Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR SECURE INFORMATION TECHNOLOGY

APPICAPTOR SECURITY INDEX 9/2016

Appicaptor Security Index
9/2016

Der Einsatz von Apps in Unternehmen erfordert einen kritischen Blick auf die Risiken, um durch Prüf- und Freigabe-Mechanismen einer Gefährdung effektiv begegnen zu können. Im Folgenden werden Ergebnisauszüge automatisierter Appicaptor Analysen für die Top 2.000 der kostenlosen iOS- und Android-Apps vorgestellt.

Fallbeispiele: App Risiken

Die etablierten App-Märkte für iOS und Android bieten eine Fülle nützlicher Apps. Dabei soll die Prüfung der App-Markt-Betreiber und die IT-Sicherheitskonzepte der Smartphones für eine sorgenfreie Nutzung sorgen. Und in der Tat können diese App-Märkte ihren Nutzer ein deutliches Sicherheitsplus im Vergleich zu ungeprüften alternativen Softwarequellen bieten, wenn es darum geht größere Malware Angriffswellen abzuwehren.

Die Sicherheitsqualität von Apps bleibt hingegen für die Nutzer nicht ersichtlich. Nutzer, die Apps mit einer schlechten Sicherheitsqualität verwenden, können über Schwachstellen seriöser Apps daher dennoch Opfer von Angriffen werden, ohne dass sich Malware auf ihrem Smartphone befindet.

Für IT-Verantwortliche stellt sich daher die Frage, welche Risiken durch die Verwendung einer App für ihr Unternehmen bestehen und ob diese tragbar sind oder nicht. Erst mit diesen Informationen über Apps besteht die Möglichkeit durch App-Freigabekonzepte Risiken bei der geschäftlichen Smartphone-Nutzung für Unternehmen zu erfassen und hinsichtlich der Sicherheitsanforderungen der Einsatzumgebung sinnvoll zu begrenzen.

Schwachpunkt: Kommunikation

Nach wie vor ist einer der häufigsten Schwachpunkte bei Apps eine ungenügende Absicherung der Kommunikation (siehe Kasten: Kommunikationsrisiken). Dadurch wird die Nutzung öffentlicher WLAN-Zugänge zum direkten Angriffspunkt auf Unternehmensdaten, wenn diese mit verwundbaren Apps bearbeitet werden. Angreifer mit umfangreicheren Mitteln können ungeschützte Kommunikationsverbindungen aber auch in Mobilfunknetzen und Internetroutern einsehen und manipulieren.

Apps mit fehlender oder unsicherer Kommunikationsabsicherung ermöglichen Angreifern die schlechte Sicherheitsqualität auszunutzen und Zugriff auf übertragene Unternehmensdaten oder Passwörter der Mitarbeiter zu erlangen.

Gemäß der Analysen der Top 2.000 kostenlosen iOS Apps mit Appicaptor (siehe Kasten Appicaptor: Analyse der Sicherheitsqualität) nutzen dennoch 81% der Apps HTTP-Verbindungen, um Inhalte wie HTML-Seiten und JavaScript-Code zu laden (Android: 86%). Das betrifft aber nicht nur News- oder Taschenlampen-Apps, sondern beispielsweise auch 85% der wesentlich kritischeren File Viewer-Apps (Android: 89%).

Apple versucht diesem Risiko mit sicheren Standardeinstellungen für die Kommunikationsabsicherung entgegenzuwirken. Mit der in iOS 9 eingeführten App Transport Security (ATS) wird für 84% der Apps, die auf dem iOS 9 Softwareentwicklungsbaukasten (SDK) aufbauen (siehe Abbildung 7), die unverschlüsselte Kommunikation über HTTP unterbunden und die TLS 1.2 Protokollversion mit dem derzeit besten Sicherheitsniveau erzwungen. Erst durch das Erstellen von Ausnahmeregeln können unsicherere Einstellungen aktiviert werden. Begründungen für diese Ausnahmen sollen[1] allerdings gegen Ende 2016 beim Einstellen in den App Store im Review-Prozess von Apple stärker geprüft werden. Gegenwärtig wird App Transport Security jedoch nur von 2% der Apps ohne Ausnahmen aktiviert und 7% nutzen App Transport Security indirekt durch die sichere Standardvorgabe ohne eine explizit durchgeführte Konfiguration (siehe Abbildung 1). Demgegenüber stehen 59% der Apps, die App Transport Security vollständig abschalten und damit auf den generellen Kommunikationsschutz verzichten. Es muss sich noch zeigen, ob die Prüfung von Begründungen für die Ausnahmen durch den Apple App Store zu signifikanten Änderungen führen wird.

[1] siehe: WWDC-Ankündigung: https://developer.apple.com/videos/play/wwdc2016/706/?time=243

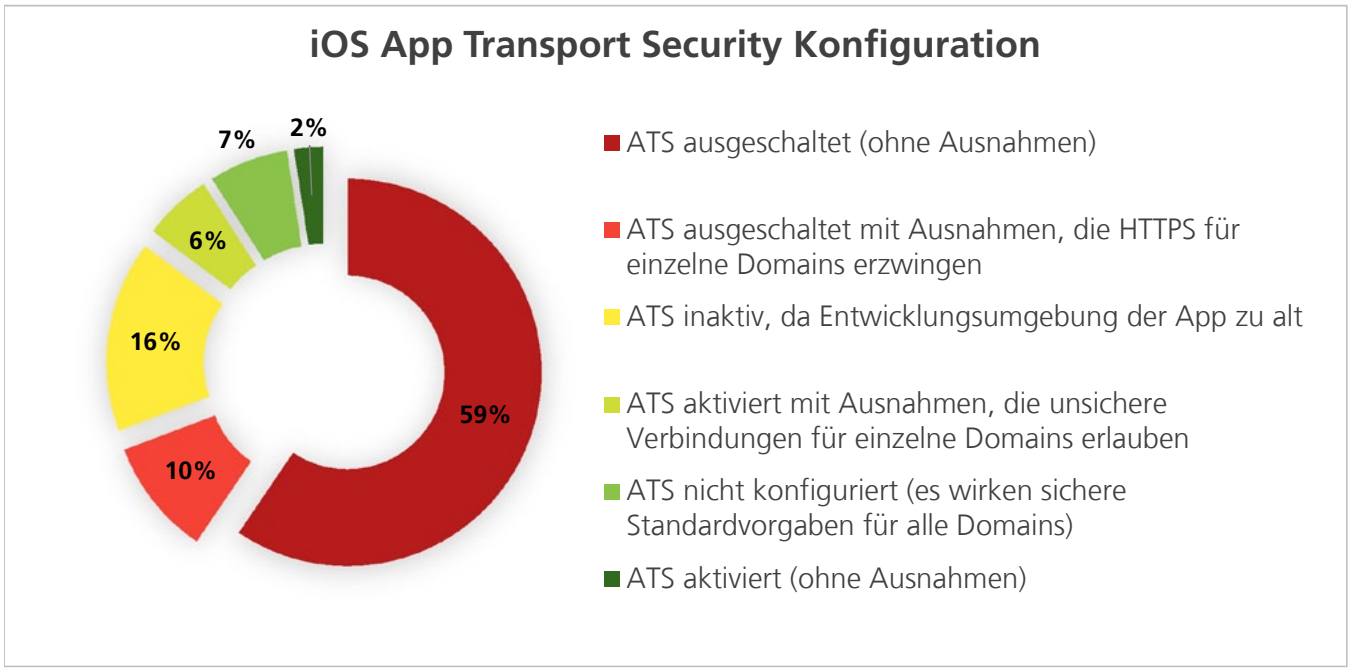

Abb. 1:
Aufteilung der Verwendung von App Transport Security bei den kostenlosen Top 2.000 iOS Apps (Appicaptor, September 2016)

Hybrid Apps:
Wenn Web-Risiken mobile Apps heimsuchen

Noch gravierender werden diese Kommunikationsrisiken, wenn die App-Funktionalität durch Web-Technologien gesteuert wird. Diese Technik, bei der App-Logik und Darstellung mittels HTML und JavaScript realisiert werden, wird immer beliebter. Sie verspricht Kostenreduktion durch plattformunabhängige Programmierung, da in der Theorie die Darstellung über HTML und die Steuerung der Abläufe mittels JavaScript nur einmal erzeugt werden muss. Den Zugriff auf Smartphone-Ressourcen übernehmen dann plattformspezifische Programmmodule, die in Bibliotheken, wie etwa Apache Cordova, für viele Smartphone-Plattformen bereits kostenlos verfügbar sind.

Die so entstehenden Hybrid-Apps müssen aber nicht nur in der Praxis dann doch oft noch für spezifische Plattformeigenheiten angepasst werden, sie haben auch einen gravierenden IT-Sicherheitsnachteil: Die gesamte Programmlogik wird in diesen Apps durch unsignierten JavaScript Programmcode gesteuert. Dies kann der Angreifer auf verschiedene Weise missbrauchen. Werden beispielsweise Inhalte ungeschützt nachgeladen, so kann ein Angreifer den fehlenden Integritätsschutz ausnutzen und die Inhalte manipulieren. So lassen sich oft direkt JavaScript-Dateien manipulieren und dadurch auch die Programmlogik ändern.

Abbildung 2 zeigt dies am Beispiel einer harmlos wirkenden iOS App zum Abruf von Fernsehprogramminformationen und Mediathekinhalten. Aufgrund einer Injection-Lücke, einer für Web-Anwendungen typischen Schwachstelle durch fehlende Integritäts- und Inhaltsprüfung, konnten Angreifer den JavaScript-Code zur Laufzeit durch einen Man-in-the-Middle-Angriff ändern. Die bestehende Berechtigung für den Zugriff auf den Kalender konnte dann missbraucht werden, um den Kalenderinhalt vollständig auszulesen und an den Angreifer zu senden. Ebenso konnte der Kalender vollständig gelöscht oder dessen Einträge beliebig vertauscht werden, sodass die Änderungen durch die Synchronisation über den Kalenderserver auch Kalender auf anderen Geräten des Nutzers betrifft. In Version 3.0 der iOS App wurde diese, durch Appicaptor automatisiert aufgedeckte Schwachstelle, geschlossen.

Ähnliche Verwundbarkeiten von Hybrid-Apps betreffen aber auch andere Ressourcen wie Telefonbuch, Kamera, Mikrofon, Zwischenablage, Positionsdaten bis hin zum Zugriff auf lokale Daten in der Sandbox der verwundbaren App oder auch der gesamten SD-Karte bei Android. In der Menge der analysierten Cordova Apps weisen 90% die Voraussetzung für einen Manipulation der App über Web-Inhalte auf. Die Auswirkungen unterscheiden sich dabei allerdings stark, je nach verwendeten Smartphone-Ressourcen und verarbeiteten Daten. Erst durch die Berücksichtigung dieser Faktoren ergibt sich eine objektive Risikobewertung.

Darüber hinaus besteht für Hybrid-Apps nicht nur die Gefahr von Schwächen in der Web-Sicherheit durch Angriff auf die Kommu-

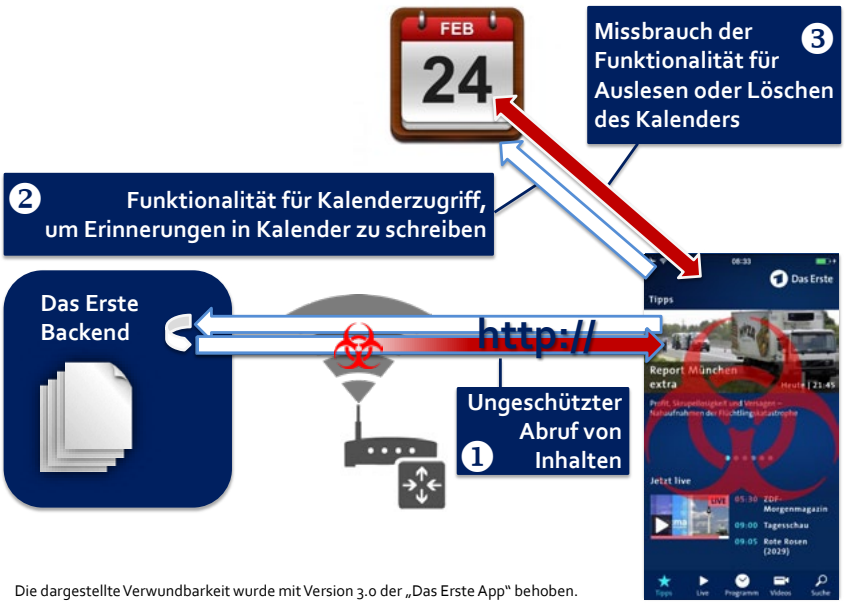

Abb. 2:
Unautorisierter Zugriff auf den Kalender: Fehlender Integritätsschutz stellt eine große Gefahr für Hybrid-Apps dar, wie der dargestellte Angriff auf die „Das Erste App" zeigt.)

nikation. Auch der App-Hersteller selber kann die Funktionsweise der App jederzeit ändern, ohne erneut die App durch den Review-Prozess der App-Märkte prüfen zu lassen. Zudem kann bei Hybrid-Apps, die Inhalte und Programmcode von Drittanbietern integrieren, auch eine Manipulation von deren Seite erfolgen. Beispielsweise wenn die App für die Darstellung von Werbung oder zur Analyse von App- und Nutzer-Verhalten JavaScript-Code von externen Quellen nachlädt.

Risiken durch Fremdbibliotheken

Programmcode aus externen Quellen ist aber auch in nativen Apps sehr häufig anzutreffen. Diese Code-Bibliotheken bieten eine Fülle an Möglichkeiten, die nicht mehr selbst programmiert werden müssen, was die App-Entwicklungskosten reduzieren kann. So werden durch Entwickler häufig viele Bibliotheken eingebunden, aus denen aber oft nur eine kleine Untermenge der vorhandenen Funktionalität genutzt wird. Dabei erfolgt die Auswahl häufig nur nach Entwicklervorlieben und Gewohnheit als aus einer Notwendigkeit der Spezifikation.

Im Falle von Schwachstellen in externen Bibliotheken ergibt sich daraus das Problem, dass Entwickler häufig die Meldung neuer Verwundbarkeiten in den von ihnen verwendeten Bibliotheken übersehen, die damit aber auch die eigenen App betreffen können. So zeigt das Beispiel einer veröffentlichten Verwundbarkeit der beliebten AFNetworking Bibliothek für iOS, dass auch 14 Monaten nach der Meldung einer kritischen Verwundbarkeit noch 20% der kostenlosen Top 2.000 iOS Apps, die diese Bibliothek verwenden, eine verwundbare Version einsetzen (siehe Abbildung 3). Diese erlaubt es Angreifern die mit der Bibliothek abgesicherte HTTPS-Kommunikation mitzulesen, da durch die Verwundbarkeit die Serverzertifikate der Kommunikationspartner nicht korrekt geprüft werden.

Bei Fehlern in Betriebssystem-Bibliotheken profitieren indes alle Apps automatisch von Betriebssystem-Updates, weshalb Entwickler versuchen sollten zunächst deren Funktionalität voll auszuschöpfen, bevor externe Bibliotheken zum Einsatz kommen. Das gezeigte Beispiel zeigt auch, dass einmal eingebundene Bibliotheken kaum aktualisiert werden: Der Anteil der inzwischen sehr veralteten AFNetworking Versionen 2.0 und kleiner nimmt kaum ab und dass obwohl 94% der Apps seit Bekanntwerden der Schwachstelle mindestens einmal aktualisiert wurden.

Klassifizierung von App-Funktionen für Risikobewertung

Die beispielhaft dargestellten Risiken zeigen den Einfluss der Sicherheitsqualität von Apps auf das Angriffspotential. Bei der Bewertung des resultierenden Risikos für Unternehmen kommt es aber immer darauf an, welche Funktion eine App erfüllt und mit welchen Daten sie arbeitet bzw. worauf sie potentiell Zugriff erlangen könnte.

Apps, die aufgrund fehlender Berechtigungen keinen Zugriff auf Smartphone Ressourcen erlangen können, haben selbst bei gra-

Kommunikationsrisiken

Kommunikationsrisiken beziehen sich auf den fehlenden, schwachen oder fehlerhaften Schutz der Geheimhaltung und Integritätssicherung von Informationen während eines Informationsaustauschs mit externen Quellen. Gründe für die Einstufung einer App in dieser Kategorie sind beispielsweise folgende:

SSL Schwachstelle: *Die App beinhaltet unsicheren Code zum Schutz der Kommunikation mit SSL/TLS. Oftmals ist unsicherer Code die Ursache für fehlerhaften Schutz vor Man-in-the-Middle Angriffen. Die Umsetzung korrekter Secure Socket Layer (SSL) oder Transport Layer Security (TLS) Kommunikation kann in der App-Entwicklung prinzipiell einfach mit den Standardfunktionen des Smartphone-Betriebssystems durchgeführt werden. In der Entwicklungsphase einer Smartphone-App wird jedoch die SSL/TLS-Konfiguration oder ihre Prozesse häufig modifiziert, um das Debugging oder die Funktion in einer Testumgebung ohne gültige Zertifikate zu ermöglichen. Dies wird benötigt, wenn die Test-Umgebung oder – weitaus schlimmer – die Produktivumgebung kein Server-Zertifikat verwendet, das durch eine Certicate Authority (CA) unterzeichnet wurde. App-Entwickler lösen dieses Problem durch die Deaktivierung oder Änderung der SSL/TLS-Sicherheitsmaßnahmen.*

Ungeschützte Kommunikation:
Die Verwendung des ungeschützten HTTP-Protokolls zur Übertragung von Parametern oder zur Abfrage von Inhalten von Servern, welche eigentlich fähig wären eine geschützte HTTPS-Kommunikation aufzubauen. Oft wird von den Entwicklern argumentiert, dass der ungeschützte Zugriff über HTTP nicht problematisch sei, da die übertragenen Informationen nicht vertraulich wären. Dies berücksichtigt jedoch nicht, dass ein Angreifer jede ungeschützte Kommunikation nicht nur lesen sondern auch manipulieren kann. Dies gibt einem potentiellen Angreifer die Möglichkeit, Server-Anfragen oder -Antworten zu verändern (oder mit eigenen Funktionen zu ergänzen) und damit die auswertende App-Umgebung zu einem anderen Verhalten (in Bezug auf das Verhalten mit unmodifizierten Daten) zu bewegen. Dies kann u.a. verwendet werden, um das Vertrauen des Benutzers in eine App auszunutzen, bspw. durch eine hinzugefügte Dialogbox mit Passwortabfrage, deren Eingaben an den Angreifer gesendet werden

Implementierungsfehler*: Fehlender oder mangelhafter Schutz gegen Injection-Angriffe. Angreifer können dann Daten manipulieren, die durch den Implementierungsfehler als Programminstruktionen verstanden werden und das Verhalten der App ändern können.*

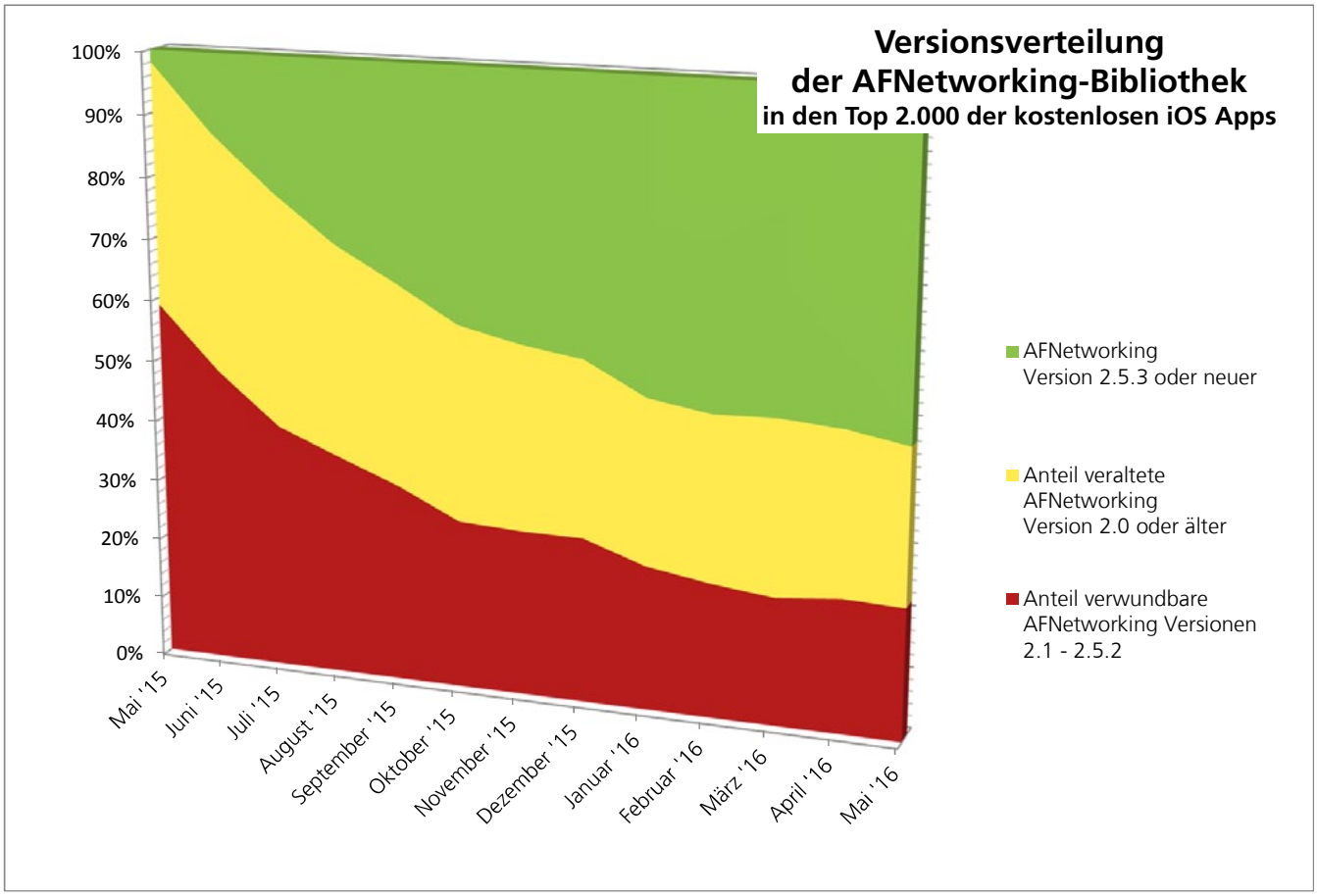

Abb. 3:
Auch 14 Monate nach der Veröffentlichung einer gravierenden Schwachstelle in der AFNetworking Bibliothek für iOS enthielten 20% der kostenlosen Top 2.000 verwundbare Versionen. (Appicaptor, Mai 2016)

vierenden Schwächen ein geringeres Risikopotential, da die Sandbox-Konzepte der Smartphone-Betriebssysteme in diesem Fall meist eine Ausweitung des Zugriffs auf kritische Ressourcen unterbinden können. Dennoch ist auch in diesem Fall zu berücksichtigen, für was die App eingesetzt wird, um z.B. ein mögliches Abgreifen von Unternehmenspasswörtern in die Risikobetrachtung mit einzubeziehen. Daher reicht die Berücksichtigung der Berechtigungen alleine nicht aus, es muss auch die übliche Verwendung der App mit einfließen.

Bei der automatischen Analyse müssen dazu Informationen über die generelle App-Funktion erfasst werden. Die Kategorisierung in den App-Märkten reicht dazu jedoch nicht aus, da beispielsweise in der App-Markt-Kategorie Finanzen sowohl die unkritischen Taschenrechner- und Börsenkurs-Apps zu finden sind, als auch die wesentlich kritischeren Mobile Banking-Apps.

Appicaptor begegnet diesem Problem durch eine Klassifizierung der Apps anhand ihrer Beschreibungstexte. Mittels eines Machine-Learning Ansatzes werden Apps der gleichen Funktionsklasse erkannt, sodass aus der Funktionsklasse mittels ihres jeweils individuellen Risikomodells eine Bewertung der analysierten Schwachstellen erfolgen kann.

Es erfolgt somit zum einen ein Abgleich der erwartbaren mit der vorgefundenen Funktionalität, als auch eine Ableitung der Auswirkungen von entdeckten Schwächen für die jeweilige Funktionsklasse. So sind detektierte Schwächen bei kryptographischen Verfahren für die Funktionsklasse der Passwortmanager schwerwiegender als für Taschenlampen-Apps. Des Weiteren geht in die Risikomodelle der Ressourcenzugriff auf Sensoren und Daten mit ein. Die Information, dass für eine App die Verarbeitung von Office-Dokumenten detektiert wurde, kann dann gegen die Funktionsklasse auf Plausibilität geprüft werden und erhöht somit die Auswirkungen bei detektierten Schwächen.

Appicaptor:
Analyse der Sicherheitsqualität

Appicaptor, eine Entwicklung des Fraunhofer SIT, scannt im Unternehmensauftrag automatisch größere Mengen von beliebigen iOS und Android Apps, untersucht sie auf IT-Sicherheit und Einhaltung von Datenschutz-Vorgaben und bewertet, ob sie für den Business-Betrieb geeignet sind oder nicht. Dabei arbeitet Appicaptor wahlweise mit Standard-Regeln (Black- und Whitelisting) oder gibt Empfehlungen entsprechend den individuellen Sicherheitsvorgaben von Unternehmen. Aufgrund der Automatisierung können die Tests wöchentlich wiederholt werden, sodass auch Änderungen bei sehr häufig aktualisierten Apps stets berücksichtigt werden. Weitere Informationen zur Nutzung finden Sie unter:

https://www.appicaptor.de

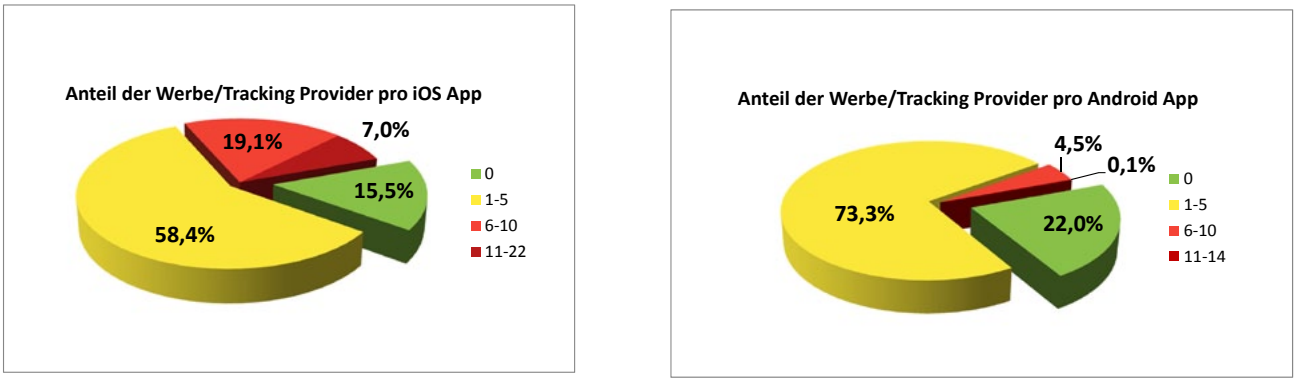

Abb. 4:
Anteil der Werbe- und Trackingnetzwerke pro iOS/Android App in den Top 2.000 der kostenlosen Apps der jeweiligen Plattform. In der Mehrzahl der Apps wurden bis zu 5 Werbe- und Trackingnetzwerke gefunden. Allerdings wurden auch Apps gefunden, die mit bis zu 22 solcher externen Dienstleistern in Verbindung stehen. (Appicaptor, September 2016)

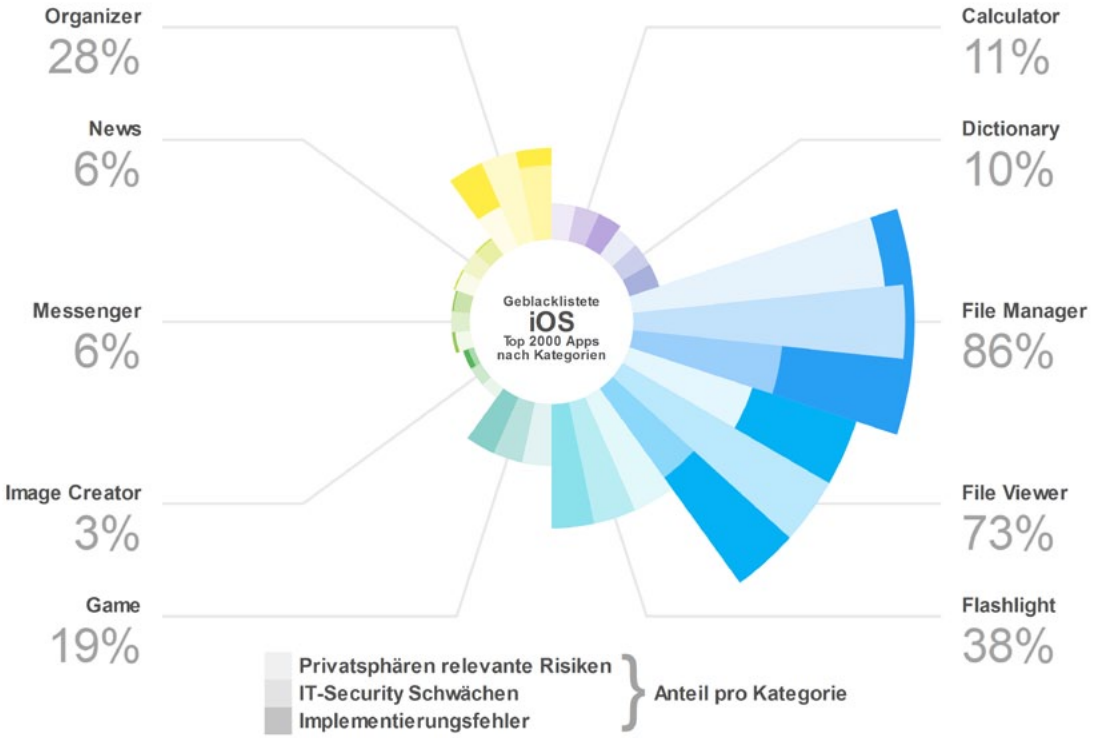

Abb. 5:
Anteil der geblacklisteten iOS Apps je Funktionsklasse. Die Balken pro beispielhaft ausgewählter Funktionsklasse zeigen den jeweiligen Anteil der drei Risikoklassen. Bei den geblacklisteten 38% der Taschenlampen-Apps treffen jeweils alle Risken zu. (Appicaptor, September 2016)

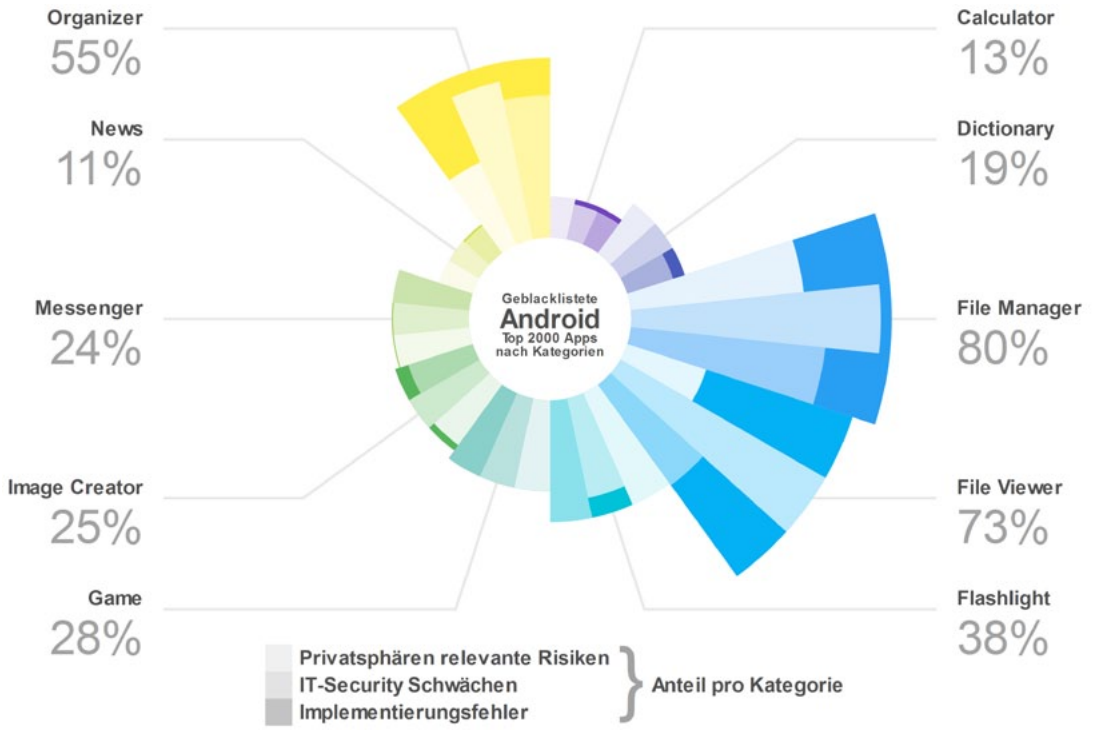

Abb. 6:
Anteil der geblacklisteten Android Apps je Funktionsklasse. (Appicaptor, September 2016)

Analysierte App-Auswahl

Die Auswahl der analysierten Apps erfolgte anhand der Einstufung der Beliebtheit durch die App-Märkte. Es wurden pro Plattform jeweils die beliebtesten 200 Apps der folgenden 10 Kategorien aus den deutschen App-Märkten monatlich mit Appicaptor analysiert.

Apple App Store Kategorien: Productivity, Utilities, Business, Socialnetworking, Finance, News, Lifestyle, Entertainment, Travel, Weather

Google Play Store Kategorien: Productivity, Tools, Business, Social, Finance, News and Magazines, Lifestyle, Entertainment, Travel and Local, Communication

Unternehmensapps mit mehr Risiken

Für die Analyse der Apps durch Appicaptor werden die vollständigen App-Binärdaten automatisiert aus den App-Märkten heruntergeladen und in eine Zwischensprache zurückübersetzt. Für den vorliegenden Bericht stammen die Apps aus den deutschen App-Märkten. Nach dem Download erfolgt eine Vielzahl automatisierter Tests und Analysen, für die das Appicaptor Framework Werkzeuge auf unterschiedlichen Ebenen zur Verfügung stellt und mit dem weiterhin die Einzelbefunde zu konsistenten Ergebnissen korreliert werden. Für den vorliegenden Bericht wurden statische Analyseverfahren verwendet. Damit wird sichergestellt, dass der gesamte App-Code untersucht wird. Es erfolgt damit eine gewisse Überapproximation, die alle Möglichkeiten der App bewertet, unabhängig davon, welche Bedingungen zum Auslösen einer Funktion notwendig sind.

Apps im Kategorievergleich

Bei der Bewertung der Tauglichkeit für den Unternehmenseinsatz zeigt sich, dass Apps für die Verarbeitung von Unternehmensdaten durchaus kritisch zu betrachten sind. Insbesondere die Funktionsklasse der File Manager-Apps zeigt mit 86% als für Unternehmen ungeeignet eingestuften iOS Apps ein deutliches Einsatzrisiko (siehe Abbildung 5). Dieses liegt bei Android mit 80% auf einem ähnlichen Niveau (siehe Abbildung 6). Die Gründe für die Blacklistung sind bei beiden Plattformen ein sehr hoher Anteil an IT-Security-Schwächen und Privatsphären relevanter Risiken (siehe Kasten: Privatsphärenrisiken). Bei Android kommt dazu noch ein höherer Anteil an Implementierungsfehlern durch die Angriffe erleichtert werden. Aufgrund der Zugriffsrechte auf Dateien und die häufig anzutreffenden Kommunikationsfunktionen sollten Unternehmen im Hinblick auf diese Analyseergebnisse bei File Manager Apps besonders auf die Einhaltung der Unternehmensrichtlinien achten.

Auch bei File Viewer-Apps zeigt die Appicaptor Analyse der Risiken Handlungsbedarf bei der geeigneten App-Auswahl. Diese Apps zeigen im Unternehmenskontext häufig vertrauliche Informationen in Form von Dokumenten an, die bei 73% der File Viewer-Apps durch detektierte IT-Security Schwächen von unautorisiertem Zugriff bedroht sind. Das Risiko bezieht sich dabei bspw. auf fehlenden Schutz in Lost-Device-Szenarien, Zugriff während der Kommunikation oder den Einsatz ungeeigneter oder zu schwacher Kryptographie.

Bei Organizer-Apps bestehen insbesondere bei den kostenlosen Android Apps aus dem Top 2.000 Katalog ebenfalls ein hohes Risiko für Unternehmen. Auch mit diesen Apps werden häufig Unternehmensdaten wie Kundenbeziehungen und -kontakte verarbeitet, die durch schlechte Sicherheitsqualität bei 55% der Android Organizer-Apps auch leicht in die falschen Hände gelangen können. Bei iOS trifft dies auf 28% der analysierten Organizer-Apps zu.

Da bei der Entscheidung für oder gegen die Unternehmenstauglichkeit bei der Appicaptor-Analyse jeweils die Risiken von Verwundbarkeiten anhand der Zugriffsrechte, der verarbeiteten Daten und des App-Typs erfolgt, ist nachvollziehbar, dass App Typen wie News oder Taschenrechner durch die Standardregeln wesentlich wenige geblacklistet werden. Hier werden insbesondere Apps geblacklistet, wie durch ihren hohen Anteil an Privatsphärenrisiken auffallen oder aufgrund ihrer Implementierung Zugriff auf Unternehmensdaten gewähren können.

Mitteilsame Apps

Auch in diesem Jahr setzt sich der Trend zu mehr Werbe- und Trackingnetzwerken in Apps fort. Der Anteil der Apps ohne detektierte Interaktion mit diesen Providern ist bei den iOS-Apps von etwa 26% im Juli 2014 auf aktuell 15,5% gesunken. Bei Android liegt dieser Anteil aktuell bei 22%. Zudem ist der Anteil der iOS Apps mit mehr als 5 Werbe- und Trackingnetzwerken im gleichen Zeitraum von 12,5% auf 26,1% gestiegen (siehe Abbildung 4).

Durch die gestiegene Nutzung der Werbe- und Trackingnetzwerke in Apps erhalten immer mehr Provider Einblick in das App-Nutzungsverhalten der Anwender und pro Provider können mehr Details der Nutzer gesammelt werden. Bei einer geschäftlichen Nutzung können somit auch immer mehr Rückschlüsse über aktuelle Abläufe im Unternehmen gezogen werden. Dies ist dadurch bedingt, dass ein Provider unter Einbeziehung von eindeutigen IDs, dem App-Kontext und der App-Aufrufhistorie konkrete Rückschlüsse über den Ablauf im Unternehmen erstellen kann. Da ein Großteil der Kommunikation mit den Werbe- und Trackingnetzwerken immer noch unverschlüsselt stattfindet, stehen diese Informationen aber auch allen anderen zur Verfügung, die Zugriff auf das genutzte Netzwerk haben.

Fazit

Sowohl Apple als auch Google verbessern stetig die Sicherheit ihrer Smartphone-Plattformen und unterstützen Entwickler durch gute Standardvorgaben für die Entwicklung sicherer Apps. Insbesondere beim Thema Transportverschlüsselung zeigt diese Initiative aber noch nicht viel Wirkung, da viele Entwickler die sicheren Standardeinstellungen deaktivieren. Teilweise sicherlich aufgrund einer nicht beeinflussbaren fehlenden Unterstützung bei der Server-Gegenstelle aber häufig auch aufgrund von Unwissenheit hinsichtlich sicherer Alternativen. Zudem nehmen die Risiken für Unternehmen durch die steigende Verwendung von unsicheren Hybrid-Apps weiter zu.

Unabhängig von der Plattform zeigen daher die Appicaptor-Ergebnisse: Die App-Auswahl stellt eine wichtige Entscheidung für die Unternehmenssicherheit dar. Gerade für dienstliche Abläufe sollten nur Apps zum Einsatz kommen, die den Unternehmensanforderungen entsprechen. Leider sind die Kriterien für Sicherheitsqualität aus den App-Märkten nicht ersichtlich und deren Prüfung nicht ausreichend.

Erst eine gezielte Schwachstellensuche hilft die einzelnen App-Schwächen zu erkennen. Wie im vorliegenden Bericht verdeutlicht ist die Bewertung der daraus resultierenden Risiken der entscheidende Faktor für die Entscheidung für oder gegen die App. Die Bewertung für ein ggf. notwendiges Untersagen der Nutzung im Unternehmen ist somit erst unter Einbeziehung von den verwendeten Daten, Zugriffsrechten, App-Funktion und -Typ möglich. Andernfalls sinkt die Nutzerakzeptanz für das Blacklisting oder die Regeln müssen aufgrund dieser fehlenden Einbeziehung des App-Kontextes für alle Apps so gelockert werden, dass eigentlich kritische Apps dann auch nicht mehr geblacklistet werden.

Aufgrund der vielen App-Updates erfordert die Schwachstellensuche eine hohe Automatisierung, um die Analyseergebnisse für jeweils aktuelle Versionen zeitnah vorliegen zu haben. Mit den so gewonnen Informationen kann dann ein App-Freigabekonzept (siehe[2]) umgesetzt werden, das die Freigabeanfragen und automatisiert erhobenen Analysedaten vollautomatisch durch vorhandene Mobile Device Management System (MDM) oder Enterprise Mobility Management System (EMM) verarbeiten lässt. Alternativ unterstützen die Analyseergebnisse aber auch einen manuellen Freigabeprozess, der die analysierte Sicherheitsqualität der Apps für den Entscheidungsprozess nutzt.

Privatsphärenrisiken

In dieser Analyse werden Befunde in Bezug auf eine unangemessene Preisgabe von Benutzerinformationen als Privatsphärenrisiken klassifiziert. Im Folgenden werden einige Beispiele erläutert:

- **Werbung/Tracking:** *Die App benutzt mehr als 5 Werbe- und Trackingnetzwerke und verbreitet dadurch persönliche Daten in Kombination mit dem Kontext der App-Nutzung.*
- **Nicht plausibler Sensorzugriff:** *Die Nutzung von Smartphone-Sensoren (z.B. Mikrofone, GPS, Kamera, etc.), außerhalb der für den detektierten App-Typ üblichen Gebrauch, birgt ein Risiko bezüglich des Zugriffs auf sensible persönliche Daten.*
- **Informationspreisgabe:** *Die Offenlegung von Standort-Daten oder Informationen über Web-Suchanfragen durch ungeschützte Kommunikation mit einem Dienstleister (z.B. Google), sodass neben dem Dienstleister auch Dritte die übermittelten Informationen einsehen können.*
- **Benutzer-Identifikation:** *Die App versucht Zugang zu Informationen zu erlangen, anhand welcher ein Benutzer eindeutig identifiziert werden kann, wie beispielsweise Telefonnummer oder eindeutige Gerätenummern. Der Zugriff widerspricht dabei der App-Beschreibung (z.B. Taschenlampe).*
- **Nutzung undokumentierter APIs (iOS):** *Die App beinhaltet Code, der Funktionen unveröffentlichter bzw. undokumentierter APIs aufruft. Diese Art der Programmierung beinhaltet das Risiko, dass diese APIs kritische Funktionen bereitstellen, die lediglich von Apps von Apple Inc. genutzt werden sollten. Apple erklärte, dass Apps, die solche APIs benutzen, vom Apple App Store ausgeschlossen werden (siehe Abschnitt 2.5 App Store Review Guidelines[3]). Dennoch findet Appicaptor regelmäßig Apps mit dieser Funktionalität im Apple App Store.*

[2] J. Heider., Die Gretchenfrage, DuD-Artikel 2014/1: https://www.sit.fraunhofer.de/fileadmin/dokumente/artikel/DUD-2014-1-Gretchenfrage-App-Sicherheit__2_.pdf

[3] siehe: https://developer.apple.com/app-store/review/guidelines/#functionality

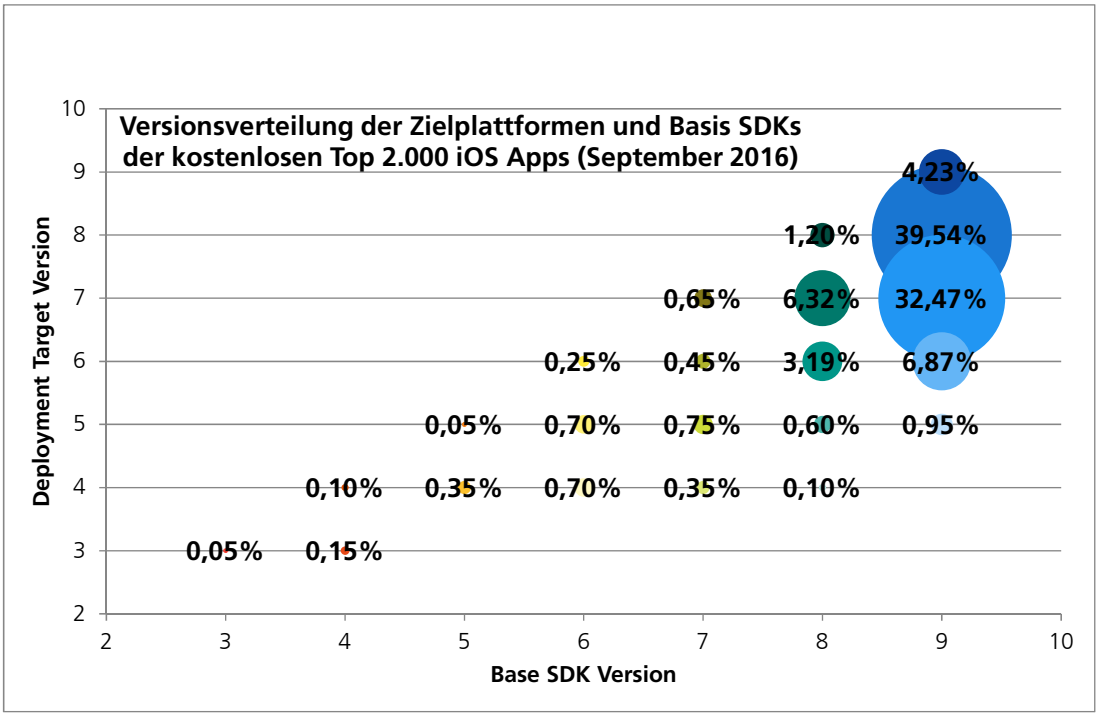

Abb. 7:
Im Vergleich zum Vorjahr unterstützen mehr Apps ältere Betriebssystemversionen. Ein Grund dafür dürften die noch weit verbreiteten iPhone 4 Geräte sein, die kein Update auf iOS 8 erhalten haben. (Appicaptor, September 2016)

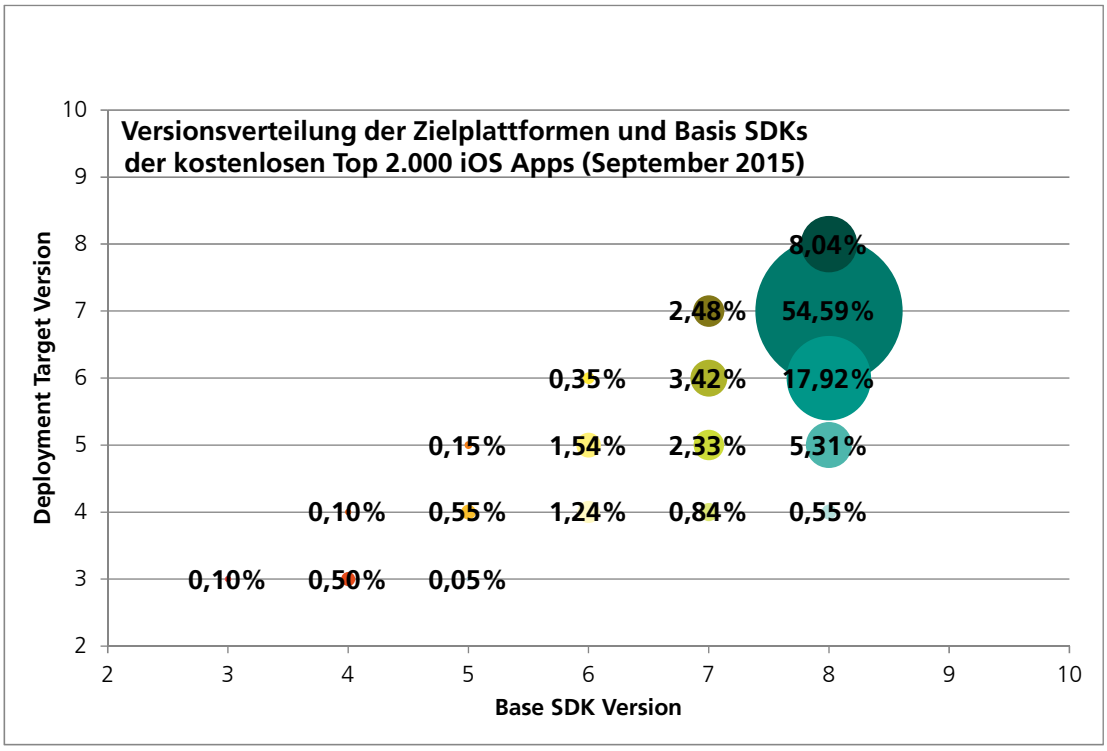

Abb. 8:
Im vergangenen Jahr hatten etwas mehr Entwickler mit dem aktuellen SDK entwickelt und damit das zur Verfügung stehende Sicherheitspotential besser genutzt. (Appicaptor, September 2015)

Kontakt:
Dr. Jens Heider

Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt, Germany

Telefon 06151 869-233
appicaptor@sit.fraunhofer.de
https://www.sit.fraunhofer.de/de/appicaptor/