MobileIron

Bewährte Erfahrungen in der Cloud: Audit-Checkliste für die Endgerätesicherheit

Diese 10-Punkte-Checkliste enthält eine Übersicht der bewährten Verfahren zu Entwicklung einer Sicherheitsarchitektur zum Schutz von Cloud-Daten im Endgerät. Die Unternehmens-Computerarchitekturen haben sich in den letzten zehn Jahren grundlegend geändert; die Mitarbeiter nutzen eine immer größere Zahl von Unternehmens-Cloud-Diensten mit mobilen Apps. Das traditionelle Sicherheitskonzept mit einer Netzwerkgrenze und versiegelten Endgeräten eignet sich für diese moderne Arbeitsumgebung mit Apps und Cloud nicht.

Cloud-Dienstanbieter sichern allgemein ihre Rechenzentren mit einem strukturierten, umfassenden Konzept und minimieren das Risiko eines Datenverlustes. Sobald die Daten jedoch den Dienstanbieter verlassen und sich auf dem Mobilgerät eines Endbenutzers befinden, können diese Daten leicht gefährdet werden oder verloren gehen, wenn keine angemessenen Sicherheitskontrollen vorhanden sind.

Viele Unternehmen müssen interne oder externe Sicherheits-Audits absolvieren, um nachzuweisen, wie gut sie Unternehmensdaten in der Cloud und auf dem Endgerät schützen. Das US-NIST Cybersecurity Framework unter www.nist.gov/cyberframework und die Datenschutz-Grundverordnung der Europäischen Union unter www.eugdpr.org sind zwei gesetzliche Regelwerke, die Einfluss auf die Audit-Kriterien haben dürften.

Diese Checkliste soll als Ausgangsbasis dienen und erhebt keinen Anspruch auf Vollständigkeit für ein Audit. Jedes Unternehmen sollte seine Analyse selbst durchführen und seine Kontrollen selbst definieren. Wenn jedoch Abweichungen zwischen Ihrer aktuellen Implementierung und dieser Checkliste vorhanden sind, könnte dies auf ein höheres Risiko hinweisen.

MobileIron

info@mobileiron.com

www.mobileiron.com

Checkliste für ein Sicherheits-Audit

1. Geräteverschlüsselung und Passwortschutz erzwingen

Mobilgeräte gehen oft verloren. Wenn Sie eine Geräteverschlüsselung und die Verwendung von Passwörtern erzwingen, können Sie den Zugriff auf Daten erschweren, wenn das Gerät nicht mehr im Besitz des Eigentümers ist. Verschlüsselung ist in den HIPAA-Vorschriften zur Portabilität und Verantwortlichkeit von Krankenversicherungsdaten in den USA sowie der Datenschutz-Grundverordnung vorgeschrieben, sofern diese das Risiko mindert. Wenn es das Gerät erlaubt, sollten auch biometrische Daten wie Fingerabdruck oder Gesichtserkennung verwendet werden, um den Zugriff durch unerwünschte Personen zu erschweren.

2. Kein Datenaustausch zwischen Unternehmens-Apps und privaten Apps

Mobile Betriebssysteme erlauben den Austausch von Daten zwischen Apps auf dem Gerät. Endbenutzer können beispielsweise Dokumentanhänge in einer Unternehmens-E-Mail empfangen und diese Dokumente dann in anderen Apps öffnen, wie in einem PDF-Reader oder Dokument-Editor. Sobald eine App ein Dokument öffnet, kann diese App das Dokument speichern oder versenden, ohne dass dies die IT-Abteilung kontrollieren kann. Dies ist eine sehr häufige Ursache für Datenverlust. Keine Unternehmens-App darf daher Daten in eine private App exportieren.

3. Automatische Löschung der Unternehmensdaten von gefährdeten Geräten

Geräte erfüllen häufig aufgrund von Sicherheitsproblemen wie Jailbreaking, Rooting, Malware oder veralteter Firmware die Compliance-Anforderungen nicht mehr. Die Maßnahmen zur Eingrenzung der Risiken müssen automatisch ohne manuelle Eingriffe der IT erfolgen. Bei schwerwiegenden Compliance-Problemen müssen die Unternehmensdaten automatisch vom Gerät gelöscht werden. Ein geschlossener Compliance-Zyklus, von der Erkennung bis zur Beseitigung, ist für die Risikominimierung unverzichtbar. Je länger ein gefährdetes Gerät Unternehmensdaten enthält, umso größer ist das Risiko eines Datenverlusts. Um den Datenschutz privater Daten zu gewährleisten, muss die IT-Abteilung die Unternehmensdaten auf dem Gerät löschen können, ohne private Daten zu verändern.

4. Tunnel-Übertragung nur von Unternehmens-Traffic, nicht von privatem Traffic

So wie Punkt 3 der Checkliste eine Trennung von Unternehmens- und privaten Daten auf dem Gerät fordert, fordert dieser Punkt eine ähnliche Trennung im Netzwerk. Eine geräteweite VPN-Verbindung sendet Daten von Unternehmens-Apps und privaten Apps über das Unternehmensnetzwerk. Eine App-spezifische VPN-Verbindung dagegen kann so konfiguriert werden, dass nur der Traffic von Unternehmens-Apps über das Unternehmensnetzwerk gesendet und damit geschützt wird, zugleich aber der Datenschutz der Übertragungen aus den Social Media des Endbenutzers und andere private Mitteilungen erhalten bleibt.

5. Kein Zugriff nicht autorisierter Geräte auf die Unternehmens-Cloud-Dienste

Die meisten Unternehmen nutzen Business-Cloud-Dienste verschiedener Anbieter, beispielsweise eine Produktivitäts-Suite von Microsoft und eine CRM-Lösung von Salesforce. Wenn ein nicht autorisiertes Gerät Zugriff auf einen dieser Dienste hat, kann es Daten von diesem Dienst auf das Gerät herunterladen. Diese Daten befinden sich nicht mehr unter Kontrolle der IT-Abteilung. Dieser Fall tritt oft dann ein, wenn ein Endbenutzer eine Unternehmens-App aus Bequemlichkeit auf ein privates Gerät herunterlädt. Unternehmensdaten dürfen sich nur dann auf einem Gerät befinden, wenn die IT die Apps löschen und die Datenfreigabe auf dem Gerät kontrollieren kann. Die IT muss diese Sicherheitskontrollen für alle Unternehmens-Cloud-Dienste unabhängig vom Anbieter anwenden können. Die Absicherung nur von Office 365 reicht nicht aus. Diese Kontrolle betrifft sowohl die Datenschutz-Grundverordnung als auch die NIST Cybersecurity Framework Category DE.CM-7 ("es erfolgt eine Überwachung, ob Mitarbeiter, Verbindungen, Geräte und Software autorisiert sind"). Damit wird verhindert, dass nicht autorisierte Geräte auf Unternehmensdaten zugreifen.

6. Kein Zugriff nicht autorisierter Apps auf Unternehmens-Cloud-Dienste

Zum Schutz der Daten muss die IT-Abteilung sicherstellen können, dass sowohl das Gerät als auch die Apps, die auf den Cloud-Dienst zugreifen, sicher sind. Wenn das Gerät sicher ist, aber die App nicht, gehen Daten verloren. Häufig tritt dieser Fall beispielsweise dann ein, wenn Endbenutzer Unternehmens-Apps direkt von Verbraucherdiensten wie dem Apple App Store oder Google Play herunterladen, statt über den internen Unternehmens-App-Store des Arbeitgebers. Zwar scheint die App für den Endbenutzer identisch zu sein und läuft auf einem sicheren Gerät, die IT-Abteilung kann jedoch weder die Datenfreigabe kontrollieren noch diese App löschen. Die IT muss verhindern können, dass nicht autorisierte Apps auf Unternehmens-Cloud-Dienste zugreifen. Dies betrifft nicht nur Office 365. Diese Kontrolle ist sowohl für die Datenschutz-Grundverordnung als auch für NIST DE.CM-7 relevant, weil damit der Zugriff von nicht autorisierter Software (Apps) auf Unternehmensdaten verhindert wird.

7. Erkennung und Eingrenzung von Sicherheitslücken vom ersten Tag an

Die bisher erwähnten Kontrollen minimieren das Risiko von Datenverlust. Kriminelle entdecken jedoch immer wieder neue Sicherheitslücken in Hardware, Software und im Verhalten, die sie ausnutzen können. Durch ständige Analyse des Geräts, der App und der Netzwerkbedrohungen mit Hilfe künstlicher Intelligenz sowie der Möglichkeit, das Endgerät anzupassen, kann die IT schnell auf neue Bedrohungen reagieren.

8. Umfangreiche Sicherheitskontrollen für Android, iOS, macOS und Windows 10

Wir leben nicht länger nur in einer Windows-Welt. Die meisten Unternehmen unterstützen Endgeräte mit verschiedenen Betriebssystemen. Ältere Betriebssysteme wie Windows 7 besitzen eigene Sicherheitstools. Moderne Betriebssysteme wie Android, iOS, macOS und Windows 10 dagegen haben Endgeräte-Architekturen entwickelt, die vereinheitlichte, Plattform-übergreifende Sicherheitslösungen unterstützen. Die IT-Abteilung muss eine Lösung mit umfangreichen Kontrollen wählen, welche die nativen Sicherheitsfunktionen dieser verschiedenen Betriebssysteme umfassend nutzt.

9. Zertifizierung der Gerätesicherheit (Common Criteria Protection Profile für MDM)

Common Criteria ist ein internationaler Standard zur Zertifizierung der Computersicherheit. Das Protection Profile für mobiles Gerätemanagement (MDM) definiert die Anforderungen an die Sicherheitsrichtlinien für Mobilgeräte, welche Unternehmensdaten verarbeiten und eine Verbindung mit Unternehmensnetzwerk-Ressourcen herstellen. Common Criteria ist oft eine Anforderung von Behörden und Hochsicherheitsorganisationen. Die IT muss eine Sicherheitslösung auswählen, die diese Zertifizierung besitzt.

10. Zertifizierung der Cloud-Sicherheit (SOC 2 Typ 2 und FedRAMP)

Wenn die von der IT bereitgestellte Sicherheitslösung selbst eine Cloud-Lösung ist, sollte sie einen Report der Service Organization Controls (SOC) 2 Typ 2 mit detaillierter Beschreibung der Funktionstests durch den Auditor und der Compliance-Kontrollen generieren können. Dieser Test bestätigt die Effektivität der Kontrollen von Sicherheit, Verfügbarkeit, Verarbeitungsintegrität, Geheimhaltung und Datenschutz der Systeme des Anbieters. Die FedRAMP-Betriebszulassung (ATO) ist eine offizielle US-Zertifizierung, mit der bestätigt wird, dass der Anbieter auch den Risiko-Managementprozess der US-Bundesbehörden für Sicherheitsanforderungen bestanden hat. Die IT muss eine Sicherheitslösung auswählen, die diese Zertifizierungen besitzt.

Diese Checkliste mit 10 Punkten ist eine Zusammenfassung der bewährten Erfahrungen, die wir bei MobileIron-Kunden kennen gelernt haben. Diese Liste soll Ausgangspunkt für Ihre Definition von Sicherheits-, Compliance- und juristischen Richtlinien sein. Wir gehen davon aus, dass jedes Unternehmen die Leitlinien entwickelt, die zu seiner Branche, Region und Risiko-Toleranz am besten passen.

Cloud-Sicherheit mit MobileIron

MobileIron ist eine für Behörden geeignete Cloud- und Endgeräte-Sicherheitsplattform. So lösen unsere Kunden mit der MobileIron-Technologie die Probleme in der oben erwähnten Checkliste:

Checkliste Nr. 1, 2, 3, 8

Gerät in MobileIron registrieren: Installieren Sie mit MobileIron ein Konfigurationsprofil auf dem Gerät, damit die IT-Abteilung die erforderlichen Sicherheitsmaßnahmen zum Schutz der Unternehmensdaten ergreifen kann.

Sicherheitsrichtlinien definieren: Definieren Sie geeignete Passwort- und Verschlüsselungsrichtlinien in MobileIron. Verwenden Sie zur Authentifizierung gegebenenfalls biometrische Daten. Wenn ein Gerät nicht mehr konform ist, wird es automatisch in Quarantäne gestellt oder selektiv gelöscht. Wenn Mitarbeiter das Unternehmen verlassen, wird das Gerät komplett gelöscht, wenn es ein firmeneigenes Gerät ist, oder selektiv, wenn es Eigentum des Mitarbeiters ist.

Unternehmens-Apps verwalten: Verteilen Sie Unternehmens-Apps mit MobileIron über den Unternehmens-App-Store Apps@Work oder Managed Google Play. Nach der Installation werden diese Apps durch Richtlinienkontrollen verwaltet, die in MobileIron definiert sind. Das heißt, die IT kann die Freigabe von Daten zwischen Unternehmens- und Verbraucher-Apps verhindern und die Apps bei Bedarf Over The Air löschen. Auf diese Weise bleibt die Kontrolle über die Unternehmensdaten bei der IT-Abteilung, ohne dass die auf dem Gerät befindlichen privaten Daten verändert werden.

Checkliste Nr. 4

App-spezifische VPN-Verbindung bereitstellen: Konfigurieren Sie die Unternehmens-Apps mit MobileIron so, dass diese nur eine App-spezifische VPN-Verbindung mit MobileIron Tunnel mit den Diensten im LAN aufbauen können. Auf diese Weise wird der Traffic der Unternehmens-App vom Traffic der Verbraucher-App getrennt und das Firmennetzwerk nicht durch private Daten überlastet.

Checkliste Nr. 5, 6

Zugriff auf Cloud-Dienste nur für vertrauenswürdige Geräte und Apps zulassen: Verhindern Sie mit MobileIron Access die Authentifizierung nicht verwalteter, nicht autorisierter oder nicht konformer Geräte und Apps bei Cloud-Diensten wie Office 365, Salesforce, ServiceNow, Workday usw. MobileIron Access ist eine auf Standards aufbauende Lösung für mehrere Clouds und mehrere Identitäten, die die vielen Cloud-Dienste und Identitätsanbieter in einem Unternehmen berücksichtigt.

Checkliste Nr. 7

Bedrohungen vom ersten Tag an erkennen und eingrenzen: Überwachen Sie mit MobileIron Threat Defense verdächtige Aktivitäten von Geräten, Apps und Netzwerk. Wenn ein Problem erkannt wird, lösen die MobileIron-Richtlinien entsprechende Gegenmaßnahmen aus, beispielsweise eine Benachrichtigung des Benutzers, eine Geräte-Quarantäne oder Datenlöschung.

Checkliste Nr. 9, 10

Keine Kompromisse bei den Sicherheitszertifizierungen: MobileIron war die erste Lösung, die eine Zertifizierung für das Common Criteria Protection Profile für MDM v2 erhielt. MobileIron ist außerdem kompatibel mit SOC 2 Typ 2 und besitzt eine FedRAMP-Betriebserlaubnis (ATO).

Die moderne Sicherheit entwickelt sich weiter, und IT-Profis fragen sich mitunter, ob Microsoft Intune diese Checkliste in vollem Umfang unterstützen kann. Unserer Meinung nach ist das nicht der Fall, insbesondere für die Checklisten-Positionen Nr. 3, 4, 5, 6, 7, 8, 9 und 10. MobileIron ist eine Sicherheitsarchitektur für mehrere Betriebssysteme, Clouds und Identitäten, die die jeweils besten Technologie-Optionen für moderne Unternehmen unterstützt.

Zusammenfassung

Die meisten Organisationen müssen in den kommenden Jahren mit (internen oder externen) Sicherheits-Audits rechnen. Das Ziel ist immer gleich – Schutz der Daten vor Schadsoftware, aber auch vor Datenverlust in bester Absicht – die Mechanismen der konventionellen und modernen Sicherheitsarchitekturen sind jedoch grundverschieden. Eine strukturierte Audit-Checkliste kann ein guter Ausgangspunkt sein für die Investitionen in Technologie, Personen und Prozesse, damit ein Unternehmen die innovativen Cloud-Dienste schnell und sicher nutzen kann.

Bei jeder Cloud-Bereitstellung müssen die Endgerätesicherheit und die Einhaltung der Datenschutz-Grundverordnung sowie der Bestimmungen des NIST Cybersecurity Framework und anderer Compliance-Modelle Priorität haben. Mitarbeiter nutzen Cloud-Dienste mit modernen Apps auf modernen Endgeräten; die Daten gehen jedoch verloren, wenn diese Endgeräte und Apps nicht sicher sind. Wie viele Daten verloren gehen, hängt davon ab, wie schnell Unternehmen eine End-to-End-Sicherheitslösung für mehrere Clouds wie MobileIron implementieren, wenn sie Microsoft Office 365, Salesforce, ServiceNow, Workday und andere Cloud-Lösungen einsetzen.