Mac 面臨的十大安全威脅

Mac 本身具備優異的安全基礎，但並非無懈可擊。隨著 Mac 越來越普及，攻擊者也越來越多地將其納入攻擊目標。要對抗這些攻擊，就必須先了解系統的弱點所在。

以下列出十種可能危及資安的威脅和漏洞。

1.

網路釣魚攻擊

惡意人士透過偽造網站誘騙使用者揭露其憑證。

解決方案

利用 Web 威脅防護功能封鎖惡意網站。

2.

勒索軟體

攻擊者鎖住裝置並勒索贖金，且不保證能成功復原資料。

解決方案

採用端點防護並實施縱深防禦策略。

3.

弱式密碼

容易被猜中的密碼，使帳戶門戶大開。

解決方案

透過行動裝置管理（MDM）強制執行複雜密碼政策。

4.

過時的軟體

過時的應用程式與作業系統更容易遭受攻擊。

解決方案

透過 MDM 啟用自動更新，以修補軟體漏洞。

5.

內部威脅

疏忽或惡意的員工替攻擊者打開大門。

解決方案

透過使用者培訓、強制執行可接受使用原則及部署資安軟體，降低這類風險。

6.

不安全的 Wi-Fi 網路

連上公共 Wi-Fi 可能讓資料暴露於惡意人士之手。

解決方案

採取 Zero Trust 網路存取（ZTNA），嚴格保護資料傳輸與存取安全。

7.

資料外洩

由於裝置上有多種通訊方式，要確保資料不外流並不容易。

解決方案

利用 MDM 停用 AirDrop 這類功能，並透過 ZTNA 確保資料在傳輸過程中的安全。

8.

惡意應用程式

從未經核准來源下載的應用程式可能含有危險的惡意軟體。

解決方案

禁止使用第三方應用程式商店，並透過 MDM 與資安軟體自動隔離惡意檔案。

9.

裝置遺失和遭竊

存有敏感資料的裝置可能遺失或遭竊，導致資料暴露於風險之中。

解決方案

透過 MDM 從遠端抹除和/或鎖住裝置。

10.

設定漏洞遭利用

設定不當的設定描述檔可能導致政策失效或不完整。

解決方案

定期稽核您的 MDM 設定檔，並隨時掌握裝置狀態。

jamf

因應首要威脅，須採用頂級解決方案。

www.jamf.com/zh-tw/

取得《頂级資安實務指南》