TRUST IN
GERMAN
SICHERHEIT

G DATA
Whitepaper

Mobile Device Management (MDM)

G DATA Anwendungsentwicklung

WhitePaper_MDM_2015_04_21

Inhalt

1. Einführung

Bisher haben Administratoren von Unternehmensnetzwerken und Systemadministratoren immer homogene Gruppen von Client-Geräten administriert. Bei der Planung und Bereitstellung von Netzwerk-Clients befasste man sich fast ausschließlich mit Desktop-Computern. Diese voraussehbaren Gegebenheiten vereinfachten die Bereitstellung der Netzinfrastruktur, der Client-Hardware und der Anwendungen. So war die Einheitlichkeit bei allen Netzwerkgeräten gewährleistet. Seit jedoch Smartphones und Tablets den Bereich Consumer Electronics im Sturm erobert haben, ist die Technologielandschaft erheblich komplizierter geworden. Durch Trends wie die Consumerization der IT und „Bring Your Own Device“ (BYOD) hat eine Vielzahl unterschiedlicher Geräte in Unternehmen Einzug gehalten. Administratoren sehen sich nun mit der Aufgabe konfrontiert, einen breitgefächerten Zugang zu den Ressourcen anzubieten und gleichzeitig die Sicherheit zu gewährleisten. Dieses Whitepaper soll Trends in der Nutzung von Smartphones und Tablets in Unternehmensnetzwerken darlegen (Kapitel 2) und praktische Management-Strategien für Administratoren aufzeigen, die sich mit der wachsenden Nutzung von Mobilgeräten beschäftigen müssen (Kapitel 3). Wenn Sie mehr darüber erfahren möchten, wie G DATA Mobile Device Management implementiert, können Sie auf unserer Website das Technische Dokument Nr. 0273 von G DATA herunterladen.

2. Mobile Endgeräte im Unternehmen

Neue Technologien halten in Unternehmen wesentlich langsamer Einzug als bei privaten Anwendern. Selbst wenn ein Produkt auf einfache Weise in Workflows integriert werden kann, muss es auf Kompatibilitätsprobleme mit der Unternehmensinfrastruktur getestet werden – ein Prozess, der sehr kostenintensiv und zeitaufwändig sein kann. Seit Apple die Kategorie der Mobilgeräte mit den Produkteinführungen von iPhone und iPad populär gemacht hat, zeigen sich Hunderte Millionen Privat- und Geschäftskunden gleichermaßen begeistert von der Kombination aus fortschrittlicher Technologie und Benutzerfreundlichkeit der Geräte. Viele Unternehmen tun sich jedoch noch immer schwer damit, diese Geräte auf angemessene Weise in die Unternehmensumgebung zu integrieren. Diese Verzögerungen bei der Einführung führen häufig zu Spannungen, da sich die Erwartungen der Endanwender nicht mit der derzeit gebotenen Funktionalität der Unternehmenslösungen decken. Zwei wichtige Trends in der IT-Landschaft der Unternehmen veranschaulichen dieses Dilemma: Consumerization der IT und „Bring Your Own Device“ (BYOD).

Die Consumerization der IT, also der Einfluss privat genutzter Consumer-Geräte auf IT-Lösungen von Unternehmen, ist immens gewachsen. Die Endanwender sind mittlerweile daran gewöhnt, ständig mobilen Zugang zum Internet zu haben und cloud-basierte Messaging- und E-Mail-Lösungen sowie zahlreiche Apps zu nutzen, mit denen die mobile Gerätenutzung den eigenen Anforderungen entsprechend gestaltet werden kann. Obwohl kein Administrator die sehr praktische Seite dieser Dienste bestreiten würde, stehen einige der dadurch erzielten Vorteile im Widerspruch zu den IT-Strukturen im Unternehmen. Die Geschwindigkeit, mit der neue Apps für mobile Plattformen auf den Markt kommen, übersteigt bei weitem die Möglichkeiten der Administratoren, einzelne Apps auf Kompatibilität und Sicherheit zu testen. Beim Einsatz von Cloud-Diensten werden Daten oft auf Servern gespeichert, die von dritter Seite administriert werden. Obgleich die Endanwender mittlerweile solche Dienste von ihren

Geräten erwarten, sind nicht alle Unternehmen technisch gerüstet, diese in einer mit den IT-Richtlinien konformen Weise bereitzustellen.

Auch wenn mobile Geräte und Dienste nicht aktiv in einer Unternehmensumgebung implementiert werden, gibt es für Administratoren Mittel und Wege, mit denen diese Geräte und Dienste im Unternehmen genutzt werden können. Dieser Trend ist unter der Bezeichnung „Bring Your Own Device" (BYOD) bekannt: Die Endanwender bringen ihre eigenen Geräte mit zur Arbeit und erwarten, dass sie die Unternehmensinfrastruktur wie etwa WLAN-Zugang und Netzwerkfreigaben nutzen können. Ebenso gestatten viele E-Mail-Serverkonfigurationen den Fernzugriff über mobile Geräte, unabhängig davon, ob das Gerät verwaltet wird oder nicht. BYOD führt oft zu reflexartigen Reaktionen: Um sicherzustellen, dass keine sensiblen Daten nach außen dringen und dass keine schädliche Software in das Netzwerk gelangen kann, werden mobile Geräte von der Unternehmensinfrastruktur vollständig blockiert, oder die Funktionalität der Geräte wird durch restriktive Richtlinien stark eingeschränkt.

So seltsam dies auch klingen mag: Es ist wichtig zu erkennen, dass bei der Nutzung von Mobilgeräten in Unternehmen kein Schwarzweiß-Denken angebracht ist. Die Konzepte BYOD und die Consumerization der IT erwecken den Eindruck, dass sie eine perfekt organisierte Umgebung destabilisieren. Doch es gibt mehrere Gründe, die für die Bereitstellung unternehmenseigener Mobilgeräte oder die Nutzung privater Mobilgeräte sprechen. Die Nutzung einer MDM-Lösung (Mobile Device Management) kann dazu beitragen, die Vorteile von Mobilgeräten zu nutzen und gleichzeitig deren Auswirkungen auf die übrige Unternehmensinfrastruktur zu begrenzen.

2.1. Vorteile

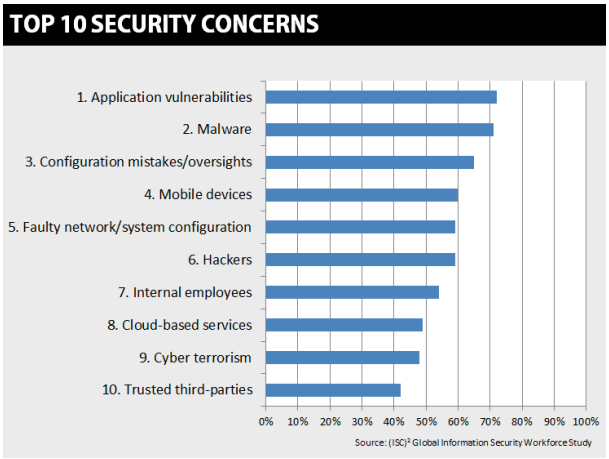
Die Integration von Smartphones und Tablets in die Arbeitsabläufe von Unternehmen bringt deutliche Vorteile, und zwar unabhängig davon, ob diese zentral bereitgestellt oder von den Mitarbeitern mitgebracht werden. Bietet man Mitarbeitern und Dienstleistern, die sich nicht am Unternehmensstandort befinden, mobilen Zugriff auf Unternehmensressourcen, kann dies deren Produktivität deutlich steigern. Eine Kombination aus Zugangskontrollen und Gerätemanagement ermöglicht eine sichere, effiziente Nutzung der Geräte für den Remote-Zugriff auf Unternehmensressourcen. Auch auf Geschäftsreisen ist die Kommunikation nicht länger eingeschränkt: Die Mitarbeiter können aus der Ferne ihre E-Mails, Kalender und Benachrichtigungen abrufen.

In vielen Fällen sind Geräte und Anwendungen im Unternehmen nicht gerade für ihre Benutzerfreundlichkeit bekannt. Die Consumer-Technologie wird hingegen oft so entwickelt, dass sie Endanwendern eine gewisse Vertrautheit bietet. Daher sind nur kurze Einarbeitungszeiten für die Mitarbeiter erforderlich, die sich schnell an die vom Unternehmen bereitgestellten Geräte gewöhnen können.

Außerdem sparen Unternehmen mit einer BYOD-Umgebung Geld, da sie keine umfangreichen Investitionen für die Bereitstellung der Geräte tätigen müssen. Statt neue Smartphones und Tablets kaufen und bereitstellen zu müssen, können die Geräte der Mitarbeiter mit MDM-Software ausgestattet und direkt für Unternehmenszwecke eingesetzt werden. Zudem sind nicht die Unternehmen für Ersatzgeräte verantwortlich, falls ein Mitarbeiter sein Smartphone oder Tablet verliert oder beschädigt.

2.2. Risiken

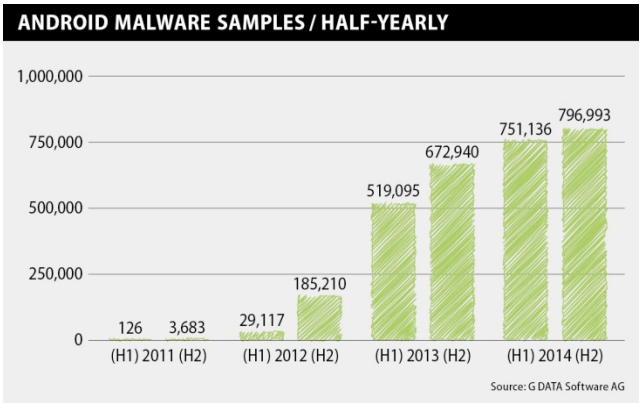
Die Nutzung mobiler Geräte kann sich in vielerlei Hinsicht positiv auf die Produktivität im Unternehmen auswirken, birgt jedoch auch einige Gefahren. Mobile Geräte wurden in der Global Information Security Workforce Study 2015 der (ISC) 2 Foundation[1] als viertwichtigstes Sicherheitsproblem genannt. Wie PCs sind auch mobile Geräte anfällig für Malware. Insbesondere Android und iOS sind großen Risiken ausgesetzt: Mit einem gemeinsamen Marktanteil von 96,3 Prozent[2] sind diese Plattformen das bevorzugte Angriffsziel Krimineller. Im Jahr 2014 untersuchten die Sicherheitsexperten von G DATA mehr als 1,5 Millionen neue Android-Malware-Samples. Das entspricht einer Steigerung um 30 Prozent im Vergleich zu 2013[3]. Android-Malware wird für eine Vielzahl krimineller Zwecke eingesetzt, z. B.:



- Ausspähen von Daten, zum Beispiel von E-Mails, Anmeldedaten und vertraulichen Dokumenten
- Verursachung hoher Kosten durch den Versand von SMS-Nachrichten an (ausländische) Telefonnummern von Premiumdiensten
- Ausspähen mobiler Banking-Apps
- Sperren von Geräten, um Lösegeld zu erpressen (Ransomware)

Malware ist jedoch nicht die einzige Bedrohung für mobile Geräte. Beim Surfen im Internet können Phishing-Webseiten versuchen, den Benutzer dazu verleiten, persönliche Daten in ein scheinbar harmloses Formular einzugeben. Auch wenn das Gerät selbst sicher ist, bedeutet dies noch lange nicht, dass es im geschäftlichen Umfeld auf sichere Weise genutzt werden kann. Wenn Mitarbeiter mit mobilen Geräten auf Unternehmensdokumente zugreifen, muss sichergestellt sein, dass keine vertraulichen Informationen nach außen dringen können, sei es versehentlich (z. B. durch Hochladen der betreffenden Dateien auf einen Filesharing-Dienst) oder absichtlich (Insider-Bedrohung).

Mobilgeräte können nicht nur Sicherheitsrisiken darstellen, sondern auch zur Senkung der Produktivität führen. Die Nutzung von Apps sollte auch dahingehend eingeschränkt werden, dass die Mitarbeiter nicht übermäßig viel Zeit mit Spielen oder anderen Freizeitbeschäftigungen verbringen. Mithilfe des Kontakte-Managements kann die Nutzung der Telefonfunktionen auf die absolut notwendigen Ansprechpartner beschränkt werden; das spart Zeit und Kosten.



Die Vorteile der Nutzung von Mobilgeräten im Unternehmen überwiegen die Risiken. Dennoch müssen letztere entschärft werden. Integrierte MDM-Richtlinien (Mobile Device Management) können dazu beitragen, Sicherheitsrisiken und Produktivitätsproblemen Herr zu werden und die sichere, effiziente Nutzung von Smartphones und Tablets zu gewährleisten.

[1] Quelle: (ISC)2 Foundation, https://www.isc2cares.org/IndustryResearch/GISWS/
[2] Kalenderjahr 2014. Quelle: IDC, https://www.idc.com/getdoc.jsp?containerId=prUS25450615
[3] Quelle: G DATA Mobile Malware Report H2/2014

3. Mobile Device Management (MDM)

Als Administrator ist es praktisch unmöglich, die Phänomene Consumerization und BYOD zu ignorieren. Die Endanwender werden im Unternehmen auch künftig auf Smartphones und Tablets pochen, an deren Benutzerfreundlichkeit sie sich gewöhnt haben. Wenn solche Geräte nicht aktiv bereitgestellt werden, werden die Mitarbeiter eigene Geräte mitbringen. Angesichts der potenziellen Vorteile mobiler Geräte für die Produktivität sollte es das Ziel des Mobile Device Management sein, die Produktivität zu maximieren und gleichzeitig die Sicherheit zu gewährleisten und Kosten zu senken.

3.1. Implementierung und Administration

Bevor Smartphones oder Tablets mit einer MDM-Lösung verwaltet werden können, müssen sie implementiert werden. Die Implementierung erfordert eine einmalige anfängliche Anmeldung des Gerätes am Server. Später meldet sich das Gerät dann in regelmäßigen Abständen beim Server und kann aus der Ferne verwaltet werden. Die Kommunikation zwischen Server und Gerät erfolgt in Form von Internet-Datenverkehr (wenn eine direkte Verbindung zum Server aufgebaut werden kann), Push-Nachrichten (welche oft auf anbieterspezifischen Cloud-Messaging-Lösungen basieren) oder SMS-Nachrichten (wenn keine mobile Internetverbindung verfügbar ist). Eine dauerhafte Verbindung zwischen Gerät und Server ist nicht erforderlich: Das Gerät kann die Serverrichtlinien auch dann umsetzen, wenn kein Kontakt zum Server besteht. Auf diese Weise sind die Geräte jederzeit geschützt, auch außerhalb der Unternehmensumgebung.

Die Implementierung sollte so weit wie möglich optimiert werden. Neue vom Unternehmen verwaltete Geräte sollten immer mit MDM-Funktionen ausgestattet werden, bevor sie den Mitarbeitern ausgehändigt werden. BYOD-Geräten sollte der Zugang zum Unternehmensnetzwerk und dessen Ressourcen verweigert werden, bevor sie mit MDM-Funktionen ausgestattet wurden. Optional kann für Geräte, die den Anforderungen nicht entsprechen, oder für Geräte von Besuchern ein Gastnetzwerk genutzt werden.

Um eine erhöhte Arbeitsbelastung zu vermeiden, sollten die Administratoren eine MDM-Lösung wählen, die sich in die vorhandenen Administrationsstrukturen integrieren lässt. Die Nutzung mehrerer Backends ist zu vermeiden. Im Idealfall können mobile Geräte mit derselben Benutzeroberfläche und mit denselben Berichtfunktionen administriert werden, die für andere Gerätetypen im Netzwerk verfügbar sind. Dies vereinfacht einen integrierten Workflow und eine konsistente Konfiguration.

Bei BYOD-Geräten ist der rechtliche Aspekt der Geräteverwaltung zu berücksichtigen. Da diese Geräte nicht Eigentum des Unternehmens sind, sind die Administratoren nicht automatisch zu deren Verwaltung berechtigt. Problematisch können sich insbesondere Berechtigungen wie etwa das Fernlöschen erweisen. Je nach Gesetzeslage müssen die Unternehmen vor der Registrierung der Geräte für das Mobile Device Management ggf. die Erlaubnis der Endanwender einholen. Es wird empfohlen, in einem Endbenutzer-Lizenzvertrag (EULA) die Maßnahmen zu erläutern, welche das Unternehmen auf dem Gerät durchführen können muss. Der Endanwender kann den Vertrag dann entweder annehmen oder ablehnen. Der Zugriff auf die Unternehmensressourcen wird jedoch nicht gewährt, wenn der EULA-Vertrag abgelehnt wird. Auch für Nicht-BYOD-Geräte kann sich ein EULA-Vertrag als nützlich erweisen.

3.2. Diebstahlschutz

Mobile Geräte erhöhen das Risiko für die Geräteinfrastruktur und für datenbasierte Workflows. Wenn Mitarbeiter vertrauliche Dateien unterwegs dabei haben oder wenn mobile Geräte verloren gehen oder gestohlen werden, kann es sehr leicht geschehen, dass vertrauliche Informationen versehentlich nach außen gelangen. Um sicherzustellen, dass auf geschäftliche E-Mails, Dokumente und andere Kommunikationsinhalte nicht zugegriffen werden kann, wenn ein Gerät verloren geht oder gestohlen wird, kann eine Reihe von Maßnahmen getroffen werden. Zunächst sollte man versuchen, das Gerät wieder zu finden. Die Ortung des Geräts mithilfe der GPS-Technologie oder das Auslösen eines Alarmtons kann dabei helfen. Wenn die Ortung des Geräts nicht möglich ist oder keine brauchbaren Ergebnisse liefert, kann das Gerät durch Sperren unbrauchbar gemacht werden. Als letzte Maßnahme können die Geräte auf die Werkseinstellungen zurückgesetzt werden, wobei alle Daten von dem Gerät gelöscht werden.

3.3. Apps

Mobile Geräte sind auch deshalb so attraktiv, weil die werksseitigen Funktionen durch die Installation von Apps erweitert werden können. Auch im geschäftlichen Umfeld kann sich diese Tatsache als sehr nützlich erweisen: Produktivitäts-Tools oder Konfigurations-Apps können die Einsatzmöglichkeiten für mobile Geräte deutlich erweitern. Gleichzeitig sollten geschäftlich genutzte Geräte eine kontrollierte Umgebung bereitstellen, um sicherzustellen, dass Apps nicht zu Kompatibilitätsproblemen führen, keine vertraulichen Informationen preisgeben oder Malware verbreiten. Das App-Management ist eine leistungsfähige Methode, um die Funktionalität mobiler Geräte zu steuern, wobei ein ausgewogenes Verhältnis von Sicherheit und Benutzerfreundlichkeit angestrebt werden sollte.

Die Trennung der guten von den schlechten Apps kann eine schwierige Aufgabe darstellen. Einige Apps, wie etwa Spiele, sind für Unternehmensumgebungen zweifellos ungeeignet. Andere können möglicherweise nützlich sein, bergen aber u. U. Datenschutzrisiken, wie zum Beispiel Online-Filehosting-Dienste. Auch Apps, die risikolos erscheinen, können sich später als manipuliert erweisen, sei es, weil die App selbst Sicherheitslücken enthält, weil ihre Backend-Dienste manipuliert sind oder weil sie Informationen auf unsichere Weise überträgt. Auch die Produktivität ist berücksichtigen: Beispielsweise kann man Mitarbeitern, die ein Smartphone allein zum Telefonieren oder für Terminvereinbarungen benötigen, nur Zugang zu den Telefon- und Kalenderfunktionen gewähren. Mitarbeiter, die unterwegs auch Dokumente bearbeiten, erhalten Zugriff auf Browser, Office-Apps und andere erforderliche Komponenten.

3.4. Echtzeit-Schutz und On-Demand-Schutz

Wie Desktop- und Laptop-Computer sind auch Mobilgeräte anfällig für Online-Angriffe. Insbesondere gerootete Android-Geräte verfügen nicht über ausreichende Schutzmechanismen gegen Malware-Apps aus unbekannten Quellen. Aber auch Malware-Apps, die sich in offizielle App-Stores einschleichen, können schwerwiegende Folgen verursachen. In ähnlicher Weise könnten auch Websites versuchen, Malware zu verbreiten, Schwachstellen im Betriebssystem auszunutzen oder den Endanwender auf andere Weise zu täuschen. Wie bei Desktop-Computern können Phishing-Websites versuchen, Benutzern Kennwörter oder andere vertrauliche Daten zu entlocken. Um diesen Bedrohungen zu begegnen, sollten Schutzmaßnahmen für alle verwalteten Mobilgeräte konfiguriert werden.

Der Echtzeitschutz schützt Geräte jederzeit ganz ohne Benutzereingriff. Dazu zählen Technologien wie Phishing-Schutz und automatische Virenprüfungen. Der On-Demand-Schutz wird hingegen nur dann aktiviert, wenn ein Endanwender oder Administrator diesen auslöst. Beispielsweise kann eine Virenprüfung manuell gestartet werden, um sicherzustellen, dass auf dem Gerät nicht bereits Malware-Apps installiert wurden.

Lösungen für den Echtzeit-Schutz und On-Demand-Schutz unterscheiden sich je nach Client-Plattform deutlich voneinander. Android-Geräte sind besonders anfällig für Malware-Apps, während iOS-Geräte anfälliger für Datenverlust oder Phishing-Angriffe sind. MDM-Lösungen sollten Maßnahmen bieten, die speziell auf die jeweilige mobile Plattform zugeschnitten sind: Ein Universalmodul wird den vielfältigen Bedrohungen, denen die Geräte ausgesetzt sind, nicht gerecht.

3.5. Kontakte-Management und -Filterung

Bei Geräten, die im geschäftlichen Umfeld genutzt werden, kann die Kontrolle der Kommunikationsströme von entscheidender Bedeutung sein. Das Blockieren von Apps kann dann sinnvoll sein, wenn die Kommunikation gänzlich verhindert werden soll. In anderen Fällen müssen jedoch feinmaschigere Filter eingesetzt werden. Anstatt die Telefonanwendung vollständig zu blockieren, wenn ein Gerät nur für die geschäftliche Kommunikation genutzt werden soll, können ankommende und abgehende Anrufe gefiltert werden, wenn sie nicht den Kriterien des Unternehmens entsprechen. So könnte beispielsweise ein Unternehmen, das seinen Mitarbeitern Mobiltelefone zur Verfügung stellt, damit diese unterwegs mit der Zentrale telefonieren können, sämtliche Anrufe blockieren, mit Ausnahme derjenigen Nummern von Gesprächspartnern, die vorab vom Unternehmen genehmigt wurden.

Von zentraler Bedeutung für das Kontakte-Management ist ein verwaltetes Telefonbuch. Die auf dem Gerät gespeicherten Kontakte können mit dem zentralen Server synchronisiert werden, und die Administratoren können die aktuellsten Telefonnummern per Push-Technologie auf die Geräte übertragen. Wie das App-Management kann auch das Kontakte-Management für einzelne Geräte verwendet werden. Idealerweise wird das Kontakte-Management jedoch mit einem gruppenbasierten Management kombiniert. Einzelne Rufnummern können für Gerätegruppen in einem Vorgang zugelassen oder gesperrt werden. Es kann aber auch das gesamte Telefonverzeichnis des Unternehmens auf alle Geräte übertragen werden.

Wenn Sie mehr darüber erfahren möchten, wie G DATA Mobile Device Management implementiert, können Sie auf unserer Website das Technische Dokument Nr. 0273 von G DATA herunterladen.