Macの10大セキュリティ脅威

Macには強固なセキュリティ基盤がありますが、それも決して無敵でありません。ビジネスでの活用が進むにつれて、Macを標的とした攻撃も増えてきています。そのような攻撃に対処するには、システムの弱点に対する理解が欠かせません。

セキュリティを脅かす10の脆弱性と脅威、その対策をご紹介します。

1.

フィッシング攻撃

攻撃者が正規のWebサイトによく似たサイトにユーザを誘導し、認証情報を窃取します。

対策
Web脅威対策機能を使って悪意のあるサイトをブロックする。

2.

ランサムウェア

攻撃者がデバイスをロックし、金銭を要求します（金銭を払ったとしても、データが復旧する保証はありません）。

対策
エンドポイントセキュリティと多層防御戦略を活用する。

3.

脆弱なパスワード

推測しやすいパスワードを使用していると、アカウント乗っ取りの被害に遭いやすくなります。

対策
モバイルデバイス管理（MDM）を使って、複雑なパスワードを強制するポリシーを適用する。

4.

古いソフトウェア

古いアプリやオペレーティングシステムは、新しいものに比べて脆弱です。

対策
MDMの自動アップデート機能を使って、ソフトウェアの脆弱性に随時パッチを適用する。

5.

内部関係者による脅威

従業員の故意・過失が原因となって攻撃の隙が生まれることがあります。

対策
ユーザのトレーニング、利用規定の適用、セキュリティソフトウェアの採用により、リスクを緩和する。

6.

安全でないWi-Fiネットワーク

公共のWi-Fiに接続すると、攻撃者にデータが漏えいするおそれがあります。

対策
ゼロトラストネットワークアクセス（ZTNA）により、データの転送およびアクセスを厳重に保護する。

7.

データ漏えい

デバイスで発生する通信にはさまざまなものがあり、データをあるべき場所から出さないのは難しいこともあります。

対策
MDMを使ってAirDropなどの機能を無効化し、ZTNAでデータの転送の安全性を確保する。

8.

悪意のあるアプリケーション

承認を受けていない場所からダウンロードしたアプリには、危険なマルウェアが仕込まれていることがあります。

対策
サードパーティのアプリストアからのダウンロードを禁じるとともに、MDMやセキュリティソフトウェアを使って悪意のあるファイルを自動的に隔離する。

9.

デバイスの紛失・盗難

機密データの入ったデバイスを紛失したり、盗難されたりすると、データの悪用や流出のリスクが高まります。

対策：
MDMを使ってデバイスをロックしたり、リモートワイプしたりできるようにする。

10.

構成の悪用

構成プロファイルの設定に不備があると、ポリシーが破綻したり、十分に機能しなくなったりするおそれがあります。

対策
MDMプロファイルを定期的に監査し、デバイスの状態を常に把握しておく。

jamf

高度な脅威に対応するには、高度なソリューションが必要です。

最重要セキュリティ対策ガイドを入手

www.jamf.com/ja/