jamf

Geht Ihre mobile Sicherheit über MDM hinaus?

Kreuzen Sie alle zutreffenden Aussagen an und zählen Sie anschließend unten die Gesamtzahl zusammen.

1.

BEDROHUNGSABWEHR

Mobile Bedrohungen enden nicht bei der Geräteregistrierung.

- [ ] Wir setzen auf MDM, um mobile Geräte ohne zusätzliche Schutzmaßnahmen gegen mobile Bedrohungen zu schützen.
- [ ] Wenn ein Benutzer auf einem iPhone oder iPad auf einen Phishing-Link tippt, haben wir nur begrenzte Möglichkeiten, dies automatisch zu erkennen oder darauf zu reagieren.
- [ ] Wir können Apps, die das Sicherheitsrisiko auf verwalteten Geräten erhöhen, nur schwer identifizieren.
- [ ] Wir haben nur begrenzten Einblick in und Schutz vor unsicherem WLAN oder anderen netzwerkbasierten mobilen Bedrohungen.

2.

KONFORMITÄT & GERÄTEZUSTAND

Was man nicht sehen kann, kann man auch nicht überwachen.

- [ ] Wir haben keinen Echtzeitüberblick darüber, welche Geräte derzeit die Anforderungen erfüllen.
- [ ] Konfigurationsabweichungen lassen sich nur schwer erkennen, bevor sie sich auf die Benutzer oder die Konformität auswirken.
- [ ] Probleme mit Geräten stellen wir in der Regel erst fest, nachdem Benutzer sie gemeldet haben.
- [ ] Wir können die Anforderungen an Betriebssystem- und App-Versionen nicht auf allen Geräten einheitlich durchsetzen.

3.

UPDATES & SCHWACHSTELLENVERWALTUNG

Jedes verspätete Update birgt unnötige Risiken.

- [ ] Wir können nicht garantieren, dass alle Geräte stets die neueste Version des Betriebssystems verwenden.
- [ ] Wichtige App-Updates hängen nach wie vor davon ab, dass die Benutzer sie installieren.
- [ ] Die Fristen für die Installation von Updates werden in unserer gesamten Mobilgeräteflotte nicht einheitlich durchgesetzt.
- [ ] Einige Geräte rutschen gelegentlich aus der Konformität, weil Updates nicht rechtzeitig installiert werden.

4.

IDENTITÄT & ZUGRIFF

Die Identitätsverwaltung ist nur ein Teil des gesamten Sicherheitspakets.

- [ ] Unsere Identitätsplattform überprüft während der Authentifizierung nicht den Sicherheitsstatus mobiler Geräte.
- [ ] Ein kompromittiertes oder nicht konformes mobiles Gerät könnte weiterhin auf Unternehmens-Apps zugreifen.
- [ ] Zugriffsrichtlinien gehen davon aus, dass registrierte Geräte vertrauenswürdig sind, unabhängig von ihrem aktuellen Sicherheitsstatus.
- [ ] Wir verweigern den Zugriff von risikobehafteten oder nicht konformen Geräten nicht automatisch.

Warum diese Fragen wichtig sind

Mobilgeräteverwaltung ist eine unverzichtbare Grundlage, doch moderne mobile Sicherheit erfordert mehr als nur die Konfiguration der Geräte. Schutz vor Bedrohungen, kontinuierliche Konformität, zeitnahe Updates und identitätsbasierter Zugriff tragen zur Risikominimierung bei.

Je mehr Aussagen Sie angekreuzt haben, desto wahrscheinlicher ist es, dass Ihre Umgebung Sicherheitslücken aufweist, die sich nicht allein durch die Verwaltung der Geräte beheben lassen.

Ihr Ergebnis

0-4 → **Solides Fundament**

Ihre Strategie für mobile Sicherheit deckt viele der Funktionen ab, die moderne IT-Teams benötigen. Das Dokument hilft, Ihren Ansatz zu validieren und weitere Chancen zur Stärkung Ihrer Umgebung aufzuzeigen.

5-9 → **Möglichkeiten zur Verbesserung**

In Ihrer Umgebung bestehen mehrere allgemeine Sicherheitslücken, die das Betriebsrisiko im Laufe der Zeit erhöhen können. Viele Unternehmen erreichen diese Phase, wenn sie ihre mobile Infrastruktur ausbauen. Erfahren Sie, wie Sie den Schutz verbessern können, ohne dabei unnötige Komplexität zu verursachen.

10-16 → **Es ist an der Zeit, Ihren Ansatz zu modernisieren**

Die Geräteverwaltung trägt mehr Verantwortung, als ursprünglich vorgesehen war. Wenn Sie Ihren Ansatz um die Bedrohungsabwehr, kontinuierliche Konformität und identitätsbasierten Zugriff erweitern, können Sie Risiken reduzieren und gleichzeitig die Betriebsabläufe vereinfachen. Das Whitepaper bietet einen praktischen Leitfaden für die Modernisierung Ihres Sicherheitskonzepts im Mobilbereich.

Sind Sie bereit, über MDM hinauszugehen?

Erfahren Sie, wie Sie Mobilgeräteverwaltung, Bedrohungsabwehr und Konformität zu einer modernen Sicherheitsstrategie für iPhone und iPad kombinieren können.

jamf

www.jamf.com/de/

Holen Sie sich das Whitepaper