jamf

KURZVORSTELLUNG DER FIRMA

Apple-eigene Sicherheit

Beweis, dass weniger (Schichten) mehr (Sicherheit) ist

Die Informationssicherheit in Unternehmen ist ein nie endender Kampf gegen sich ständig weiterentwickelnde Bedrohungen. Angreifer werden immer raffinierter und ihre Angriffstechniken verändern sich ständig. Die Bedrohungen wachsen täglich mit jedem neuen Gerät, das im Unternehmensnetzwerk angemeldet wird. Eine Lösung für diese Sicherheitsherausforderung ist die Implementierung der Apple-Plattform, sodass die Vorteile des Apple-eigenen Sicherheitsframeworks genutzt werden können. Für eine moderne, mobile Belegschaft bedeutet das eine hervorragende Gerätesicherheit, ohne dass die Benutzererfahrung leidet.

DIE VIER ECKPFEILER DER MOBILEN SICHERHEIT

Die Sicherung eines mobilen Computers, ganz egal, ob es sich um einen Laptop, ein Smartphone oder ein Tablet handelt, muss vier wichtige Bereiche abdecken:

1. Daten im Ruhezustand – Sicherung der Daten auf einem Gerät
2. Daten bei der Übertragung – Sicherung der Daten bei der Übermittlung über eine Netzwerkverbindung zum Gerät
3. Anwendungssicherheit – Installation vertrauenswürdiger Software aus einer sicheren Quelle
4. Patching – Software auf dem Laufenden halten, um Sicherheitslücken zu vermeiden

Um gute Sicherheit zuverlässig und unternehmensweit zu implementieren, sind drei weitere Punkte von besonderer Bedeutung:

- Gerätemanagement – Bereitstellung, Anwendung, Verteilung und Durchsetzung von Sicherheitsrichtlinien
- Berichterstattung – Inventarisierung aller Geräte und ihre Konfiguration
- Auditierung & Korrektur – Prüfung auf Compliance hinsichtlich Sicherheitsstandards und Tools, um je nach Bedarf zu korrigieren

FÜGEN SIE KEINE SCHICHTEN HINZU, WENN SIE NICHT MÜSSEN

Komplexität in einem System macht die Absicherung dieses Systems schwieriger. Jede Schicht führt neue Fehlerstellen, Sicherheitslücken und potenzielle Konflikte ein. In der IT-Welt kommt die Komplexität in Form zusätzlicher Software-Schichten daher. Die IT-Sicherheitssoftware-Branche bietet viele Lösungen für die vier Eckpfeiler der Gerätesicherheit, meist jedoch auf Kosten einer einfachen Infrastruktur. Bei ansonsten gleichen Bedingungen ist ein Computersystem mit eigenen Sicherheitskontrollen einfacher zu verwalten und an sich sicherer. Durch die Integration des Sicherheitsframeworks und der Betriebssystemschicht wird der Update-Vorgang erleichtert und die Komplexität minimiert.

APPLE-EIGENE SICHERHEIT NIMMT VORREITER EIN

Apple ist bekannt für seine marktführende Rolle in der Branche in puncto Design und intuitiver Funktionalität. Weniger bekannt ist die Implementierung der eigenen Sicherheitsframeworks für iOS und OS X. In den vergangenen Jahren hat Apple mit Mac, iPad und iPhone neue Maßstäbe gesetzt. Heute bietet keine andere Plattform im Desktop- oder mobilen Ökosystem eine vergleichbare Kombination aus Benutzerfreundlichkeit, Datenschutz und robuster IT-Sicherheit.

WIE APPLE DIE VIER ECKPFEILER FESTIGT

Die OS X (Mac) und iOS (iPhone, iPad) Betriebssysteme von Apple beinhalten eigene Sicherheitskontrollen für jeden der vier Eckpfeiler:

1. **Daten im Ruhezustand**—Das iPhone und das iPad bieten auf der Hardware basierende Verschlüsselung für Daten im Ruhezustand, die automatisch aktiviert ist. Für Mac bietet FileVault ein eigenes Festplattenverschlüsselungssystem (eine Apple-eigene Funktion in OS X), das Daten praktisch mit keinerlei Auswirkungen auf die System- oder Akkuleistung schützt.
2. **Daten bei der Übertragung**—Apple-Geräte können per VPN (Virtual Private Network) verbunden werden, um eine sichere Datenübertragung zu gewährleisten. Für diese Sicherheitsfunktion ist keine weitere Software erforderlich. Nach der Konfiguration ist sie für den Benutzer nicht mehr sichtbar.
3. **Anwendungssicherheit**—Einer der besten Beiträge von Apple im Bereich der IT-Sicherheit ist das App Store-Ökosystem. Apple prüft jede Software, die im App Store eingesendet wird, um Malware auszuschließen. Jedes Softwarepaket wird digital signiert, um eine Manipulation der Dateien zu verhindern. OS X und iOS sind so konfiguriert, dass sie

Software ablehnen, die über keine Signatur verfügt. Die IT-Mitarbeiter können ihre eigenen Softwarepakete signieren, um von dieser Ebene der Anwendungssicherheit zu profitieren.

4. **Patching**—Seit Beginn des Computerzeitalters enthält jede Software Mängel oder Fehler. Einige dieser Mängel können von bösartigen Angreifern ausgenutzt werden, um Zugang zu erhalten oder Informationen zu stehlen. Die IT-Sicherheit reagiert üblicherweise mit häufigen Updates für die Software, um Sicherheitslücken zu beseitigen, sobald sie auftreten. Apple erleichtert diese Aufgabe mit eigenen Software-Patch-Dienstprogrammen, die in das OS integriert sind. Die IT-Mitarbeiter können einen Apple Software Update Server im Firmennetzwerk hosten, um das Patching zu beschleunigen.

APPLE-EIGENE SICHERHEIT, VERWALTET

Die Apple-eigenen Sicherheitskontrollen sind auf Benutzerfreundlichkeit ausgerichtet und erfordern nach ihrer Konfiguration kaum ein Eingreifen durch den Benutzer. Dies ist ideal für Einzelne oder Kleinunternehmen. Größere Organisationen benötigen jedoch Remote-Management-Tools, um Sicherheitskonfigurationen einzurichten, bereitzustellen und zu prüfen. Die Casper Suite von JAMF Software wurde für die Apple-Plattform entwickelt und integriert sich in alle Apple-eigenen Sicherheitskontrollen. Sie bietet eine komplette Auswahl an Bereitstellungs- und Konfigurationstools, dynamische Bestandsaufnahme sowie Prüf- und Korrekturfunktionen.

FAZIT

Die Implementierung guter Sicherheitsvorkehrungen muss kein komplexer und aufwändiger Vorgang sein. Im letzten Jahrzehnt hat Apple ein umfangreiches Ökosystem an Geräten, Software und Diensten entwickelt, das die beste Benutzererfahrung für Computer zur Verfügung stellt. Gleichzeitig stellen die eigenen Sicherheitskontrollen des Apple-Betriebssystems ein Framework auf Unternehmensebene bereit. In Kombination mit einem auf Apple ausgerichteten Management-Tool wie die Casper Suite bietet das Apple-Ökosystem die beste Erfahrung für Endnutzer und IT-Mitarbeiter.

jamf

www.jamf.com/de

Weitere Informationen über Apple-eigene Sicherheitskontrollen und die Tools der Casper Suite erhalten Sie unter **jamf.com/de**