jamf

Appleデバイス環境で確認すべき5つの潜在的なセキュリティギャップ

該当する項目にチェックを入れ、
最後に合計数を確認しましょう。

1.

構成ドリフト

デバイスがチェックインしていても、その構成がIT部門の想定と異なる。

- [ ] 一部デバイスの設定が、気づかないうちに登録時点から変更されている可能性がある
- [ ] 構成の変化の検出について、継続的な監視ではなく定期的なインベントリ確認に依存している
- [ ] 構成が想定から逸脱したデバイスを是正するための自動プロセスは展開していない

2.

デバイスのパッチ漏れ

大部分のデバイスにパッチを適用していても、漏れがあればリスクが生じる。

- [ ] 手作業なしでは、デバイス全体のパッチの適用状況を把握できない
- [ ] デバイスがオフラインであるか接続ネットワークが異なると、アップデートの対象から外れることがある
- [ ] デバイスで旧バージョンのOSが実行されていた期間をすぐに確認できない

3.

MDMでは把握できない脅威

デバイスが登録済みで報告状態が正常でも、実際には侵害を受けている場合がある。

- [ ] Macデバイスに、MDM以外の専用エンドポイントセキュリティツールを導入していない
- [ ] 現在のツール環境では不審な挙動、疑わしいプロセス、またはセキュリティ侵害インジケータの兆候を可視化できない
- [ ] MDMダッシュボードで違反なしと表示されているデバイスに脅威が潜んでいるとしても把握できない

4.

アクセス権の陳腐化

役割が変更されてもアクセス権は古いままになっていることが多い

- [ ] 従業員の異動や退職時に、アクセス権が更新されていないことがある
- [ ] ユーザの状態が変わってもデバイスのアクセス権は自動的には調整されない
- [ ] 過去の契約社員や異動後の従業員が当時のリソースへのアクセス権を保持している可能性がある

5.

ツールの分断

リスクは、ツール間の隙間に蓄積されがち。

- [ ] デバイス管理、ID管理、セキュリティの各ツールを別々に運用している
- [ ] MDMでコンプライアンス違反と判定されたデバイスでも、ID認証レイヤーでブロックされずに通過できる可能性がある
- [ ] エンドポイントでセキュリティイベントが検出されても、管理プラットフォームで自動対応できない

5

こうしたギャップが見過ごされやすい理由

上記のギャップは「MDMに登録され、状態を報告しながら稼動している」という、一見普通にしか見えないデバイス状態の影に潜んでいます。これらの存在が、アラートで明かされることはまずありません。それどころか、監査やインシデント、セキュリティ調査の過程で初めて表面化するケースがほとんどです。

チェック数

0〜3個 → **リスクは少ない**
潜在的ギャップの兆候はほとんどありませんが、一部の見えないリスクが生じている可能性があります。

4〜8個 → **見えないリスクが生じている**
明白な兆候が見られなくても、すでにギャップが生じている可能性があります。

9〜15個 → **潜在的ギャップが多数ある**
正常かつ準拠しているように見えるデバイスの背後に、複数のリスクが潜んでいる可能性があります。

こうしたギャップはアラートではなく、インシデントとして表面化します。

「macOSのセキュリティ機能をJamfで強化」で、現在ご使用のツールではわからないギャップとその解消方法を解説しています。

jamf

ホワイトペーパーをダウンロード

www.jamf.com/jaf/