Lagebestimmung des Geräts ermöglichen. Aufgrund der Vielzahl und Diversität an Informationen, die durch Sensoren gesammelt werden können, stellen diese ein besonders relevantes Asset dar. Auf Möglichkeiten einzelner Sensoren wird daher in Sektion 2.2 dieses Abschnitts näher eingegangen.
B1.4	***Zugriff auf Sensordaten:*** Ein Angreifer kann auf Daten, die durch Sensoren aufgezeichnet und am Smartphone gespeichert wurden, zugreifen. Bedrohungen, die sich durch Zugriff auf verschiedene Sensordaten ergeben, werden in Sektion 2.2 dieses Abschnitts noch näher behandelt.

2 Smartphone-Plattform

Daten wurden als Kern-Asset jeder Smartphone-Infrastruktur sowohl in Unternehmen als auch im M-Government Bereich identifiziert. Im vorangegangenen Abschnitt wurde das Kern-Asset „Daten“ differenziert betrachtet und basierend auf diesem Kern-Asset verschiedene Kategorien von Daten definiert. Für jede dieser Kategorien wurden wiederum Assets identifiziert und mögliche Bedrohungen skizziert.

Gemäß Abbildung 2 sind die drei Hauptbereiche einer Smartphone-Infrastruktur „Smartphone-Plattform“, „Zentrale Infrastruktur“ und „Kommunikation“ unmittelbar mit dem

Kern-Asset „Daten“ verknüpft. Im Folgenden werden diese drei Hauptbereiche näher betrachtet, bestehende Assets identifiziert und mögliche Bedrohungsszenarien für diese drei Bereiche skizziert. Dieser Abschnitt widmet sich zunächst dem Bereich „Smartphone“. Die Bereiche „Kommunikation“ und „Zentrale Infrastruktur“ werden in den folgenden Abschnitten betrachtet.

Der Bereich „Smartphone-Plattform“ ist in der öffentlichen Umgebung einer Smartphone-Infrastruktur angesiedelt. Die Smartphone-Plattform besteht aus dem Smartphone inklusive seines Betriebssystems und aller zugehörigen Hardwarekomponenten. Basierend auf der Smartphone-Plattform gibt es weitere für eine Sicherheitsüberprüfung relevante und in Abbildung 2 skizzierte Komponenten, die im Folgenden ebenfalls berücksichtigt werden sollen. Im Speziellen wird dabei auf die beiden Komponenten „Software“ und „Sensoren“ eingegangen, die für die Sicherheit von Smartphone-Plattformen eine besondere Rolle spielen.

A2	***Smartphone-Plattform:*** Die Smartphone-Plattform stellt dem Benutzer die Grundfunktionalität zur Nutzung mobiler Dienste und Möglichkeiten zur Kommunikation mit der zentralen Infrastruktur zur Verfügung. Während die Hardware einer Smartphone-Plattform im Großen und Ganzen festgelegt ist und nur eingeschränkt erweitert werden kann, ist der Softwareumfang von Smartphones in der Regel flexibel erweiterbar und kann den jeweiligen Bedürfnissen von Benutzerinnen und Benutzern angepasst werden. Eine Smartphone-Plattform besteht im Allgemeinen aus den folgenden relevanten Komponenten: • *Hardware:* Dazu gehören unter anderem Touchscreen, Lautsprecher oder auch diverse Sensoren wie Mikrofon, GPS und Kompass. • *Betriebssystem:* Dieses stellt dem Benutzer Grundfunktionalitäten wie Telefonie, Datenkommunikation und Softwareverwaltungsmechanismen zur Verfügung. • *Software:* Die Software von Smartphones kann in der Regel flexibel erweitert werden. Für die sichere Verarbeitung von sicherheitskritischen Daten am mobile Gerät ist die Integrität und Sicherheit dieser Komponenten eine zwingende Voraussetzung.
B2	***Kompromittierung der Smartphone-Plattform:*** Gelingt es einem Angreifer eine oder mehrere Komponenten der Smartphone-Plattform zu kompromittieren, kann die Sicherheit der in der Smartphone-Infrastruktur gespeicherten und verarbeiteten Daten unter Umständen nicht mehr gewährleistet werden. Die Schwere der Bedrohung hängt dabei von der kompromittieren Komponente und der Art der sicherheitskritischen Daten ab.

Die Smartphone-Plattform bzw. deren Integrität und Sicherheit kann als generelles Asset betrachtet werden. Der Schutz dieses Assets bedarf des Schutzes diverser untergeordneter Komponenten. In den folgenden Unterabschnitten werden die besonders relevanten Komponenten „Software“ und „Sensoren“ vorgestellt, relevante Sub-Assets dieser Komponenten definiert und mögliche Bedrohungen, die diese Assets gefährden können, skizziert.

2.1 Software

Die Software eines Smartphones ist im Gegensatz zu dessen Hardwarekonfiguration flexibel und einfach erweiterbar. Smartphone-Plattformen bieten Benutzerinnen und Benutzern in der Regel die Möglichkeiten zusätzliche Software-Module – sogenannte „Apps“ – über einen vordefinierten Installationsvorgang auf dem mobile Gerät zu installieren. Abbildung 4 illustriert die für diesen Vorgang relevanten Komponenten.

Trotz diverser Unterschiede zwischen verschiedenen Smartphone-Plattformen ist der prinzipielle Ablauf einer Softwareerweiterung meist ähnlich. Die Benutzerin oder der Benutzer wählt die geeignete App aus verschiedenen zur Verfügung stehenden Quellen aus und installiert diese über einen vom Betriebssystem des Smartphones bereitgestellten Installationsmechanismus auf dem mobilen Gerät. Die Flexibilität der Softwareverwaltung von Smartphone-Plattformen bietet Angreifern verschiedene Möglichkeiten die Sicherheit der Plattform und damit der gesamten Smartphone-Infrastruktur zu kompromittieren.

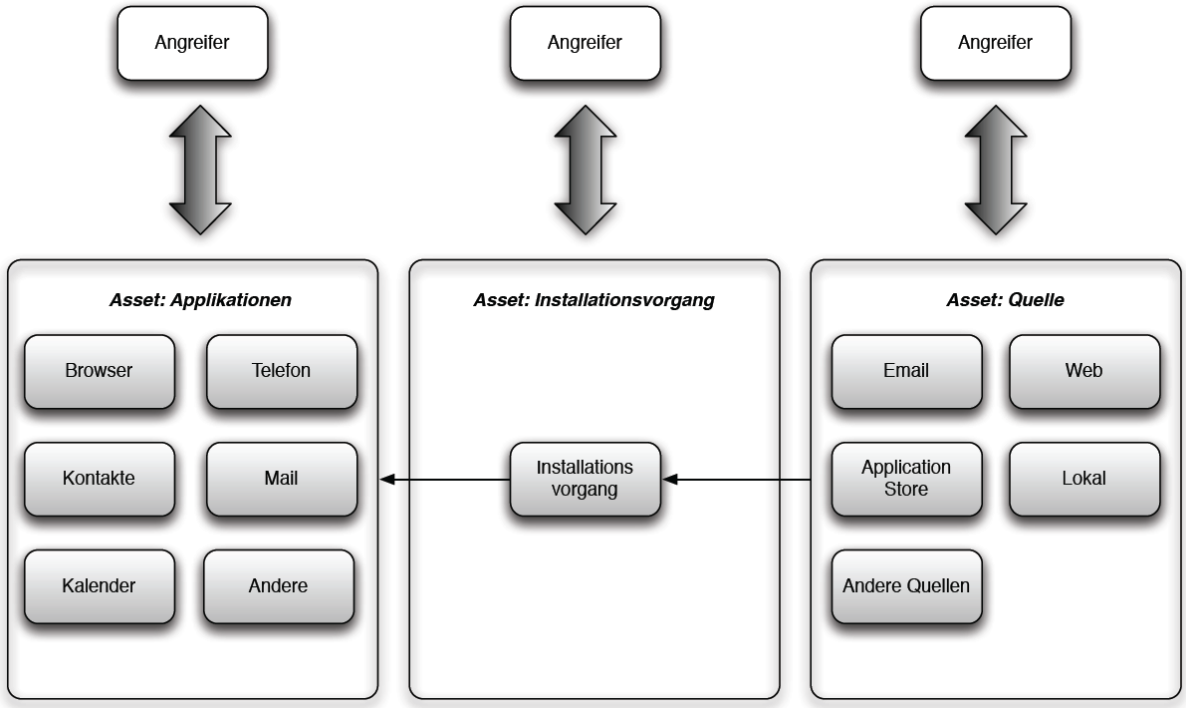

Abbildung 4 – Softwareverwaltung moderner Smartphone-Plattformen

A2.1	***Software:*** Smartphones verfügen in der Regel über ein umfangreiches Softwareangebot und ein flexibles Softwaremanagementsystem, über das die Funktionalität des Geräts dynamisch erweitert und angepasst werden kann.
B2.1	***Kompromittierung der Software:*** Funktionsreiche Softwarekomponenten und komplexe Softwaremanagementsysteme können eine Bedrohung für die Sicherheit von Smartphones und der auf ihnen gespeicherten Daten darstellen. Angreifer können die verschiedenen in Abbildung 4 dargestellten Angriffspunkte nutzen um das Gerät zu kompromittieren.

A2.1.1	***Applikationen (Apps):*** Applikationen sind eine Kernkomponente jeder Smartphone-Plattform. Durch Applikationen wird der Zugriff auf und die Verarbeitung von Daten ermöglicht. Da Applikationen potentiell Zugriff auf schützenswerte Daten am Smartphone haben, ist die Integrität und Sicherheit

	dieser Applikationen von besonderer Relevanz.
B2.1.1.a	***Zugriff auf Daten über bestehende Applikationen (Apps):*** Angreifer können Zugriff auf bestehende Applikationen am Smartphone erlangen und diese für ihre Zwecke missbrauchen. Beispielsweise könnte eine Kamera-Applikation von der Benutzerin oder dem Benutzer unbemerkt visuelle Daten der Umgebung aufnehmen, falls ein Angreifer Zugriff auf diese App hat. Dieses Angriffsszenario spielt vor allem in Unternehmensinfrastrukturen eine bedeutende Rolle. Generell sind folgende Angriffsszenarien denkbar: • Private oder geschäftliche Daten, die am Smartphone gespeichert sind, können extrahiert werden. • Funktionen des Smartphones wie zum Beispiel Sensoren können benutzt werden, um nicht gespeicherte Daten wie Position, Gespräche, visuelle Daten oder andere Sensordaten zu erhalten. Prinzipiell sind für derartige Angriffe alle Arten von Applikationen geeignet. Abhängig von der Funktionalität der App stehen dem Angreifer mehr oder weniger Möglichkeiten zur Verfügung um Daten auszuspionieren. Von besonderem Interesse sind daher Applikationen, die einen möglichst umfangreichen Zugriff auf Daten und Funktionalitäten des Smartphones erlauben. Dazu gehören zum Beispiel: • *Sicherheitstools:* Speziell in offenen Märkten wie dem Android Market werden Sicherheitstools angeboten, die in unterschiedlichen Bereichen eingesetzt werden können. Dazu gehören die Durchführung von Port Scans in Netzwerken, das Aufspüren von WLAN Access Points, das Finden offener WLANs, die Analyse von Mobilfunkzellen und vieles mehr. Viele dieser Applikationen sammeln benutzerbezogene Applikationsdaten, die von einem Angreifer direkt oder indirekt für weitere Angriffe verwendet werden können. Zusätzlich existieren noch eine Reihe von Sicherheitstools, die Benutzerinnen und Benutzern unterschiedliche Features zur Absicherung des Smartphones – zum Beispiel im Falle des Diebstahls[6] – bieten. Erlangt ein Angreifer Kontrolle über derartige Tools, können diese als Spionageprogramme verwendet werden. Je größer die Sicherheitsfunktionalität solcher Tools, desto besser können diese auch von Angreifern für deren Zwecke verwendet werden. • *Spionageapplikationen:* Viele Applikationen können Daten sammeln, die für einen Angreifer wertvoll sind. In vielen Fällen werben die Hersteller dieser Programme sogar damit, dass nach erfolgter Installation der Applikation deren Erkennen und Entfernen erschwert wird und zum Beispiel eine Fernsteuerung des Smartphones per SMS einfach möglich ist. Ein Zugriff auf diese Applikationen eröffnet einem Angreifer im Prinzip alle Möglichkeiten, die zum

[6] Siehe dazu zum Beispiel http://www.theftaware.com

	Verlust persönlicher oder kritischer Daten führen können. In diese Kategorie fallen prinzipiell auch die im vorherigen Punkte genannten Sicherheitstools, sofern diese von einem Angreifer für eigene Zwecke benutzt werden.
B2.1.1.b	***Zugriff auf Daten über Schadsoftware:*** Applikationen, die vom Benutzer auf das Smartphone installiert werden, können mit Schadcode versehen sein. Dadurch ergeben sich prinzipiell dieselben Angriffsszenarien wie in B2.1.1.a. Da der Angreifer die Funktionalität der Schadsoftware jedoch selbst bestimmen kann und nicht auf die vorgegebene Funktionalität bereits installierter Apps limitiert ist, sind in diesem Szenario effizientere Angriffe möglich.

A2.1.2	***Installationsmechanismus:*** Moderne Smartphone-Plattformen verfügen über einen Installationsmechanismus, über den von Benutzerinnen und Benutzern jederzeit zusätzliche Softwarekomponenten nachinstalliert werden können.
B2.1.2.a	***Einschleusen eigener Applikationen:*** Durch Umgehung der Sicherheitsvorkehrungen des Installationsmechanismus kann es einem Angreifer gelingen eigene Applikationen oder Schadsoftware auf einem Smartphone zu installieren.
B2.1.2.b	***Modifikation zu installierender Applikationen:*** Durch Umgehung der Sicherheitsvorkehrungen des Installationsmechanismus kann ein Angreifer unter Umständen zu installierende Applikationen während des Installationsvorgangs seinen Anforderungen entsprechend modifizieren und auf diese Weise zum Beispiel Schadcode einschleusen.

A2.1.3	***Quelle:*** Benutzerinnen und Benutzer können zusätzliche Softwarekomponenten von verschiedenen Quellen beziehen und über einen definierten Installationsmechanismus auf dem Smartphone installieren. Als Quelle kommen dabei beispielsweise Application-Stores oder das Web in Frage.
B2.1.3.a	***Einschleusen von Schadsoftware:*** Angreifer können unzureichend geschützte Quellen verwenden um eigene Schadsoftware einzubringen. Ist die Schadsoftware als solche nicht zu erkennen, kann sie über den vorgesehenen Installationsmechanismus den Weg auf Smartphones finden.
B2.1.3.b	***Verändern bestehender Applikationen:*** Sind Quellen, in denen Applikationen zentral gespeichert werden, nicht ausreichend geschützt, können Angreifer bestehende Applikationen modifizieren und mit Schadcode versehen.

2.2 Sensoren

Sensoren stellen für Smartphones ein wichtiges Instrument dar, welches die Implementierung funktionsreicher Applikationen wie zum Beispiel GPS-basierter Systeme erlaubt. Durch die Möglichkeit Informationen aus der unmittelbaren Umgebung des Smartphones aufzuzeichnen und detaillierte Lage- und Positionsbestimmungen durchzuführen, stellen Sensoren jedoch auch für Angreifer ein attraktives Ziel dar. Abbildung 5 zeigt einen Überblick über gängige Sensoren, die aktuell in modernen Smartphones integriert sind. Daten von diesen Sensoren werden entweder auf dem Speicher des Smartphones gesichert oder stehen bei Zugriff auf die Sensoren direkt zur Verfügung. Je

nach Sensor kann es sich bei diesen Daten um akustische und visuelle Informationen, Positionsdaten oder beliebige Daten anderer Sensoren handeln.

Prinzipiell ist jeder Sensor bzw. die Daten, die dieser Sensor aufzeichnet, als einzelnes Asset zu interpretieren. Mögliche Bedrohungsszenarien für die diese Assets werden im Folgenden skizziert.

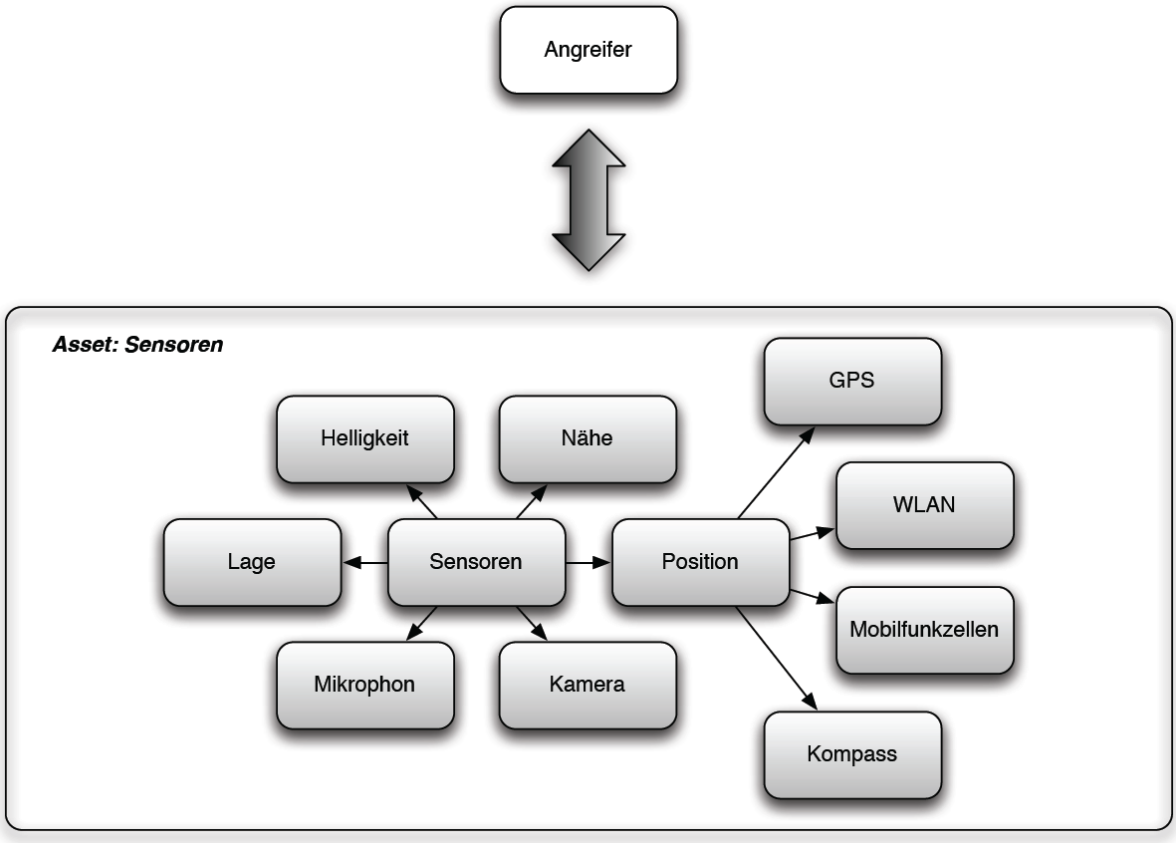

Abbildung 5 – Sensoren

A2.2	***Sensoren:*** Smartphones sind mit einer Reihe von Sensoren ausgestattet, die Rückschlüsse auf die Umgebung des Geräts zulassen. Dazu gehören unter anderem Kameras, GPS-Empfänger, Kompasse, sowie Helligkeits-, Lage- und Annäherungssensoren.
B2.2	***Zugriff auf Sensordaten:*** Bekommt ein Angreifer Zugriff auf Sensoren oder die von diesen Sensoren aufgezeichneten Daten, können diese kompromittiert oder als Basis für weitere Angriffe verwendet werden.

A2.2.1	***Positionsdaten:*** Damit werden alle Daten bezeichnet, die für die Positionsbestimmung der Benutzerin oder des Benutzers verwendet werden können. In erster Linie handelt es sich hierbei um Positionsangaben die anhand von WLANs, Mobilfunknetzwerken oder direkt über GPS bezogen werden. Es müssen jedoch auch Daten berücksichtiget werden, die eine indirekte Ableitung der Position ermöglichen. Dies kann beispielsweise über MAC Adressen von WLAN Access Points, Identifikationsnummern von Mobilfunkzellen oder textuelle Positionsangaben wie Ortsnamen erfolgen.

B2.2.1	***Zugriff auf Positionsdaten:*** Ein Angreifer kann entweder auf gespeicherte Positionsdaten am Smartphone oder direkt auf die Positionssensoren des Geräts zugreifen um Informationen über die aktuelle Position der Benutzerin oder des Benutzers zu erhalten. Diese Informationen können als Basis für weitere Angriffe verwendet werden. Auf folgende Informationen könnte so beispielsweise indirekt rückgeschlossen werden: • Tagesabläufe der Benutzerin oder des Benutzers • An/Abwesenheit der Benutzerin oder des Benutzers an bestimmten Orten • Lokationen, die für die Benutzerin oder den Benutzers relevant sind • Daten über das soziale Netzwerk der Benutzerin oder des Benutzers und über geschäftliche oder private Beziehungen

A2.2.2	***Akustische Daten:*** Hierbei handelt es sich um Audiodaten, die sich entweder auf dem Speicher des Smartphones befinden oder direkt über das Mikrofon zur Verfügung stehen.
B2.2.2	***Zugriff auf akustische Daten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf gespeicherte akustische Daten oder direkt auf das Mikrofon bekommen. Dadurch kann der Angreifer zum Beispiel Zugriff auf folgende Daten erlangen: • Aufzeichnen von vertraulichen Gesprächen • Aufzeichnen von Telefongesprächen der Benutzerin oder des Benutzers

A2.2.3	***Visuelle Daten:*** Hierbei handelt es sich um Bild- oder Videodaten, die entweder auf dem Speicher des Smartphones liegen, oder direkt über die Kamera zur Verfügung stehen.
B2.2.3	***Zugriff auf visuelle Daten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf gespeicherte visuelle Daten oder direkten Zugriff auf die Kamera erlangen. Im Gegensatz zum Mikrofon ist hier aufgrund der Notwendigkeit der Positionierung des Smartphones die Wahrscheinlichkeit geringer, dass gewünschte Informationen gezielt aufgezeichnet werden können. Durch Zugriff auf am Smartphone verfügbare visuelle Daten kann ein Angreifer zum Beispiel Zugriff auf folgende Informationen erlangen: • Erstellen von Videos/Fotos von kritischen Daten (z.B. Dokumente) • Erkennen von Sicherheitsmaßnahmen innerhalb eines Unternehmens oder einer Behörde

	• Erkennen von anderen Merkmalen wie Personen, Objekte oder Zugangscodes, die als Basis für weitere Angriffe dienen können.

A2.2.4	***Helligkeitsdaten:*** Helligkeitssensoren erlauben modernen Smartphones die Feststellung der Helligkeit der aktuellen Umgebung.
B2.2.4	***Zugriff auf Helligkeitsdaten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Helligkeitsdaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

A2.2.5	***Lagedaten:*** Lagesensoren erlauben modernen Smartphones die Feststellung der aktuellen Lage des Smartphones im Raum.
B2.2.5	***Zugriff auf Lagedaten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Lagedaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

A2.2.6	***Annäherungsdaten:*** Annäherungssensoren erlauben modernen Smartphones die Feststellung von Objekten in der Nähe des Geräts. Dies wird hauptsächlich dazu verwendet, um während eines Telefonats das Display des Smartphones automatisch auszuschalten.
B2.2.6	***Zugriff auf Annäherungsdaten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Annäherungsdaten erlangen. Dadurch ist es ihm beispielsweise möglich, auf Anzahl und Dauer von Telefonaten rückzuschließen, falls diese Information auf direktem Weg nicht zugänglich ist.

A2.2.7	***Beschleunigungsdaten:*** Beschleunigungssensoren erlauben modernen Smartphones die Messung der aktuellen Beschleunigung des Geräts.
B2.2.7	***Zugriff auf Beschleunigungsdaten:*** Nach der erfolgreichen Installation von Schadsoftware auf einem Smartphone kann ein Angreifer Zugriff auf die Beschleunigungsdaten erlangen. Auch wenn eine mögliche dadurch entstehende Bedrohung nicht offensichtlich ist, kann ein Angreifer in bestimmten Szenarien durch Zugriff auf diese Daten eventuell relevante Informationen extrahieren.

3 Kommunikation

Im Zusammenhang mit dem Schutz sicherheitskritischer Daten eines Smartphone-Infrastruktur spielt die Kommunikation zwischen den einzelnen Komponenten der Infrastruktur eine zentrale Rolle. Dieser Umstand wird auch durch Abbildung 2 verdeutlicht. Kommunikation steht in direktem Zusammenhang mit dem Kern-Asset „Daten“ und den

beiden Hauptbereichen „Smartphone-Plattform“ und „Infrastruktur“. Die Komplexität des Aspekts „Kommunikation“ einer Smartphone-Infrastruktur wird in Abbildung 6 verdeutlicht.

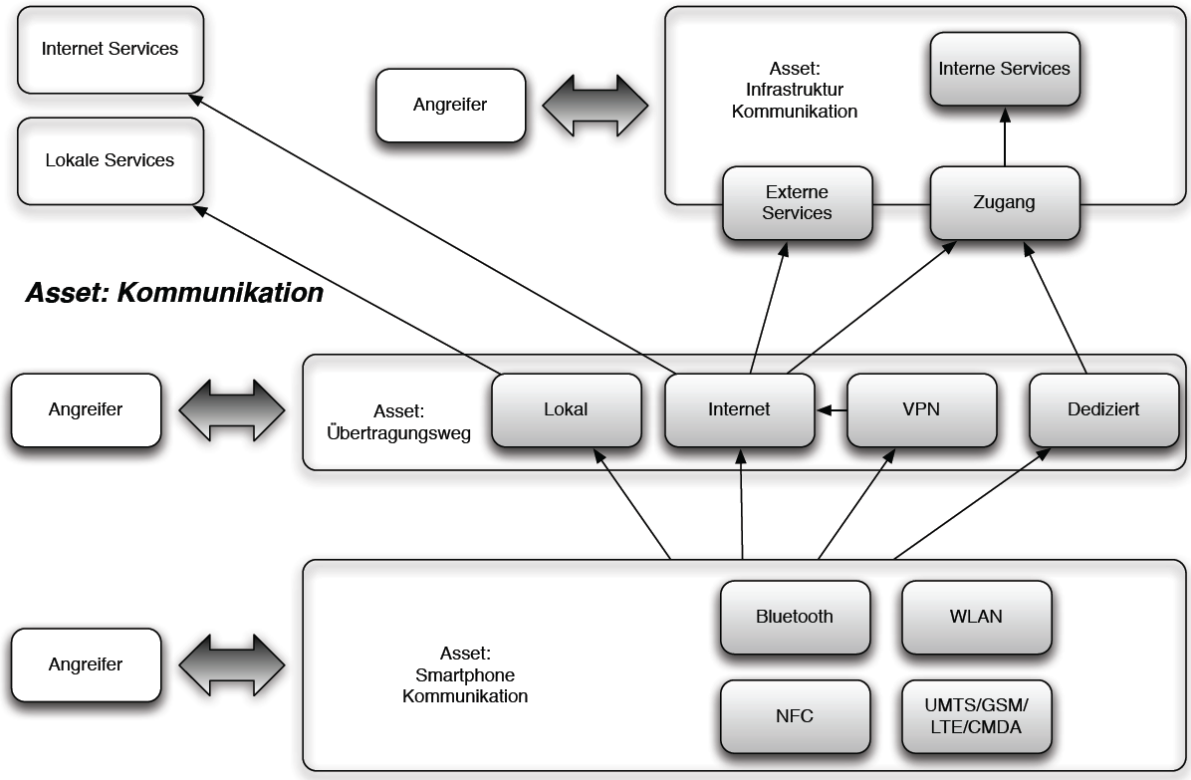

Abbildung 6 – Kommunikationspfade innerhalb einer Smartphone-Infrastruktur

Das Asset „Kommunikation“ kann generell in drei den einzelnen Bereichen einer Smartphone-Infrastruktur entsprechenden Assets unterteilt werden. Sämtliche für die Kommunikation verantwortliche Komponenten der Smartphone-Plattform werden im Asset „Smartphone Kommunikation“ zusammengefasst. Relevante Kommunikationskomponenten der zentralen Infrastruktur werden hingegen durch das Asset „Infrastruktur Kommunikation“ abgedeckt[7]. Neben diesen beiden Assets gibt es noch das Asset „Übertragungsweg“, welches Aspekte des Kommunikationspfades zwischen zentraler Infrastruktur und Smartphone-Plattform abdeckt.

Da sowohl das Asset „Smartphone Kommunikation“ als auch das Asset „Übertragungsweg“ der öffentlichen Umgebung zuzuordnen sind, sind diese beiden Assets für Angreifer besonders interessant. Zunächst wird das Asset „Kommunikation“ definiert und für dieses und weitere verwandte Assets der öffentlichen Umgebung mögliche Bedrohungsszenarien in den folgenden Unterabschnitten skizziert.

A3	***Kommunikation:*** Dieses Asset betrifft einerseits die Kommunikation zwischen der Smartphone-Plattform und der zentralen Infrastruktur eines Unternehmens oder einer Behörde, andererseits aber auch die Kommunikation der Smartphone-Plattform mit anderen externen Komponenten. Dabei kommen unterschiedliche im folgenden näher analysierten Kommunikationskanäle und Interfaces zum Einsatz.

[7] Jene Assets der Infrastruktur, die im Zusammenhang mit der Kommunikation relevant sind, werden in Abschnitt II:4 detailliert analysiert. In diesem Abschnitt werden diese Infrastruktur-Assets nur erwähnt, wenn sie für die hier beschriebenen Assets relevant sind.

B3	***Angriffe auf die Kommunikation:*** Erhält ein Angreifer Zugriff auf einen Kommunikationskanal, so hat er unter Umständen auch auf übermittelte Daten lesend und/oder schreibend Zugriff. Dadurch ergeben sich unterschiedliche Bedrohungen, deren Details von den jeweiligen unterschiedlichen Subkomponenten abhängen.

3.1 Smartphone-Kommunikation

In diesem Abschnitt werden Assets der Smartphone-Plattform, die die Kommunikation mit der zentralen Infrastruktur oder mit externen Komponenten betreffen, definiert und mögliche Bedrohungsszenarien entworfen.

A3.1	***Smartphone-Kommunikation:*** Smartphones verfügen über diverse Kommunikationsmöglichkeiten, die einen Datenaustausch mit zentralen Infrastrukturen, externen Komponenten, oder auch anderen Smartphones erlauben.
B3.1	***Angriffe auf die Smartphone-Kommunikation:*** Aufgrund der Exponiertheit von Smartphones und der meist kabellosen Übertragungstechniken, ergeben sich für die Smartphone-Kommunikation zahlreiche Angriffsmöglichkeiten und Gefahren. Gelingt es einem Angreifer die Kommunikation zu kompromittieren, können übermittelte und potentiell sicherheitskritische oder persönliche Daten gestohlen werden.

A3.1.1	***WLAN:*** WLANs werden vor allem dann verwendet, wenn kein Zugriff auf ein Mobilfunkdatennetzwerk besteht. In diesen Fällen ermöglichen WLANs den Zugang zum Internet und erlauben Zugriff auf Ressourcen und Daten der zentralen Infrastruktur.
B3.1.1	***Angriffe auf WLANs:*** Vor allem für öffentliche WLANs ergeben sich vielseitige Bedrohungen. Diese Bedrohungen sind prinzipiell seit Längerem bekannt, gewannen jedoch mit der weiten Verbreitung von WLANs zunehmend an Bedeutung. Folgende Angriffsszenarien kompromittieren die Sicherheit von WLANs: • *Nicht vertrauenswürdige WLANs*: WLAN Hotspots können sehr einfach in Betrieb genommen werden und sind prinzipiell an allen Orten einsetzbar. Zusätzlich zu den seit einigen Jahren üblichen stationären Geräten kommen nun auch mobile Geräte hinzu, die es sehr einfach machen einen Ad-hoc Access Point zu konfigurieren. Beispielsweise können Smartphones meist sehr einfach als WLAN Hotspot konfiguriert werden. Generell gilt, dass WLANs nur eingeschränkt vertraut werden kann, da diese auch von Angreifern betrieben werden können. • *Schutz der Daten:* Bei WLANs, die Dienste ohne weitere Schutzmechanismen wie WPA anbieten, hat ein Angreifer, der sich in der Empfangs und Sendereichweite des WLANs befindet, die Möglichkeiten, Zugriff auf alle im WLAN übermittelten Daten zu erhalten. Dies betrifft einen Großteil aller WLANs, da Schutzmechanismen wie WPA bei

	Hotspots typischerweise durch nachgelagerte Authentifizierungsmaßnahmen ersetzt werden. Demzufolge müssen folgenden Implikationen für Daten beachtet werden: ° Unverschlüsselte Daten wie jene, die über die Protokolle HTTP oder DNS übertragen werden, sind von einem Angreifer einsehbar und manipulierbar. Einem Angreifer stehen daher viele Methoden zur Verfügung, die verschiedene Arten von Angriffen ermöglichen. Diverse Phishing-Angriff ermöglichen beispielsweise das Fälschen von DNS Einträgen, ARP Poisoning, oder die direkte Manipulation des HTTP Verkehrs. Ungeschützt übertragene Informationen werden dem Angreifer im Klartext zugänglich gemacht und erlauben ihm, übertragene Daten während des Transfers zu manipulieren. Dadurch kann beispielsweise Schadsoftware in den nicht geschützten Transfer von Daten eingefügt werden. ° Verschlüsselte Daten, die beispielsweise über HTTPS gesichert sind, sind für MITM Angriffe anfällig. Ein Angreifer kann etwa ein Zertifikat einer HTTPS Verbindung fälschen. Akzeptiert die Benutzerin oder der Benutzer dieses geänderte Zertifikat im Browser, hat der Angreifer Zugriff auf die übertragenen Daten, da er sie mit dem gefälschten Schlüssel entschlüsseln kann. Außerdem muss berücksichtigt werden, dass Applikationen, die über HTTPS kommunizieren, nur dann sicher sind, wenn auch die eingesetzten Zertifikate von der Applikation verlässlich geprüft werden. Geschieht dies nicht, kann ein Angreifer einen MITM Angriff durchführen, um unerlaubten Zugriff auf Daten zu erhalten.

A3.1.2	***UMTS/GSM/LTE/CDMA:*** Datenverbindungen können auch über Mobilfunktechnologien wie GSM, UMTS, LTE oder CDMA hergestellt werden.
B3.1.2	***Angriffe auf UMTS/GSM/LTE/CDMA:*** Hier werden keine spezifischen Bedrohungen genannt. Die Unsicherheit von GSM Netzen ist bekannt, spielt aber weiterhin keine entscheidende Rolle. Für die Übertragung von Daten über das Internet muss ohnehin davon ausgegangen werden, dass die verwendeten Netzwerke nicht vertrauenswürdig sind.

A3.1.3	***Bluetooth:*** Bluetooth kommt hauptsächlich zur Anbindung externer Geräte oder zur Verbindung mit anderen Smartphones zur Anwendung.
B3.1.3	***Angriffe auf Bluetooth:*** Gelingt es einem Angreifer die Bluetooth-Kommunikation zu kompromittieren, kann er Zugriff auf die über diese Schnittstelle übertragenen Daten erhalten.

A3.1.4	***NFC:*** NFC basiert auf der RFID Technologie und ermöglicht sowohl das Auslesen passiver RFID-Tags mit Smartphones als auch eine RFID basierte Kommunikation zwischen Smartphones.
B3.1.4	***Angriffe auf NFC:*** Gelingt es einem Angreifer die NFC-Kommunikation zu kompromittieren, kann er Zugriff auf die über diese Schnittstelle übertragenen Daten erhalten.

3.2 Übertragungsweg

In diesem Abschnitt werden Assets, die dem Kommunikationspfad zwischen Smartphone-Plattform und zentraler Infrastruktur zugeordnet werden können, detaillierter beschrieben.

A3.2	***Übertragungsweg:*** Als Übertragungsweg bezeichnet man die Strecke zwischen dem Smartphone und dem jeweiligen Kommunikationspartner. Als Kommunikationspartner kann beispielsweise eine zentrale Infrastruktur oder auch ein anderes Smartphone fungieren.
B3.2	***Angriffe auf den Übertragungsweg:*** Sind Daten am Übertragungsweg nicht geeignet gesichert, können dieses von einem Angreifer kompromittiert werden. Je nach Übertragungsweg ergeben sich dabei unterschiedliche Gefahrenpotentiale.

A3.2.1	***Übertragungsweg zu lokalen Services:*** Darunter versteht man den Kommunikationspfad zu Services, die in der lokalen Umgebung des Smartphones zur Verfügung stehen. Diese können von einfachen Bluetooth Freisprecheinrichtungen, über den direkten Datenaustausch mit anderen Smartphones via Bluetooth oder WLAN bis zu von der lokalen Infrastruktur angebotenen Intranet Services reichen.
B3.2.1	***Angriffe auf den Kommunikationspfad zu lokalen Services:*** Für den Zugriff auf lokale Services kommen üblicherweise Bluetooth und lokale Netzwerkverbindungen (WLAN) zur Anwendung. Es gelten hier also alle Bedrohungen, die auch bei diesen Services auftreten. In diesem Zusammenhang besonders relevant sind die Bedrohungsszenarien B3.1.1 und B3.1.3. Inkludieren diese Übertragungswege auch weitere öffentliche Netzwerke, so muss auch das Bedrohungsszenario B3.2.3.a speziell beachtet werden.

A3.2.2	***Dedizierte Übertragungswege:*** Hierbei handelt es sich um potentiell proprietäre Kommunikationsverbindungen, die zwischen den Smartphones und der zentralen Infrastruktur zur Verfügung gestellt werden. Die Verbindungen können dabei sowohl auf privaten als auch auf öffentlichen Netzwerken aufbauen.
B3.2.2	***Angriffe auf dedizierte Übertragungswege:*** Mögliche Angriffe hängen von der jeweiligen Implementierung des dedizierten Übertragungsweges ab. Aus diesem Grund ist eine differenzierte Betrachtung der eingesetzten Protokolle nötig.

A3.2.3	***Internet:*** Bei diesem Übertragungsweg werden Daten über öffentliche Netzwerke transportiert. Dies ist in der Regel der am häufigsten gebrauchte Übertragungsweg, sofern keine dedizierten Übertragungswege zur Verfügung stehen.
B3.2.3.a	***Angriffe auf öffentliche Netzwerke:*** Generell gelten hier alle Bedrohungen und Probleme, die mit dem Transport von Daten über öffentliche Netzwerke verbunden sind. Ein Angreifer kann Zugriff auf nicht verschlüsselte Daten erhalten und diese auslesen oder manipulieren. Ein direkter Angriff auf diese öffentlichen Netzwerke ist für einen Angreifer mit großem Aufwand verbunden, da er typischerweise keinen Zugriff auf die Komponenten dieser Netzwerke hat. Diese Bedrohung spielt daher vor allem in Szenarien, in denen Angreifer mit sehr großen Ressourcen oder Kontrolle über diese Netzwerke im Spiel sind, eine große Rolle. Ein aktuelles Beispiel ist die Manipulation von Facebook Konten in Tunesien[8].
B3.2.3.b	***Zugang zum Internet:*** Um Zugriff auf das Internet zu bekommen werden entsprechende Zugangspunkte benötigt. Speziell die weite Verbreitung von WLANs bietet einem Angreifer in diesem Zusammenhang viele Möglichkeiten Zugriff auf Daten zu erhalten. In diesem Zusammenhang wird wiederum auf Bedrohungsszenario B3.1.1 verwiesen.

A3.2.4	***VPN-Verbindungen:*** VPN-Verbindungen dienen dem sicheren Zugriff auf die zentrale Infrastruktur eines Unternehmens. Im Rahmen von M-Government Diensten spielen diese Verbindungen daher eine untergeordnete Rolle. Über eine VPN-Verbindung wird im Prinzip die geschützte Umgebung einer zentralen Infrastruktur auf das mobile Smartphone ausgedehnt. Sämtliche Kommunikation zwischen Smartphone-Plattform und zentraler Infrastruktur wird über Secure Messaging abgesichert. VPN-Verbindungen bauen dabei in der Regel auf öffentlichen Netzwerken wie dem Internet auf. Da der erfolgreiche Aufbau einer VPN-Verbindung einen Zugang zu internen Services der zentralen Infrastruktur ermöglicht, muss eine VPN-Verbindung selbst als Asset betrachtet werden. Im Besonderen gilt dies für Berechtigungsnachweise wie Passwörter, kryptographische Schlüssel und Zertifikate, die auf dem Smartphone gespeichert sind und für den Aufbau einer VPN-Verbindung benötigt werden.
B3.2.4	***Angriffe auf VPN-Verbindungen:*** Gelingt es einem Angreifer eine VPN Verbindung zur zentralen Infrastruktur aufzubauen, kann dieser unter Umständen Zugriff auf interne Services und Ressourcen eines Unternehmens erlangen. Berechtigungsnachweise, die für den Aufbau einer VPN Verbindung erforderlich sind, müssen daher sicher verwahrt und dürfen für einen Angreifer nicht zugänglich sein.

3.3 Infrastruktur-Kommunikation

Auch in der zentralen Infrastruktur gibt es einzelne Komponenten, die für die Kommunikation mit Smartphones im Rahmen der Smartphone-Infrastruktur verwendet werden. Obwohl sich diese Komponenten in der Regel in der geschützten Umgebung befinden, unterliegen diese aufgrund ihrer externen Schnittstelle einem erhöhten Gefahrenpotential. Im Folgenden werden kritische zentrale Kommunikationskomponenten identifiziert und mögliche Bedrohungen skizziert.

[8] http://www.wired.com/threatlevel/2011/01/tunisia/

A3.3	***Infrastruktur-Kommunikation:*** Die Infrastruktur-Kommunikation umfasst jene Komponenten, die für eine Kommunikation mit externen Smartphones verantwortlich sind. Dazu gehören beispielsweise zentrale Zugangspunkte oder externe Services.
B3.3	***Zugriff auf die Infrastruktur-Kommunikation:*** Erhält ein Angreifer Zugriff auf diese Komponenten, kann er über diese unter Umständen auf Daten innerhalb der zentralen Infrastruktur zugreifen.

A3.3.1	***Externe Services:*** Externe Services werden in der Regel verwendet um ausgewählte Daten aufzubereiten und zu repräsentieren. Beispiele für solche Services sind etwa Webauftritte von Behörden im Rahmen von M-Government Diensten oder Services zur Kommunikation mit Partnerunternehmen. Diese Services stehen in keinem ausschließlichem Zusammenhang mit Smartphones, können über diese jedoch meist auch genutzt werden. Da externe Services potentiell ebenfalls Zugriff auf interne Daten bzw. ein Subset davon haben, ist deren Sicherheit von Bedeutung.
B3.3.1	***Zugriff auf externe Services:*** Durch das Ausnützen von Sicherheitslücken in externen Services kann ein Angreifer Zugriff auf kritische Daten der zentralen Infrastruktur bekommen.

A3.3.2	***Zugang:*** Über einen definierten Zugang können externe Geräte wie Smartphones in die zentrale Infrastruktur eingebunden werden und Zugriff auf interne Services erlangen. In den meisten Fällen wird es sich bei diesem Zugang um einen VPN-Endpunkt handeln, theoretisch sind aber auch andere Ansätze denkbar. Diese Komponente spielt vor allem in Unternehmensinfrastrukturen eine wichtige Rolle.
B3.3.2.a	***Kompromittierung des Zugangs:*** Gelingt es einem Angreifer die Sicherheitsmechanismen des Zugangs zu umgehen, kann über diesen Zugang Zugriff auf interne Services und damit auf interne Daten der zentralen Infrastruktur erlangt werden.
B3.3.2.b	***Missbräuchliche Verwendung eines Smartphones:*** Erhält ein Angreifer Zugang zu einem Smartphone, auf dem die Verbindung zum Zugang zur zentralen Infrastruktur konfiguriert ist und benötigte Berechtigungsausweise gespeichert sind, kann er Zugriff auf interne Services und damit auf Daten der zentralen Infrastruktur erlangen.

4 Zentrale Infrastruktur

Die zentrale Infrastruktur stellt neben der Smartphone-Plattform und dem Kommunikationsweg zwischen Infrastruktur und Smartphone-Plattform den dritten relevanten Bereich einer Smartphone-Infrastruktur dar. Die zentrale Infrastruktur wird prinzipiell der geschützten Umgebung zugeordnet. Durch den Einsatz von Smartphones können jedoch auch für die in der Infrastruktur gespeicherten und verarbeiteten Daten zusätzliche Bedrohungen entstehen. Die in diesem Abschnitt angestellten Überlegungen betreffen

speziell Smartphone-basierte Unternehmensinfrastrukturen. Einige Aspekte sind jedoch auch für zentrale Komponenten von M-Government Infrastrukturen relevant.

Abbildung 7 zeigt relevante Komponenten der zentralen Infrastruktur, die in Zusammenhang mit den in der Infrastruktur gespeicherten oder verarbeiteten Daten stehen. Die Daten werden wiederum als Kern-Asset betrachtet. Auf diese Daten kann über externe und interne Services zugegriffen werden. Externe Services stehen externen Benutzerinnen und Benutzern beispielsweise in Form von Web-Applikationen (z.B. M-Government Services) zur Verfügung. Interne Services sind hingegen Benutzerinnen und Benutzern, die sich innerhalb der zentralen Infrastruktur befinden, vorbehalten. Um über ein Smartphone Zugriff auf diese Services zu erhalten, ist ein entsprechender Zugang zum Beispiel über VPN nötig. Diese Anforderung betrifft meist Unternehmensinfrastrukturen. Interne Services können die Daten auf unterschiedlichste Art und Weise weiterverarbeiten. Dazu gehören Verfahren zur visuellen und akustischen Aufbereitung, oder auch die Weiteleitung der Daten über interne Kommunikationsschnittstellen.

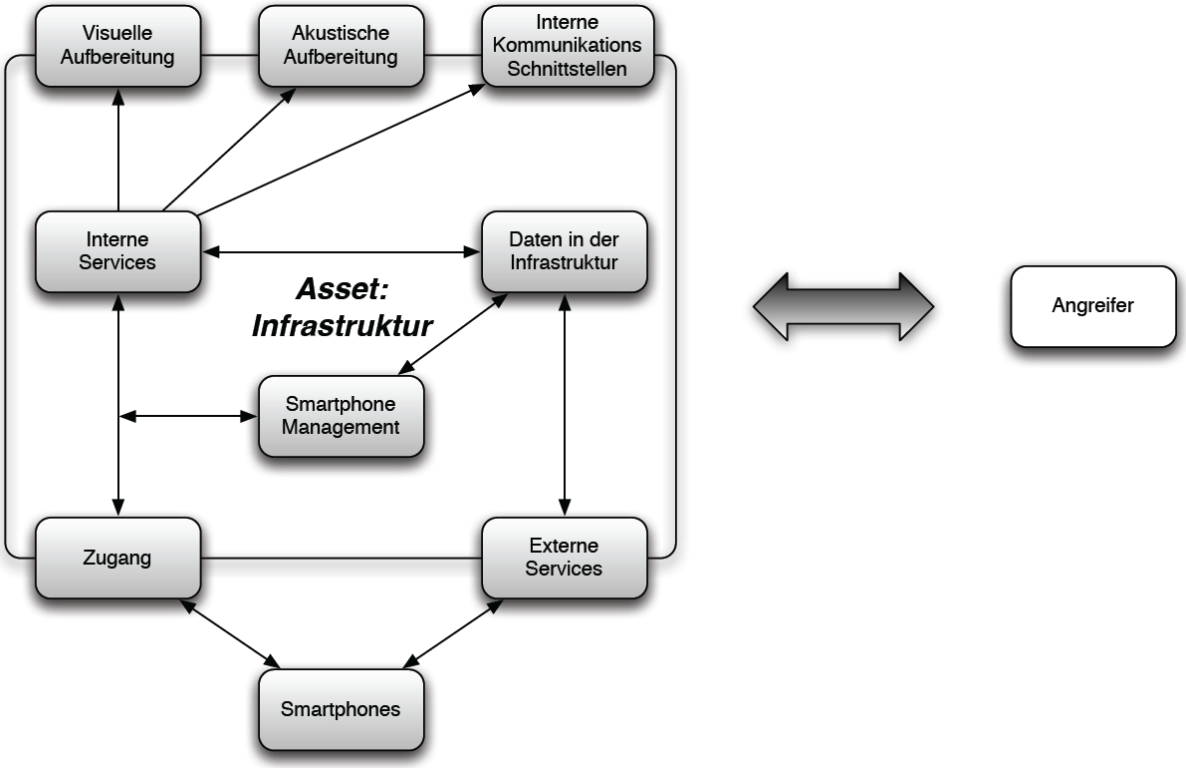

Abbildung 7 – Relevante Komponenten der zentrale Infrastruktur

Ziel eines Angreifers ist es in jedem Fall, unter Verwendung von Smartphones Zugriff auf die in der zentralen Infrastruktur gespeicherten Daten zu erhalten. Ziel von Betreibern von Smartphone-Infrastrukturen muss es dagegen sein, diese dahingehend zu schützen, sodass ein derartiger Zugriff nicht möglich ist.

A4	***Zentrale Infrastruktur:*** Die zentrale Infrastruktur enthält in der Regel diverse Komponenten, die durch den Einsatz von Smartphones gefährdet werden können.
B4	***Zugriff auf Komponenten der zentralen Infrastruktur:*** Durch unerlaubten Zugriff auf einzelne Komponenten der zentralen Infrastruktur können die in der Infrastruktur gespeicherten und verarbeiteten Daten kompromittiert werden.

A4.1	***Interne Services:*** Hierbei handelt es sich um interne Services, die nicht vom Internet aus zugänglich sind. Dies können beispielsweise Email-Dienste oder andere Services sein, die ausschließlich im Intranet eines Unternehmens zur Verfügung stehen. Diese Services sind prinzipiell nicht Bestandteil dieser Analyse, es wird aber davon ausgegangen, dass diese Services den Zugriff auf kritische Informationen ermöglichen würden.
B4.1	***Zugriff auf interne Services:*** Erhält ein Angreifer Zugriff auf interne Services, kann er damit Zugriff auf interne Daten der zentralen Infrastruktur erlangen. Für M-Government Infrastrukturen spielt diese Bedrohung eine untergeordnete Bedeutung, da Benutzerinnen und Benutzer in der Regel über keinen VPN-Zugang zu internen M-Government Services verfügen.

A4.2	***Visuelle Aufbereitung:*** Zusätzlich zu internen und externen Services, die den Zugriff auf Daten ermöglichen, werden interne Daten von Behörden oder Unternehmen intern oft visuell aufbereitet. Bei der visuellen Aufbereitung handelt es sich neben der elektronischen Aufbereitung auf Bildschirmen zum größten Teil um das Ausdrucken von Dokumenten.
B4.2.a	***Aufzeichnen von visuellen Informationen mit einem Smartphone, das im Besitz des Angreifers ist:*** Ein Angreifer, der visuellen Zugriff auf die Infrastrukturkomponenten des Unternehmens hat, kann sein Smartphone benutzen, um visuelle Informationen in Form von Videos oder Fotos aufzuzeichnen. Diese Informationen können je nach Beschaffenheit des Unternehmens und der verfügbaren Informationen sehr unterschiedlicher Natur sein. Beispiele für Informationen, die durch das Erstellen von Fotos oder Videos kompromittiert werden können sind: • Kritische oder persönliche Informationen auf Bildschirmen • Zugangsdaten wie Eingaben auf PIN Pads, Tastaturen und anderen Eingabegeräten • Ausgeruckte Dokumente, die kritische oder persönliche Informationen beinhalten • Sicherheitsfunktionen wie Schließsysteme, Wachpersonal oder andere Vorkehrungen
B4.2.b	***Aufzeichnen von visuellen Informationen mit einem Smartphone, das ein Angreifer mit Schadsoftware infiziert hat:*** Diese Bedrohung ist ähnlich zur Bedrohung B4.2.a. Allerdings wird hier davon ausgegangen, dass der Angreifer keinen persönlichen Zugriff auf visuelle Informationen hat, sondern ein Smartphone eines Benutzers mit Schadsoftware infiziert hat, die ihm einen Zugriff auf die Kamera oder Daten der Kamera erlaubt. Prinzipiell können dabei die gleichen visuellen Informationen wie im Bedrohungsszenario B4.2.a kompromittiert werden. Allerdings ist aufgrund der Tatsache, dass der Angreifer das Smartphone nicht selbst ausrichten kann, die Wahrscheinlichkeit Zugriff auf relevante Informationen zu bekommen bedeutend geringer[9].

[9] Anmerkung: Bei Bedrohungsszenarien für akustische Daten ist das Bedrohungspotential genau umgekehrt.

A4.3	***Akustische Aufbereitung:*** Darunter versteht man die akustische Wiedergabe von Daten etwa in Form von persönlichen Gesprächen oder mündlichen Präsentationen.
B4.3.a	***Aufzeichnen von akustischen Informationen mit einem Smartphone, das im Besitz des Angreifers ist:*** Ein Angreifer, der mit seinem Smartphone in der Reichweite von vertraulichen Gesprächen ist, kann das Gerät benutzen um diese Gespräche aufzuzeichnen. Diese Informationen können je nach Beschaffenheit des Unternehmens oder der Behörde sehr unterschiedlicher Natur sein und prinzipiell ein breites Spektrum an relevanten Informationen umfassen. Beispiele für derartige akustische Informationen sind etwa: • Gespräche zwischen Mitarbeiterinnen und Mitarbeitern des Unternehmens oder der Behörde, bei denen kritische Informationen diskutiert werden • Gespräche, die in Meetings geführt werden • Alle anderen Informationen, die im Rahmen von persönlichen Gesprächen behandelt werden
B4.3.b	***Aufzeichnen von akustischen Informationen mit einem Smartphone, das ein Angreifer mit Schadsoftware infiziert hat:*** Diese Bedrohung ist ähnlich zur Bedrohung B4.3.a. Allerdings geht man hier davon aus, dass der Angreifer keinen persönlichen Zugriff auf akustische Informationen hat, sondern ein Smartphone eines Benutzers mit Schadsoftware infiziert hat, die ihm den Zugriff auf das Mikrofon oder gespeicherte Daten des Mikrofons erlaubt. Prinzipiell können dabei die gleichen akustischen Informationen wie in B4.3.a kompromittiert werden. Da eine persönliche Anwesenheit des Angreifers in diesem Szenario nicht nötig ist, geht hiervon eine größere Bedrohung aus als bei B4.3.a[10].

A4.4	***Interne Kommunikationsschnittstellen:*** Interne Kommunikationsschnittstellen der zentralen Infrastruktur können Zugriff auf interne Services und damit auch auf kritische Daten erlauben. Beispiele für derartige Schnittstellen sind Netzwerkbuchsen aber auch WLAN Access Points.
B4.4	***Zugriff auf interne Kommunikationsschnittstellen:*** Angreifer können Smartphones benutzen um interne Kommunikationsschnittstellen wie WLANs zu scannen und relevante netzwerkbezogene Informationen zu sammeln. Dieses Bedrohungsszenario ist prinzipiell nicht auf eine Verwendung von Smartphones beschränkt, deren Mobilität und Unauffälligkeit kann derartige Angriffe für Angreifer jedoch signifikant erleichtern.

A4.5	***Smartphone Management:*** Über die Smartphone Management Komponente können allgemein gültige Policies für Smartphones festgelegt werden. Da diese Policies die sichere Verwendung von Smartphones im Rahmen einer Smartphone-Infrastruktur gewährleisten, ist diese Komponente als relevantes Asset zu betrachten. Diese Komponenten ist ausschließlich in

[10] Anmerkung: Bei Bedrohungsszenarien für visuelle Daten ist das Bedrohungspotential genau umgekehrt.

	Unternehmensinfrastrukturen, in denen Smartphones vom Unternehmen an Mitarbeiter ausgegeben werden, verfügbar. Im Rahmen von Smartphone-basierten M-Government Diensten hat die Behörde in der Regel keine Handhabe über die von Benutzerinnen und Benutzern der Dienste verwendeten Endgeräte.
B4.5	***Zugriff auf das Smartphone Management:*** Erhält ein Angreifer Zugriff auf die Smartphone Management Komponente, kann er unter Umständen Policies einsehen oder verändern und so Sicherheitsvorkehrungen außer Kraft setzen.

Abschnitt III: Schutzfunktionen

Die Sicherheit der verschiedenen für Smartphone-Infrastrukturen definierten Assets wird durch eine Vielzahl an Bedrohungen gefährdet. Zur Abwendung dieser Bedrohungen stehen verschiedenste Sicherheits- bzw. Schutzfunktion zur Verfügung. Schutzfunktionen finden sich dabei in allen drei Hauptbereichen von Smartphone-Infrastrukturen: Zentrale Infrastruktur, Kommunikation und Smartphone-Plattform. Das Ziel sämtlicher Schutzfunktionen ist im Allgemeinen stets die Sicherung des Kern-Assets „Daten“. Diese sollten durch geeignete Maßnahmen vor unerlaubtem Zugriff und Modifikation geschützt werden. Erreicht wird dies je nach Art der Bedrohung durch unterschiedliche Funktionen und Mechanismen, die jedoch stets nur auf ein Subset aller Bedrohungen anwendbar sind.

In diesem Abschnitt werden die einzelnen verfügbaren Schutzfunktionen näher beschrieben. Hauptaugenmerk wird dabei auf Smartphone-Plattformen und die für mobile Endgeräte verfügbaren Sicherheitsfunktionen gelegt. Neben einer Beschreibung der einzelnen Schutzfunktionen wird außerdem für jede Schutzfunktion eine Checkliste definiert. Anhand der in dieser Checkliste definierten Fragen können beliebige Smartphone-Infrastrukturen auf eine Unterstützung der jeweiligen Schutzfunktion hin überprüft werden.

1 Smartphone-Plattform

Aufgrund ihrer Exponiertheit stellen mobile Endgeräte in der Regel den verwundbarsten Bereich einer Smartphone-Infrastruktur dar. Aufgrund der vielen neuen Technologien und Möglichkeiten von Smartphones ergeben sich für Angreifer neue Varianten diese Funktionalität für bösartige Aktivitäten auszunutzen.

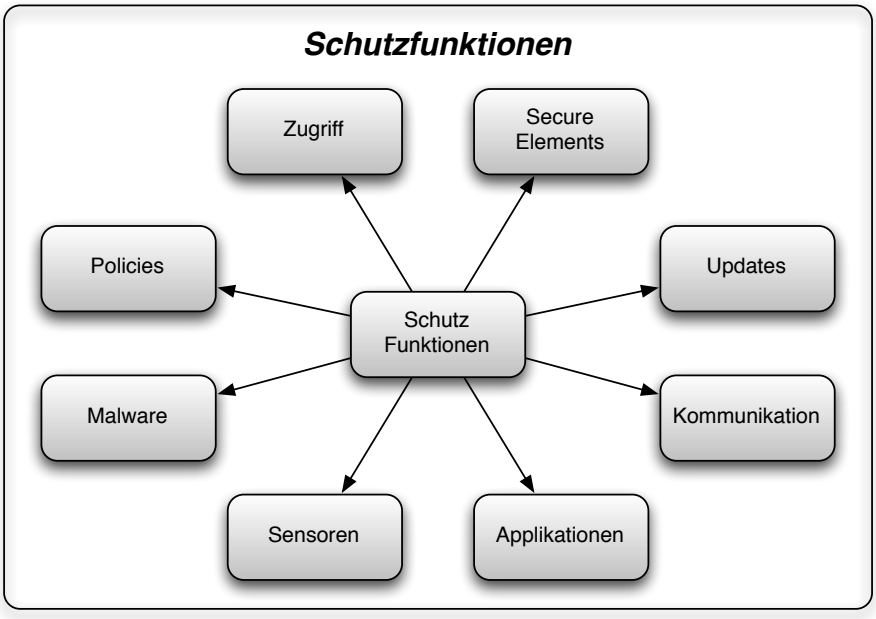

Abbildung 8 - Smartphone Schutzfunktionen

Hersteller von Smartphone-Plattformen sind sich dieser Gefahren durchaus bewusst und versuchen die Sicherheit mobiler Endgeräte durch verschiedenste Maßnahmen zu verbessern. Diese Maßnahmen decken zwar grundsätzlich stets nur einen bestimmten Teilaspekt ab, greifen jedoch oft auch ineinander um so ein möglichst engmaschiges Sicherheitsnetz zu implementieren. Bedrohungen wird so zumeist mit einer Kombination aus verschiedenen Sicherheitsmechanismen begegnet.

Aufgrund der fließenden Grenzen verschiedener Sicherheits- und Schutzfunktionen ist eine eindeutige Strukturierung oder Klassifizierung schwierig. Die im Folgenden verwendete Hierarchie versucht die verschiedenen Schutzfunktionen einer Smartphone-Plattform anhand der durch die Funktion geschützten Komponenten und Funktionen zu strukturieren. Ein Überblick wird dazu in Abbildung 8 gegeben.

1.1 Applikationsschutz

Die Möglichkeit eine Vielzahl an Applikationen (Apps) am mobilen Gerät betreiben zu können ist eine der größten Vorteile von Smartphones. Gleichzeitig bringt diese Flexibilität jedoch auch zahlreiche Gefahren mit sich. Je nach Art der Applikation kann diesen Gefahren mit verschiedenen Schutzfunktionen begegnet werden. Ein Überblick über diese Schutzfunktionen wird in Abbildung 9 gegeben.

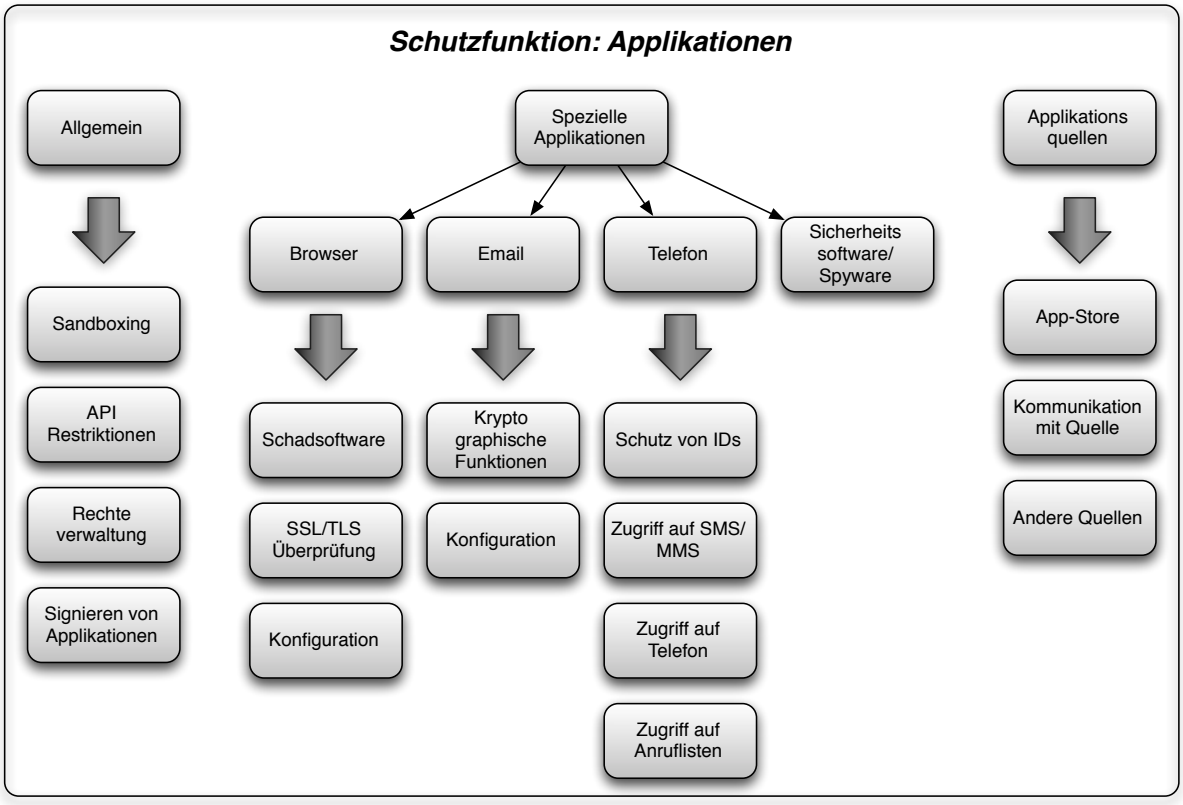

Abbildung 9 - Schutzfunktion: Applikationen

1.1.1 Allgemeine Schutzfunktionen

Um einen Schutz gegen bösartige Software zu bieten, muss eine Smartphone Plattform verschiedene allgemeine Schutzfunktionen bieten, die für alle Applikationen anwendbar sind. Prinzipiell gibt es zwei Möglichkeiten wie bösartige Software auf ein Smartphone gelangen kann:

- *Über einen legitimen Installationspfad*: In diesem Fall wird die bösartige Software direkt vom Benutzer installiert, oder das Smartphone gelangt in die Hände des Angreifers, der eine Installation der bösartigen Software vornimmt.
- *Installation einer bösartigen Software durch Ausnutzen einer Sicherheitslücke*: In diesem Fall wird davon ausgegangen, dass das Smartphone über eine Sicherheitslücke verfügt, die von einem Angreifer ausgenutzt wird. Hier greifen dann vor allem die Basissicherheitsfunktionen des Systems, die eine weitere Infektion durch die bösartige Software verhindern.

1.1.1.1 Sandboxing

Beschreibung

Unter einer Sandbox versteht man eine abgesicherte Laufzeitumgebung für Applikationen. Da Applikationen die Sandbox in der Regel nicht verlassen bzw. nicht auf Ressourcen außerhalb der Sandbox zugreifen können, können durch diesen Ansatz andere Systemkomponenten vor bösartigen Applikationen geschützt werden.

Checkliste

- *Wie ist das Sandboxing technisch umgesetzt?*
- *Welche Bereiche werden davon erfasst? Betrifft das Sandboxing nur den dauerhaften Speicher des Smartphones (z.B. Flash Speicher) oder auch den RAM Speicher?*
- *Gibt es dazu Hardwareunterstützung?*

1.1.1.2 API-Restriktionen

Beschreibung

Für die Erstellung von Smartphone-Apps stehen Entwicklern je nach Plattform unterschiedliche APIs (Application Programming Interface) zur Verfügung. Über diese APIs kann auf die von der Hardware des jeweiligen Geräts unterstützte Funktionalität zugegriffen werden. Dementsprechend wird der mögliche Funktionsumfang von Apps neben der Hardware selbst auch durch die zur Verfügung stehenden APIs definiert. In diesem Sinne können APIs als Sicherheitsfunktion betrachtet werden. Wird eine sicherheitskritische Funktion (z.B. das Abfangen von SMS-Nachrichten) von der API der Plattform nicht unterstützt, kann diese durch Schadsoftware auch nicht missbräuchlich verwendet werden. Da allerdings viele sicherheitskritische API Funktionen auch für den normalen Betrieb von Applikationen benötigt werden, sollen hier technische Maßnahmen zur Verfügung stehen, die den Zugriff auf die diversen APIs regeln.

Checkliste

- *Welche APIs stehen zur Verfügung?*
- *Können kritische Systemfunktionen über ein API aufgerufen werden?*
- *Wie wird der Zugriff der Applikationen auf diese APIs geregelt?*
- *Welche technischen (z.B. Rechteverwaltung am Smartphone) oder organisatorischen Maßnahmen (z.B. App Store Richtlinien) werden hier umgesetzt?*

1.1.1.3 Rechteverwaltung

Beschreibung

Indem Benutzer Applikationen explizit Berechtigungen für bestimmte Funktionen erteilen müssen, können Applikationen nicht ohne Wissen des Smartphonebesitzers beliebige Aktionen durchführen. Denkbar ist die Zuteilung entsprechender Berechtigungen im Zuge der Installation der Applikation oder auch während der Laufzeit.

Checkliste

- *Gibt es ein Berechtigungssystem, das den Benutzer darauf hinweist, dass eine Applikation auf kritische Funktionen oder Daten zugreift?*
- *Wie ist dieses Berechtigungssystem aufgebaut?*
- *Wie wird der Benutzer auf diese Rechte hingewiesen? Erfolgt dies bei der Verwendung der Applikation oder bei der Installation?*
- *Müssen alle Rechte akzeptiert werden oder kann hier ein Benutzer granular vorgehen?*

- *Wie verständlich ist das Berechtigungssystem für einen technisch nicht versierten Benutzer?*

1.1.1.4 Signieren von Applikationen

Beschreibung

Das Signieren von Software ist ein gängiges und probates Mittel um deren Integrität von Authentizität zu gewährleisten. Dementsprechend kann diese Methode auch verwendet werden um Smartphone-Apps zu schützen und eindeutig mit deren Urhebern zu verknüpfen. Bei der Verwendung elektronischer Signaturen zum Schutz von Apps ist auf eine geeignete Umsetzung des gesamten Signaturprozesses zu achten. Die umfasst unter anderem die generelle Vorgehensweise beim Signieren, ein sicheres Schlüsselmanagement, sowie verlässliche Signaturprüfkomponenten.

Checkliste

- *Wie sind die Signaturerstellung und Signaturprüfung technisch umgesetzt?*
- *Kann die Signaturprüfung leicht umgangen werden?*
- *Wie ist der organisatorische Ablauf? Muss sich ein Entwickler identifizieren, um einen Schlüssel zu erhalten, oder können Schlüssel beliebig erstellt werden?*
- *Auch wenn die Signatur in einer Applikationsquelle umgesetzt ist (z.B. im App Store), wie wird bei anderen Quellen vorgegangen (z.B. lokale Installation)?*

1.1.2 Absicherung des Web-Browsers

Der Web-Browser wird getrennt von anderen Applikationen betrachtet, da er eine Hauptkomponente des System darstellt. Außerdem ist ein Browser meistens tiefer als andere Applikationen in die Plattform integriert, was im Falle eins Angriffs weitere Folgen für das System haben kann.

1.1.2.1 Schutz vor Schadsoftware

Beschreibung

Manche mobilen Web-Browser verfügen über einen integrierten Schutz vor Schadsoftware. Als Beispiel kann hier das *Google Safe Browsing Feature* genannt werden, welches einen gewissen Schutz vor Phishing-Attacken bietet.

Checkliste

- *Bietet der Browser einen Malware Schutz (z.B. Google Safebrowsing)?*
- *Wie ist der Plattform-Browser in das System integriert?*
- *Wird der Browser als privilegierter Prozess ausgeführt?*
- *Greifen die anderen Sicherheitsmaßnahmen, wie Sandboxing, API Restrictions etc. auch beim Plattform-Browser?*
- *Welche Technologie wird für den Browser verwendet? Handelt es sich dabei um ein Derivat eines Desktop Browsers?*

1.1.2.2 Überprüfung von TLS/SSL Zertifikaten

Beschreibung

Die korrekte Verarbeitung und Validierung von TLS/SSL Zertifikaten ist eine grundlegende Voraussetzung und wichtige Schutzfunktion von Web-Browsern. Eine korrekte Implementierung der Überprüfung von vorgewiesenen Zertifikaten ist für die sichere Authentifizierung von Servern entscheidend. Dies spielt vor allem deshalb eine wichtige

Rolle, da Smartphones oft in unsicheren WLANs eingesetzt werden, die ein Angreifer nutzen kann um zu Daten zu gelangen oder diese zu manipulieren.

Checkliste

- *Wie wird ein Benutzer gewarnt wenn ein Zertifikat ungültig ist?*
- *Kann die Zertifikatprüfung so konfiguriert werden dass ungültige Zertifikate automatisch abgelehnt werden?*
- *Wie ist der Zertifikatspeicher des Browsers geschützt?*

1.1.2.3 Konfiguration

Beschreibung

Ausreichende Konfigurationsmöglichkeiten mobiler Web-Browser stellen ebenfalls eine wichtige Schutzfunktion dar. Die Möglichkeit einer geeigneten Konfiguration des Browsers kann die Sicherheit dabei auf zwei Arten erhöhen. Zum einen können geeignete Konfigurationsmöglichkeiten ein Anpassen des Web-Browsers auf spezielle Anforderungen ermöglichen. Zum anderen können Web-Browser und damit Smartphones durch eine zentrale Vorgabe der Konfiguration (z.B. in Unternehmen) geschützt werden.

Checkliste

- *Wird erfahrenen Benutzern durch flexible Konfigurationsmöglichkeiten die Gelegenheit geboten den Web-Browser auf ihre speziellen Anforderungen hin anzupassen und so mögliche Sicherheitsgefahren (z.B. Aktivierung von JavaScript) zu eliminieren?*
- *Können durch eine zentrale Vorgabe der Konfiguration (z.B. bei Smartphones im Besitz eines Unternehmens) Browser potentiell unerfahrener Benutzer mit einer sicheren Minimalkonfiguration versehen werden?*

1.1.3 Absicherung des E-Mail Verkehrs

1.1.3.1 Kryptographische Funktionen

Beschreibung

Zur Absicherung von über E-Mail übertragenen Daten stehen eine Reihe erprobter kryptographischer Verfahren zur Verfügung. Diese erlauben sowohl die Verschlüsselung als auch die elektronische Unterzeichnung von E-Mails, wodurch deren Vertraulichkeit, Integrität und Authentizität gewährleistet werden kann. Auf Seiten der Smartphone-Plattform bzw. des verwendeten E-Mail Clients kann eine Unterstützung dieser Verfahren daher als wichtige Schutzfunktion gesehen werden.

Checkliste

- *Werden Verfahren wie PGP oder S/MIME unterstützt? Wie wird das Schlüsselmaterial dabei geschützt?*
- *Welche Mail Protokolle werden unterstützt?*
- *Wie erfolgt die Anbindung an den Mailserver im Unternehmen?*

1.1.3.2 Konfiguration

Beschreibung

Ähnlich wie bei Web-Browsern stellen ausreichende Konfigurationsmöglichkeiten auch für E-Mail Clients eine relevante Schutzfunktion dar. Auch hier kann die Sicherheit durch geeignete Konfigurationsmöglichkeiten auf zwei Arten erhöht werden.

Checkliste

- *Wird erfahrenen Benutzern wird durch flexible Konfigurationsmöglichkeiten die Gelegenheit geboten, den E-Mail Client auf ihre speziellen Anforderungen hin anzupassen und so mögliche Sicherheitsgefahren (z.B. durch eine sichere Authentifizierung am Mail-Server) zu eliminieren?*
- *Können durch eine zentrale Vorgabe der Konfiguration (z.B. bei Smartphones im Besitz eines Unternehmens) E-Mail Clients potentiell unerfahrener Benutzer mit einer sicheren Konfiguration versehen werden.*

1.1.4 Absicherung der Telefonapplikation

Trotz aller zusätzlichen Features ist ein Smartphone in erster Linie ein Telefon. Dementsprechend spielt die Telefonfunktionalität auch eine zentrale Rolle auf sämtlichen Smartphone-Plattformen. Da Benutzer auf Smartphone-Plattformen unter Umständen direkten Zugriff auf Telefonie und verwandte Features wie SMS erlangen können, sind wiederum spezielle Schutzfunktionen notwendig.

1.1.4.1 Schutz vor Zugriff auf IDs

Beschreibung

Im Rahmen der Telefonfunktionalität kommen diverse IDs zur Anwendung. Dazu gehören beispielsweise die Telefonnummer, die eindeutige ID der verwendeten SIM-Karte und in vielen Fällen eine Plattform spezifische ID.

Checkliste

- *Wie ist der Zugriff auf diese IDs abgesichert?*
- *Welche IDs gibt es am System?*
- *Können diese IDs von anderen Applikationen ausgelesen werden?*

1.1.4.2 Schutz vor Zugriff auf SMS und MMS Nachrichten

Beschreibung

Neben der Telefonie selbst ist der Austausch von SMS und MMS Nachrichten einer der beliebtesten Mobilfunkdienste. Da SMS und MMS Nachrichten unter Umständen vertrauliche Daten beinhalten können, kann ein entsprechender Schutz dieser Nachrichten notwendig sein. Der Schutz sollte dabei idealerweise sowohl die auf dem mobilen Gerät gespeicherten Nachrichten, als auch die Empfangs- und Sendeeinheit betreffen und es Angreifern unmöglich machen Nachrichten unbemerkt vom Besitzer des Smartphones zu empfangen oder zu senden.

Checkliste

- *Wie ist der SMS/MMS Prozess in das Betriebssystem integriert?*
- *Kann eine Applikation auf die SMS/MMS Funktionalität zugreifen?*
- *Wie ist dieser Zugriff geregelt?*
- *Können über die APIs SMS/MMS von einer Applikation und unbemerkt vom Benutzer empfangen/gesendet werden?*

1.1.4.3 Schutz vor Zugriff auf Telefonfunktionalität

Beschreibung

Eine missbräuchlicher Verwendung der Telefonfunktionalität kann für den Besitzer des mobilen Geräts unangenehme finanzielle Folgen haben. Des Weiteren können durch Zugriff

auf die Telefonfunktionalität des Smartphones vertrauliche Gespräche belauscht werden. Ein expliziter Schutz der Telefonfunktionalität ist daher von besonderer Bedeutung.

Checkliste

- *Wie ist der Telefon Prozess in das Betriebssystem integriert?*
- *Kann eine Applikation auf die Telefon Funktionalität zugreifen?*
- *Wie ist dieser Zugriff geregelt?*
- *Können über die APIs Anrufe getätigt oder entgegengenommen werden, ohne dass der Benutzer etwas davon bemerkt?*

1.1.4.4 Schutz vor Zugriff auf Anruflisten

Beschreibung

Anruflisten können unter Umständen vertrauliche Kontakte enthalten. Ein Schutz dieser Daten kann gewährleistet werden, wenn auf diese Listen von Apps aus nicht zugriffen werden kann. Dadurch ist auch Schadsoftware nicht in der Lage, die in den Anruflisten enthaltenen Daten zu extrahieren und für eigene Zwecke zu missbrauchen.

Checkliste

- *Wie ist der Zugriff auf diese Daten geregelt?*
- *Ist ein Zugriff über ein API möglich?*
- *Welche Sicherheitsmaßnahmen kommen dabei zum Einsatz?*

1.1.5 Schutz von Applikationsquellen

Die Möglichkeit, deren Funktionsumfang durch diverse Softwarepakete (Apps) flexibel zu erweitern ist eine große Stärke von Smartphone-Plattformen. Gleichzeitig bringt diese Flexibilität jedoch auch einige Risiken mit sich, da auf diese Weise auch Schadsoftware relativ einfach den Weg auf das Smartphone finden kann. Ausreichende Schutzmechanismen für den gesamten Prozess der Installation neuer Applikationen sind für Smartphone-Infrastrukturen daher unumgänglich.

Prinzipiell existieren abhängig von der Smartphone-Plattform verschiedene Quellen, über die neue Applikationen bezogen werden können. Jede dieser Quellen muss über geeignete Schutzmechanismen verfügen, um die Sicherheit der Smartphone-Plattform zu gewährleisten und das Einschleusen von Schadsoftware zu verhindern.

1.1.5.1 Schutzfunktionen des App-Stores

Beschreibung

Ein App Store wird in den meisten Fällen vom Hersteller der verwendeten Plattform eingesetzt um weitere Applikationen für das Smartphone anzubieten. Hier ist es von Bedeutung zu verstehen welche technischen und organisatorischen Sicherheitsmaßnahmen vom App-Store Betreiber umgesetzt werden um das Einschleusen von bösartiger Software zu verhindern. Sollte eine Infizierung des App-Stores dennoch stattgefunden haben, sind entsprechende Gegenmaßnahmen auf Seiten des Betreibers notwendig.

Checkliste

- *Wird ein „Walled Garden“ oder ein offener Ansatz verwendet?*
- *Welche organisatorischen und technischen Maßnahmen gibt es seitens des Herstellers?*
- *Wie kann ein Entwickler Applikationen in den App Store einbringen?*

- *Welche technischen Sicherheitsmaßnahmen werden unterstützt: Kill Switch, Remote Installation von Applikationen?*
- *Gibt es andere Installationsquellen außerhalb des App Stores?*
- *Wie kann auf den App Store zugegriffen werden und von wo aus kann die Installation von Applikationen erfolgen (Smartphone, Web, etc.)?*

1.1.5.2 Absicherung der Kommunikation mit dem App-Store

Beschreibung

Um eine Applikation aus einem App Store beziehen zu können müssen verschiedene Daten vom Smartphone zum App Store und umgekehrt übermittelt werden. Dazu gehören Benutzerdaten, Informationen die für die Bezahlung von Applikationen notwendig sind, Informationen die für das Herunterladen einer Applikation notwendig sind (z.B. Applikations-IDs) und die zu installierende Applikation selbst. Die dabei übertragenen Informationen müssen geschützt werden, um deren Manipulation durch einen Angreifer zu verhindern.

Checkliste

- *Wie erfolgt die Installation einer Applikation?*
- *Wie ist der Kommunikationspfad dabei abgesichert?*
- *Erfolgt der kritische Informationsaustausch verschlüsselt?*
- *Kann eine Applikation während des Downloads verändert werden (z.B. in einem offenen WLAN)?*

1.1.5.3 Andere Quellen

Beschreibung

Neben den App Stores bieten verschiedene Hersteller die Möglichkeit, Applikationen auch von alternativen Quellen zu installieren. Beispiele dafür sind die lokale Installation über Speichermedien oder der direkte Download von beliebigen URLs. Solche Quellen können das Einschleusen bösartiger Applikationen für Angreifer erleichtern.

Checkliste

- *Welche Applikationsquellen stehen für die Plattform zur Verfügung (URL, lokale Speichermedien, etc.)?*
- *Gibt es bei diesen Quellen Sicherheitsmaßnahmen wie z.B. das Signieren von Applikationen?*
- *Falls es potentiell unsichere Quellen gibt, wie einfach ist es einen Benutzer erfolgreich aufzufordern diese zu akzeptieren?*

1.1.6 Sicherheitssoftware und Spyware

Beschreibung

Für beinahe jede Smartphone-Plattform gibt es eine beträchtliche Anzahl an Applikationen, die Benutzern eine Reihe von Sicherheitsfunktionen zur Verfügung stellen. Dazu gehört beispielsweise auch sogenannte Spyware, die es erlaubt, das Smartphone für Spionagezwecke (vor allem im privaten Bereich) zu verwenden.

Aufgrund der vielfältigen Funktionen und Möglichkeiten, die diese Tools bieten, können diese durchaus als Schutzmechanismus, der zum Absichern des eigenen Geräts verwendet werden kann, klassifiziert werden. Die Verwendung derartiger Applikationen birgt jedoch auch diverse Risiken, da sich hinter solchen scheinbar nützlichen Tools unter Umständen auch Schadsoftware verbergen kann, die über nahezu uneingeschränkten Zugriff auf die Smartphone-Plattform verfügen und daher beträchtlichen Schaden anrichten können.

Checkliste

- *Wie tief kann eine Sicherheitsapplikation in das System eingreifen? Ist diese beispielsweise in der Lage SMS Nachrichten abzufangen oder Zugriff auf kritische APIs zu erlangen?*
- *Wie einfach können solche Applikationen installiert werden? Ist es vor allem im privaten Bereich leicht möglich die Software als Spyware zu missbrauchen und ohne das Wissen von Drittpersonen zu installieren?*
- *Wie gut kann sich die Sicherheitssoftware in die Plattform integrieren? Läuft diese als Systemapplikation oder Hintergrundprozess?*

1.2 Schutz von Sensordaten

Abbildung 10 - Schutzfunktion: Sensoren

Smartphones sind in der Regel mit einer Vielzahl unterschiedlicher Sensoren ausgestattet. Die von diesen Sensoren gesammelten und aufgezeichneten Daten können vertraulicher Natur sein. Ein adäquater Schutz dieser Daten ist daher für die Gesamtsicherheit von Smartphone-Plattformen unumgänglich.

1.2.1 Zugriffsschutz auf Sensoren

Beschreibung

Um den Zugriff auf Sensoren eines Smartphones zu schützen, kommt zumeist eine entsprechende Zugriffsrechteverwaltung zur Anwendung. Benutzer müssen bei der Installation einer Applikation angeben, auf welche Sensoren des Smartphones die zu installierende App Zugriff erlangen darf.

Checkliste

- *Auf welche Sensoren können Applikationen zugreifen?*
- *Welcher Sicherheitsmaßnahmen gibt es um diesen Zugriff zu regeln?*
- *Ist es für den Benutzer ersichtlich auf welche Sensoren eine Applikation zugreift?*
- *Können Sensoren deaktiviert werden?*

1.2.2 Schutz von Sensordaten

Beschreibung

Abhängig von der Art des Sensors können aufgezeichnete Sensordaten unter Umständen auch am mobilen Gerät gespeichert werden. Zum Schutz dieser gespeicherten Daten vor unerlaubtem Zugriff können verschiedene Schutzmechanismen wie Verschlüsselung oder Passwort-Schutz zur Anwendung kommen. Hier spielt das Betriebssystem des Smartphones eine entscheidende Rolle, indem es geeignete Schutzmechanismen anbietet, einen verantwortungsvollen Umgang mit Sensordaten implementiert und beispielsweise aktuelle Positionsdaten nicht ohne Zutun des Besitzers an Dritte überträgt. Dies betrifft beispielsweise lokal am Gerät gespeicherte GPS-Positionsdaten.

Checkliste

- *Werden von der Plattform Sensordaten aufgezeichnet (z.B. Positionsdaten) und wenn ja wie werden diese verwendet?*
- *Wie werden Sensordaten, die von der Plattform aufgezeichnet werden, gesichert?*

1.2.3 Anzeige aktiver Sensoren

Beschreibung

Während Benutzer in der Regel sehr wohl über die Ausstattung ihres Smartphones informiert sind und daher wissen, über welche Sensoren dieses verfügt, bleibt oft unklar welche Sensoren zu welchem Zeitpunkt gerade aktiv sind. Somit könnte eine böswillige Applikation beispielsweise das Mikrofon des Smartphones vom Benutzer unbemerkt einschalten um vertrauliche Gespräche aufzuzeichnen.

Ein Schutz gegen diese Art von Angriffe ist die verpflichtende Anzeige aktiver Sensoren. Da böswillige Applikationen in der Regel ihre Aktivität zu verstecken versuchen, muss dieser Schutzmechanismus vom Betriebssystem implementiert werden. Jede Aktivierung eines Sensors muss eine entsprechende Anzeige zur Folge haben. Dies kann beispielsweise über das Display des Smartphones, oder aber auch über ein eigenes LED erfolgen.

Checkliste

- *Ist es möglich die Aktivität von Sensoren dem Benutzer anzuzeigen? Können Benutzer beispielsweise feststellen ob GPS, Mikrophon oder Kamera gerade aktiv sind?*
- *Erfolgt dies intuitiv für den Benutzer?*

1.3 Schutz vor Schadsoftware

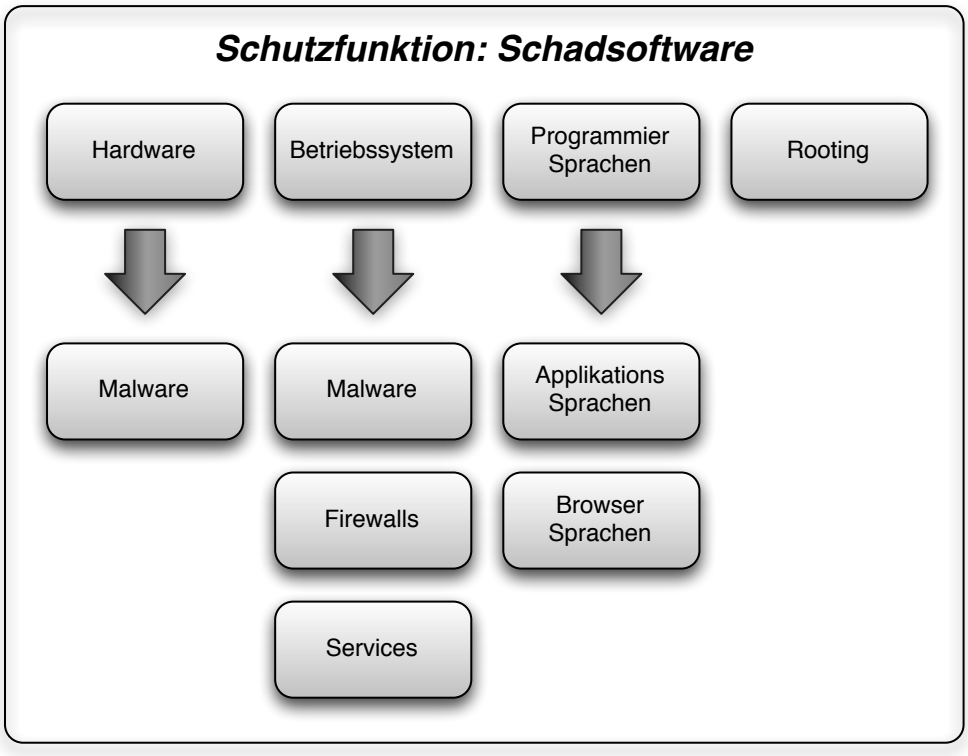

Abbildung 11 - Schutzfunktion: Schadsoftware

Durch ihren ständig wachsenden Funktionsumfang werden moderne Smartphones Desktop PCs und Laptops zunehmend ähnlicher. Damit werden für Smartphones auch diverse Probleme ein Thema, die für herkömmliche Mobiltelefone noch gänzlich irrelevant waren. Dies betrifft vor allem den Umgang mit Schadsoftware wie Viren, Würmer und Trojaner, für welche auf Smartphones einige Schutzfunktionen existieren.

1.3.1 Schutzmechanismen der Hardware

1.3.1.1 Malware

Beschreibung

Aktuelle CPUs verwenden hardwarebasierte Mechanismen die vor Malwareinfektionen schützen sollen.

Checkliste

- *Welche hardwarebasierten Maßnahmen (NX Flags, Trust Zones, etc.) werden unterstützt?*
- *Gibt es Secure Elements (siehe Beschreibung der Sicherheitsfunktion)?*

1.3.2 Schutzmechanismen des Betriebssystems

1.3.2.1 Malware

Beschreibung

Das Betriebssystem kann selbst diverse Basismethoden implementieren, die einen Schutz vor bösartiger Software bieten.

Checkliste

- *Welche Maßnahmen (z.B. Address Space Layout Randomization (ASLR)) werden vom Betriebssystem unterstützt?*
- *Gibt es Antiviren Software?*
- *Wie kann diese in das System integriert werden?*
- *Welche Funktionen stehen solchen Softwareprodukten zur Verfügung?*
- *Welche Aspekte werden von dieser Software untersucht?*

1.3.2.2 Firewalls

Beschreibung

Durch den Einsatz von Firewalls kann die Netzwerkkommunikation eines Smartphones geeignet abgesichert bzw. der Netzwerkverkehr überwacht werden. Firewalls kommen in herkömmlichen Desktop-PC und Laptop basierten Systemen bereits regelmäßig zur Anwendung. Mit der steigenden Funktionalität von Smartphones spielen Firewall-Lösungen auch für diese Geräte eine zunehmend wichtige Rolle.

Checkliste

- *Sind Firewalls auf dem Smartphone vorhanden?*
- *Wenn ja, welche Technologien werden dabei eingesetzt?*
- *Wie wird die Firewall konfiguriert?*
- *Wie hoch ist der Grad an Benutzerfreundlichkeit beim Umgang mit verfügbaren Firewall-Lösungen?*

1.3.2.3 Services

Beschreibung

Je nach Plattform werden Netzwerkservices auf den Netzwerkschnittstellen angeboten die im Internet zur Verfügung stehen. Diese Services werden für unterschiedliche Anwendungen wie z.B. für die Synchronisation mit dem PC verwendet. Stehen solche Services auf Internetschnittstellen zur Verfügung, muss beachtet werden, dass diese auch von einem Angreifer erreicht werden können. Befinden sich in diesen Schnittstellen Sicherheitslücken, kann ein Angreifer diese über das Internet ausnutzen.

Checkliste

- *Gibt es Netzwerkservices des Smartphones die aus dem Internet erreichbar sind?*
- *Wie sind diese abgesichert?*

1.3.3 Programmiersprachen

1.3.3.1 Sprachen für Applikationen

Beschreibung

Die der Smartphone-Plattform zugrundeliegende Programmiersprache kann für die Sicherheit des Systems von Relevanz sein. Die Programmiersprache Java™ verfügt beispielsweise über eine automatische Überprüfung der Grenzen von Speicherfeldern (Array Bound Checking). Buffer-Overflows, die beispielsweise in C-basierten Programmen stets ein gewisses Sicherheitsrisiko darstellen, sind auf Java™ basierten Systemen wie Android daher grundsätzlich nicht möglich.

Checkliste

- *Welche Sprachen werden auf der Smartphone Plattform unterstützt?*
- *Welche Sprachen stehen dabei den Applikationsentwicklern zur Verfügung, welche wird für das System selbst verwendet?*
- *Über welche Sicherheitsmaßnahmen verfügt die eingesetzte Sprache? Ist ein Schutz vor Buffer-Overflows gegeben?*

1.3.3.2 Sprachen im Browser

Beschreibung

Auch im Browser werden unterschiedliche Sprachen unterstützt. Dies spielt eine zunehmend wichtige Rolle, da viele bisher plattformspezifische Applikationen in die Cloud verlegt werden. Dort spielen neue Technologien wie HTML5 und der vermehrte Einsatz von JavaScript eine entscheidende Rolle. Durch die neuen Features ergeben sich aber auch neue Angriffsmöglichkeiten, die auch für das Smartphone relevant sind.

Checkliste

- *Welche Sprachen und Plug-ins (JavaScript, Actionscript (Flash)) werden vom Plattform Browser unterstützt?*
- *Welche Sicherheitsrisiken ergeben sich für die unterstützten Technologien?*

1.3.3.3 Schutz vor Rooting

Beschreibung

Unter Rooting oder Jailbreaking versteht man den Vorgang der nötig ist, um vollen Zugang zu allen Systemressourcen als privilegierter Benutzer zu bekommen. Dem Anwender stehen

dann Funktionen zur Verfügung, die im normalen Betriebsmodus nicht aufgerufen werden können. Wenn das System keine definierte Möglichkeit bietet diesen Root Zugang zu bekommen (z.B. über Bootloader), werden in den meisten Fällen diverse Sicherheitslücken ausgenutzt um dies zu ermöglichen.

Generell sind zwei Aspekte zu betrachten: Zum einen stehen nach dem Rooten/Jailbreaken viel mehr Möglichkeiten zur Verfügung, die auch von einem Angreifer ausgenutzt werden können. Zum anderen kann durch die Analyse der bestehenden Rooting/Jailbreaking Methoden ein Überblick über die Sicherheit des Systems erlangt werden. Kann ein Jailbreak z.B. über den Browser durchgeführt werden, deutet dies auf eine Sicherheitslücke im Browser hin, die einen Zugriff auf alle Systemressourcen ermöglicht..

Checkliste

- *Wie kann ein Rooting oder ein Jailbreak durchgeführt werden?*
- *Welche Sicherheitslücken werden hierbei ausgenützt? Welche Auswirkungen haben diese auf das System?*
- *Wenn dies vom Hersteller definierte Funktionen sind, können diese über Konfigurationseinstellungen deaktiviert werden?*

1.4 Zugriffsschutz

Abbildung 12 - Schutzfunktion: Zugriff

Ein Vorteil und Risiko zugleich ist die Mobilität von Smartphones. Da diese vom Benutzer meist mitgeführt werden, ist das Risiko für Verlust oder Diebstahl ungleich größer als bei stationären Geräten wie Desktop PCs. Mit dem Verlust des Smartphones fallen einem Finder oder Dieb potentiell auch sämtliche am Smartphone gespeicherten Daten in die Hände. Ein geeigneter Schutz der am Smartphone gespeicherten Daten ist daher unbedingt notwendig.

1.4.1 Datenverschlüsselung

Beschreibung

Werden sicherheitskritische oder vertrauliche Daten am Smartphone verschlüsselt gespeichert, können diese nur von Personen, die Zugriff auf den entsprechenden kryptographischen Schlüssel haben, eingesehen und bearbeitet werden. Eine Verschlüsselung stellt also in jedem Fall einen adäquaten Zugriffsschutz dar, ist jedoch auch mit zusätzlichem Aufwand verbunden. Zusätzlich bedarf es eines wohlüberlegten Schlüsselmanagements um die Sicherheit der gespeicherten Daten tatsächlich zu gewährleisten.

Checkliste

- *Steht eine systemweite Verschlüsselung von Daten zur Verfügung?*
- *Wo werden die eingesetzten Schlüssel aufbewahrt?*
- *Wird ein Schlüssel aus dem von Benutzer gesetzten PIN/Passwort abgeleitet?*
- *Stehen APIs zur Verfügung die es Applikationen erlauben Daten zu verschlüsseln?*
- *Welche Algorithmen werden eingesetzt?*

- *Ist die Verschlüsselung standardmäßig aktiviert?*

1.4.2 Sperre des Smartphones

Beschreibung

Ähnlich wie PCs oder Laptops können auch Smartphones in der Regel durch eine PIN oder ein Passwort geschützt werden. Ein Zugriff auf Daten und Funktionalität des Smartphones sind in diesem Fall nur nach Eingabe eines gültigen Passworts möglich. Das Telefon wird dabei in der Regel nach einer definierbaren Dauer der Inaktivität automatisch gesperrt und muss danach vor einer weiteren Verwendung wieder entsperrt werden.

Obwohl der direkte Zugriff auf Daten durch diese Schutzfunktion verhindert wird, sind die Daten im Speicher des Smartphones unverschlüsselt hinterlegt. Erlangt ein Angreifer über einen anderen Kanal Zugriff auf diese Daten (im einfachsten Fall durch Entfernen der Speicherkarte und Einsetzen dieser in ein anderes Gerät), wird diese Schutzfunktion wirkungslos.

Zur Gewährleistung der Sicherheit dieser Schutzfunktion bedarf es einer sicheren Eingabeeinheit, über die das geheime Passwort sicher eigegeben werden kann. Angreifern darf es nicht möglich sein, durch eine Kompromittierung der Eingabeeinheit (d.h. der Tastatur) das vom Benutzer eingegebene Passwort zu extrahieren. Als Alternative zur Authentifizierung über Passwort oder PIN können auch biometrische Merkmale herangezogen werden.

Checkliste

- *Welche Sperrfunktionen (PIN/Passwort/Patterns/Biometrie) stehen Benutzern zur Verfügung?*
- *Wie lange können/müssen eingegebene Passwörter/PINs sein?*
- *Hängen Verschlüsselungsfunktionen mit den definierten PINs/Passwörtern zusammen?*
- *Gibt es Konfigurationsoptionen, die Details der PIN/Passwortsperre berücksichtigen?*

1.4.3 Remote Wipe/Location

Beschreibung

Eine Remote Wipe Funktion erlaubt das Löschen von Daten am Smartphone ohne unmittelbaren Zugriff auf dieses zu haben. Wird das Gerät beispielsweise gestohlen, kann der Besitzer des Smartphones vertrauliche Daten remote löschen. Die entsprechenden Befehle werden dabei über ein OTA Interface an das mobile Gerät übertragen. Zusätzlich bieten diverse Hersteller auch die Möglichkeit die Position eines gestohlenen Smartphones festzustellen.

Checkliste

- *Wird eine Remote Wipe Funktion unterstützt?*
- *Wie kann die Remote Wipe Funktion ausgeführt werden?*
- *Wird bei Remote Wipe eine etwaige vorhandene Verschlüsselung berücksichtigt, und nur die Schlüssel anstelle der Daten gelöscht?*
- *Kann die aktuelle Position des Smartphones remote bestimmt werden?*
- *Wie ist die Remote Wipe Funktion am Smartphone geschützt?*
- *Wie ist das Ausführen der Remote Wipe Funktion geschützt?*

1.4.4 Schutz von Zugangsdaten

Beschreibung

Auf Smartphones sind in der Regel eine Reihe von Passwörtern gespeichert. Beispielsweise werden Passwörter für E-Mail Konten oder VPN-Zugänge lokal am Gerät hinterlegt um dem Benutzer eine wiederholte Eingabe dieser Passwörter zu ersparen.

Generell ist diese Maßnahme zur Steigerung der Benutzerfreundlichkeit kritisch zu hinterfragen, da lokal gespeicherte Passwörter stets ein gewisses Sicherheitsrisiko darstellen. Dies gilt auch für PC oder Laptop basierte Systeme, besonders jedoch für Smartphones, die aufgrund ihrer Mobilität einem erhöhten Risiko für Diebstahl oder Verlust ausgesetzt sind. Wenn Passwörter lokal gespeichert werden müssen, sollten diese daher ausschließlich verschlüsselt am Smartphone hinterlegt werden. Der Passwortspeicher sollte zudem durch ein Passwort oder eine PIN abgesichert sein.

Checkliste

- *Gibt es einen zentralen Dienst, der das Speichern von Zugangsdaten anbietet?*
- *Welche Arten von Zugangsdaten (private Schlüssel, Passwörter/PINs, Shared Keys) können dort abgelegt werden?*
- *Wie wird dieser Dienst vor unbefugten Zugriffen geschützt?*
- *Welche kryptographischen Methoden werden zum Sichern der Zugangsdaten eingesetzt?*
- *Werden die Schlüssel für das Verschlüsseln des Zugangsdatenspeichers aus PINs/Passwörtern abgeleitet, in einem HSM oder im Speicher des Geräts aufbewahrt?*
- *Hat ein Angreifer nach der Durchführung eines Jailbreaks (Rooten) die Möglichkeit die Zugangsdaten zu verwenden ohne einen PIN oder ein Passwort einzugeben?*

1.5 Policies

Beschreibung

Eine sehr wichtige Komponente für die Sicherheit einer Smartphone–Plattform, die in einem Unternehmen oder im Rahmen von M-Government Anwendungen in einer Behörde eingesetzt wird, ist ein Policy Management Framework. Diese Technologie ermöglicht das Vorschreiben technischer Sicherheitsmaßnahmen und deren zwingende Umsetzung auf verwendeten Smartphones. Benutzer haben in der Regel keine Möglichkeit diese Vorgaben zu ändern. Dies spielt vor allem im Bereich Verschlüsselung, bei der Vorgabe von Mindestlängen bei PINs und Passwörtern, oder beim Installieren von externen Applikationen eine Rolle. Abhängig vom Hersteller existieren auch noch viel tiefergehende Policies, die alle Funktionen eines Smartphones abdecken können. Ein Policy Framework ist beim Einsatz einer Smartphone Plattform in Unternehmen und Behörden unabdingbar, da nur so eine existierende IT Security Policy auf Smartphones abgebildet werden kann.

Checkliste

- *Ist ein Policy Management Framework vorhanden?*
- *Welche Policies werden unterstützt?*
- *Wie sicher sind diese bei der Anwendung am Smartphone?*
- *Existieren entsprechende Lösungen von Drittanbietern falls es kein entsprechendes Framework des Herstellers gibt?*
- *Unterstützt die Plattform elementare Sicherheitsfeatures (z.B. Verschlüsselung) um ein Policy-Framework sinnvoll anzuwenden?*

1.6 Secure Elements

Beschreibung

Secure Elements bergen aus sicherheitstechnischer Sicht ein großes Potential. Diese Hardwarekomponenten können einerseits als sicherer Schlüsselspeicher fungieren und stellen andererseits eine Reihe kryptographischer Operation zur Verfügung. Mit Hilfe von Secure Elements können daher verschiedene auf Kryptographie basierende Schutzmechanismen implementiert und die Sicherheit von Smartphone-Plattformen erhöht werden.

Checkliste

- *Stehen vorhandene Secure Elements den Applikationen zur Verfügung?*
- *Wie ist der Zugriff auf Secure Elements abgesichert?*
- *Wie erfolgt eine sichere PIN/Passwort Eingabe des Benutzers?*
- *Steht ein systemweites Service/API zur Verfügung, das den Zugriff auf Secure Elements erlaubt?*

1.7 Updates

Beschreibung

Ein funktionierender Update-Mechanismus stellt ebenfalls eine wichtige Schutzfunktion dar. Da die Erstellung fehlerfreier Software in der Realität kaum zu erfüllen ist, ist die Möglichkeit einer schnellstmöglichen Korrektur entdeckter Fehler und Sicherheitslücken umso wichtiger. Zuverlässige Updatemechanismen gewährleisten, dass aktualisierte und verbesserte Version von Softwarekomponenten rasch und zuverlässig an die einzelnen mobilen Endgeräte übermittelt und auf diesen installiert werden können. Dadurch können Smartphones stets auf einem aktuellen Stand gehalten und deren Sicherheit gewährleistet werden.

Checkliste

- *Gibt es regelmäßige Updates?*
- *Wie lange braucht der Hersteller um kritische Sicherheitslücken zu patchen?*
- *In welcher Form wird das Update durchgeführt? Kommen Delta Updates oder komplette Update des ganzen Systems zur Anwendung?*
- *Kann das Update Over The Air (OTA) erfolgen oder muss hier das Gerät an einen PC angeschlossen werden?*
- *Wie erfolgt das Update der Applikationen aus App Stores?*
- *Wie lange wird ein Smartphone Modell des Herstellers mit Updates versorgt?*

2 Kommunikation

Der Kommunikationspfad zwischen zentraler Infrastruktur und Smartphone stellt den zweiten Hauptbereich einer Smartphone-Infrastruktur dar. Über diesen Kommunikationspfad werden Daten zwischen zentralen Komponenten und entfernten mobilen Geräten ausgetauscht. Die Datenübertragung erfolgt dabei in der Regel über drahtlose Kommunikationsprotokolle. Um ein Abhören der übertragenen Daten zu unterbinden, ist die Anwendung verschiedener Schutzmaßnahmen nötig. Auf die verschiedenen verfügbaren Maßnahmen zur Absicherung der Kommunikation zwischen zentraler Infrastruktur und mobilen Endgeräten wird in diesem Abschnitt näher eingegangen.

2.1 Schutz von Kommunikationskanälen

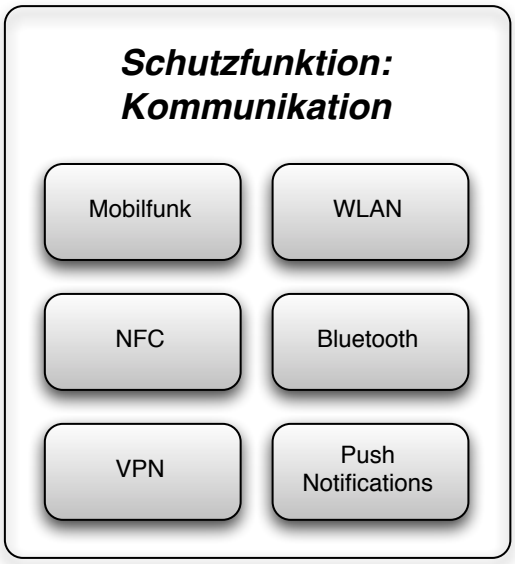

Abbildung 13 - Schutzfunktion: Kommunikation

Die verschiedenen von Smartphones verwendeten mobilen Kommunikationskanäle bieten unterschiedliche Möglichkeiten der Absicherung. Im folgenden werden Schutzfunktionen der am häufigsten verwendeten Kommunikationstechnologien diskutiert.

2.1.1 WLAN

Beschreibung

Zur Absicherung der Kommunikation über WLAN stehen diverse erprobte Protokolle zur Verfügung. Als Beispiel kann hier der Wi-Fi Protected Access (WPA) Standard bzw. dessen Nachfolger WPA2 genannt werden. Basierend auf kryptographischen Methoden ermöglichen diese Protokolle eine sichere Kommunikation über drahtlose Netzwerke. Auf Seiten der Smartphone-Plattform ist dazu die Unterstützung dieser Protokolle und Standards notwendig.

Checkliste

- *Welche WLAN Sicherheitsfeatures werden unterstützt?*

2.1.2 Bluetooth

Beschreibung

Bluetooth stellt eine Kommunikationsmethode dar, mit der das Smartphone über kurze Entfernungen mit anderen Geräten kommunizieren kann. Anwendungsbeispiele sind Freisprecheinrichtungen, der Austausch von Kontaktdaten, der Transfer von Daten oder das zur Anbieten einer Internetanbindung für ein anderes Gerät (Tethering).

Checkliste

- *Können sicherheitsrelevante Bluetooth Einstellungen am Smartphone konfiguriert werden?*
- *Können diese über das etwaige Policy Framework konfiguriert werden?*

2.1.3 Mobilfunk

Beschreibung

Die gängigen Mobilfunkprotokolle GSM, UMTS und LTE sind die Basistechnologien die für den Zugang zum Internet verwendet werden. Vor allem für GSM sind viele Sicherheitsprobleme bekannt. Um einen adäquaten Schutz übermittelter Daten zu erreichen, ist die Verwendung kryptographischer Methoden auf höheren Abstraktionsebenen nötig (siehe dazu auch Abschnitt 2.2).

Checkliste

- *Speziell der GSM Standard gilt als unsicher. Sicherheitsmaßnahmen müssen auf höheren Schichten implementiert werden. Es muss allerdings für alle Analysepunkte beachtet werden, dass eine spezielle Eigenschaft bei Smartphones die dauerhafte Datenverbindung ist. Dies eröffnet weitere Angriffsmöglichkeiten, die alle Komponenten betreffen.*

2.1.4 NFC

Beschreibung

NFC ist eine relativ neue Technologie und scheint vor allem im Rahmen des bargeldlosen Bezahlens eine vielversprechende Zukunft zu haben. Durch die Verwandtschaft zur RFID Technologie können einige der für RFID entwickelten Sicherheitsmechanismen auch für NFC basierte Kommunikation verwendet werden.

Checkliste

- *Hier gibt es zum aktuellen Zeitpunkt keine Punkte.*

2.2 VPN

Beschreibung

Virtuelle private Netzwerke (VPN) bieten die Möglichkeit durch Verwendung kryptographischer Verfahren abgesicherte Netzwerke auf ursprünglich unsicheren Netzen zu betreiben. Damit können beispielsweise Endgeräte wie PCs, Laptops, aber auch Smartphones über eine abgesicherte Verbindung an zentrale Netze angebunden werden. Virtuelle private Netzwerke können über unterschiedliche Protokolle implementiert werden. Zu den am häufigsten verwendeten Protokollen zählen dabei IPsec, L2TP und PPTP.

Checkliste

- *Welche VPN Protokolle werden unterstützt?*
- *Wie werden die Zugangsdaten gesichert?*
- *Wo werden Truststores (z.B. Zertifikate) abgelegt und wie werden diese gesichert?*
- *Kann ein Smartphone mit aktivierter VPN Verbindung als Reflector verwendet werden? Dies bedeutet, dass das Smartphone sowohl mit dem internen Netzwerk als auch dem Internet verbunden ist und Verkehr von oder zu beiden Bereichen gleichzeitig möglich ist. Im Falle des Einschleusens von Schadsoftware steht somit einem Angreifer ein Zugangspunkt über das Internet zur Verfügung.*

2.3 Benachrichtigungen (Push-Services)

Beschreibung

Push-Services werden vom Plattformhersteller benutzt, um Benachrichtigungen an das Smartphone zu schicken. Dabei können die hier eingesetzten Technologien und

Anwendungen unterschiedlichster Natur sein. Vor allem für Applikationsentwickler spielt es aber eine Rolle wie ein Push-Service abgesichert ist, wenn kritische Informationen an Applikationen übermittelt werden sollen.

Checkliste

- *Welche Technologie wird beim Push-Service eines Herstellers eingesetzt?*
- *Wie wird die Kommunikation zum mobilen Gerät abgesichert?*
- *Typischerweise ist bei solchen Services ein Server des Herstellers beteiligt, um die Nachrichten an die Smartphones weiterzuleiten. Gibt es eine Ende-zu-Ende Verschlüsselung die das Lesen der Nachrichten des Herstellers verhindert?*

3 Zentrale Infrastruktur

Zentrale Infrastrukturen werden meist in entsprechend abgesicherten Rechenzentren betrieben. Der Schutz von Rechenzentren bedarf umfassender Maßnahmen, auf die im Rahmen dieses Dokuments nicht im Detail eingegangen werden soll. In der Regel wird die Gewährleistung eines adäquaten Sicherheitsniveaus beim Betrieb von Rechenzentren ohnehin durch externe Audits anhand bewährter nationaler und internationaler Standards überprüft.

Durch die Integration von Smartphones in bestehende Infrastrukturen können sich jedoch zusätzliche Risiken ergeben. Im Folgenden sollen diverse Schutzfunktionen, mit denen diesen Risiken auf zentraler Seite begegnet werden kann, diskutiert werden.

3.1 Smartphone Plattform

Beschreibung

Bevor eine Smartphone Plattform in Unternehmen oder Behörden eingesetzt werden kann, müssen die Sicherheitsfeatures der geplanten Verwendung gegenübergestellt werden. Im Prinzip müssen dabei alle bisher diskutierten Schutzfunktionen überprüft werden.

Checkliste

- *Für welche Aufgaben sollen Smartphones verwendet werden, auf welche Daten wird dabei zugegriffen und wie erfolgt dieser Zugriff (z.B. über interne oder externe Services)?*
- *Für wie lange sind Updates für die gewünschte Smartphone Plattform verfügbar?*
- *Welche Sicherheitsfunktionen werden unterstützt? Hier muss vor allem auf Zugriffschutz, Verschlüsselung und Remote Wipe für den Fall eines Diebstahls geachtet werden.*
- *Gibt es ein Policy Management Framework, das das Abbilden einer IT-Sicherheitspolicy am Smartphone zulässt?*

3.2 IT-Sicherheitspolicy und Schulungen

Beschreibung

Da sich Smartphones durch ihre Mobilität sowohl in Bezug auf Möglichkeiten als auch in Bezug auf Gefahren signifikant von anderen mobilen Geräten wie Laptops unterscheiden, muss eine an Smartphones angepasste Sicherheitspolicy erstellt werden. Die für Mitarbeiter relevanten Punkte und potentielle Gefahren bei Smartphones müssen in geeigneter Weise (z.B. in Form von Schulungen) vermittelt werden, um so ein Bewusstsein für die Gefahren im Umgang mit Smartphones zu schaffen. Nur wenn sich sämtliche Mitarbeiter eines Unternehmens oder einer Behörde über Bedrohungen und entsprechende

Gegenmaßnahmen im Klaren sind, kann die Sicherheit von Smartphone-Infrastrukturen gewährleistet werden.

Checkliste

- *Werden die eingeschränkten Zugriffschutzmechanismen des Smartphones berücksichtigt (z.B. PIN/Passwortlänge)?*
- *Gibt es Richtlinien für die Verwendung von Smartphones?*
- *Wie werden die Mitarbeiter geschult? Auf welche Punkte wird hier eingegangen?*
- *Wie wird bei Verlust eines Geräts vorgegangen?*
- *Wird in den Policies geregelt auf welche Dienste und Daten das Smartphone Zugriff haben darf?*
- *Gibt es Policies, die das Verwenden von (eigenen und fremden) Smartphones in den Gebäuden des Unternehmens bzw. der Behörde (z.B. bei Meetings) regeln?*

3.3 Anbindung von Smartphones

3.3.1 VPN-Unterstützung

Beschreibung

Wie auch in Abschnitt 2.2 erläutert, spielt die VPN Technologie eine entscheidende Rolle bei der sicheren Anbindung von Smartphones an zentrale Infrastrukturen. Eine Unterstützung dieser Technologie und die Bereitstellung und Wartung entsprechender VPN Entry-Points stellt daher auch für zentrale Infrastrukturen eine wichtige Schutzfunktion dar.

Für den Fall dass die verwendeten VPNs korrekt konfiguriert sind und die für den externen Zugang verwendeten Zugangsdaten ausreichend geschützt bleiben, bietet VPN eine sichere und zuverlässige Möglichkeit der Anbindung externer Komponenten. Ein kompromittierter VPN-Zugang stellt hingegen eine ernstzunehmende Bedrohung für die Sicherheit der gesamten Smartphone-Infrastruktur dar. Eine ausreichende Absicherung der gesamten VPN-Infrastruktur ist daher eine zwingende Voraussetzung für den erfolgreichen Einsatz von VPN als Schutzfunktion.

Checkliste

- *Welche VPN Lösung wird verwendet?*
- *Wie werden die Zugangsdaten am Smartphone abgesichert?*
- *Wird hier eine Technologie eingesetzt die den schnellen Austausch von Schlüsseln im Falle des Kompromittierens ermöglicht (z.B. keine Shared IPsec Keys)?*
- *Wird der gesamte Verkehr des Smartphones über die VPN Verbindung geleitet (also auch der HTTP Verkehr des Browsers)?*

3.3.2 Zonen

Beschreibung

Eine Verbindung von Smartphones zum Unternehmen oder zur Behörde wird dann benötigt, wenn diese auf Daten oder Dienste des Unternehmens oder der Behörde zugreifen müssen. Dabei handelt es sich entweder um den Zugriff auf die E-Mail Server des Unternehmens, oder um den Zugriff auf interne Dienste via Browser oder eigenen am Smartphone installierte Applikationen. Dabei muss das Smartphone also einen Zugriff auf das interne Netzwerk haben.

Checkliste

- *Kann das Smartphone nur auf die absolut notwendigen Dienste zugreifen?*

- *Werden dazu eigene Zonen im internen Netzwerk für Smartphones und andere Geräte verwendet?*
- *Sind andere Netzwerke, auf die die Smartphones keinen Zugriff haben dürfen, durch Firewalls abgesichert?*

3.4 Smartphone Verwaltung

Beschreibung

Um Smartphones verwalten zu können muss typischerweise ein dedizierter Server in der zentralen Infrastruktur eingesetzt werden. Da die dafür benötigten Daten wie Policies oder Schlüsselmaterial unbedingt geschützt werden müssen, ist sicherzustellen, dass der Server so in das Unternehmensnetzwerk integriert ist, dass Angriffe verhindert werden können.

Checkliste

- *Ist ein dedizierter Konfigurationsserver notwendig bzw. vorhanden?*
- *Wie ist der Konfigurationsserver in die zentrale Infrastruktur des Unternehmens bzw. der Behörde integriert?*
- *Werden die Daten mit anderen Applikationen zusammen abgelegt, die leichter angreifbar sind (z.B. über externe Webservices)?*
- *Wo wird etwaiges Schlüsselmaterial aufbewahrt?*
- *Wie ist der Zugriff auf diesen Server im Unternehmen technisch und organisatorisch geregelt?*

3.5 E-Mail Anbindung

Beschreibung

Smartphones werden typischerweise für den mobilen Zugriff auf E-Mail Server des Unternehmens oder der Behörde verwendet. Dabei muss davon ausgegangen werden, dass E-Mails vertrauliche Daten enthalten, die eine sichere Verwendung unbedingt nötig machen.

Checkliste

- *Wie sind die Smartphones an den internen E-Mail Server angebunden? Welche Lösung kommt hier zum Einsatz? Erfolgt der Zugriff direkt oder über eigenen Server?*
- *Werden Maßnahmen wie S/MIME oder PGP verwendet?*
- *Welche Daten der E-Mails werden an die Smartphones weitergeleitet (z.B. Attachments)?*
- *Gibt es Funktionen die etwaige Phishing E-Mails filtern?*