Jens Heider

Die Gretchenfrage: Wie halten Sie's mit der App-Sicherheit?

Herausforderungen und Strategien für den Umgang mit Apps im Arbeitsumfeld

Durch die immer stärkere Integration von Smartphones und Tablets in den Arbeitsalltag basiert heute die Sicherheit von Unternehmensdaten nicht mehr nur auf der Absicherung auf Netzwerk-und Endgeräteebene. Die Vertrauenswürdigkeit und Sicherheitsqualität der Flut von Apps für die Anforderungen von Unternehmen sicherzustellen, erfordern auch einen kritischen Umgang mit der Software. Mit den Ergebnissen von App-Massentests werden Beispiele dieser Herausforderung aufgezeigt und Strategien im Umgang mit den Risiken diskutiert.

1 Apps im Unternehmen

Das riesige Softwareangebot der App-Stores ist verlockend. Durch die freie Wahl von Software und dem Trend der parallelen Nutzung von Smartphones für Arbeit und Privates erhält jedoch auch häufig Software Zugang zu Unternehmensdaten, die nicht als Arbeitsmittel freigegeben wurde. Aber auch wenn Unternehmen Apps explizit für den dienstlichen Gebrauch freigeben wollen, stellt sich die Frage, wie die Unternehmensrichtlinien zur IT-Sicherheit erfüllt werden können, wenn eine Vielzahl von Apps zur Auswahl steht. Das Angebot kommt dabei von großen wie auch Ein-Mann-Unternehmen, weltweit verstreut und mit dem Versprechen der App-Stores für Sicherheit zu sorgen.

So hat sich eine neue Situation beim Umgang mit Unternehmensdaten ergeben: Nicht die Reputation einzelner weniger Softwareprodukte und die Administration entscheiden über die verwendete Software, sondern die Nutzer im Vertrauen auf die App-Stores. Dabei ist jedoch zu beachten, dass bei der Risikobewertung des Einsatzes von Apps im Unternehmen sowohl die Vertrauenswürdigkeit als auch die Sicherheitsqualität der Apps zu berücksichtigen sind. Die Vertrauenswürdigkeit beschreibt die Absichten des App-Entwicklers und die Sicherheitsqualität deren Umsetzung, jeweils dem Unternehmen beziehungsweise dem Nutzer nicht zu schaden.

Leider bieten die App Stores jedoch nur sehr wenig Informationen für den Entscheidungsprozess welche Apps für den Unternehmenseinsatz und dessen Anforderungen an die IT-Sicherheit geeignet sind. Auch wenn im Vergleich zu freien Quellen im Internet die Prüfung der App Stores das Risiko für Schadsoftware deutlich reduziert, so ersetzen diese Prüfungen nicht eine dezidierte App-Kontrolle zur Einhaltung der Sicherheitsanforderungen von Unternehmen. Insbesondere wenn mit Smartphones Daten mit mittlerem bis hohen Schutzbedarf bearbeitet werden ist eine Kontrolle der Software unabdingbar. Wichtige Aspekte, wie beispielsweise die Beschränkung des Umgangs mit den Daten des Smartphones, der korrekten Verschlüsselung bei Kommunikation und Speicherung, sowie die Härtung der Software zum Schutz vor Angriffen sind keine Kriterien der App Store Prüfprozesse, die gegenwärtig auf den Verbraucher ausgerichtet sind. Aus Sicht eines potentiellen Angreifers existiert in Unternehmen jedoch ein entscheidender Angriffspunkt: die Schwächen der eingesetzten Software mit Zugriff auf Unternehmensdaten. Zwar können sogenannte Sandbox-Konzepte der Smartphone Betriebssysteme die Manipulation und Informationsgewinnung zwischen Apps eingrenzen. Wird aber die verwundbare App ohnehin zur Bearbeitung von Unternehmensdaten eingesetzt, so können über sie Daten zum Angreifer abfließen oder manipuliert werden.

Im Folgenden wird daher zunächst auf den Aspekt der Sicherheitsqualität eingegangen. Auf Basis praktischer Tests werden die Risiken des Einsatzes von Software dargestellt, die generalisierte Unternehmensanforderungen nicht erfüllen.

Wie mit dieser Situation umgegangen werden kann wird anschließend diskutiert. Sowohl das Verhalten von Nutzern ist dabei zu beachten, aber auch welche unterschiedlichen Strategien Unternehmen verwenden können, jeweils in Abhängigkeit eigener Anforderungen an den Schutz von Unternehmensdaten.

Dr. Jens Heider

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

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

2 IT-Sicherheitsqualität bei Apps

Die Sicherheitsqualität beschreibt die nicht-funktionalen Qualitätseigenschaften einer Software gegen potentielle Angriffe. Daher

stellt sie ein wichtiges Kriterium in der Absicherung von Unternehmensdaten dar. Dieses Qualitätsmerkmal lässt sich jedoch nicht in der normalen Benutzung feststellen oder bewerten. Erst eine praktische Sicherheitsevaluierung kann Sicherheitsmängel der Software aufdecken.

Manuelle Tests zeigen bei einer Vielzahl von Apps immer wieder Schwächen, die zum einen durch fehlendes IT-Sicherheits-Knowhow der Entwickler und zum anderen durch mangelnde Prüfung beim Hersteller verursacht werden. Eine Übersicht häufiger Fehlerkategorien ist beispielsweise allgemein in [1] beschrieben. Aber auch ein ungenügender Privatsphärenschutz, ein unerwünschter Zugriff auf Smartphone-Daten [5,6] oder die Nutzung anderer Smartphone-Funktionen wie das Aufzeichnen von Audio und Video im Hintergrund sind für den Nutzer häufig nicht ersichtlich.

Um das Risiko für Unternehmen zu reduzieren, ist daher eine Kontrolle wichtig. Doch durch die Flut von Apps, die potentiell im Unternehmen zum Einsatz kommen kann, steigt auch der Aufwand schnell in Bereiche, die mit klassischen manuellen Tests häufig nicht wirtschaftlich vertretbar sind.

Da für den Freigabeprozess jedoch objektive Informationen über die Sicherheitsqualität nicht vorliegen und je nach Unternehmensstrategie auch eine Vielzahl von Apps zu beurteilen sind, ergibt sich die Notwendigkeit der automatisierten Prüfung der Apps. Ziel dieser ist das Gewinnen von objektiven Kriterien für den Entscheidungsprozess. Im Vergleich zu manuellen Tests kann zwar nicht umfassend die Sicherheit analysiert werden, jedoch können typische Fehlerklassen erkannt werden und so mit einem vergleichsweise geringen Aufwand ein wesentlicher Risikoanteil reduziert werden.

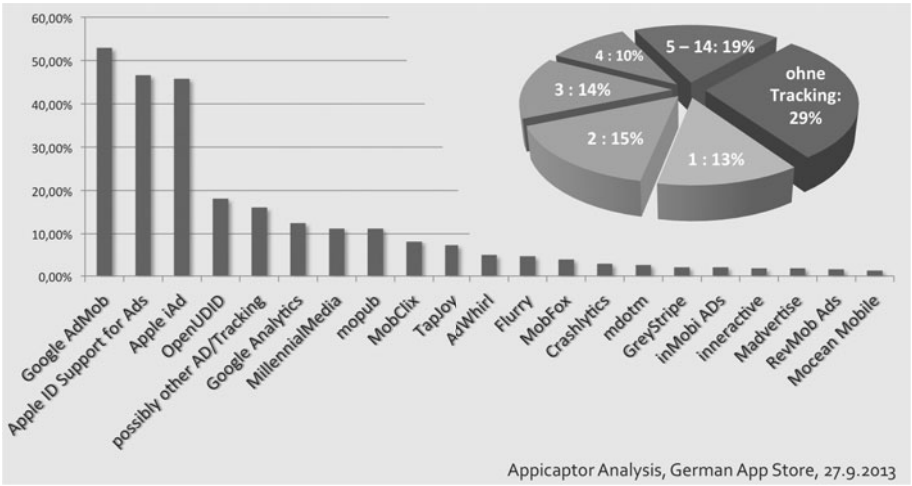
Im Folgenden wird eine kleine Auswahl dieser Kriterien exemplarisch beschrieben und es werden anhand von Massentests die gegenwärtigen Risiken dargestellt. Die Tests wurden mit dem Appicaptor Werkzeug [2] im Testlabor Mobile Sicherheit am Fraunhofer-Institut für Sichere Informationstechnologie durchgeführt.

2.1 Umgang mit Daten

Der Umgang mit Daten durch Apps geschieht für den Nutzer im Wesentlichen nicht nachvollziehbar. Gerade die Übermittlung von diesen an Dritte über das Internet entzieht sich einer Kontrollmöglichkeit und erfordert daher großes Vertrauen in die Anwendung. Umso interessanter ist es daher zu untersuchen, welche Kommunikationsbeziehungen mit Servern bestehen und zu korrelieren, welche Daten dorthin gesendet werden. Auch wenn eine App das Vertrauen hinsichtlich der verarbeiteten Daten nicht direkt verletzt, so senden doch viele Apps eine Vielzahl von Informationen unbemerkt an Dritte, über die diese ein sehr genaues Bild des Nutzers erhalten können.

Diese Informationsweitergabe passiert unter anderem häufig über das Einbinden von Werbe-Netzwerken. Ebenso aber auch über Dienste für Entwickler, die über das Nutzungsverhalten, den Speicherverbrauch und Fehlersituationen informieren und dazu

Abbildung 1 | Übersicht der Verteilung von detektierten Werbe- und Tracking-Bibliotheken, sowie Anzahl pro App in den Top 400 iOS Utilities



unbemerkt vom Nutzer Informationen einsammeln. Die erhobenen Informationen enthalten eindeutige Identifikationsmerkmale, die auch mit Informationen aus der Nutzung von anderen Web-Diensten und den dort hinterlegten Identitäten verknüpft werden können. Der einzelne Entwickler erhält dabei lediglich die Informationen zu seiner App, der Anbieter dieser Dienstleistung sieht jedoch die Nutzungsdaten aller Apps, die das entsprechende Diagnosemodul oder Werbenetzwerk enthalten. So erhält der Dienstleister ein detailliertes Bild darüber, wann welche App in welchem Kontext genutzt wird.

Bemerkenswert dabei ist die weite Verbreitung dieser Informationssammler. In einer automatisierten Analyse mittels des Appicaptor Analyse Frameworks enthielten von den kostenlosen Top 400 iOS Utilities etwa 71% sogenannte Werbe- und Tracking-Module (siehe Abbildung 1). Besonders kritisch ist zudem, dass bei 19% der Apps die Entwickler zwischen fünf und vierzehn verschiedene dieser Module in ihre Software integrierten. Ein Umstand, der auch bei aufmerksamem Studium der App-Beschreibung nicht ersichtlich ist.

2.2 Kommunikation

Übermittelte Daten können häufig von Dritten mitgelesen werden, da immer noch viele Apps auf geeignete Verschlüsselung verzichten bzw. viele Inhaltsanbieter auf Ihren Servern keine verschlüsselte Kommunikation anbieten. Gerade beim mobilen Zugriff ist dies jedoch problematisch, wenn der Zugriff über öffentliche Netzwerke erfolgt, die es einem Angreifer leichter machen den Datenverkehr mitzulesen oder sogar zu manipulieren.

Aber auch wenn die App die Kommunikation mit SSL/TLS verschlüsselt und diese Eigenschaft durch Beobachtung des Netzwerkverkehrs als gesichert gilt, besteht dennoch das Risiko, dass die Authentizität des Kommunikationspartners nicht korrekt verifiziert wird. Dadurch erhält ein potentieller Angreifer die Möglichkeit für einen sog. Man-in-the-Middle-Angriff, bei dem Sender und Empfänger die jeweils andere Identität vorgetäuscht wird. Die Daten werden dabei zwar weiterhin verschlüsselt übertragen, doch wurden in diesem Fall die verwendeten Schlüssel mit dem Angreifer ausgehandelt und sind diesem daher bekannt, sodass die Daten mitgelesen und verändert werden können.

Häufig findet sich dieser Implementierungsfehler in Apps, wenn der Entwickler nur ein unsicheres, selbst-signiertes Zertifikat zur Verfügung hatte und die Prüfung daher in einem Programmabschnitt bewusst ausschalten musste (ähnliche und weitere Gründe schildert auch [3]). Im Produktiveinsatz wird zwar dann ein sicheres Zertifikat verwendet, aber der problematische Programmabschnitt wurde nicht wieder entfernt.

Im Internet finden Entwickler aber auch eine Vielzahl von Seiten, die Hilfe bei immer wiederkehrenden Problemen für den Umgang mit Problemen bei der Zertifikatsprüfung anbieten, aber leider nicht die vollständig korrekte Variante beschreiben.

Bei der automatisierten Analyse mit Appicaptor von Android Apps auf ein einzelnes kritisches Fehlermuster zeigten 40 von etwa 2500 namhaften Apps Schwächen, die Angreifern in öffentlichen Netzen das Mitlesen von Daten trotz SSL/TLS-Verschlüsselung erlaubt und dessen Verwundbarkeit auch praktisch nachgewiesen werden konnte. Neben diesem Fehlermuster gibt es eine Vielzahl weiterer, die sich teilweise stark zwischen Smartphone-Plattformen unterscheiden.

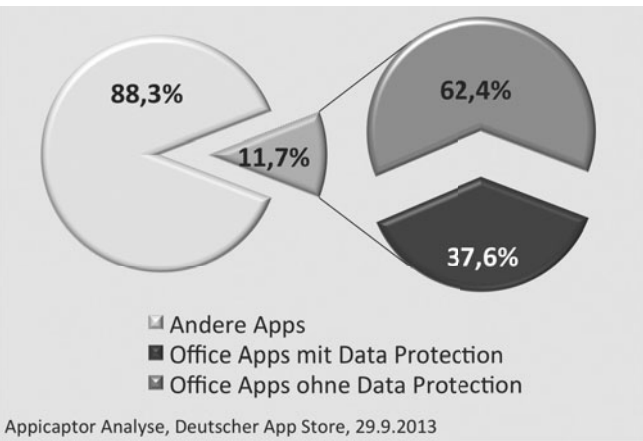
Obwohl iOS aufgrund des Designs der Programmierschnittstellen weniger Fehlerpotential bietet, sind auch hier bereits Fehlermuster bekannt, die auch auf fehlerhaften Internet-Ratschlägen oder fehlendem Sicherheits-KnowHow beruhen.

2.3 Daten-Verschlüsselung

Aufgrund der täglichen Nutzung in den unterschiedlichsten Umgebungen besteht für Smartphones ein höheres Risiko für Verlust und Diebstahl. Daher ist der Schutz von lokal abgespeicherten Unternehmensdaten durch deren Verschlüsselung eine wichtige grundlegende Maßnahme. Bei iOS können App-Entwickler diesen als Data Protection bezeichneten Schutz u.a. durch Aktivieren einer Einstellung in der App-Entwicklung umsetzen. Die Daten sind dann mit einem Plattformschlüssel geschützt und bei Nutzung des Passcodes und Wahl der entsprechenden Schutzklasse zusätzlich an dieses Nutzergeheimnis gebunden. Obwohl dieser Schutz einfach durch Entwickler zu aktivieren ist, enthielten jedoch nur 37,6% der getesteten Top 400 iOS Apps, die für den Umgang mit besonders schützenswerten Office-Daten konzipiert sind, dieses Schutzmerkmal (siehe Abbildung 2).

Mit iOS 7 ändert sich das Standardverhalten und damit erhält jede App stets den Schutz, solange dieser nicht explizit deaktiviert wird. Jedoch bleibt für den Nutzer die Situation, dass er nicht erkennen kann, ob der Schutz aktiviert ist oder nicht. Apps die bereits bei iOS 6 das Merkmal explizit deaktivieren sind bereits in den Massentests aufgefallen.

Abbildung 2 | Anteil der Office Apps mit Data Protection in den Top 400 Business Apps



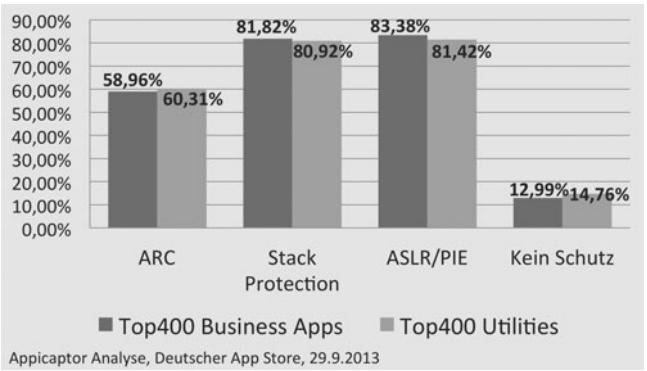
2.4 Schutzmaßnahmen

Da das Vorhandensein von Schwächen nicht ausgeschlossen werden kann, sollte gerade bei Apps im Unternehmenseinsatz das aktive Ausnutzen potentieller Schwachstellen durch Angreifer zumindest mit den verfügbaren Mitteln erschwert werden. Dieser als Härtung bezeichnete Ansatz kann durch verschiedene Maßnahmen umgesetzt werden.

Für iOS können beispielsweise Einstellungen zur Entwicklungszeit vorgenommen werden, die bei der Übersetzung des Quellcodes durch den Compiler zusätzliche Schutzmechanismen aktiviert, die das Ausnutzen fehlerhafter Implementierungen zum Ausführen von Angriffen erschwert. Automatic Reference Counting (ARC) reduziert das Risiko, das durch Speichermanagementfehler entstehen kann. Der Schutz des „Stacks" kann Angriffe auf die Programmintegrität verhindern und mittels Address Space Layout Randomization (ASLR) wird der Aufwand erhöht, den Angreifer für das Ausnutzen von Schwachstellen investieren müssen.

Dennoch zeigt Abbildung 3, dass bei fast 13% der Top 400 Business Apps dieser Schutz nicht vorhanden ist. Der Vergleich zu den unkritischeren Top 400 Utility Apps zeigt: ein stärkeres Bewusstsein für die Notwendigkeit der Absicherung von Unternehmensdaten ist nicht zu erkennen.

Abbildung 3: Vergleich der Härtung bei Business und Utility Apps



3 Strategien

In Abhängigkeit der Unternehmensrichtlinien bestehen verschiedene Strategien mit den Risiken beim Einsatz von IT umzugehen. Um das Risiko zu reduzieren ist zunächst der Nutzer ein wichtiges Element der Schutzkette. Im Folgenden werden daher die Möglichkeiten der Nutzer betrachtet bevor auf die unterschiedlichen Herangehensweisen von Unternehmen eingegangen wird, die Einflussfaktoren für die Risikobetrachtung und mögliche Handlungsoptionen diskutiert werden.

3.1 Was kann der Nutzer tun?

Im Privaten und geschäftlichen Umfeld sind Nutzer gut beraten beim Einsatz des Smartphones Vorsicht walten zu lassen. Ähn-

lich den Verhaltensregeln auf Internet-fähigen Desktop-PCs besteht ebenfalls die Gefahr Opfer von Angriffen zu werden, die finanziellen Schaden, zumindest aber Unannehmlichkeiten verursachen können, wenn etwa die eigene Identität für Betrugsversuche missbraucht wird.

Beim Einsatz im Unternehmen ist es sinnvoll weitere Regeln zu beachten:

- **Die Seriosität des App-Anbieters prüfen**: Verfügt der Anbieter über eine Unternehmenswebseite über die der Firmensitz mit Postanschrift identifizierbar ist? Wird lediglich eine Free-Mail-Adresse veröffentlicht oder gar Anonymisierungsdienste für die Registrierung von Domainnamen verwendet, besteht ein erhöhtes Risiko aufgrund fehlender Rückverfolgbarkeit.
- **Verfügt die App über Sicherheitsfunktionen wie Verschlüsselung?** Auch wenn die Beschreibung der App im Wesentlichen die Funktionalität enthält, ist das Fehlen eines Hinweises auf die Sicherheitsfunktionen ein erstes Indiz dafür welchen Stellenwert die Sicherheit bei der Entwicklung der Anwendung spielt.
- **Kritisch prüfen, ob Anfragen von Apps zum Erteilen von Berechtigungen** für die **Funktion der Anwendung notwendig sind**. Durch die gestiegene Awareness beschreiben inzwischen viele Hersteller für welchen Zweck eine App die Berechtigungen benötigt. Ob diese Berechtigungen derart verwendet werden, lässt sich vom Nutzer nicht prüfen, aber Ungereimtheiten, wie beispielsweise der Zugriff auf das Adressbuch durch eine Taschenlampen App sollten dennoch hellhörig machen.
- **Vor dem Einsatz einer App, die Zugang zu Unternehmensdaten bekommen soll, Rücksprache mit der unternehmensinternen IT-Abteilung halten**. Spätestens, wenn mit einer App Unternehmensdaten bearbeitet werden, empfiehlt es sich aufgrund des höheren Risikos zu klären ob der Einsatz zugelassen ist.

3.2 Maßnahmen der IT-Abteilung

Auf Seiten der IT-Abteilung besteht die Herausforderung eine Balance zwischen der Verbraucher-orientierten Erwartungshaltung und den Sicherheitsanforderungen des Unternehmens herzustellen.

Zur Absicherung der Endgeräte empfiehlt sich der Einsatz einer Mobile Device Management Lösung, um wichtige Sicherheitseinstellungen der Geräte durchzusetzen, wie die automatische Sperrung des Bildschirms, die Verschlüsselung des Datenspeichers und ein obligatorisches Nutzerpasswort.

Für die Sicherheit des Unternehmens ist es dann hilfreich über ein App-Freigabekonzept zu entscheiden, um sowohl die (mitunter bereichsabhängigen) Sicherheitsanforderungen berücksichtigen zu können und den Mitarbeitern eine klare Richtlinien im Umgang mit Apps im beruflichen Umfeld zu geben. Für die Umsetzung des Freigabekonzeptes sollten Kriterien aus den Sicherheitsanforderungen abgeleitet werden. Je nach Anforderung ist es dann jedoch auch häufig notwendig spezifische Tests durchführen, um die Sicherheitsqualität von Apps beurteilen zu können. Der Aufwand steigt dabei natürlich mit der Anzahl der zu testenden Apps, was zum Teil durch unternehmenseigene App-Stores mit Empfehlungen bereits freigegebener Apps reduziert werden kann. Aber auch dann ist es empfehlenswert über ein Verfahren zum regelmäßigen Überprüfen aller eingesetzten Apps nachzudenken, da Apps häufig einer sehr dynamischen Entwicklung unterliegen. So werden regelmäßig viele neue Funktionen hinzugefügt die potentiell nicht mit den Sicherheitsanforderungen vereinbar sind, vom Risiko von Implementierungsfehlern durch die gestiegene Softwarekomplexität ganz abgesehen. Bei steigender App-Zahl ist es daher bereits eine ernstzunehmende Herausforderung, einen Überblick über die Veränderungen der eingesetzten Apps zu behalten.

3.3 Wie begegnen Unternehmen dieser Situation?

Aus Gesprächen und Dienstleistungsprojekten mit unterschiedlich strukturierten Unternehmen und der Betrachtung ihrer Sicherheitsanforderungen ergeben sich die in den folgenden Abschnitten beschriebenen Charakteristiken im Umgang mit Apps.

3.3.1 App-Auswahl

Basis für die Unterscheidung der Unternehmensstrategien ist die Frage, wer für die Auswahl von Apps verantwortlich ist, die für den Einsatz im Unternehmen verwendet werden. Der klassische Ansatz dabei ist, dass von der IT-Abteilung eine Auswahl der notwendigen Anwendungen nach abgestimmten Kriterien beschafft und zur Verfügung gestellt wird. Auf die Smartphone-Welt lässt sich dies aber nicht 1-zu-1 übernehmen, da zum einen die Distribution der Apps auf die Geräte neue Prozesse erfordert und zum anderen die Lizensierung der Software auf die Nutzer erfolgt. Zudem sind die Nutzer von der privaten Nutzung gewohnt auf beliebige Apps zurückgreifen zu können. Daher wird es auch in immer mehr Unternehmen dem Nutzer gestattet auf dem Smartphone eine eigene Auswahl der Apps zu treffen. Dennoch sollte auch geregelt werden, welche alternativen Installationsquellen als zulässig erachtet werden, da die Prüfung in den App-Märkten eine wichtige erste Hürde darstellt. Die Qualität alternativer App-Märkte für Android variiert jedoch stark.

Aus der Sicherheitsperspektive können Apps mittels zentralisierter Auswahl durch die IT-Abteilung effizienter auf Konformität mit den Unternehmensrichtlinien geprüft werden. Erfolgt die Auswahl durch die Mitarbeiter stellt sich die Frage, wie die Einhaltung von Richtlinien überprüfbar bleibt. Andernfalls dürfte diese Software nicht für die Verarbeitung von Unternehmensdaten eingesetzt werden. Da bei der freien Auswahl wesentlich mehr Apps auf deren Sicherheitseigenschaften zu überprüfen sind, sollte bei der Entscheidung für diese Vorgehensweise auch ein entsprechendes Budget für die Prüfung vieler Apps vorgesehen oder das höhere Risiko eines Datenlecks einkalkuliert werden.

3.3.2 Geräte-Frage

Wer Eigentümer der Geräte ist, auf denen die Apps installiert werden, verändert die Situation hinsichtlich der Durchsetzungsmöglichkeiten. Dabei ist aus Sicherheitssicht in vielen Punkten das Bring-Your-Own-Device-Konzept sicherlich ein eigenes Thema. Für die App-Sicherheit bedeutet es allerdings, dass entweder organisatorische Richtlinien für den Einsatz von Apps mit Zugriff auf Unternehmensdaten gelten sollten oder technische Lösungen mit den Nutzern vereinbart werden. Als Beispiel sind hier Container-Lösungen zu nennen, über die der Arbeitgeber eine gewisse Kontrolle der dort bearbeiteten Daten behält.

Bei BlackBerry 10 Geräten, Android-Smartphones und anderen Plattformen mit offener Architektur, kann bei Geräten, die vom Unternehmen gestellt werden, jedoch auch eine weitreichendere Trennung zwischen privaten und dienstlichen Apps erfolgen (siehe bspw. [4]). Diese Techniken erhöhen die Sicherheit gegen Angriffe oder Schwächen nicht-vertrauenswürdiger Apps im privaten Bereich auf die Daten des dienstlichen Bereichs. Allerdings

ist auch in diesem Fall eine Sicherheitsanalyse der installierbaren Apps im dienstlichen Bereich notwendig.

3.3.3 Freigabeprozess

Auch bei dem Freigabeprozess gibt es eine Vielzahl von unterschiedlichen Ansätzen. Im Wesentlichen unterscheiden sich die Ansätze bezüglich des Freigabezeitpunkts: Vor der Installation einer App oder eher im Sinne eines Monitorings erst während der App-Nutzung. Im letzteren Fall wird somit versucht eine möglichst große Flexibilität bei der App-Auswahl zu ermöglichen und den Nutzer bei der Arbeit nicht durch den Freigabeprozess zu behindern. So kann zumindest beim Bekanntwerden möglicher Schwächen reagiert und die Nutzung der App untersagt werden. Eine notwendige Freigabe vor der Nutzung erhöht das Sicherheitsniveau, muss jedoch auch entsprechend effizient umgesetzt werden, gerade wenn Nutzer beliebige Apps auswählen können sollen. Hilfreich für einen Freigabeprozess ist in jedem Fall die Kenntnis welche Apps in welchen Versionen bereits im Einsatz sind und mit welcher Sicherheitsqualität die Funktionalität umgesetzt ist. Die Inventarfunktion vieler Mobile Device Management (MDM) Systeme bietet einen Überblick der installierten Apps. Andere Lösungen fokussieren sich direkt auf die Apps, was auch als Mobile Application Management (MAM) bezeichnet wird.

Informationen über Sicherheitseigenschaften der Apps können entweder durch Tests der Fachabteilung, externe Blackbox Tests oder über Anbieter von automatisierten Analyselösungen als Entscheidungsgrundlage eingeholt werden.

3.3.4 Schutzkonzept

Im Schutzkonzept drückt sich die generelle Risikobetrachtung bei der App-Nutzung aus. Bei hohen Sicherheitsanforderungen ist nach wie vor der Einsatz einer App Whitelist notwendig. Diese enthält welche Anwendungen für die Nutzung im Unternehmen freigegeben wurden. Alle nicht aufgeführten Anwendungen sind somit nicht zugelassen.

Häufiger wird aber aus Gründen der Nutzerakzeptanz und der Effizienz ein Blacklist-Konzept verwendet, bei dem bekannt gewordene „schlechte" Apps von der Nutzung ausgeschlossen werden. Alle Apps, die nicht aufgeführt sind, können somit frei verwendet werden. Das hat jedoch den Nachteil, dass nicht aktiv nach Schwächen gesucht wird. Es wird somit auch nicht nach Apps mit höherer Sicherheitsqualität gesucht und damit im Markt kein Impuls für einen Wettbewerb der besseren Sicherheitsfunktionen geschaffen.

Ebenso kann zwischen proaktivem und reaktiven Blacklisting unterschieden werden. Im ersten Fall kann durch Massenscans von Apps die Blacklist mit Apps befüllt werden, die den Sicherheitskriterien nicht entsprechen, bevor Incidents der Apps allgemein bekannt werden. Im reaktiven Fall werden lediglich Apps mit bekannten Schwächen ausgeschlossen.

3.4 Szenarien

Aus der Vielzahl möglicher Szenarien sollen zum Abschluss nun noch beispielhaft relevante Kombinationen in Abhängigkeit der Schutzwürdigkeit der verarbeiteten Daten betrachtet werden:

Ein *hohes Schutzniveau* lässt sich realistisch nur mit einer kleinen Auswahl benötigter Apps und einem White-List-Ansatz umsetzen. Im Prozess der Auswahl der Apps sollte dabei neben den funktionalen Anforderungen geprüft werden, welche Sicherheitsfunktionen und welche Sicherheitsqualität vorliegen. Die Geräte sollten dabei unter der Kontrolle des Unternehmens stehen. Zusätzliche Apps können dann in einem Freigabeprozess vorgeschlagen werden, der jedoch keinen Anspruch auf zeitnahe Entscheidungen hat, sondern die vorgeschlagenen Apps hinsichtlich der Eigenschaften kritisch untersucht oder Alternativvorschläge unterbreitet.

Für ein *mittleres Sicherheitsniveau* besteht die Möglichkeit zunächst zwischen Apps mit und ohne Zugriff auf Unternehmensdaten zu unterscheiden. Dann können Mitarbeiter liebgewonnene Werkzeuge ohne Bezug zu Unternehmensdaten aus dem privaten Umfeld ohne weitere Detailprüfung nutzen, für die übrigen Apps besteht aber eine Freigabepflicht nach der Analyse der Sicherheit. Zu beachten ist dann jedoch, dass die Entscheidung, ob eine App mit Unternehmensdaten arbeitet, häufig auch eine erste Analyse erfordert, da die Informationen nicht vollständig in der App-Beschreibung vorhanden sind (bspw. kann Office-Dokumente öffnen oder Unternehmensdienste nutzen). In diesem Fall wird auf das Sandbox-Konzept der Smartphone-Plattform vertraut, das bei fehlerfreier Umsetzung ein Zugriff anderer Apps auf die Daten der geprüften Apps verhindert.

Bei *geringem Sicherheitsniveau* reicht der Einsatz eines Blacklist-Verfahrens, insbesondere wenn auch auf dem Desktop die Installation beliebiger Software gestattet wird. Dennoch ist die Analyse der im Unternehmen eingesetzten Software sinnvoll, um App-Empfehlungen anzubieten, das Risiko besser beurteilen zu können und bei Bekanntwerden von Schwachstellen zu wissen, ob und in welchem Umfang bzw. Bereich das eigenen Unternehmen betroffen ist.

4 Fazit

Unabhängig davon, ob ein Unternehmen aktiv den Einsatz von Smartphones vorantreibt oder nicht, mit einem Konzept für App-Sicherheit lässt sich eine Reihe von Risiken für Unternehmensdaten vermeiden. Die Strategie dazu hängt im wesentlich von den Sicherheitsanforderungen ab. Dennoch ist immer ein wesentlicher Bestandteil die Bewertung der Sicherheitsqualität der Apps im Unternehmenskontext. Erst mit dieser zusätzlichen Information kann reproduzierbar beurteilt werden, ob eine App ein Risiko darstellt. Der Schutz mittels MDM-Lösungen stellt eine sinnvolle Ergänzung dar, kann aber die Verarbeitung von Unternehmensdaten mit verwundbaren Apps nicht verhindern.

Literatur

[1] Heider, J.: Smartphone Apps in Unternehmen: Security ist Pflicht, IEE 2013/07, Hüthig Verlag

[2] Fraunhofer SIT, Appicaptor Webseite, http://www.appicaptor.de

[3] Sascha Fahl, Marian Harbach, Henning Perl, Markus Koetter, Matthew Smith: Rethinking SSL Development in an Appified World, Proceedings of the 20th ACM Conference on Computer and Communications Security (ACM CCS 2013)

[4] Fraunhofer SIT, BizzTrust Webseite, http://www.bizztrust.de

[5] Heise-Online, iOS-App verschickt Adressbuch an den Hersteller, http://www.heise.de/security/meldung/iOS-App-verschickt-Adressbuch-an-den-Hersteller-1430793.html

[6] Heise-Online, Auch Twitter, Foursquare und Foodspotting übertragen Adressbuch an Hersteller, http://www.heise.de/security/meldung/Auch-Twitter-Foursquare-und-Foodspotting-uebertragen-Adressbuch-an-Hersteller-1435069.html