ZEBRA

Endverbraucher- kontra Enterprise-Geräte

Überblick

In diesem Dokument erhalten Sie einen kurzen Überblick (stützende Daten auf Anfrage erhältlich) über die Probleme, die bei Kunden auftraten, die versuchten, Endverbrauchergeräte für Unternehmensanwendungen zu nutzen. Es ist zwar nicht auf einen bestimmten Anbieter von Endverbraucherprodukten ausgerichtet, aber viele der Aussagen betreffen Apple, da es ein sehr einzigartiges Plattform-/Betriebsmodell aufweist. Auf keinen Fall sollen Endverbrauchergeräte per se darin verdammt werden. Es soll lediglich auf die Kompromisse aufmerksam gemacht werden, die Hersteller von sowohl Unternehmens- als auch Endverbrauchergeräten eingehen.

Wenn jemand die Verwendung von Endverbrauchergeräten für Unternehmensanwendungen in Betracht zieht, sollte er sich folgende Fragen stellen:

- Wird meine Lösung sicher sein und werden meine Daten geschützt sein?
- Werden die Geräte dem Verschleiß standhalten, der in einem Unternehmensnutzungsszenario herrscht?
- Kann die Lösung (Anbieter, Gerät, Zubehör) meine Anforderungen an den Lebenszyklus erfüllen?
- Wird die IT-Abteilung das Geräteportfolio angemessen handhaben/verwalten können?
- Kann der Anbieter den nötigen Support bieten, wenn etwas nicht nach Plan läuft?
- Kann ich darauf bauen, dass die Lösung zuverlässig genug ist, um nicht die Mitarbeiterproduktivität oder das Kundenerlebnis zu beeinträchtigen?
- Habe ich wirklich die möglichen Probleme untersucht, die mit einer mehrteiligen Lösung einhergehen können?
- Erfüllt die Lösung wirklich aktuelle und zukünftige funktionelle Anforderungen (WLAN-Performance, Barcode-Scanning, Audio, Temperaturunempfindlichkeit usw.)?
- Habe ich sekundäre Probleme, wie z. B. Gerätediebstahl, bedacht?
- Wird mein Lieferant mir eine angemessene Vorausplanung ermöglichen? (z. B. Roadmap-Transparenz)
- Werden meine Entwickler und Drittanbieter-ISVs über ausreichenden Programmierzugang (API) verfügen?
- Ermöglicht mir mein Plan, meine Betriebssystemumgebung zusammenzuführen oder zu vereinheitlichen?

Endverbraucher- kontra Enterprise-Geräte

VERGLEICH: VON IT-ABTEILUNG ODER VON BENUTZERN DURCHGEFÜHRTE OS-UPDATES

Beim Kundenerlebnis geht es um den Komfort und die Kontrolle durch den Endbenutzer. Im Gegensatz dazu geht es beim Enterprise-Erlebnis um die Maximierung der Produktivität und Kontrolle durch die IT-Abteilung. Beim Endverbrauchermodell werden OS-Updates dem Endbenutzer überlassen, d. h. die IT-Abteilung wird übergangen. Bei der Herausgabe von Updates erhalten Endbenutzer die Berechtigung/Option, die Aktualisierung durchzuführen oder sie zu ignorieren.

In vielen Fällen haben Kunden versucht, Updates für die Geräte ihrer Mitarbeiter mithilfe von Proxy-URL-Filtern zu blockieren. Leider wurden auch Download-URLs hinzugefügt und so konnten die Mitarbeiter trotzdem ihre Geräte aktualisieren. Diese Updates erzeugten Anwendungsinkompatibilitäten und/oder eine zerstückelte OS-Umgebung. Unglücklicherweise war nach dem Laden der Updates keine Möglichkeit mehr vorhanden, das OS auf die vorherige Version zurückzusetzen.

Beim Enterprise-Ansatz ist dies völlig anders. Kunden erhalten Updates von Zebra. Updates werden in ein MDM (Mobilgerätemanagement) geladen, über das die IT-Abteilung die komplette Kontrolle hat. Die IT-Abteilung bestimmt, wann (oftmals außerhalb der Betriebszeiten, um die Netzwerklast während Spitzenzeiten zu verringern) und welche Geräte Updates erhalten (z. B. ein schrittweises Rollout, bei dem bestimmte Einrichtungen ausgewählt werden, um so katastrophale Ausfälle zu vermeiden). Da die IT-Abteilung über die Möglichkeit verfügt, „unbeaufsichtigte Updates“ durchzuführen, geschieht die Transaktion unabhängig und auf transparente Weise für den Endbenutzer. Natürlich kann die IT-Abteilung auch eine neuere Version einführen oder eine Rücksetzung auf eine vergangene Version vornehmen für den Fall, dass ein Problem aufgetreten ist.

WLAN-PERFORMANCE

Geschäftskritische oder grundlegende Konnektivität

Bei der WLAN-Performance gibt es einen klaren Unterschied zwischen Endverbraucher- und Unternehmensprodukten. Endverbrauchergeräte werden normalerweise in AP-Umgebungen mit wenigen weiteren Endgeräten genutzt, d. h. die AP-Roaming-Effizienz spielt für gewöhnlich hier keine große Rolle. Ein schlechtes Roaming kann zu deutlichen Latenzschwankungen führen, was sich stark auf die Sprach- und Anwendungsreaktionszeiten auswirken und somit die Mitarbeiterproduktivität beeinträchtigen kann.

Anbieter von Endverbrauchergeräten gleichen die schlechtere WLAN-Konnektivität mit geringeren Kosten und Abmessungen aus. Geräte von Zebra dagegen sind mit mehreren Antennen ausgestattet. Durch die Verwendung von zwei Antennen anstatt einer werden die Abmessungen zwar größer, aber dies sorgt für eine robuste WLAN-Konnektivität, indem auf transparente Weise zur optimalen Antenne umgeschaltet wird. Dadurch können sogenannte „Phantomeffekte“ vermieden werden, bei denen die Verbindung basierend auf der Position der Hand oder des Kopfes im Verhältnis zum Gerät schlechter wird (dies war in der Vergangenheit ein Problem bei Apple-Geräten im Mobilfunknetz). Zusätzlich werden durch den Einsatz mehrerer Antennen die Auswirkungen von HF-Reflexionen (d. h. Multipath) gemindert, die große Schwankungen bei der Konnektivität erzeugen und sich in Innenumgebungen des Unternehmens ausbreiten.

Außerdem werden WLANs zunehmend stärker ausgelastet und es kommt zu immer mehr Interferenzen im 2,4-GHz-Frequenzband. Aus diesem Grund gewinnt das 5-GHz-Band an Bedeutung. Apple führte bei seinen Handheld-Geräten erst in der fünften Gerätegeneration Unterstützung von 5 GHz ein. Im Gegensatz zu Endverbrauchern nutzen viele Unternehmen bereits 5 GHz, um mehr Kapazität zu erhalten und Interferenzen im 2,4-GHz-Band zu umgehen. Doch die 5-GHz-Leistung kann variieren. In einer Gartner-Studie heißt es bei der Beurteilung von Apple iPads: „Bei 5 GHz benötigt die IT-Abteilung 300 % mehr Zugangspunkte“ (d. h. aufgrund der schlechten Performance). Dieser Bericht ist käuflich von Gartner erhältlich.

BILDSCHIRMGRÖSSE

Verbesserte Produktivität

Enterprise-Kunden fordern einen größeren Bildschirm (der trotzdem die Handlichkeit nicht zu sehr beeinträchtigt). Ein Kunde berichtete, dass seine Firma dank des größeren Touchscreens in der Lage war, die Benutzeroberfläche von sechs Menüebenen auf zwei Ebenen zu reduzieren. Dies hatte eine höhere Mitarbeiterproduktivität zur Folge. Die größeren Bildschirme haben ebenfalls die wahlweise Nutzung im Hoch- und Querformat möglich gemacht.

Als Apple bei seinen Produkten von der vierten zur fünften Generation überging, änderten sich die Bildschirmgröße und das Seitenverhältnis. Die neuen Bildschirme sind 4,0 Zoll groß und haben das Seitenverhältnis 16:9. Der MC40 hingegen weist ein 4,3 Zoll großes Display auf. Auf den ersten Blick scheint dieser Unterschied vernachlässigbar zu sein, doch man muss bedenken, dass der Bildschirmbereich eine Exponentialfunktion der Diagonale ist. Somit verfügt der MC40 über eine 19,3 % größere Bildschirmfläche als die Apple-Geräte der fünften Generation. Außerdem führte Zebra 2014 aufgrund des Feedbacks von Enterprise-Kunden ein 4,7-Zoll-Produkt ein, das eine um 38,1 % größere Fläche bietet als Apple-Produkte der fünften Generation.

GERÄTELAUTSTÄRKE
Zweiteilige kontra integrierte Lösungen

Endverbrauchergeräte ohne Zubehör sind normalerweise kleiner und leichter als vollintegrierte Unternehmenslösungen. Doch bei Nutzung einer Steckhalterung (beispielsweise für eine Bezahlfunktion, zusätzliche Akkukapazität, und/oder Erfassung von Barcodes) stellt sich die zweiteilige Endverbraucherlösung im Vergleich zur integrierten Enterprise-Konfiguration letztlich als größer heraus.

Beispiel: Ein iPod Touch der vierten Generation hat die äußerst kompakten Abmessungen von ca. 47 mm^3. Wenn man ihn mit einer Infinite Peripheral-Steckhalterung ausstattet, um Barcode-Scanning und eine mit dem MC40 vergleichbare Akkukapazität zu erreichen, steigt das Volumen dieser zweiteiligen Lösung auf 199 mm^3 an. Das ist größer als die 173 mm^3 des MC40. Zudem beträgt die Bildschirmgröße der iPod-basierten (4. Generation) Lösung 3.661 mm^2 und die des MC40 5.264 mm^2 (eine 43 % größere Bildschirmfläche).

Zusammengefasst ist der MC40 mit einer vergleichbaren Funktionalität 13,1 % kleiner und hat eine um 43 % größere Bildschirmfläche.

STECKHALTERUNGSLÖSUNG
Fallfestigkeit

Unternehmensgeräte werden oft als „langlebig“, „strapazierfähig“ oder „robust“ klassifiziert. Von robusten Enterprise-Geräten wird erwartet, dass sie selbst nach 26 Stürzen (6 Stürze auf die Seite, 8 Stürze auf die Ecke, 12 Stürze auf die Kante) aus 122 cm Höhe auf Sperrholz noch voll funktionsfähig sind. Zebra hat eine bekannte Steckhalterungslösung (für Barcode-Scans und zusätzliche Akkukapazität) dem 26-Sturz-Test unterzogen. Die Lösung (Steckhalterung und iPod) wies sechs schwerwiegende Fehler auf, wie z. B.: 1) abgebrochener Teil am linken Schnappverschluss; 2) Ausfall beider Lautstärketasten (an der Steckhalterung); 3) Ausfall von Lautsprechern und Scannern; 4) fehlerhaftes Aufladen des Geräts; 5) herausgesprungener Teil der LED-Leiste an Unterseite des Geräts; 6) hörbares Klappergeräusch im oberen Teil des Geräts. Das Gerät zeigte zudem drei temporäre Fehler (d. h. nach einem Reset war die Funktion wiederhergestellt).

STECKHALTERUNGSLÖSUNG
Schalter- und Kontaktspezifikationen

Für Endverbrauchergeräte werden normalerweise keine Schalter- und Kontaktspezifikationen für zweiteilige Steckhalterungen angegeben und diese sind auch schwer zu bestimmen.
Diese weisen allerdings eine hohe Ausfallquote bei der Nutzung in einer Unternehmensumgebung auf. Beispiel: Die Ein/Aus-Taste des MC40 hat eine Spezifikation von 500.000 Drückvorgängen, die Scan/Kamera-Taste eine von 1.000.000 und die Akku-Einsteckspezifikation beträgt 2.000 Einsteckvorgänge (die des Terminals beträgt 6.000).

STECKHALTERUNGSLÖSUNG
Akku-Aufbau

Zebra hat Rückmeldungen erhalten, dass bei einer Reihe von Steckhalterungsdesigns der Hauptakku vom Halterungsakku isoliert ist (d. h. sie haben keinen gemeinsamen Strom). Das bedeutet, dass sowohl der Akku des iPod als auch der der Steckhalterung aufgeladen sein muss, um eine funktionsfähige Einheit zu erhalten. Es sind mehrere Steckhalterungen auf dem Markt erhältlich, d. h. Kunden sollten den Akkubetrieb der beurteilten Lösung überprüfen. Bedenken Sie, dass ein unabhängiger Akkubetrieb im Laufe der Zeit zu Lebenszyklusproblemen führen kann.

AKUSTISCHE EIGENSCHAFTEN
Schalldruckpegel

Endverbrauchergeräte sind meistens extrem dünn und dies geht oftmals zu Lasten von wichtigen Unternehmensfunktionen. Enterprise-Kunden suchen zunehmend nach einem zusammengefassten Sprach-/Datengerät. Indoor-Benutzer führen herkömmliche Push-to-Talk-Geräte mit Datenerfassungsgeräten zusammen. In allen Fällen suchen Unternehmen nach einem Gerät, das auch in relativ lauten Umgebungen zuverlässig zu hören ist.

Um den gewünschten Formfaktor zu erzielen, gibt man sich bei Endverbrauchergeräten häufig mit einem geringeren Schalldruckpegel (SPL) und Frequenzgang zufrieden. Zebra hat herausgefunden, dass viele beliebte Endverbrauchergeräte einen um 9 bis 20 dB niedrigeren Schalldruckpegel haben als Enterprise-Geräte von Zebra. Obwohl dies subjektiv und nicht-linear basierend auf dem absoluten Ausgang ist, kommt ein SPL-Unterschied von 9 dB normalerweise einer empfundenen doppelten Lautstärke gleich.

FUNKTIONALITÄT DER STECKHALTERUNG

Integrierte Barcode-Scanfunktion

In vielen Fällen wollen Enterprise-Kunden jederzeit eine herausragende Scan-Funktionalität auf allen Geräten und MPoS auf bestimmten Geräten und/oder während bestimmter Zeiten im Jahr. Bei der Wahl von Steckhalterungsoptionen sind sie gezwungen, zwei verschiedene Halterungskonfigurationen bereitzustellen (eine nur für Scans, eine andere für Scans und Zahlungen) oder 100 % ihrer Geräte mit einer teureren, größeren Scan-/Bezahloption auszustatten. Die meisten ziehen eine im Gerät integrierte Scanfunktion und eine Bezahlfunktion in der Halterung vor.

ERWEITERUNGSSTECKPLATZ

Enterprise-Kunden brauchen häufig Wechselspeicher zum Portieren von Daten, für Datensicherungen und/oder als Speichererweiterung. Apple-Geräte haben keine Nutzung von Wechselmedien (z. B. SD-Karten, Flash-Laufwerke usw.) zu bieten.

NFC-UNTERSTÜTZUNG

Apple im Speziellen hat wiederholt beschlossen, NFC nicht zu unterstützen. Viele Enterprise-Kunden brauchen NFC zum Lesen von Positionsmarkern, für die Zubehörkopplung, zum Erfassen von Asset-Tags und für die Zugangskontrolle.

LAUNCHER-FLEXIBILITÄT

Im Fall von Apple haben Benutzer keine Option, den Launcher zu ersetzen oder zu modifizieren.

VERLUSTRATEN

Verschwinden/Diebstahl von Geräten

Der Aftermarket-Bedarf für Endverbrauchergeräte ist extrem hoch, was die Motivation für Diebstahl steigert. Für Endverbrauchergeräte ohne Wechselakku stellen Kunden oftmals zwei Geräte bereit – während eines in Betrieb ist, befindet sich ein zweites in einer Ladestation. Kunden haben berichtet, dass Geräte im Ladebereich häufig abhanden kommen.

TEMPERATUR

Betrieb und Lagerung

Endverbrauchergeräte weisen meistens nur einen eingeschränkten Betriebs- und Lagertemperaturbereich auf. Apple-Geräte beispielsweise haben einen Betriebstemperaturbereich zwischen 0 und 35 °C. Wenn das Gerät überhitzt, kommt es zu einer Fehlfunktion und es erscheint ein Ausrufezeichen mit dem Hinweis, dass man das Gerät abkühlen lassen soll. Mehrere Benutzer haben von solchen Ausfällen in relativ harmlosen Umgebungen berichtet. Im Gegensatz dazu ermöglichen Geräte der Unternehmensklasse wie der Zebra MC65 eine Betriebstemperatur zwischen -10 und 50 °C (das ist ein um 25 Grad größerer Bereich als bei Apple). Ein Kunde berichtete, dass er Geräte auf einer Kühlvorrichtung vor Ort ablegen musste, um sie wieder betriebsbereit zu machen. Ein anderer Kunde erlebte eine Überhitzung im November in Texas während des Tests einer direkten Filialbelieferung.

Es sollte dabei erwähnt werden, dass es sich bei den Temperaturangaben um Umgebungswerte handelt. D. h., wenn das Gerät sich in einer Steckhalterung befindet, kann die Hitze durch die Halterung und fehlende Temperaturableitung nach draußen den oberen Temperaturwert zusätzlich herabsetzen.

Auch die Lagerungstemperatur scheint Berichten zufolge ein Problem bei Apple-Geräten zu sein. Laut einem Kundenbericht führte eine geringfügig höhere Lagerungstemperatur als die der maximalen Spezifikation des Geräts zu einer dauerhaft geminderten Akkulebensdauer. Die Spezifikation der Lagerungstemperatur von Apple-Geräten liegt bei -20 bis +45 °C im Gegensatz zum Zebra MC65 mit einer Spezifikation von -40 bis +70 °C.

LEBENSZYKLEN VON ENTERPRISE-GERÄTEN

Endverbrauchergeräte müssen mit den neuesten Trends und der Mode Schritt halten. Die typische Laufzeit (die Dauer, nach der das Gerät nicht mehr zum Verkauf geeignet ist) eines Smartphones beträgt sechs bis neun Monate. Bei Apple-Geräten beträgt dieser Zeitrum ungefähr 12 Monate. Inwieweit Unternehmen für Endverbraucher ältere Geräte nach deren Einführung noch verfügbar halten, lässt sich nicht eindeutig sagen. Enterprise-Kunden sind hier gezwungen, sich entweder für einen kompletten Austausch aller Geräte oder für eine schrittweise Änderung zu entscheiden, was logistisch komplex ist und eine extrem uneinheitliche Implementierung zur Folge hat.

Im Endverbraucherbereich wird die Kompatibilität von altem Zubehör zwar berücksichtigt, ist jedoch meistens keine primäre Anforderung. Bei Apple führten die Einführung des Lightning-Anschlusses (der den 30-Pin-Anschluss ablöste) und der neue Formfaktor beim iPhone 5 dazu, dass Enterprise-Kunden gezwungen waren, ihre Steckhalterungen, Ladeschächte und anderen Zubehörteile komplett zu ersetzen, um den Umstieg auf das neue Gerät durchzuführen.

Enterprise-Geräte, wie z. B. die von Zebra, verfügen für gewöhnlich über einen Lebenszyklus von 3+3 (6 Jahre) oder 5+5 (10 Jahre). Die erste Zahl steht für die Geräteverfügbarkeit und die zweite für den Gerätesupport. Somit können 3+3-Kunden das Gerät 3 Jahre lang erwerben und für weitere 3 Jahre Service erhalten (was einen Gesamtlebenszyklus von 6 Jahren ergibt).

SICHERHEIT UND DATENSCHUTZ IM UNTERNEHMEN

Apple und Google (über Google Mobile Services, GMS) nutzen Geräte, um Dienste zu bewerben und zu verkaufen. Diese Dienste fordern normalerweise (z. B. über einen EULA) Zugriff auf Gerätedaten; dies kann ein Verstoß gegen die Datenschutz- und Sicherheitsrichtlinien des Unternehmens darstellen. So hat beispielsweise IBM öffentlich bekannt gegeben, dass es Siri blockiert.[1] Im EULA von Siri heißt es, dass man zustimmt, dass Apple, seine Tochtergesellschaften und Vertreter diese Informationen übertragen, sammeln, verwalten, verarbeiten und verwenden, einschließlich Spracheingaben und Benutzerdaten. Da solche Geräte eine Cloud-Anbindung erfordern, wurden Kunden dazu genötigt, Lücken in ihre Firmen-Firewalls zu reißen. Zebra-Kunden, einschließlich mehrere der 10 größten Einzelhändler, haben angegeben, dass sie wegen Sicherheitsbedenken keine GMS-Geräte in ihrem Firmennetzwerk zulassen.

ENDVERBRAUCHER-ROADMAPS

In Schweigen gehüllt

Verschwiegenheit und Geheimhaltung um Roadmaps sind zwar wichtig bei Endverbraucher-Produkten, aber dies läuft der Planung und Service-Kontinuität von Unternehmen zuwider. Apple rühmt sich mit Geheimnistuerei:

- „Fehlende Informationen halten das hohe öffentliche Interesse aufrecht, da die Verbraucher spekulieren“, so Regis McKenna, einer der ursprünglichen Marketing-Berater von Apple.
- „Ohne feste Roadmap als Grundlage scheuen sich viele Käufer vor dem Erwerb von Apple-Produkten.“ – Jeff Gamet, MAC Observer

APP STORE-MALWARE

Gerätesperre (MAM – Mobiles Anwendungsmanagement)

Gemäß der NIST Mobile-Sicherheitsrichtlinien ist es eine Best Practice in Bezug auf Sicherheit, den Zugang zum öffentlichen App-Store zu blockieren. Natürlich stellt dieser für Endverbrauchergeräte wie denen von Apple eine starkes Wertangebot dar, das man nicht deaktivieren kann.

Obwohl der Android-Store Google Play ebenfalls schon zahlreiche schadhafte Inhalte aufwies, können Apps im Apple App-Store auch Unternehmensdaten verletzen. Über die Apple-Bildschirmanwendungen ist es Apps möglich, sensible Gerätedaten abzufragen und hochzuladen.

Zu den wichtigen Ressourcen, die über iOS-Anwendungen leicht zugänglich (d. h. anfällig) sind, gehören:

- Kabellose Kommunikation mit anderen Geräten
- Adressbuch – Anschriften, Notizen zu Kontakten usw.
- Kalender
- Geräteidentifikation (eine individuelle ID, über die jedes Apple-Gerät verfügt)
- Telefonnummer des Geräts (kann über eine Konfigurationsänderung deaktiviert werden)
- Musik-/Videodateien und Fotogalerie
- Suchverlauf von Safari
- Verlauf der autom. Textvervollständigung
- Inhalte, die kürzlich auf YouTube angesehen wurden
- WLAN-Verbindungsprotokolle
- Mikrofon und Videokamera

[1] http://www.zdnet.com/blog/btl/ibm-bans-siriprivacy-risk-or-corporateparanoia-at-its-best/77843

ENTFERNUNG UNERWÜNSCHTER DIENSTE

Wegen der entstehenden Sicherheitsschwachstellen versuchte eine Reihe von Kunden, den öffentlichen Apple App-Store von ihren iOS-Geräten zu entfernen und musste feststellen, dass er „immer wieder zurückkommt“.

MOBILES ANWENDUNGSMANAGEMENT (MAM) – KEINE MÖGLICHKEITEN FÜR WHITELISTS

Geräte, die für Unternehmen sicher sind (CLDs), haben meistens eine Sperre hinsichtlich der Anwendungen, die geladen und ausgeführt werden dürfen. Kunden haben ihre Frustration darüber geäußert, dass sie keine sogenannte „Whitelists“ (eine Liste mit zulässigen Anwendungen) für Endverbrauchergeräte erstellen dürfen, wie z. B. diejenigen mit Apple/iOS (Whitelisting ist eine Standardfunktion von Android/Mx).

MINDSHARE

Wahl eines Partners, nicht eines Geräts

Im dritten Quartal 2013 verkaufte Apple 33,8 Millionen iPhones und Samsung 88,4 Millionen Smartphones. Das sind hochgerechnet Jahresraten von 135,2 Millionen bzw. 353,6 Millionen Geräten. Das bedeutet, dass Samsung über das Jahr gesehen fast 1 Million Geräte pro Tag ausliefert. Somit stellt ein Unternehmens-Rollout von 10.000 Geräten nur ungefähr 10 % der Auslieferungen eines einzigen Tages dar. Im Gegensatz dazu liefern Firmen, die für den Enterprise-Bereich produzieren, weniger als 1,5 Millionen Geräte im Jahr aus. Somit stellt ein Verkauf von 10.000 Geräten eine große Gelegenheit dar und garantiert starke Bemühungen.

Ein Zebra-Kunde sagte einmal, dass sein Unternehmen bei der Wahl eines Endverbraucherprodukts ein Gerät wählte, keinen Partner. Dies spiegelt wider, was kürzlich in einem WSJ-Artikel zu lesen war[3].

ÜBERGANGENE LOGISTIK

Aktualisierungen von Distributionszertifikaten

Um Apple-Anwendungen verteilen zu können, muss man sich beim Apple Enterprise-Entwicklerprogramm registrieren (Enterprise-Zertifikat mit Laufzeit von drei Jahren) und ein Distributionszertifikat erwerben. Danach werden Anwendungen implementiert. Doch wenn das Distributionszertifikat einmal abläuft (1 Jahr), müssen Sie Ihre Anwendungen mit einem verlängerten Zertifikat neu erstellen und anschließend erneut implementieren. Mehrere Enterprise-Kunden berichteten, dass die installierten Apps einfach nicht ausgeführt werden konnten (sie können auch mehrere Tage so lange funktionieren, bis das Zertifikat beim Apple OCSP-Server für ungültig erklärt wird).

REMOTE-NEUSTART

Egal, wie viele Sicherheitsmaßnahmen auch getroffen werden, erfordern Geräte manchmal einen Neustart. Ein Geräteneustart mit einem Programm erfordert einen API-Zugang, der bei Endverbrauchergeräten (z. B. Apple iOS) häufig nicht vorzufinden ist. Im Gegensatz dazu macht Zebra Android/Mx APIs für vertrauenswürdige/signierte Anwendungen verfügbar, um das Gerät über ein Programm neu starten zu können (normalerweise per Fernzugriff mittels MDM).

AKKUMANAGEMENT

Unterbrechungsfreier Betrieb

Eine Nutzung im Unternehmensbereich stellt häufig eine starke Beanspruchung der Akkulebensdauer dar (sowohl kurz- als auch langfristig gesehen). In vielen Fällen ist es bei Endverbrauchergeräten nicht möglich, Akkus auszutauschen (z. B. bei Apple). Dann sind Enterprise-Kunden dazu gezwungen, zwei Geräte anstelle eines und zudem einen Ersatzakku zu kaufen. In einigen Szenarios ist der Akku zwar austauschbar, aber der mechanische Verriegelungsmechanismus ist nicht für ein häufiges Ersetzen gedacht und kann defekt werden.

„Designer Dustin Curtis erzählt, dass er eine kurze Umfrage zu 15 Entwicklern von beliebten iOS-Apps durchführte. Das Ergebnis: ‚13 von ihnen sagten mir, dass sie eine Kontaktdatenbank mit Millionen von Datensätzen haben. Eine Firmendatenbank enthält die Handynummer von Mark Zuckerberg, die private Telefonnummer von Larry Ellison und die Mobiltelefonnummer von Bill Gates.‘“[2]

[2] http://www.pcworld.com/article/250007/path_isnt_only_app_to_upload_store_address_book_data.html
[3] http://blogs.wsj.com/cio/2013/06/12/apple-stilllags-in-enterprise-support/

GERÄTEZUGRIFF

Beispiel: Remote-Zugriff auf Geräte

Die iOS-Plattform von Apple ist systembedingt ziemlich geschlossen. Obwohl dies die Gefahr durch schadhafte Inhalte in Grenzen hält, schränkt es auch die Möglichkeit von Enterprise-Entwicklern ein, erweiterte Funktionen hinzuzufügen. Eine häufig angefragte Enterprise-Funktion ist beispielsweise die Übernahme der Kontrolle über das Benutzergerät durch die IT-Abteilung per Fernzugriff. Dies kommt häufig bei Schulungszwecken und Diagnosen zum Einsatz. Um diese Funktionalität zu erhalten, muss eine vertrauenswürdige Anwendung Zugang zum Display-Puffer erhalten, was bei Apple-Plattformen nicht möglich ist. Lösungen wie Android/Mx von Zebra hingegen erlauben vertrauenswürdigen Anwendungen (die entsprechend signiert sind), auf Ressourcen wie den Frame-Puffer zuzugreifen.

So ermöglicht der Android-Signierungsprozess vertrauenswürdigen, signierten/authentifizierten Anwendungen die erforderliche Zugriffsstufe zum Aktivieren von Enterprise-Funktionen.

EXTREM HOHE AUFLÖSUNG

Ausgeglichener Enterprise-Nutzen

Endverbrauchergeräte tendieren immer mehr zu extrem hochauflösenden Displays. So ging Apple beispielsweise bei seinem Schritt vom iPad 2 zum iPad New von 1024x768 zu 2048x1536 über. Es wurde berichtet, dass dieser Wechsel doppelt so viele LEDs für die Hintergrundbeleuchtung und eine Zunahme von 68 % beim Akku des IPad New erforderte. Laut einer Studie[4] hat sich die Energieeffizienz des Displays deutlich verringert (d. h. die 2,5-fache Energie für die gleiche Helligkeit). Außerdem wurden Anwendungen, die die Vorteile der extrem hohen Auflösung nutzen wollten, deutlich größer (die Größe von Bjango stieg zum Beispiel von 18,3 MB auf 35 MB). Die Beförderung größerer Datenmengen kann die Kosten erhöhen, wenn man einen Tarif mit einem mehrstufigen Datenpreismodell hat.

Eine hohe Auflösung ist für Enterprise-Kunden zwar wichtig, aber die extremen Werte von Endverbrauchergeräten wirken sich negativ auf die Akkulebensdauer und/oder das Gewicht aus, was nicht wünschenswert ist.

DATEIMANAGEMENT

Enterprise-IT-Manager wollen häufig die Möglichkeit, Dateien und Ordner auf einem Gerät anzuzeigen und zu verwalten. Leider ist das Dateisystem von Apple iOS nicht offen. Es gibt zwar Drittanbieteranwendungen, aber diese sind aufgrund der iOS-Architektur in ihrem Nutzen beschränkt.

VERSCHLÜSSELUNG

Dateigrößenoptimierung als Kompromiss

Die Effizienz von Verschlüsselungsimplementierung kann abhängig vom Ziel variieren. Apple und Samsung haben eine Hardware-basierte Verschlüsselung implementiert. Von Zebra durchgeführte Tests haben gezeigt, dass bei sehr großen Dateien (d. h. mit ca. 128 MB, wie z. B. Multimedia-Dateien) die Apple-Hardwareverschlüsselung effektiv ist. Doch bei kleinen Dateien (1 KB) zeigten die Zebra-Tests, dass die Zebra-Verschlüsselung um 306 % schneller ist. Die Hardwareverschlüsselung erfordert wohl eine Initialisierung und Einrichtung, die sich bei großen Dateien zwar amortisiert, sich aber bei kleinen Dateien bemerkbar macht. Die Hardwareverschlüsselung mag zwar für große Multimedia-Dateien äußerst effektiv sein (z. B. DRM bei Filmen), doch für die kleineren Dateien, die häufig in Enterprise-Anwendungen verwendet werden, ist sie nicht optimal.

ZENTRALISIERTER SPEICHER

Bei iOS ist eine App wie ein eigenes Universum mit einem eigenen Speicher, der nur für diese App zugänglich ist. Dies erschwert das Teilen großer Datenstrukturen (Apps müssen normalerweise eine weitere Kopie erstellen). Wenn Apps Daten teilen, bleibt das Profil (z. B. die Verschlüsselung) der ursprünglichen Datenstruktur möglicherweise nicht in der kopierten Struktur erhalten, was gegen Sicherheitsrichtlinien verstößt.

Enterprise-Kunden brauchen häufig Wechselspeicher zum Portieren von Daten, für Datensicherungen und/oder als Speichererweiterung. Apple-Geräte unterstützen/bieten keine Wechselmedien (z. B. SD-Karten, Flash-Laufwerke usw.).

[4] http://www.slashgear.com/ipad-retina-displaysquashes-rivals-but-its-notperfect-20219167/

MLC-FLASH-SPEICHER KANN BEI LÄNGERER NUTZUNG FEHLERHAFT WERDEN

Flash-Speicher wird normalerweise entweder als MCL- (MLC kurz für englisch multi-level cell) oder als SLC-Speicherzelle (SLC kurz für englisch single-level-cell) konfiguriert. MLC-Konfigurationen bieten normalerweise die zweifache Kapazität vergleichbarer SLC-Konfigurationen, aber dies kann im Laufe der Zeit zu fehlerhaften Daten führen. Nach einer wiederholten Nutzung („Verschleiß“) variieren die Floating-Gate-Spannungspegel, die Bits von Informationen in der MLC darstellen, und es kommt zu fehlerhaften Bit-Auslesevorgängen.

Aufgrund der relativ kurzen Lebenszyklen und der relativ harmlosen Nutzung (im Vergleich zu Unternehmen) verwenden Endverbraucher- und einige Unternehmensgeräte MLC-Flash-Speicher. Kunden sollten ihr Nutzungsfallmodell bzw. ihren Lebenszyklus überprüfen, um die optimale Flash-Konfiguration zu bestimmen.

FEHLENDE MÖGLICHKEIT ZUM SPERREN VON KONFIGURATIONSPROFILEN PER MDM

Apple-Geräte können mithilfe von „Konfigurationsprofilen (CP)“ konfiguriert werden. Konfigurationsprofile sind XML-Dateien nach Spezifikation von Apple. Wenn ein IT-Administrator ein Gerät mit einem CP konfiguriert, kann das CP entweder offen (leicht modifizierbar), nur mit einem Passcode modifiziert oder gesperrt (sämtliche Modifikationen führen dazu, dass das Gerät komplett zurückgesetzt wird) sein.

Bei der Nutzung von Profilen, die von einem MDM generiert wurden, gibt es keine entsprechende Maßnahme zum Sperren des CP. Aus diesem Grund können die Geräteprofile eines MDM problemlos von einem Endbenutzer geändert oder gelöscht werden.

„EIN BETRIEBSSYSTEM, VOM LAGER BIS HIN ZUM VERKAUFSRAUM“ – UNWAHRSCHEINLICH BEI PRODUKTEN FÜR ENDVERBRAUCHER

Ein führender Einzelhändler (neben anderen) hat gesagt: „Wir wollen ein einziges Betriebssystem von den Lagern bis hin zu den Verkaufsräumen.“ Lager benötigen normalerweise sehr anwendungsspezifische Geräte, die wahrscheinlich nicht von Apple stammen. Im Gegensatz dazu bietet Zebra (und unserer Meinung nach der Großteil der Branche) Android-Lösungen, die überall genutzt werden können: vom Lager, über das Backoffice und den Verkaufsräumen bis hin zum Außendienst.

AUSWAHLMÖGLICHKEITEN

Der Wert der Konkurrenz

Wenn es um iOS geht, ist Apple der alleinige Anbieter mit einem Portfolio von drei grundlegenden Geräten: iPod, iPhone und iPad. Es gibt keine anwendungsspezifischen Geräte; sämtliche zweckbestimmten Aufgaben werden mittels Steckhalterungen realisiert. Im Gegensatz dazu gab es im März 2013 über 48 verschiedene Hersteller von Android-Geräten mit über 550 erhältlichen Geräten. Dies umfasst Hersteller von Unternehmensgeräten (z. B. Zebra, Honeywell, Bluebird usw.) und von Endverbrauchergeräten. Diese vielfältige Landschaft ermöglicht Unternehmen eine aggressivere Preisgestaltung und die vollen Vorteile von Multisourcing (z. B. geringeres Risiko).

BEGRENZTER API-ZUGANG

Ermöglichen von Enterprise-Zugriff

Bei Apple iOS und WP8 sind APIs gesperrt, so dass die Angriffsfläche für schadhafte Anwendungen minimiert wird. Dies ist zwar für Endverbraucher, die unbekannte Anwendungen von unbekannten Quellen herunterladen, potentiell etwas Gutes, aber dieser Ansatz schränkt bestimmte Funktionen in Unternehmen ein (z. B. wünschen sich viele Enterprise-Kunden detaillierte kabellose Kontrollmöglichkeiten oder Zugriff auf Hardware-Zubehör).

ANFÄLLIGKEIT DES SCHLÜSSELBUNDS

Fraunhofer-Forscher haben eine bedeutsame Schwachstelle von iOS bekannt gegeben. Viele Kennwörter (VPN-Zugang, Exchange Active Sync-Kennwörter, das WLAN-Kennwort, Voicemail) in iOS werden im iOS-Schlüsselbund gespeichert. Dieser Schlüsselbund in iOS wird mit „Material“ (Daten) verschlüsselt, das sich lokal auf dem Gerät befindet. Somit kann ein Hacker das Material vom Gerät extrahieren und den Schlüsselbund entschlüsseln … was gespeicherte Kennwörter leicht zugänglich macht. Hinweis: Es ist immer noch ein Update dieser Analyse für die neueste Version von iOS 7 ausstehend.[5]

SICHERHEITSSCHWACHSTELLE VON SIRI

Siri ist eine natürliche Spracherkennungsanwendung, die beim iPhone 4S eingeführt wurde. Ein großer Teil des Nutzens von Siri beruht auf der Möglichkeit für Benutzer, unkomplizierte Anfragen per Sprache zu stellen. Bei einer standardmäßigen

[5] „Fraunhofer researchers circumvent encryption devices iPhone“, Latest IT News, 9. Februar 2011

Konfiguration wird diese Funktion per Tastendruck außerhalb der Gerätesperre aktiviert. Wenn also das Gerät verlorengeht oder gestohlen wird, kann die Person, die das Gerät dann hat, auf E-Mails, Kontakte und Textnachrichten zugreifen. Siri kann zwar auch hinter die Sperr-Firewall gesetzt werden, doch dies würde den Nutzen deutlich mindern.

ENDVERBRAUCHERKAMERAS FÜR BARCODE-ERFASSUNG

Zebra teilt Imaging-Teilsysteme in zwei Kategorien ein: „Kamera“ und „Imager“. Wie der Name schon sagt, ist die „Kamera“ ein Mehrzwecksystem, ähnlich dem einer Digitalkamera für Endverbraucher. Kamerasysteme weisen normalerweise folgende Eigenschaften auf: chromatisch (Farbe), Autofokus, hohe Pixelzahl, Weitwinkelobjektiv und kein weiterer Zielmechanismus neben dem Sucher. Zudem nehmen Kameras für gewöhnlich von der Rückseite des Geräts auf. Im Gegensatz dazu ist ein „Imager“ monochromatisch (einfarbig) und hat einen festen Fokus, eine geringere Pixelzahl mit einem größeren Pixel-Öffnungsverhältnis, einen globalen Verschluss, einen schmäleren Sichtwinkel und zudem einen Zielmechanismus bzw. ein Zielmuster. Imager befinden sich normalerweise vorne im Gerät.

Ebenso wichtig sind für ein robustes Barcode-Erfassungssystem die Signalverarbeitungsalgorithmen zum Erfassen und Dekodieren von Barcodes im Bild. Apple-Geräte, die die Kamera für Barcode-Dekodierung verwenden, nutzen häufig die Dekodierungssoftware Red Laser. Empirische Tests der Software Red Laser haben häufige fehlerhafte Dekodierungen, eine begrenzte Unterstützung von Symbologien und Probleme bei der Dekodierung beschädigter oder verwitterter Barcodes ergeben.

Wenn es um Barcode-Leseanwendungen geht, bietet das Imager-Teilsystem einen längeren Lebenszyklus, eine höhere Empfindlichkeit, eine bessere Ausrichtung (Zielmechanismus) und bessere Ausgleichmöglichkeiten von Vibrationen durch zitternde Hände.

WLAN-FIPS-VERSCHLÜSSELUNG

Kunden aus Behörden, dem Gesundheitswesen und dem Einzelhandel (mit Pharma und/oder PCI für MPOS) wollen, dass die kryptografischen Module (d. h. diejenigen, die für die Verschlüsselung/Entschlüsselung verwendet werden) des Geräts für FIPS 140-2 Level 1 zertifiziert sind. Diese FIPS-Stufe gewährleistet das beste Design für eine kommerzielle Nutzung. FIPS-zertifizierte kryptografische Module sind zwar normalerweise für Enterprise- und Endverbrauchergeräte verfügbar. Allerdings sind diese Module für gewöhnlich nicht für die WLAN-Link-Kryptografie gedacht (d. h. nur für die Anwendungsnutzung). Zebra hat in der Vergangenheit FIPS auf Microsoft-basierten WLAN-Produkten angeboten, und im Jahr 2014 begann Zebra damit, FIPS für WLAN bei einer Reihe seiner Android-Produkte bereitzustellen.

Nähere Informationen finden Sie auf www.zebra.com/mobilecomputers

Zentrale Nordamerika und Unternehmenszentrale
+1 800 423 0442
inquiry4@zebra.com

Zentrale Asien-Pazifik
+65 6858 0722
contact.apac@zebra.com

Zentrale EMEA
zebra.com/locations
mseurope@zebra.com

Zentrale Lateinamerika
+1 847 955 2283
la.contactme@zebra.com