jamf

5 versteckte Sicherheitslücken, die Sie in Ihrer Apple-Geräteflotte überprüfen sollten

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

1.

KONFIGURATIONSABWEICHUNG

Das Gerät meldet sich weiterhin. Die Konfiguration entspricht nicht mehr den Vorgaben der IT-Abteilung.

- [ ] Möglicherweise haben sich die Einstellungen auf einigen Geräten seit der Registrierung ohne unser Wissen geändert.
- [ ] Wir setzen auf planmäßige Bestandsüberprüfungen, um Konfigurationsänderungen zu erkennen, anstatt die Geräte kontinuierlich zu überwachen.
- [ ] Es gibt keinen automatisierten Prozess zur Korrektur von Konfigurationsabweichungen.

2.

GERÄTE OHNE PATCH

Die meisten Geräte sind auf dem neuesten Stand. Die Ausnahmen machen den Reiz aus.

- [ ] Die vollständige Patch-Abdeckung lässt sich nicht ohne manuellen Aufwand verifizieren.
- [ ] Geräte, die offline sind oder sich in anderen Netzwerken befinden, erhalten kein Update.
- [ ] Wir können nicht ohne Weiteres feststellen, wie lange ein Gerät bereits mit einer veralteten Betriebssystemversion läuft.

3.

BEDROHUNGEN, DIE MDM NICHT ERKENNT

Ein Gerät kann registriert sein, den Status „grün“ anzeigen und gleichzeitig aktiv kompromittiert sein.

- [ ] Abgesehen von MDM haben wir keine speziellen Tools für die Endpunktsicherheit unserer Macs.
- [ ] Verhaltenssignale, verdächtige Prozesse oder Kompromittierungsindikatoren sind mit unseren derzeitigen Tools nicht detektierbar.
- [ ] Wir wüssten nicht, ob eine Bedrohung auf einem Gerät läuft, das im MDM-Dashboard als konform angezeigt wird.

4.

ABGELAUFENER ZUGRIFF

Gestrige Zugriffsrechte überleben heutige Rollenwechsel.

- [ ] Zugriffsberechtigungen werden nicht immer aktualisiert, wenn ein Mitarbeiter die Position wechselt oder das Unternehmen verlässt.
- [ ] Der Zugriff auf Geräte wird nicht automatisch angepasst, wenn sich der Status eines Benutzers ändert.
- [ ] Ehemalige Auftragnehmer oder versetzte Mitarbeiter haben möglicherweise weiterhin Zugriff auf Ressourcen, die sie nicht mehr benötigen.

5.

ISOLIERTE TOOLS

Risiko kumuliert oft zwischen Tools.

- [ ] Verwaltungs-, Identitäts- und Sicherheitstools arbeiten unabhängig voneinander.
- [ ] Ein vom MDM als nicht konform markiertes Gerät könnte unsere Identitätsebene weiterhin ungehindert passieren.
- [ ] Ein am Endpunkt erkannter Sicherheitsvorfall löst keine automatische Reaktion in unserer Verwaltungsplattform aus.

5

Warum diese Lücken leicht zu übersehen sind

Hinter diesen Lücken verbergen hinter völlig normalen Gerätezuständen: registriert, meldend und aktiv. Sie kündigen sich selten durch Warnmeldungen an. Meistens kommen sie erst nach einem Audit, einem Vorfall oder einer Sicherheitsüberprüfung ans Licht.

Ihr Ergebnis

0-3 → **Begrenzte Exposition**

Es gibt nur wenige Anzeichen für versteckte Lücken, auch wenn möglicherweise noch einige blinde Flecken bestehen.

4-8 → **Es gibt blinde Flecken**

Möglicherweise bestehen bereits einige Lücken, ohne dass es dafür offensichtliche Anzeichen gibt.

9-15 → **Mehrere versteckte Lücken**

Hinter scheinbar intakten und konformen Geräten können sich mehrere Risiken verbergen.

Diese Lücken werden nicht als Warnmeldungen angezeigt. Sie werden als Vorfälle angezeigt.

Lücken schließen: macOS Sicherheit identifiziert Sicherheitslücken, die Ihre derzeitigen Tools nicht aufzeigen, und zeigt Ihnen, wie Sie diese schließen können.

jamf

www.jamf.com/de/

Laden Sie das Whitepaper herunter