RATGEBER FÜR UNTERNEHMEN – UMSTIEG VON WINDOWS CE oder MOBILE AUF ANDROID

Informationen und Hinweise

Präsentiert von Honeywell Sensing and Productivity Solutions (S&PS)

Honeywell
PLATINUM
PERFORMANCE PARTNER

Einführung

In der Betriebssystemlandschaft für Mobilgeräte hat sich in den letzten Jahren ein Wandel vollzogen. Immer mehr Systeme werden von Windows® auf ein anderes Betriebssystem umgestellt. Und obwohl dies unbestreitbare Vorteile hat, bringt es jeweils auch gewisse Nachteile bzw. Kompromisse mit sich. In diesem Dokument werden Pro und Kontra ausführlich dargestellt und Empfehlungen ausgesprochen.

Inhalt

Kurzer Rückblick

Google-OEMs und andere begannen mit der Entwicklung von Erweiterungen für das Open-Source-Betriebssystem Android, die Geräteverwaltungsfunktionen ermöglichten, mehr Kontrolle über Benutzeraktionen boten und die Unterstützung für industrielle Wi-Fi-Netzwerke und Barcode-Scanning-Funktionen erweiterten.

Vor zehn Jahren kamen die Betriebssysteme für Mobilgeräte im Enterprise-Bereich fast ausschließlich von Microsoft. Windows CE und Windows Mobile (später Windows Embedded Handheld) boten alle für die Bereitstellung in Unternehmen erforderlichen Funktionen und Features, und dank der unzähligen Entwickler- und Fremdanbietertools war es möglich, für jedes Unternehmen eine individuelle Lösung für einen effizienten Geschäftsbetrieb zu implementieren. Apple hatte erst vor kurzem das erste iPhone® herausgebracht. Ein paar Jahre zuvor hatte Google Android™ erworben, aber noch kein Mobiltelefon auf den Markt gebracht. Die anderen zu dieser Zeit verfügbaren Optionen waren alle für den Einsatz im Büro gedacht und daher für zweckgebundene Anwendungsumgebungen eher ungeeignet. Windows lief stabil und kam in vielen Unternehmen zum Einsatz, die ein robustes Mobilgerät für typische Geschäftsanwendungen benötigten.

Enterprise-Funktionen kamen bei iOS und Android erst einige Jahre später hinzu und entwickelten sich anfangs auch eher schleppend, während sich Apple und Google auf den schnell wachsenden Smartphone-Markt für Verbraucher konzentrierten. Google-OEMs und andere begannen, Erweiterungen für das Open-Source-Betriebssystem Android zu entwickeln, mit denen Geräteverwaltungsfunktionen, mehr Kontrolle über die Benutzeraktionen, zusätzliche Unterstützung für betriebliche WLAN-Netzwerke und Barcode-Scanfunktionen möglich waren. So kam die erste Generation von Android-Geräten für Enterprise-Bereitstellungen auf den Markt, die immer wieder verbessert und aufgrund der positiven Resonanz bei den Kunden, vor allem wegen der benutzerfreundlichen Touch-Displays und der wachsenden Zahl verfügbarer Apps, ständig um Produkte erweitert wurde. Dieser unternehmerische Ansatz führte jedoch zu einer Aufsplitterung.

Je mehr das Basisbetriebssystem modifiziert wurde, desto weiter wichen die Anwendungen vom Standard ab, was eine Ausführung auf Produkten verschiedener Anbieter erschwerte. Damit sank auch die Wahrscheinlichkeit, dass stark modifizierte Geräte schnell auf die nächste Version des Basisbetriebssystems aktualisiert werden konnten.

Daraufhin brachte Apple, das über eine große Entwickler-Community verfügt, seine eigenen Verwaltungstools und Enterprise-Erweiterungen für iOS heraus. Aber das geschlossene System von Apple hat nach wie vor Schwierigkeiten mit der Steuerung von Updates und der Verwaltung einiger Gerätefunktionen. Da die Hardwaregeräte auf Verbraucher-Smartphones und Tablets beschränkt sind, eignet sich iOS nur für Anwendungsfälle, in denen Mobilgeräte ausreichen, die durch zusätzliche robuste Gehäuse für die Anwendung im Industriebereich tauglich gemacht werden.

Ältere Betriebssysteme

Angesichts der Tatsache, dass der Support für ihr aktuelles Betriebssystem bald eingestellt wird, müssen viele Kunden jetzt entscheiden, wie es weitergehen soll, da die Anwendungsentwicklung ein zeitaufwändiger und kostspieliger Prozess ist.

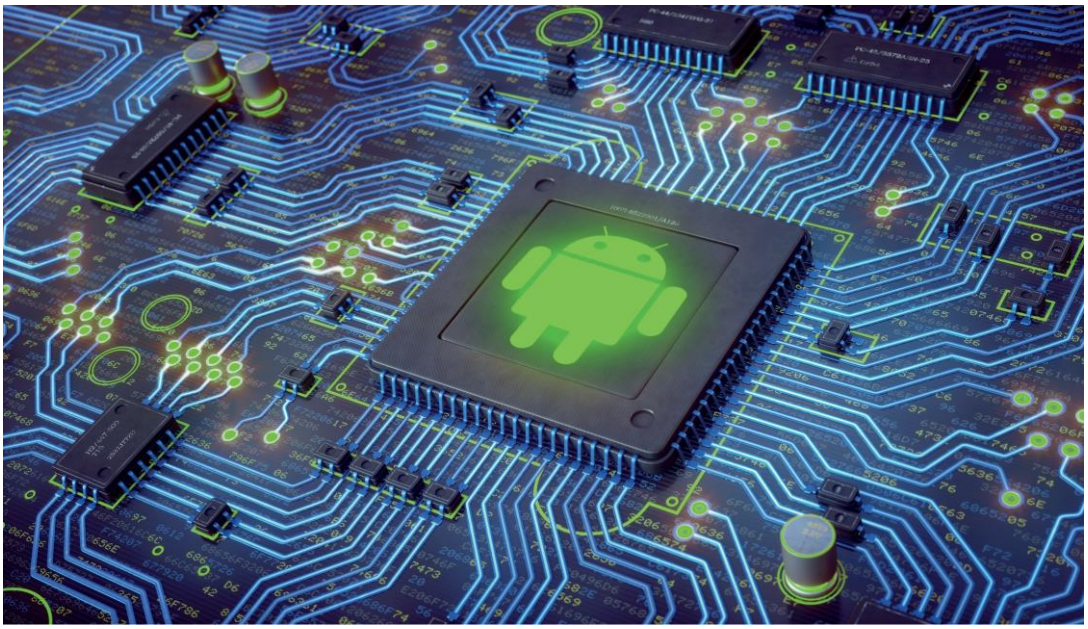
Der Support für die Microsoft-Plattformen Windows CE 6 und Windows Mobile/ Windows Embedded Handheld 6.5 wird in absehbarer Zeit eingestellt, dies betrifft also alle Kunden, deren Anwendungen derzeit darauf ausgeführt werden. Der Mainstream-Support mit regelmäßigen Aktualisierungen wurde für beide Systeme bereits eingestellt. Der erweiterte Microsoft-Support (Sicherheits-Updates) endet für Windows CE 6 Anfang 2018 und für Windows Embedded Handheld 6.5 Anfang 2020. Danach können keine Patches mehr für Schwachstellen oder Fehler bereitgestellt werden, die im Microsoft-Code auftreten. Aus diesen Gründen haben viele Unternehmen bereits den Umstieg auf andere Anwendungen geplant, die auf einem modernen Betriebssystem ausgeführt werden.

Angesichts der Tatsache, dass der Support für ihr aktuelles Betriebssystem bald eingestellt wird, müssen viele Kunden jetzt entscheiden, wie es weitergehen soll, da die Anwendungsentwicklung ein zeitaufwändiger und kostspieliger Prozess ist. Eine Möglichkeit, die endgültige Entscheidung noch etwas hinauszuzögern und sich alle Optionen offenzuhalten, besteht darin, auf Hardware umzusteigen, die mehrere Betriebssysteme unterstützen kann. So hat man bei den mobilen Computern der Serien CN75 und CK75 von Honeywell und dem mobilen Computer CN51 von Honeywell beispielsweise die Auswahl zwischen Windows Embedded Handheld und Android. Außerdem können Kunden, die sich jetzt für Windows Embedded Handheld entschieden haben, zu einem späteren Zeitpunkt problemlos auf Android umsteigen. Damit können vorhandene Anwendungen so lange fortgeführt werden, bis der Wechsel zu Android umfassend vorbereitet ist, wofür dann lediglich eine Softwareumstellung vor Ort durchgeführt werden muss. An dieser Stelle ist nur eine kleine Softwareinvestition erforderlich, es müssen keine Hardwareänderungen vorgenommen werden.

Androids große Marktpräsenz unterstützt ein breites Spektrum an OEMs und Hardwarevarianten, wodurch die Wahrscheinlichkeit steigt, dass eines der Geräte genau die gewünschten Anwendungs- und Kostenanforderungen erfüllt, auch bei Geräten mit integrierten Tastenfeldern.

Die Entwicklung von Android Enterprise

In den letzten drei Versionen hat Google enorm in die Enterprise-Funktionen investiert und Android for Work in Android Enterprise umbenannt.



Vor der Veröffentlichung von Android 4.0 Ice Cream Sandwich war dieses Betriebssystem nicht für Unternehmensanwendungen ausgelegt. Die Steuerung und Verwaltung in Unternehmensumgebungen war nur durch OEM-Erweiterungen und die Integration von Fremdanbietersoftware in das anwenderorientierte Betriebssystem möglich. Enterprise-Funktionen kamen erst schrittweise in den Versionen 4.2 Jelly Bean und 4.4 KitKat hinzu, was schließlich in der Einführung von Android for Work in 5.0 Lollipop mündete. Android for Work bot eine Reihe von Management-APIs und ein Containersystem, mit dem persönliche und arbeitsbezogene Apps und Daten voneinander getrennt verwaltet werden konnten.

In den letzten drei Versionen hat Google enorm in die Enterprise-Funktionen investiert und Android for Work in Android Enterprise umbenannt. Zu den neuen Funktionen gehört die Massenbereitstellung zur Beschleunigung der Geräteeinrichtung, der Geräteinhabermodus, mit dem vollständig verwaltete Geräte auf Unternehmensebene möglich sind, ständig verfügbares VPN und eine standardmäßig aktivierte Verschlüsselung zum Schutz von persönlichen und Unternehmensdaten.

Mit weitverbreiteten Betriebssystemen für Mobilgeräte wie Android können die Unternehmen auf ein großes Ökosystem von Anwendungen, Entwicklertools und anderen Ressourcen zugreifen, dies birgt jedoch auch Sicherheitsrisiken, die identifiziert und eingegrenzt werden müssen. Android hat sein Sicherheitskonzept ständig weiterentwickelt.

Mit steigendem Marktanteil wurde Android immer häufiger zum Ziel von Exploits und Malware-Angriffen. Google hat darauf mit erhöhten Sicherheitsanforderungen zum Schutz vor potenziell gefährlichen Apps (Potentially Harmful Apps, PHAs) und der Implementierung von Schutzmaßnahmen innerhalb des Betriebssystems reagiert, die verhindern sollen, dass das System im Falle einer PHA-Installation kompromittiert wird. Einige dieser Schutzmaßnahmen werden weiter unten erläutert. Ausführliche Informationen hierzu finden Sie im Android-Jahressicherheitsbericht 2016 von Google unter folgendem Link:

https://source.android.com/security/reports/Google_Android_Security_2016_Report_Final.pdf

So können wir Sie unterstützen

Das Cyber-Sicherheits-Team überwacht verschiedene Informationsquellen, um so frühzeitig wie möglich auf potenzielle Sicherheitsprobleme aufmerksam zu werden (normalerweise lange vor den Mainstream-Medien) und hat ein Eskalationsprotokoll implementiert, mit dem unternehmensweite Ressourcen in einer Prioritätsreihenfolge mobilisiert werden, um gegen diese Probleme vorzugehen.

Honeywell legt größten Wert auf Cyber-Sicherheit. Unser globales Unternehmen ist auch in der Luft- und Raumfahrt- sowie in der Prozesstechnik tätig, wo für alle verfahrenstechnischen Aspekte extrem hohe Sicherheitsanforderungen gelten. Ein internes Expertenteam ist für die Festlegung und Umsetzung von Sicherheitsrichtlinien und -standards zuständig, wozu auch Produktentwicklungstestverfahren zur Identifizierung von Softwareproblemen gehören, durch die Systeme anfälliger für Angriffe werden. So können potenzielle Schwachstellen noch vor der Produktveröffentlichung eliminiert werden.

Das Cyber-Sicherheits-Team überwacht verschiedene Informationsquellen, um so frühzeitig wie möglich auf potenzielle Sicherheitsprobleme aufmerksam zu werden (normalerweise lange vor den Mainstream-Medien) und hat ein Eskalationsprotokoll implementiert, mit dem unternehmensweite Ressourcen in einer Prioritätsreihenfolge mobilisiert werden, um gegen diese Probleme vorzugehen. Sobald eine Android-Schwachstelle entdeckt und die entsprechende Gegenmaßnahme von Google veröffentlicht wurde, implementieren Honeywells Android-Sicherheitsexperten das Update und leiten es umgehend an die Kunden weiter. Durch die direkte Verteilung von Patches und Updates ist die Reaktionszeit bei Honeywell deutlich kürzer als bei anderen OEMs, die ihre Updates über Sekundärkanäle verbreiten müssen.

Für alle Produkte von Honeywell gibt es Sicherheitshandbücher mit Best-Practice-Verfahren zum Schutz der Umgebung und Geräte beim Kunden. Sie enthalten Anweisungen zur Konfiguration von Geräte- und Netzwerkeinstellungen und zur Aufrechterhaltung einer sicheren IT-Umgebung. Mit diesen Präventivmaßnahmen soll die Kundenumgebung vor Angriffen von außen geschützt werden.

Viele Unternehmenskunden schränken die Endbenutzer weiter ein, indem sie die Geräte über einen Agenten zur mobilen Geräteverwaltung oder eine App wie den Honeywell Enterprise Launcher „sperren". Mit diesen Tools kann der Benutzerzugriff auf die Systemressourcen kontrolliert werden und der Administrator kann festlegen, welche Apps ausgeführt werden dürfen. Wenn die Benutzer keine nicht autorisierten Apps installieren oder ausführen dürfen, ist das System viel weniger anfällig für Sicherheitsbedrohungen, die durch Benutzeraktionen entstehen. Honeywell bietet eine Enterprise-Toolkit-API-Bibliothek, mit der die Benutzer Whitelists und Blacklists für Anwendungen erstellen, die Verfügbarkeit einer großen Anzahl von Gerätefunktionen steuern und kontrollieren können, welche IP-Adressen die Firewall passieren dürfen. Der Honeywell Launcher ersetzt den standardmäßigen Android-Startbildschirm

durch eine Kiosk-Ansicht, in der jeder Benutzer nur die Apps anzeigen und ausführen darf, die für seinen Job erforderlich sind. Honeywell bietet auch einen Enterprise-Browser, der das Rendern von Webseiten über die Android-Standardzugriffskontrolle ermöglicht und über den kontrolliert werden kann, welche Seiten die Benutzer aufrufen dürfen. Durch die Beschränkung der Geräteverwendungsmöglichkeiten werden der IT-Support vereinfacht und die Möglichkeiten für das Eindringen von Malware in das System erheblich reduziert.

Ein weiterer wichtiger Sicherheitsaspekt ist die regelmäßige Durchführung aller verfügbaren Updates. Experten entdecken ständig Schwachstellen in der Android-Codebasis, die potenziell zum Ziel bösartiger Angriffe werden können. Google betreibt sogar ein eigenes Bug-Bounty-Programm, um Experten dazu zu animieren, potenzielle Schwachstellen zu finden und zu melden. Google und Chipset-Hersteller wie Qualcomm leiten Sicherheits-Patches regelmäßig an OEMs zur Integration in ihre Software-Builds weiter. Honeywell aktualisiert seine Android-System-Images alle 60 Tage, wobei Patches für besonders kritische Bedrohungen ggf. innerhalb weniger Tage verfügbar gemacht werden. Für eine einfachere Bereitstellung im gesamten Kundennetzwerk werden die Patches in kleinen, inkrementellen Updates des Baseline-Images bereitgestellt. Anders als bei Verbraucher-OEMs können die Update-Pakete von Honeywell in einem Webportal heruntergeladen und vor der vollständigen Bereitstellung von Verbrauchern getestet werden. Für die sofortige Benachrichtigung über neue Updates steht ein E-Mail-Benachrichtigungsabonnement zur Verfügung.

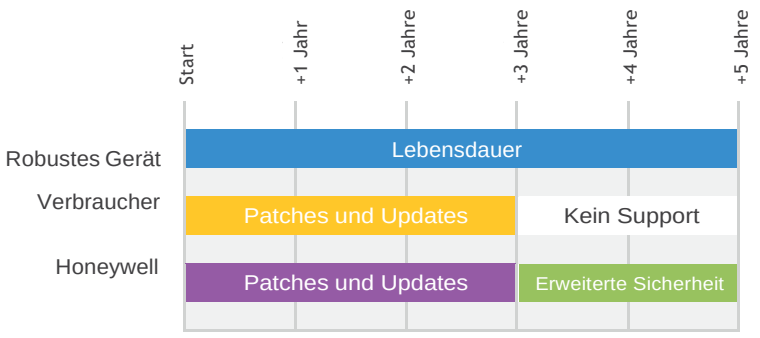
Android-Lifecycle-Management

Honeywell bietet ein Programm zur regelmäßigen Bereitstellung von Patches bei schwerwiegenden Sicherheitss-chwachstellen für das jeweils unterstützte Betriebssystem für zwei oder mehr Jahre, nachdem der Support von Google-Sicherheits-Patches eingestellt wurde.

Kunden, die eine mobile Computerlösung für anspruchsvolle Unternehmensumgebungen einsetzen, erwarten von ihren Geräten eine längere Lebensdauer als bei Verbrauchergeräten üblich. Während die Nutzungsdauer bei Verbraucher-Smartphones allgemein 2—3 Jahre beträgt, erwarten Unternehmen, dass ihre Systeme mindestens 3—5 Jahre zum Einsatz kommen. Traditionell entspricht der Lebenszyklus eingebetteter Betriebssysteme, die in robusten mobilen Computern verwendet werden, der Nutzungsdauer in Unternehmen. Für Windows CE und Windows Embedded Handheld bietet Microsoft nach der ersten Veröffentlichung einen Support von 10 Jahren.

Obwohl Android von Google bei jeder neuen Hauptversionsveröffentlichung mit vielen neuen Enterprise-Funktionen ausgestattet wird, gehört ein längerer Support leider nicht dazu. Android-Hauptversionen (die auch als „Dessert-Versionen“ bezeichnet werden, da Google sie immer nach Süßspeisen benennt) werden ca. einmal pro Jahr veröffentlicht und werden generell durch Sicherheits-Patches von Google und Chipset- Herstellern über einen Zeitraum von 3 Jahren unterstützt. Dadurch entsteht eine Lücke zwischen tatsächlichem Support und den Erwartungen der Unternehmen bezüglich der Nutzungsdauer. Wenn ein OEM-Chipset ausgewählt wird, der die nächste Hauptversion unterstützt, kann die Zeitspanne etwas verlängert werden, aber den Erwartungen der Unternehmenskunden wird die Google-Supportrichtlinie trotzdem nicht gerecht.

Honeywell bietet ein Programm zur regelmäßigen Bereitstellung von Patches bei schwerwiegenden Sicherheitsschwachstellen für das jeweils unterstützte Betriebssystem für zwei oder mehr Jahre, nachdem der Support von Google-Sicherheits-Patches eingestellt wurde.



- Die Bereitstellung an die Kunden erfolgt vierteljährlich oder seltener, wenn keine schwerwiegenden Patches für die entsprechende unterstützte Betriebssystemversion gemeldet wurden. Verfügbare Patches werden generell innerhalb von 90 Tagen nach der öffentlichen Bekanntgabe bereitgestellt, bei unmittelbaren Bedrohungen sind Ausnahmen möglich.
- Kunden, die diesen Service nutzen, müssen alle zuvor veröffentlichten Patches angewendet haben, um den aktuellsten Patch anwenden zu können. Patches sind also bezogen auf die letzte Betriebssystem-Wartungsversion kumulativ. Bestimmte Patches können nicht einzeln angewendet werden.
- Sicherheits-Patches werden entsprechend den Honeywell-Standardtestverfahren getestet. Dies gilt für alle Softwareversionen. Es obliegt dem Kunden, alle von Honeywell empfangenen Software-Updates vor der Bereitstellung im gesamten Unternehmen zu seiner Zufriedenheit zu testen.
- Dieser Service wird im Rahmen eines Servicevertrags bereitgestellt. Hierbei kann es sich um einen unabhängigen Vertrag oder einen in eine andere Art von Servicevereinbarung integrierten Vertrag handeln. Kunden ohne Vertrag erhalten keine Sicherheits-Patches, nachdem der Support von Google-Sicherheits-Patches eingestellt wurde.

Dieses Programm ist auf Honeywell-Geräten unter Android 6.0 Marshmallow und höher nach Ablauf des Google-Sicherheits-Patch-Supports verfügbar.

Fazit und Empfehlungen

Android ist ein sicheres Betriebssystem, das Anwendungsisolation und Exploit-Abwehrtechniken nutzt, um dem Benutzer ein hohes Maß an Sicherheit zu bieten. Durch das Sperren von Geräten über eine mobile Geräteverwaltung oder den Honeywell Enterprise Launcher kann das Risiko einer Malware-Infektion durch die Beschränkung der Benutzerrechte und der zur Verfügung stehenden Apps weiter gesenkt werden.

Honeywell-Produkte sind prinzipiell so konzipiert, dass sie die strikten Honeywell-Sicherheitsstandards erfüllen. Schon in der Entwicklungsphase wird die Sicherheit fortlaufend evaluiert und Schwachstellen werden identifiziert und umgangen, noch bevor das Produkt veröffentlicht wird. Die gezielte Sensibilisierung der Kunden und eine fortlaufende Überwachung der Sicherheitsschwachstellen und Bedrohungen sowie genau festgelegte Prozesse zum Umgang mit entdeckten Problemen tragen dazu bei, dass die Systeme unserer Kunden umfassend geschützt sind. Über ein abonnierbares Benachrichtigungssystem werden die Kunden sofort über neue Patches informiert, sodass sie umgehend Maßnahmen zur Risikominimierung treffen können. Unsere Systeme erfüllen höchste Sicherheits- und Qualitätsstandards, sodass sich unsere Kunden stets auf die erworbene Technologie verlassen können mit der Gewissheit, dass Honeywell alles daran setzt, sie bei der Aufrechterhaltung der Sicherheit dieser Systeme zu unterstützen.

Honeywell bietet Lösungen für die drei wesentlichen Betriebssysteme im Bereich industrietauglicher Mobilgeräte: Android, iOS und Windows. Seit vielen Jahren verhält sich Honeywell in Bezug darauf, welches Betriebssystem am besten für mobile Computer geeignet ist, neutral und rät den Kunden stets, bei der Auswahl eines Betriebssystems für ihre spezielle Umgebung alle Faktoren in Betracht zu ziehen.

Mit seinem großen Marktanteil und dem umfangreichen Ökosystem an Apps, Entwicklern und VARs ist Android jedoch mittlerweile zum klaren Favoriten für viele Unternehmen in unterschiedlichen Branchen geworden. Für den Umstieg auf Android müssen neue Apps geschrieben, einige Workflows angepasst und die Mobilgeräte ausgetauscht werden, die bisher im Unternehmen zum Einsatz kamen. Dies kann einen erheblichen Aufwand bedeuten. Eine Möglichkeit, die endgültige Entscheidung noch etwas hinauszuzögern und sich alle Optionen offenzuhalten, besteht darin, auf Hardware umzusteigen, die mehrere Betriebssysteme unterstützen kann. So hat man bei den mobilen Computern der Serie CK75 von Honeywell beispielsweise die Auswahl zwischen Windows Embedded Handheld und Android. Außerdem können Kunden, die sich jetzt für Windows Embedded Handheld entschieden haben, zu einem späteren Zeitpunkt problemlos auf Android umsteigen. Damit können vorhandene Anwendungen so lange fortgeführt werden, bis der Wechsel zu Android umfassend vorbereitet ist.

Weitere Informationen finden Sie unter:
www.opal-solutions.de

OPAL Solutions GmbH
Karl-Heinz-Beckurts-Str. 31
D-52428 Jülich
Tel.: 02461 690 280

Umstieg auf ein anderes Mobilgeräte-Betriebssystem – Informationen und Hinweise | Rev A | 10/17

Präsentiert von
Honeywell