Wie Samsungs KNOX BYOD-Smartphones sichert

E-Fort

Christoph Puppe

Mit KNOX und SAFE schickt sich Samsung an, auch die geschäftlichen Anwender verstärkt anzusprechen. Durch die tiefe Integration der Sicherheitsfunktionen in Betriebssystem und Hardware sollen die neuen Geräte ein Sicherheitslevel bieten, das bisher nur spezialisierten Angeboten vorbehalten war.

Smartphones sind die Werkzeuge, mit denen viele ihr Privatleben genauso organisieren wie ihren Arbeitstag. In beiden Welten fallen vertrauliche Daten an, dank Bring Your Own Device oft auf demselben Gerät. Diverse Angebote sind bereits auf dem Markt, die einerseits die Privatsphäre der Mitarbeiter vor der Firma und andererseits die Daten der Firma vor unberechtigtem Zugriff schützen sollen – von SIMKo3, dem Merkelphone, über BlackBerry 10 bis hin zu diversen Apps.

In allen Fällen werden zwei Welten definiert, die jeweils füreinander unsichtbar sind und so Datenabflüsse verhindern sollen. Während SIMKO3 auf Virtualisierung setzt, hat BlackBerry eine Trennung durch Sicherheitslabels. Im privaten Bereich installierte Apps müssen der Sicherheit des Betriebssystems vertrauen, da sie zwar die Daten der Container verschlüsseln, aber dennoch nur Apps sind. Denselben Schwachpunkt haben die üblichen Mobile-Device-Management-Produkte (MDM). Auch sie sind nur Apps, die ein Benutzer deinstallieren kann, und laufen in einem Betriebssystem, über das sie keine Kontrolle haben. Daran ändert auch nichts, wenn, wie etwa auf dem iPhone, diese Apps über ein Profil installiert sind.

iX-Wertung

- ⊕ Zwei-Faktor-Authentifizierung durch Smartcard-Integration
- ⊕ wirksame Trennung privater und geschäftlicher Daten
- ⊕ für private Nutzung kostenlos

Tiefe Integration statt aufgesetzter App

Zum Synchronisieren von Mails und Kontakten nutzen derzeit die meisten Firmen den vorinstallierten Exchange Active Sync Client der Smartphones. Sicherheitsbewusstere Anwender verwenden ein eigenständiges Mail-Programm, das die Daten in einem – zumeist – verschlüsselten Container speichert und einen eigenen VPN-Zugang mitbringt. Allerdings kann man innerhalb dieses Containers nicht im Intranet surfen oder Apps installieren, die auf firmeninterne Ressourcen zugreifen. Dafür gibt es wiederum Container, die virtuelle Androids enthalten. In diesen kann man jede Art von App installieren. Durch Verschlüsseln der Daten und eigene VPN-Zugänge sind auch bei diesen Containern die Daten der Firma gut geschützt, sofern nicht eine Malware das zugrunde liegende Betriebssystem verändert hat.

KNOX sieht auf den ersten Blick aus wie eine Virtualisierungs-App, da beim Umschalten zwischen privater und geschäftlicher Umgebung ein komplett neuer Desktop angezeigt wird, auf dem sich jede Art von Anwendung installieren lässt. Im Hintergrund werkelt allerdings nur ein Android-Kernel für beide Welten und die SE-Linux-Erweiterungen sorgen für die Separierung der Daten und Prozesse. Das gleiche Prinzip also, das auch BlackBerry bei der Version 10 seines Betriebssystems anwendet.

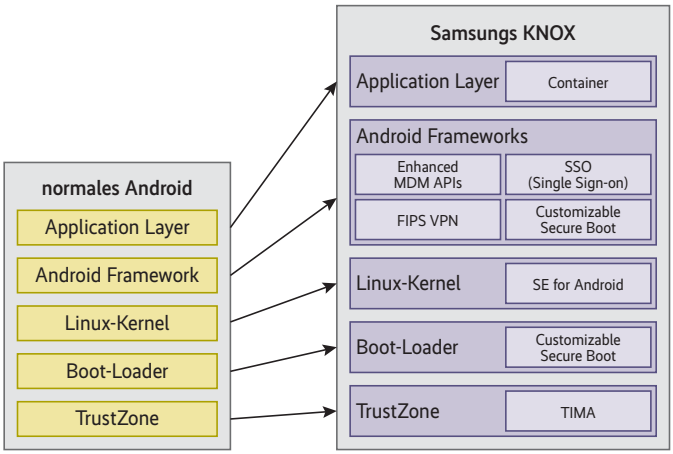
Worin sich KNOX von anderen Angeboten unterscheidet, ist die tiefe Integration in das Betriebssystem. Hier ist ein Hardwarehersteller, der ein Betriebssystem an seine Zwecke anpassen kann, klar im Vorteil gegenüber den Anbietern reiner Sicherheitserweiterungen. Apple, ebenfalls Anbieter von Hard- und Software aus einer Hand, nutzte diesen Vorteil durch die Integration eines Fingerabdruck-Sensors. Samsung setzt dagegen auf ein Interface für Smartcards und hat somit eine der großen Schwierigkeiten bei der Authentifizierung auf Smartphones ausgeräumt. Denn es gibt endlich eine Zwei-Faktor-Authentisierung, die darüber hinaus von Single-Sign-on-Lösungen unterstützt wird. Realisiert wird dies über ein vom mitgelieferten Single-Sign-on-Produkt unterstützten Cardreader, der per Bluetooth angebunden ist.

Bei der VPN-Anbindung sind bis zu 5 Kanäle gleichzeitig aktiv, wobei jede App eine eigene VPN-Einstellung haben kann. KNOX bietet auch die Möglichkeit, sich in ein MDM zu integrieren. KNOX-Container können von aktueller MDM-Software über eine KNOX-API eingerichtet, administriert und auch sicher gelöscht werden. Bei entsprechender

Konfiguration können die Administratoren auch nur die Daten im Container sehen, so ist die Privatheit der Daten des Benutzers gewährleistet.

Ein netter Nebeneffekt für private Anwender ist übrigens, dass jeder mit einem S3 (nach einem Update) oder einem S4 sich selbst einen Container einrichten kann, der vertrauliche Daten vom Rest des Gerätes trennt.

KNOX implementiert ein eigenes Schichtenmodell, dem auf jeder Ebene sichere Varianten des normalen Android entsprechen.



Sicherheitsarchitektur als Basis: TIMA und SAFE

Die Sicherheit der Apps und Funktionen ist eng mit der Sicherheitsarchitektur verbunden. Wenn eine App nur eine App ist, kann eine Malware den Schutz umgehen und zum Beispiel Speicher zur Laufzeit auslesen, Benutzereingaben abfangen und simulieren oder einfach einen Screenshot machen. Der erste Schritt beim Aufbau einer Sicherheitsarchitektur ist die hardwaregesteuerte Kontrolle des Boot-Vorgangs, die nicht via Software auszuhebeln ist. Samsung setzt dabei TrustZone von ARM ein, bei dem ein eigener Kernel gebootet wird, der über einen vom Anwender anpassbaren Mechanismus vor Veränderung geschützt ist. Dieser richtet TIMA ein (TrustZone-based Integrity Measurement Architecture), das den eigentlichen SE-Linux Kernel startet und auch im laufenden Betrieb die Integrität des Betriebssystems überwacht.

TIMA ist Teil der „Samsung for Enterprise“-Funktionen (SAFE) neuerer Samsung-Smartphones und -Tablets. Neben dem Boot-Vorgang kann SAFE allerdings noch einiges mehr absichern. So bietet es Funktionen zur Kontrolle des Gerätes und des Betriebssystems, die teilweise im Sicherheitskernel und teilweise im Kernel mit SE-Linux implementiert sind. Damit sind sie außerhalb der Einflussmöglichkeiten einer App, Malware oder auch des Anwenders selbst. Der Anwender oder die Malware kann eine MDM-App also dank SAFE nicht mehr einfach deinstallieren. Selbst wenn ein Angreifer den Kernel manipulieren sollte, kann TIMA durch Prüfsummen auf den Speicher des Kernels und das Überwachen von ladbaren Modulen diese Veränderung erkennen und gemäß einer hinterlegten Richtlinie reagieren.

Zudem schützt das SE-Linux die Daten und Anwendungen durch den Einsatz von Mandantory Access Control (MAC), das die Discretionary Access Control (DAC) des regulären Android-Kernels ersetzt. So kann eine Malware mit Root-Rechten nicht auf die Daten der durch MAC geschützten Anwendungen zugreifen, sofern diese in einer anderen Security Domain laufen. Die Geschäfts- und die Privatwelt sind bei KNOX als zwei verschiedene Security-Domains voreingestellt.

Damit die Daten auf dem Gerät bei Verlust geschützt sind, verschlüsselt Samsung die Daten mit einer FIPS-140-2 zertifizierten AES-256-Implementierung entweder für den gesamten Speicher oder nur für den KNOX-Container – also mit der doppelten Schlüssellänge im Vergleich zu einem Standard-Android. Zum Transport der Daten zwischen Gerät und Firma sieht SAFE ein VPN vor, dessen Konfiguration der Benutzer nicht mehr verändern kann, wenn sie einmal durch eine SAFE Policy gesetzt ist. Das VPN kann für den Container und den privaten Teil des Betriebssystems oder einzelne Apps unterschiedlich sein.

Neben diesen Erweiterungen bietet SAFE zusammen mit KNOX über 500 Policies, die eine MDM-Software setzen kann, also deutlich mehr als BlackBerry oder iPhone.

KNOX ist werksseitig auf dem Galaxy Note 3 und dem Tab 3 7.0 verfügbar. Eine Reihe bereits ausgelieferter Geräte wie das S4 und das S4 mini können durch Aufspielen von Android 4.3 Samsung Premium Suite Upgrade KNOX-fähig gemacht werden.

Fazit

Samsung bietet einen Ansatz, der die Nachteile der MDM-Apps behebt und auch Container sicherer macht. In Sachen Sicherheit sind die Koreaner damit auf Augenhöhe mit dem BlackBerry 10 und um einiges besser als andere Android-Varianten oder das iPhone. KNOX wurde als erstes Smartphone seit dem BlackBerry 7 für den Einsatz in den Netzen des US-Verteidigungsministeriums zertifiziert. Erst kurz danach folgten iOS 6 und BB 10.

Damit bietet es ein Maß an Sicherheit für Privat- und Business-Anwender, das in einem kostengünstigen und weitverbreiteten Smartphone wie dem S4 so noch nicht auf dem Markt erhältlich war. (js)

Christoph Puppe

ist seit 24 Jahren in der IT-Sicherheit aktiv, Lead Auditor sowie IS-Revisor und verantwortet seit 12 Jahren die technischen Audits bei der HiSolutions AG in Berlin.

Alle Links: www.ix.de/ix1401080