KASPERSKY lab

BEST PRACTICES

Mobile Sicherheit

www.kaspersky.de

LEITFADEN ZU BEST PRACTICES BEI DER SICHERHEIT VON MOBILEN GERÄTEN

Die Bedrohungen für mobile Geräte wachsen exponentiell an.

Über einen Zeitraum von **12** Monaten wurden auf Sicherheitsprodukten von Kaspersky Lab **3,5** Millionen von Malware-Vorkommen auf den mobilen Geräten von mehr als **1** Million Benutzer erkannt.[1]

Mobile Geräte gehören heute zur geschäftlichen Grundausstattung. Ihr Funktionsumfang vergrößert sich ständig, aber damit steigen auch die Sicherheitsrisiken für Ihre Daten. Die Nutzung von Social Media und Cloud-basierten Technologien nimmt weiter zu und es wird immer schwieriger, die Geräte der zunehmend mobilen Mitarbeiter zu schützen. Aber es ist durchaus möglich, mobile Technologien (einschließlich BYOD), die zur Produktivitätssteigerung überaus wichtig sind, zuzulassen, ohne neuen Sicherheitsverletzungen Tür und Tor zu öffnen.

Gerade die Funktionen, die intelligente Endgeräte für Mitarbeiter so wichtig machen, machen sie auch attraktiv für Hacker, Datendiebe, Verbreiter von Malware und andere Kriminelle. Ganz zu schweigen davon, wie leicht sie gestohlen oder in Taxis oder beim Flughafen-Checkin vergessen werden können.

Forschungen von Kaspersky Lab haben ergeben, dass bei durchschnittlich 23 Prozent der Unternehmen bereits mobile Geräte gestohlen wurden, bei 19 Prozent von ihnen war dies mit dem Verlust von Daten verbunden, und bei 14 Prozent ist es zu Datenlecks oder zu einer unangemessenen Datenfreigabe über mobile Geräte gekommen.[2]

Da sich die durchschnittlichen Kosten einer Sicherheitsverletzung in einem kleinen bis mittelgroßen Unternehmen inzwischen auf etwa 50.000 $ belaufen[3], überrascht es nicht, dass der Schutz vertraulicher Daten vor Datenlecks für 38 Prozent von IT-Sicherheitsexperten heute höchste Priorität einnimmt.[4]

Ist BYOD wirklich so gefährlich?

Es geht aber nicht nur um Malware oder Diebstahl: Der Trend zur Förderung der Nutzung mitarbeitereigener Geräte in Unternehmen aller Größenordnungen trägt auch zu einer immer komplexeren Vielfalt an verschiedenen Geräten im Unternehmen bei. Da sich die Grenzen zwischen geschäftlicher und persönlicher Nutzung immer mehr verwischen, entstehen allein dadurch große Probleme bei IT-Management und -Kontrolle. Wenn Ihre Aufgabe darin besteht, den Mitarbeitern ein möglichst produktives Arbeiten bei gleichzeitig hoher Datensicherheit zu ermöglichen, sind mobile Geräte ein zweischneidiges Schwert. 69 Prozent aller IT-Sicherheitsfachleute sehen mobile Geräte daher als das größte Risiko für die Preisgabe vertraulicher Daten an.[5] Mehr als die Hälfte von Mitarbeitern im Alter zwischen 21 und 31 Jahren geben an, dass sie eine Richtlinie, die die Nutzung persönlicher Geräte am Arbeitsplatz untersagt, umgehen würden.[6]

1 Securelist, http://securelist.com/analysis/publications/66978/mobile-cyber-threats-a-joint-study-by-kaspersky-lab-and-interpol/ October 2014
2 Bericht von Kaspersky Lab zu globalen IT-Risiken 2014
3 Kaspersky Lab, IT-Sicherheit: Kampf gegen die stille Bedrohung, 2013
4 Bericht von Kaspersky Lab zu IT-Risiken, 2014
5 Ponemon Institute, Risk of Regulated Data on Mobile Devices and in the Cloud, 2013.
6 Forbes, http://fortune.com/2013/10/21/employees-really-want-to-use-their-personal-devices-at-work/

Wie können Sie die Nutzung mitarbeitereigener Geräte 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?

Die Antworten auf die meisten dieser Fragen sind Mobile Device Management (MDM) und Mobile Application Management (MAM) ...

1. SETZEN SIE MOBILE DEVICE MANAGEMENT UMFASSEND EIN

Mobile Device Management ermöglicht es, die Sicherheitsstrategie und -richtlinien, die für die stationäre Infrastruktur verwendet werden, auch auf alle anderen Geräte anzuwenden, wo immer diese sich gerade befinden. Mit MDM-Software können Sie wichtige Management- und Kontrollaufgaben wie Gerätekonfiguration, Software-Updates und Sicherung und Wiederherstellung kosteneffektiv automatisieren. Gleichzeitig gewährleisten Sie die Sicherheit vertraulicher Geschäftsinformationen im Fall von Diebstahl, Verlust oder Missbrauch durch den Endbenutzer.

Die wichtigsten Merkmale einer MDM-Lösung

- Unterstützung mehrerer Plattformen

  Schutz und Wartung mehrerer Geräte und Plattformen sind eine große Herausforderung. Eine MDM-Lösung, die mehrere Plattformen über eine einheitliche Schnittstelle und integrierte Richtlinien unterstützt, ist nicht nur kosteneffektiv, sondern erleichtert auch die Verwaltung mehrerer Systeme. Gleichzeitig erhalten Sie Flexibilität für aktuelle und zukünftige Geräte.

- Möglichkeit zum Erstellen starker Richtlinien

  Um einen Best-Practice-Ansatz beim Mobile Device Management zu verfolgen, müssen Sie auf mobile Geräte angepasste Richtlinien erstellen, in denen u. a. die folgenden Punkte klar festgelegt sind:

  - Wie gestaltet sich die Bereitstellung der Geräte?
  - Welche Programme dürfen ausgeführt werden?
  - Wer kann über die Netzwerke des Unternehmens was tun?
  - Welche Verfahren greifen im Fall von Verlust oder Diebstahl des Geräts?

  Die Richtliniendefinitionen sollten fein abgestuft und flexibel sein, d. h., Sie sollten je nach Anforderungen unterschiedliche Richtlinien für verschiedene Benutzer und Gruppen vorsehen. Wenn Sie diese Feinabstufung auf das Gerät selbst ausdehnen – beispielsweise durch Verhindern, dass per Jailbreak entsperrte oder auf andere Weise kompromittierte Geräte auf Unternehmensdaten zugreifen können oder sie per Fernzugriff gesperrt werden –, sorgen Sie für eine weitere Sicherheitsebene.

2. PROFITIEREN SIE VOM MOBILE APPLICATION MANAGEMENT

Beim Mobile Application Management (MAM) geht es um die Bereitstellung, Verwaltung und Kontrolle von Programm-Software auf den Smartphones und Tablets von Endbenutzern. Jede effektive Enterprise Mobility Management (EMM)-Lösung sollte das Management von Programmen und Programmdaten sowie der Geräte-Firmware und der Konfigurationseinstellungen umfassen. So wird das MAM zu einer Ergänzung und sogar zu einem Teil des MDM.

Der Verlust oder Diebstahl von Geräten ist bei Smartphones und Tablets natürlich ein sehr viel größeres Problem, als bei stationären Workstations, aber die hauptsächliche Eingangsroute für Malware auf allen Endpoints, einschließlich mobilen Geräten, liegt bei den Programmen. Darüber hinaus ist das Deployment von Apps bei der Nutzung von mobilen Geräten heute unerlässlich, wobei Sie keine Kontrolle über Qualität und Umfang der auf ein mitarbeitereigenes mobiles Gerät heruntergeladenen Freizeit- und Unterhaltungs-Apps ausüben.

Eine MAM-Lösung muss in der Lage sein, Unternehmens- und persönliche Daten zu trennen, sodass Sie für die Geschäftsprogramme auf dem Gerät zusätzliche Sicherheitsrichtlinien einrichten können. Eine solche Trennung wird durch Containerisierung erzielt.

Containerisierung

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 Containerisierung zum Einsatz. Es handelt sich um eine einfache Lösung, mit der persönliche und geschäftliche Inhalte auf dem Gerät getrennt werden. Auf diese Weise erhalten Sie umfassende Kontrolle über Ihre Unternehmensdaten und können Sie vor den Risiken einer persönlichen Gerätenutzung schützen.

Sicherheits- und Datenschutzrichtlinien können auf Programme angewendet werden, die in einem geschäftlichen „Container“ auf einem mitarbeitereigenen oder einem unternehmenseigenen Gerät angewendet werden. Diese Methode ist daher für BYOD besonders nützlich. Die Funktion zur „selektiven Löschung“ von Kaspersky Lab bedeutet Folgendes: Wenn ein Mitarbeiter das Unternehmen verlässt und sein persönliches Gerät mitnimmt, kann der Inhalt des bzw.der Container vom Mobiltelefon des Mitarbeiters gelöscht werden, einschließlich aller vertraulichen Geschäftsdaten, ohne dass die persönlichen Daten des Mitarbeiters betroffen sind.

Möglichkeiten zur Container-Verschlüsselung sorgen für eine weitere Schutzebene in Ihrer Sicherheitsstrategie für mobile Geräte. Gemäß Best Practices beim Diebstahlschutz für mobile Geräte lassen sich durch eine erzwungene Datenverschlüsselung die Auswirkungen einer verzögerten Löschung eines verlorenen oder gestohlenen Geräts mindern.

Wenn Sie sicherstellen, dass nur verschlüsselte Daten aus dem Container auf einem Gerät abgerufen werden können, verhindern Sie Verstöße gegen die Datensicherheit und sorgen für Compliance im Bereich Datenschutz. Die Verschlüsselungstechnologie für mobile Geräte von Kaspersky Lab kann automatisiert werden. Darüber hinaus gewährleistet Transparenz bei der Nutzung die Einhaltung von Sicherheitsrichtlinien. Weiterhin kann das ganze mobile Gerät mithilfe der MDM-Funktionen von Kaspersky Lab verschlüsselt werden.

3. AKTIVIEREN SIE DIEBSTAHLSCHUTZ UND DIE SICHERHEIT DER INHALTE

Physische Sperren für kleine, ultramobile Geräte einzurichten, ist so gut wie unmöglich. Sie können aber die Daten auf diesen Geräten sperren und steuern, was passiert, wenn Geräte abhanden kommen.

Die Enterprise Mobility Management (EMM)-Lösung von Kaspersky Lab umfasst Funktionen für den Schutz im Fall von Diebstahl und die Sicherheit der Inhalte. Diese Funktionen können per Fernzugriff ausgelöst werden, um den unbefugten Zugriff auf vertrauliche Daten zu verhindern. Hier einige der gebotenen Funktionen:

- **Sperren per Fernzugriff**: Verhindern des unbefugten Zugriffs auf ein Gerät, ohne dass Daten gelöscht werden müssen.
- **Geräte-/Standortüberwachung**: Ermitteln des Gerätestandorts mithilfe von GPS-Koordinaten. Diese Informationen können an den Geräteeigentümer gesendet werden.
- **SIM-Kontrolle**: Sperren eines verlorenen/gestohlenen Telefons, selbst wenn die SIM ersetzt wird. Die neue Nummer wird an den rechtmäßigen Eigentümer gesendet.
- **Gezieltes Löschen per Fernzugriff**: Vollständiges Löschen der Daten auf allen Geräten oder ausschließliches Löschen von sensiblen Unternehmensdaten.
- **Alarm- und Fahndungsfoto**: Machen Sie den Dieb Ihres mobilen Geräts darauf aufmerksam, dass Sie ihn kennen – Sie können das gestohlene Telefon sogar anweisen, den Dieb zu Identifikationszwecken zu fotografieren.

4. GEBEN SIE IHREN BENUTZERN DIE KONTROLLE

Eine Methode, um die Aktivierung der oben genannten Maßnahmen zur Diebstahlsicherung zu beschleunigen, besteht darin, die Kontrolle hierüber an die Benutzer zu übertragen. Durch Einsatz eines Self-Service-Portals können Mitarbeiter unabhängig von ihrem jeweiligen Standort umgehend auf den Verlust eines Geräts reagieren. Zunächst kann versucht werden, den Standort des Geräts auf einer Karte zu ermitteln, einen Screenshot anzufertigen oder ein Alarmsignal an das Gerät zu senden. Wenn dies nichts nützt, kann der Benutzer das Gerät blockieren und das Unternehmensprofil bzw. alle Daten von dem verlorenen Smartphone oder Tablet löschen.

Wenn Sie Ihren Mitarbeitern Tools an die Hand geben, mit denen sie Maßnahmen zur Diebstahlsicherung selbst aktivieren können, sinkt im Durchschnitt die Zeit zur Aktivierung der Maßnahmen zur Diebstahlsicherung und damit steigt die Sicherheit Ihrer Daten.

Das Self-Service-Portal von Kaspersky Lab ermöglicht Benutzern auch, ihre Geräte im Unternehmensnetzwerk zu registrieren, was Ihnen eine Verwaltungsaufgabe erspart.

5. SCHÜTZEN SIE GERÄTE VOR MOBILER MALWARE

Nicht nur verlorene oder gestohlene Geräte sind Risiken ausgesetzt. Es überrascht, wie viele Unternehmen darauf bestehen, Malware- und Spam-Schutz auf ihren festen Netzwerken einzurichten, diese Strategie dann aber bei mobilen Geräten ignorieren.

Viele MDM-Lösungen bieten im Grunde einen reaktiven Schutz über die Containerisierung. Dagegen umfassen die Sicherheitstechnologien für mobile Geräte von Kaspersky Lab eine solide Engine zum Schutz vor Malware, Spam und Phishing, die durch Cloud-Technologien unterstützt wird. Diese Engine ermittelt und blockiert Angriffe in Echtzeit, noch bevor sie ein Gerät erreichen, statt sich ganz auf den Container als Schutzbarriere zu verlassen.

Darüber hinaus tragen bedarfsorientierte und geplante Scans zu einem maximierten Schutz bei. Automatische OTA-Scans und -Updates sind wichtige Bestandteile einer effektiven MDM-Strategie.

6. PROFITIEREN SIE VON EINER ZENTRALEN VERWALTUNG

34 Prozent alle KMUs haben im letzten Jahr mobile Geräte in ihre IT-Systeme integriert. Diese Rate entspricht annähernd der größerer Unternehmen.[7] Mit den Technologien von Kaspersky Lab können Sie die Sicherheit von mobilen Geräten über dieselbe Konsole steuern, wie die Netzwerk- und die Endpoint-Sicherheit. So fällt kein zusätzlicher Administrationsaufwand zur manuellen Integration von oftmals inkompatiblen Steuerungskonsolen an.

Größere Unternehmen mit hochgradig strukturierten IT-Umgebungen sind sicher auch daran interessiert, dass das Kontrollzentrum den rollenbasierten Zugriff unterstützt. Auf diese Weise kann beispielsweise die Verantwortung für Administrationsaufgaben bei mobilen Geräten oder für die Programmkontrolle einer bestimmten Person im Team zugewiesen werden.

7. ERZIELEN SIE EFFIZIENZSTEIGERUNGEN DURCH AUTOMATISIERUNG

Durch Vereinfachen und Automatisieren der sicheren Konfiguration auf mehreren Geräten entlasten Sie nicht nur die IT-Abteilung, sondern unterstützen gleichzeitig bessere Vorgehensweisen bei der mobilen Sicherheit. Viele der Aufgaben des Sicherheitsadministrators für mobile Geräte, wie z. B. die Windows- oder PKI-basierte Zertifizierung, können sicher und effektiv automatisiert werden. Größere Unternehmen entscheiden sich wahrscheinlich für eine weitere Vereinfachung und nutzen Technologien wie Kerberos Key Distribution Center.

Die Verwaltung über ein Web-Portal hat bei mobilen Geräten klare Vorteile. Und anhand eines Self-Service-Portals kann dem Benutzer ein gewisser Grad an persönlicher Verantwortung übertragen werden.

Sind die Richtlinien und Grundregeln erst einmal definiert, lässt sich die Kontrolle von einer zentralen Stelle aus mit einem einzigen Klick einführen – ganz gleich, ob Sie 10 oder 1000 Geräte zu verwalten haben.

7 Bericht von Kaspersky Lab zu IT-Sicherheitsrisiken, 2014

ZU GUTER LETZT ...

Die Bereitstellung, Verwaltung und Sicherung Ihrer mobilen IT-Umgebung muss weder kompliziert noch teuer sein. Mit der Enterprise Mobility Management-Lösung von Kaspersky Lab können Sie die Sicherheit von mobilen Geräten auf denkbar einfache Weise konfigurieren. Dabei stellt ein auf den Geräten installierter mobiler Agent alle Maßnahmen zur Verfügung, die Sie für einen effektiven Schutz vor aktuellen Bedrohungen benötigen. Alle mobilen Geräte sind mit den von der IT abgesegneten Einstellungen konfiguriert, sodass sie im Fall von Verlust, Diebstahl oder Missbrauch durch den Benutzer umfassend geschützt sind.

Wenn es um die Sicherheit und den Datenschutz auf mobilen Geräten geht, kommt es nicht auf die Menge der Geräte an. Unabhängig davon, wie viele Benutzer und Geräte Sie verwalten, gilt: Wenn Sie nicht für eine angemessene Kontrolle sorgen, werden sie sich schon bald als Ressourcenbelastung und sogar als Sicherheitsrisiko entpuppen.

Müssen Sie sich wirklich zwischen Sicherheit und Datenschutz auf der einen Seite und Mobilität, Produktivität und Einfachheit auf der anderen Seite entscheiden? Dank des Mobile Device Management und der fortschrittlichen Sicherheitstechnologien für mobile Geräte von Kaspersky Lab ist dies zum Glück nicht der Fall.


Twitter.com/
Kaspersky_DACH


Facebook.com/
Kaspersky.Lab.DACH


Youtube.com/
KasperskyLabCE

Kaspersky Lab, Moskau,
Russland
www.kaspersky.de

Informationen zur
Internetsicherheit:
www.viruslist.de

Informationen zu Partnern in Ihrer
Nähe finden Sie hier:
www.kaspersky.com/buyoffline

KASPERSKY lab