Die 10 größten Sicherheitsbedrohungen für Mac

Macs verfügen über eine hervorragende Sicherheitsgrundlage, aber sie sind nicht unbesiegbar. Da sie immer beliebter werden, geraten sie zunehmend ins Visier von Angreifern. Um diese Angriffe abzuwehren, müssen wir verstehen, wo unsere Systeme Schwachstellen aufweisen.

Hier sind zehn Bedrohungen und Schwachstellen, die Ihre Sicherheit gefährden.

1.

Phishing-Angriffe

Cyberkriminelle verleiten Benutzer dazu, ihre Zugangsdaten über täuschend echt wirkende Websites preiszugeben.

LÖSUNG

Blockieren Sie bösartige Websites mit dem Schutz vor Internetbedrohungen.

2.

Ransomware

Die Angreifer sperren Geräte und verlangen eine Lösegeld ohne Garantie für die Wiederherstellung der Daten.

LÖSUNG

Verwenden Sie Endpunktschutz und eine Defense-in-Depth-Strategie.

3.

Schwache Passwörter

Leicht zu erratende Passwörter machen Ihre Benutzerkonten anfällig für unbefugte Zugriffe.

LÖSUNG

Durchsetzung komplexer Kennwortrichtlinien mit Mobile Device Management (MDM).

4.

Veraltete Software

Veraltete Apps und Betriebssysteme sind anfälliger.

LÖSUNG

Automatische Updates mit MDM schließen Schwachstellen in der Software.

5.

Insider-Bedrohungen

Nachlässige oder böswillige Mitarbeiter öffnen Angreifern Tür und Tor.

LÖSUNG

Schulungen für Benutzer, Durchsetzung von Nutzungsrichtlinien und Sicherheitssoftware minimieren die Risiken.

6.

Ungesicherte WLAN-Netzwerke

Wenn sich Geräte mit öffentlichem WLAN verbinden, können Daten an böswillige Akteure weitergegeben werden.

LÖSUNG

Zero-Trust-Netzwerkzugriff (ZTNA) sorgt dafür, dass die Übertragung der Daten und der Zugriff darauf unter Verschluss bleibt.

7.

Datenlecks

Es gibt so viele Möglichkeiten, auf Ihrem Gerät zu kommunizieren – da kann es schwierig sein, die Daten unter Verschluss zu halten.

LÖSUNG

Deaktivieren Sie Funktionen wie AirDrop mit MDM und sorgen Sie für eine sichere Datenübertragung mit ZTNA.

8.

Bösartige Apps

Apps, die aus nicht genehmigten Quellen heruntergeladen werden, können gefährliche Malware enthalten.

LÖSUNG

Blochieren Sie App-Stores von Drittanbietern und isolieren Sie bösartige Dateien automatisch mit MDM- und *Sicherheitssoftware*.

9.

Geräteverlust und -diebstahl

Geräte mit sensiblen Daten können verloren gehen oder gestohlen werden, wodurch die Daten gefährdet werden.

LÖSUNG

Löschen und/oder Sperren von Geräten aus der Ferne mit MDM.

10.

Ausnutzung von Fehlkonfigurationen

Unzureichend eingerichtete Konfigurationsprofile können dazu führen, dass Richtlinien nicht funktionieren oder unvollständig sind.

LÖSUNG

Überprüfen Sie regelmäßig Ihre MDM-Profile und bleiben Sie über den Status der Geräte auf dem Laufenden.

jamf

Diese Top-Bedrohungen erfordern Top-Lösungen.

Holen Sie sich den Leitfaden für Top-Sicherheitspraktiken

www.jamf.com/de/