Sicherheit beim Mobile-Device-Management

Die berufliche und zugleich private Nutzung von Mobilgeräten birgt hohe Risiken

Die Verwendung von (mindestens) zwei Smartphones ist mittlerweile ein weitverbreiteter Trend: eines für die Arbeit, das andere für die private Nutzung – dazu noch ein Tablet. Leider ist das in vielen Fällen kaum vermeidbar, weil es an einem sicheren Management der Geräte mangelt.

Besondere Herausforderungen im Mobile-Device-Management (MDM) tauchen vornehmlich bei der Umsetzung von Bring Your Own Device (BYOD) auf. Eine Lösung dieser Aufgaben ist für den Datenschutz und die Compliance dringend notwendig und soll gleichzeitig der unerfreulichen Entwicklung hin zum Zweitgerät entgegenwirken. BYOD birgt eine Reihe ernst zu nehmender Sicherheitsrisiken, und das nicht nur bei der Auswahl der Apps. Ein den speziellen Bedürfnissen des Unternehmens angepasstes MDM-System ist daher äußerst empfehlenswert. Doch welche Maßnahmen zum Schutz vor schädlichen Apps und anderen Bedrohungen sind nötig und auch machbar?

BYOD-Risiken

Die meisten Apps benötigen Zugriff auf verschiedene Sensoren und Daten, um ihren Zweck zu erfüllen. Fordert eine App aber mehr Rechte, als sie für ihre Funktion tatsächlich benötigt, sollte man sie bedenkenlos aussortieren. Denn warum muss etwa eine Taschenlampen-App auf die GPS-Daten des Nutzers zugreifen, um das Smartphone zur Lichtquelle zu machen? Möchte man jedoch beispielsweise eine Taxi-App wie Uber benutzen, dann benötigt sie sowohl die GPS-Daten wie auch einen Zugang zum Internet, denn irgendwie muss der Taxifahrer ja wissen, wo er hinfahren soll. Allerdings erfährt man mittels dieser Daten aber auch viel über einen Anwender, wie Uber unlängst mit dem Offenlegen von One-Night-Stands seiner Nutzer bewiesen hat. Für den Fall, dass die Daten legitim verwendet werden, aber dennoch ein Missbrauchspotenzial nicht auszuschließen ist, muss man als Unternehmen entweder dem Anbieter ein hohes Maß an Vertrauen entgegenbringen oder das Risiko vertraglich – falls möglich auch technisch – absichern.

Da oft nur schwer nachvollziehbar ist, wie die Kommunikation zwischen verschiedenen Apps untereinander sich auf die verfügbaren Zugriffsrechte auswirkt, wird das Einschätzen der verlangten Aktionen zusätzlich erschwert. Verlangt eine App beispielsweise zwar selbst keinen Internet-Zugriff, kann aber eine andere App auffordern, eine bestimmte Webseite zu besuchen, so genügt dies bereits, um einen unkontrollierten Datenabfluss zu initiieren. Dieses Phänomen, das eine eigentlich gutartige App zweckentfremdet, um (verborgene) Zugriffe zu gewähren, wird in der Literatur oft als Confused-Deputy-Angriff bezeichnet.

Eine andere Unwägbarkeit liegt beim Nutzer selbst: seine Gewohnheiten. Apps wie WhatsApp oder der Facebook-Messenger sind in Bezug auf den Datenschutz zumindest bedenklich. Als Unternehmen darf man ihnen keinen Zugriff auf sensible Daten gewähren. Das heißt, privates und geschäftliches Adressbuch müssen klar voneinander getrennt werden. Der Nutzer darf generell mit seinen privaten Apps auch nur mit den eigenen Daten interagieren. Eine rein organisatorische Maßnahme, die ihm verbietet, bestimmte Apps privat zu nutzen, ist hier vollkommen fehl am Platz. Eine Separierung dient nicht zuletzt auch dazu, arbeitsrechtliche Probleme zu vermeiden. Schließlich muss man die Unternehmensdaten genau überwachen, um nicht den Über-

Quelle: Backes SRT

Risiken \ Maßnahmen	Fernadministration					mobile Sicherheit							BYOD			
	Fernlöschung	Ortung verlorener Geräte	Updates aus der Ferne	Backups	Policies	sichere Container	Einschränken von Zugriffsrechten	Kontrolle Inter-App Kommunikation	Verschlüsselung persistenter Daten	Analyse von Apps	Netzwerkkommunikation via VPN	Monitoring von Datenfluss und Gerätezustand	keine OS-Modifikation	keine Root-Rechte	hohe Marktabdeckung	einfaches Rollout
Zugriffsrechte																
Auswahl Business Apps																
Confused Deputies																
(blinder) Datenabfluss																
Kommunikation durch ungesicherte Netze																
physikalischer Zugriff von Unbefugten																
ungewisse Update-Zyklen																
Verlust von Geräten																
Gerätevielfalt																
Einschränkung privater Nutzung																
Nutzerakzeptanz																

Kriterien zur Auswahl eines sicheren MDM

blick zu verlieren. Der Blick auf private Mitarbeiterdaten ist hingegen absolut tabu.

Ein weiteres Problemfeld, das direkt mit BYOD zusammenhängt, ist die Handhabung einer großen Vielzahl an einzelnen Endgeräten. Zudem verlassen Mobilgeräte – im Unterschied zu anderen firmeneigenen IT-Systemen – häufig die Räumlichkeiten des Unternehmens. Zum einen sind sie somit nicht jederzeit für Administratoren verfügbar, beispielsweise für Updates. Zum anderen kann nicht sichergestellt werden, dass nur autorisiertes Personal physikalischen Zugriff auf die Geräte bekommt. Nicht zuletzt kommt es auch immer wieder zum Verlust bzw. Diebstahl von Geräten. Es muss also dafür gesorgt werden, dass Unbefugte, die unbegrenzt lange physikalischen Zugriff auf das Gerät haben, dennoch keine sensiblen Daten extrahieren können. Es ist zwar denkbar, durch Ortungsfunktionen das Auffinden des Gerätes im Verlustfall zu erleichtern. Dabei muss man aber darauf achten, dass der Betriebsrat einbezogen wird und die Nutzung der Ortung technisch regulierbar ist.

Auswahl sicherer Apps

Beurteilt man Apps nur nach ihren angeforderten Zugriffsrechten, wären einige als klar gefährlich, ein paar als angemessen, die weitaus größte Zahl aber als ungewiss einzustufen. Das liegt daran, dass für die Beurteilung der Rechte nicht das potenzielle Risiko von Interesse ist, sondern die tatsächliche Verwendung. Dafür braucht man mehr Informationen, als das Manifest oder die Beschreibung der App bietet. Man benötigt eine tief gehende Analyse, die aufzeigt, was die App mit den Daten macht, auf die sie Zugriff bekommt.

Bei Softwareanalysen unterscheidet man üblicherweise zwischen statischen und dynamischen. Statische Analysen führen den Code nicht aus, sondern inspizieren ihn, und geben Garantien, die für jede Ausführung des Codes gelten. Die Ergebnisse statischer Analysen werden dadurch eingeschränkt, dass Informationen versteckt werden können, beispielsweise durch das Nachladen von Code aus dem Internet. Dynamische Analysen führen hingegen den Code meist in einer kontrollierten Umgebung aus und sehen sich an, was bei genau dieser Ausführung gerade passiert. Sie haben allerdings den Nachteil, dass ihre Aussagekraft auf eine Ausführung des Codes beschränkt ist und dieser Vorgang nicht ohne Weiteres jedes Verhalten offenlegt. Ideal wäre eine statische Analyse, die für die meisten Apps aussagekräftige Ergebnisse liefert und bei den restlichen auf die Limitierung der Analyse hinweist. Wie vertrauenswürdig bewertet man eine App, auf der mit Geschäftsdaten gearbeitet werden soll, die Code aus dem Internet nachladen muss?

Um die Verwendung von Daten zu bestimmen, ist eine sogenannte Informationsflussanalyse eine geeignete statische Analyse. Sie findet heraus, ob beispielsweise ein Zugriff aufs Internet von einem Wert im Adressbuch abhängig ist, und kann somit bestimmen, ob Informationen abfließen. Es gibt hier eine Vielzahl von Analyse-Frameworks, die alle ihre unterschiedlichen Vor- und Nachteile haben. Einen Nachteil haben alle präzisen Methoden: Sie sind sehr rechenintensiv und ihre Ergebnisse werden meistens nur für Experten verständlich aufbereitet. Auch können legitime, aber unerwartete Flüsse auftauchen, die dann weiter analysiert werden müssen. So kann beispielsweise eine Synchronisationsfunktion im Adressbuch für einen Informationsfluss ins Internet führen. Geht dieser Prozess jedoch ausschließlich über den konfigurierten Server und somit verschlüsselt vonstatten, ist er zulässig und für die gewünschte Funktionalität notwendig. Kurz: Wie bei Schadsoftware ist es auch bei allen eingesetzten Apps gut zu wissen, was sie tun. In den meisten Fällen genügt es aber, wenn man sich vor eventuellen unerwünschten Funktionen schützen kann.

Schutz vor unsicheren Apps

Bei unsicheren Apps gibt es grundsätzlich zwei Szenarien: Die App greift das Betriebssystem an, oder sie greift die Daten an. Ein Angriff aufs Betriebssystem lässt sich oft nur beobachten und nicht verhindern, sodass sich in diesem Szenario die MDM-Lösung sperren und weitere Interaktion verweigern kann. Dennoch ist diese Situation besonders gefährlich, da man sich ab diesem Zeitpunkt nicht mehr auf die Sicherheitsmechanismen des Betriebssystems verlassen solte. Im anderen Fall, wenn die App also direkt die Daten abzugreifen versucht, kann eine MDM-Lösung intervenieren und Zugriffe unterbinden. Eine App kann schließlich nur die Daten stehlen, zu denen sie Zugang hat. Der Zugriff auf Sensoren lässt sich hingegen oft nur schwer abschätzten. Beispielsweise kann über Bewegungssensoren von Smartphones ein Password abgegriffen werden, wenn es neben der Tastatur liegt.

Im Vergleich zu klassischen Desktop-Betriebssystemen bieten mobile Betriebssysteme bereits dadurch Schutz, dass jede App ihre Daten kapseln kann, andere Apps also nicht einfach auf die Daten zugreifen können. Das MDM-System muss die Zugriffsrechte insgesamt beschneiden, aber auch Apps voneinander trennen können, damit diese nicht mehr beliebig untereinander kommunizieren, um etwa einen Confused-Deputy-Angriff auszulösen. In diesem Fall spricht man von sicheren Container-Lösungen. In solchen Containern sollte das MDM-System dann klar definieren, welche App auf welche Daten und Sensoren zugreifen darf. Hier ist es hilfreich, wenn das MDM es erlaubt, verständliche Policies festzulegen und zu kombinieren. Das vereinfacht es auch, die Compliance nachzuweisen. So könnte man für verschiedene gesetzliche Regelungen Policies definieren. Das MDM erzwingt dann, dass ein Zugriff nur gewährt wird, wenn alle Policies erfüllt sind. Ein sicherer Container sollte auch garantieren, dass die Daten nur verschlüsselt abgelegt werden, damit im Fall eines Betriebssystem-Exploits oder Gerätediebstahls der Schlüssel gelöscht werden kann, um zeitnah den Zugriff auch auf größere Datenmengen zu sperren.

Ein weiterer Schutz, der erfolgreich bei Desktop- und Serversystemen genutzt wird, sind Netzwerk-Gateways wie Firewalls oder Virenscanner, die den Datenverkehr untersuchen und gegebenenfalls blockieren, bevor er das Endgerät erreicht. Diese Schutzmaßnahme ist auf Mobilgeräten aus zwei Gründen schwerer umzusetzen. Zum einen muss das Gerät ja nicht mit dem Firmennetz verbunden sein, es kann beispielsweise gerade in einem Starbucks das offene WLAN nutzen. Organisatorische Maßnahmen sind hier zwar möglich, etwa eine Vorschrift: „Mobilgeräte dürfen nicht mit offenen WLANs genutzt werden“. Jedoch muss man der Realität ins Auge blicken und davon ausgehen, dass es trotzdem passieren wird. Daher ist eine technische Lösung des Problems, beispielsweise ein VPN (Virtual Private Network), das den Datenverkehr immer verschlüsselt durch das interne Netz tunnelt, zu bevorzugen. So können die Mobilgeräte zudem dieselben Netzwerk-Gateways verwenden, die auch die Desktoprechner im Unternehmen absichern.

Zum anderen möchte man keine privaten Apps auf den Geräten über das Unternehmensnetz kommunizieren lassen, genießen sie doch in der Kommunikation mit Firmenservern oft mehr Vertrauen und somit Zugriffsrechte. Folglich sollte es ein zuverlässiges MDM ermöglichen, gezielt die Businesscontainer per VPN mit dem Firmennetz zu verbinden. Insbesondere umgeht man bei solchen Lösungen arbeitsrechtliche Problemstellungen, da man die Firmenpakete per Deep Packet Inspection (DPI) analysieren kann, ohne zu riskieren, mit den privaten Daten der Mitarbeiter in Berührung zu kommen.

Fazit

Große Trends wie das Internet of Things (IoT) und Industrie 4.0 wirken sich auch auf BYOD aus. So steigt etwa Anzahl und Art der verbauten Sensoren in den Geräten kontinuierlich an. Die sogenannten Wearables bringen Sensoren auch an Orte, die es vereinfachen, Daten abzugreifen. Die Bewegungen des Handgelenks, gemessen von einer Smartwatch, geben beispielsweise deutlich präzisere Auskunft über Tastatureingaben als ein neben der Tastatur liegendes Smartphone. Sensoren, die den Puls oder die Körpertemperatur messen, bieten bislang ungeahntes Potenzial für neuartige Seitenkanalangriffe.

Auch das Wachstum der Hausautomation (Smart Homes) sorgt dafür, dass neuartige Angriffsmethoden und Einfallstore für Schadsoftware beachtet werden müssen. Zukünftig könnte z.B. ein Botnetz aus Kontrolleinheiten der Hausautomation den Strompreis manipulieren oder ein infizierter Toaster im Privathaushalt über ein privat genutztes Business-Smartphone angreifen und zu einer realen Bedrohung für die Unternehmensinfrastruktur werden. Es ist also höchste Zeit, sich um ein sicheres MDM-System zu bemühen, das alle verwendeten Mobilgeräte sowohl voll einsatzfähig als auch sicher macht.

Fabian Bendun,
Geschäftsführer Backes SRT