BEST-PRACTICE-LEITFADEN: VERWALTUNG MOBILER GERÄTE UND MOBILE SECURITY

INHALT

GEFÄHRLICH BEWEGLICH: VERWALTUNG MOBILER GERÄTE UND MOBILE SECURITY

1. BETRIEB RUND UM DIE UHR

Auch von unterwegs Zugriff auf wichtige Geschäftsanwendungen zu haben, macht Mitarbeiter produktiver und verleiht Ihrem Unternehmen mehr Agilität und Flexibilität.

Aber Mobilität hat ihren Preis: Gerade die Funktionen, durch die intelligente Endgeräte für Mitarbeiter so wertvoll sind, machen sie auch attraktiv für Hacker, Datendiebe, Verbreiter von Malware und andere Kriminelle. In den vergangenen 12 Monaten waren weltweit 51 % aller Unternehmen mit Datenlecks aufgrund unzureichend gesicherter Mobilgeräte konfrontiert.[1]

Es geht aber nicht nur um Malware: Der Trend zur Nutzung mitarbeitereigener Geräte in Unternehmen aller Größenordnungen (Bring Your Own Device, BYOD) trägt zu einer immer komplexeren Vielfalt an verschiedenen Geräten im Unternehmen bei. Da die Grenzen zwischen beruflicher und privater Nutzung zunehmend verschwimmen, wird die Verwaltung und Steuerung der IT-Unternehmensumgebung immer komplexer.

Wie können Sie BYOD-Initiativen fördern, ohne sich den Kopf über die damit einhergehenden Probleme zerbrechen zu müssen? Wie können Sie die Aktivitäten des Endbenutzers überwachen, wenn er gerade in einem Hotelzimmer in einer anderen Zeitzone Anwendungen herunterlädt? Was sind die Folgen, wenn ein Mitarbeiter sein Smartphone im Taxi liegen lässt? Können Sie all dies unkompliziert und von einer zentralen Stelle aus kontrollieren? Mobile Device Management (MDM, Verwaltung mobiler Geräte) liefert die Antwort auf die meisten dieser Fragen.

2. WAS BEDEUTET MOBILE DEVICE MANAGEMENT (MDM)?

Mit Mobile Device Management können IT-Mitarbeiter die Sicherheitsstrategie und die Sicherheitsrichtlinien, die für die ortsfeste Infrastruktur gelten, auch auf alle anderen Geräte anwenden, wo immer diese sich gerade befinden. Mithilfe von MDM-Software können IT-Manager wichtige Verwaltungs- und Kontrollaufgaben automatisieren, wie etwa die Gerätekonfiguration, Software-Updates und Sicherung/Wiederherstellung. Gleichzeitig kann für den Fall von Diebstahl, Verlust oder missbräuchlicher Verwendung durch den Endbenutzer die Sicherheit vertraulicher Geschäftsdaten gewährleistet werden.

3. DIE WAHL DER RICHTIGEN MDM-LÖSUNG

3.1 Unterstützung mehrerer Plattformen

Android, BlackBerry, iOS, Symbian, Windows Mobile: Wer Initiativen zur Nutzung mitarbeitereigener Geräte unterstützt, weiß genau, wie schwierig es sein kann, die Sicherheit und Wartung auf vielen verschiedenen Plattformen zu gewährleisten.

Eine MDM-Lösung mit Unterstützung für mehrere Plattformen ist nicht nur kostengünstig, sondern erspart Ihnen auch den Aufwand, mehrere unterschiedliche Systeme verwalten zu müssen. Außerdem gewinnen Sie an Flexibilität, da nicht nur Ihre aktuellen Geräte unterstützt werden, sondern auch die Marken und Produkte, für die Sie sich in Zukunft entscheiden.

1 Quellennachweis: Ponemon: The Cost of a Lost Laptop (2009)

4. EFFEKTIVE MDM-ANWENDUNG

4.1 Eindeutige Richtlinien

Schaffen Sie mobilgerätespezifische Richtlinien, durch die unter anderem Folgendes klar definiert wird:

- Wie gestaltet sich die Bereitstellung der Geräte?
- Auf welche Daten sollen mobile Mitarbeiter Zugriff haben?
- Wer kann über die Netzwerke des Unternehmens was tun?
- Welche Vorgehensweise ist im Falle von Verlust oder Diebstahl vorgesehen?

Richtlinien sollten auf flexible und detaillierte Weise kontrolliert und umgesetzt werden. Sie müssen also unterschiedliche Richtlinien auf unterschiedliche Benutzer und Gruppen anwenden können. Für zusätzlichen Schutz sollten sich diese detaillierten Kontrollmöglichkeiten auch auf Ebene des Geräts anwenden lassen, beispielsweise auf inoffiziell entsperrte (sog. „Jailbreak") oder anderweitig manipulierte Geräte, die auf diese Weise am Zugriff auf Unternehmensdaten gehindert werden oder per Fernzugriff gesperrt werden können.

4.2 Containerisierung

89 % der befragten Benutzer, die ein privates Endgerät auch beruflich nutzen, gaben an, dass sie damit auf wichtige Unternehmensdaten zugreifen. 41 % gaben zu, ihre privaten Geräte ohne Erlaubnis am Arbeitsplatz einzusetzen.[2]

Auch den gewissenhaftesten Nutzern kann es passieren, dass sie unabsichtlich Unternehmenssysteme und -inhalte gefährden, indem sie mit ihrem Gerät Privatanwendungen herunterladen oder private Inhalte abrufen.

Hier kommt die so genannte Containerisierung ins Spiel. Containerisierung bedeutet eine Trennung von persönlichen und Unternehmensdaten auf dem Gerät. Dies versetzt IT-Abteilungen in die Lage, Unternehmensdaten ohne Auswirkung auf die persönlichen Daten vor Risiken zu schützen, die durch private Nutzung entstehen. Durch Containerisierung können IT-Abteilungen ihre Sicherheitsund Datenschutzrichtlinien auf private oder unternehmenseigene Geräte anwenden. Diese Option ist besonders in BYOD-Szenarien nützlich.

4.3 Verschlüsselung

Zu den bewährten Praktiken für das MDM gehört auch eine Option zur Verschlüsselung vertraulicher Daten im Container, denn sie ist eine wirkungsvolle Ergänzung zum Diebstahlschutz: Wenn vertrauliche Daten obligatorisch verschlüsselt sind, birgt eine Verzögerung vor dem Löschen aller Daten auf dem Gerät ein viel geringeres Risiko.

Wenn sichergestellt ist, dass nur verschlüsselte Daten den Container für Unternehmensdaten auf einem Gerät verlassen können, können sich Unternehmen gegen Datenlecks schützen und Datenschutzvorschriften effektiver einhalten. Die MDM-Verschlüsselungstechnologie von Kaspersky Lab lässt sich automatisieren und wird so für den Endbenutzer völlig transparent, wodurch sichergestellt wird, dass vorhandene Sicherheitsrichtlinien eingehalten werden.

2 Quellennachweis: Juniper Networks, Trusted Mobility Index 2012.

4.4 Diebstahlschutz und Inhaltssicherung

Es ist kaum möglich, solch kleiner, höchst mobiler Geräte physisch habhaft zu werden. Sehr wohl möglich ist hingegen, die darauf gespeicherten Inhalte zu sperren und die Kontrolle darüber zu behalten, was geschieht, wenn sie abhandenkommen.

Die MDM-Lösung von Kaspersky Lab sieht Funktionen für den Schutz im Fall von Diebstahl und die Sicherheit der Inhalte vor. Diese Funktionen können per Fernzugriff ausgelöst werden, um den unbefugten Zugriff auf vertrauliche Daten zu verhindern. Zu den Funktionen gehören u. a.:

- SIM-Kontrolle: Sperrt ein abhanden gekommenes oder gestohlenes Smartphone, selbst wenn die SIM-Karte ausgetauscht wurde, und übermittelt die neue Telefonnummer an den rechtmäßigen Besitzer.
- Gerätestandort/-überwachung: Ermittelt den Gerätestandort mithilfe von GPS, GSM oder WiFi.
- Löschen aller/ausgewählter Daten per Fernzugriff: Lassen Sie entweder alle Daten auf einem Gerät oder nur vertrauliche Unternehmensdaten löschen.
- Per Fernzugriff sperren: Verhindert den unbefugten Zugriff auf ein Gerät, ohne gleich alle Daten löschen zu müssen.

4.5 Mobile Anti-Malware

Sie benötigen eine Strategie für den Umgang mit abhanden gekommenen oder gestohlenen Geräten, aber für Geräte besteht immer ein gewisses Risiko, selbst wenn sie sich in Händen ihrer rechtmäßigen Besitzer befinden. Viele Unternehmen scheuen keine Mühen, wenn es um die Umsetzung von Malware- und Spambekämpfungsmaßnahmen für die ortsfeste Infrastruktur geht, unternehmen gleichzeitig aber wenig dagegen, dass sich Viren oder sonstige Malware über mobile Geräte verbreiten.

Die mobilen Sicherheitstechnologien von Kaspersky Lab beinhalten eine Mischlösung aus herkömmlicher, signaturbasierter Erkennung und proaktiven, Cloud-unterstützten Technologien, durch die sich die Erkennungsrate verbessern und ein Echtzeitschutz vor Malware erzielen lässt. Bedarfsorientierte und planmäßige Überprüfungen gewährleisten einen optimalen Schutz – wobei automatische OTA-Updates (Over-the-Air) für jede MDM-Strategie von essenzieller Bedeutung sind.

4.6 Einfach statt kompliziert – Kontrolle von einer zentralen Konsole aus

Mit Kaspersky Lab können Sie die Sicherheitsfunktionen für mobile Geräte von derselben Konsole aus verwalten, von der auch die Netzwerk- und Endpoint-Sicherheit gemanagt wird. Hierdurch verringert sich die Komplexität, die durch getrennte Lösungen entsteht, und es erübrigt sich der Einsatz mehrerer, nicht selten inkompatibler Konsolen. Technische Ausuferung macht eine ohnehin schon schwierige Aufgabe unnötig komplex.

Durch die Vereinfachung und Automatisierung der sicheren Konfiguration einer Vielzahl von Geräten können Sie nicht nur den IT-Aufwand reduzieren, sondern auch bessere Praktiken für mobile Sicherheit fördern. Wenn die Richtlinien und Grundregeln erst einmal definiert sind, lässt sich die Kontrolle von einer zentralen Stelle aus mit einem einzigen Klick einführen – ganz gleich, ob Sie 10 oder 1.000 Geräte zu verwalten haben.

4.7 Die Balance

Die Bereitstellung, Verwaltung und Sicherung Ihrer mobilen IT-Umgebung muss weder kompliziert noch teuer sein. Mit der MDM-Lösung von Kaspersky Lab ist die sichere Konfiguration von Mobilgeräten einfach und unkompliziert. Ein mobiler Agent wird auf dem Gerät installiert, um den erforderlichen Schutz vor heutigen Bedrohungen bereitzustellen. IT-Administratoren können sich darauf verlassen, dass Benutzergeräte mit den korrekten Einstellungen konfiguriert und bei Verlust, Diebstahl oder Benutzermissbrauch abgesichert sind.

Egal, wie groß oder klein Ihr Unternehmen ist: Wenn Sie Ihre mobilen Geräte nicht korrekt verwalten, werden sie bald zur Belastung für Ihre Ressourcen und – schlimmer noch! – zu einem Sicherheitsrisiko und potenziellen Datenleck. Ob Sie sich vom verstärkten Einsatz von mitarbeitereigenen Geräten Kosteneinsparungen versprechen oder bei mobilen Geräten strikt auf unternehmenseigene Geräte setzen, die Risiken sind letzten Endes dieselben: Ihre Mitarbeiter tragen eine ständig wachsende Menge an vertraulichen Geschäftsdaten mit sich herum, die in Taxis liegen gelassen, gestohlen werden oder anderweitig verloren gehen können.

Müssen Sie sich wirklich zwischen Sicherheit und Datenschutz auf der einen Seite und Mobilität, erhöhter Produktivität und Einfachheit auf der anderen Seite entscheiden? Nein, das müssen Sie nicht mehr – dank Mobile Device Management und optimierten Technologien für mobile Sicherheit.

5. FAZIT

Unternehmen müssen ihre Daten mit intelligenter Sicherheitstechnologie schützen. Zugleich benötigen sie intuitiv bedienbare, unkomplizierte Tools zur Steigerung der IT-Effizienz. Die 2.500 Mitarbeiter von Kaspersky Lab engagieren sich mit voller Kraft, diese Anforderungen für die über 300 Millionen von ihnen geschützten Systeme zu erfüllen – und natürlich auch für die 50.000 Systeme, die jeden Tag neu hinzukommen.

Kaspersky MDM ist eine Komponente von Kaspersky Endpoint Security for Business. Dank der Kombination aus preisgekrönter Malwarebekämpfung, Tools zur Durchsetzung von IT-Richtlinien, zentraler Verwaltung und Cloud-unterstützten Schutztechnologien sind die Unternehmenssicherheits-produkte von Kaspersky Lab die richtige Wahl für Ihr Unternehmen.

Sprechen Sie mit Ihrem Sicherheitsanbieter darüber, wie Kaspersky bei der Bereitstellung Ihrer mobilen Endgeräte für eine sichere Konfiguration – und vieles mehr – sorgen kann.

SEE IT. CONTROL IT. PROTECT IT.

With Kaspersky, now you can.
kaspersky.de/business-security

Be Ready for What's Next

Kaspersky Lab DACH
www.kaspersky.de

3132a/Stand: März 2013