jamf

5 failles de sécurité cachées à rechercher dans votre parc Apple

Cochez toutes les affirmations qui décrivent votre situation, puis calculez le total ci-dessous.

1.

DÉRIVE DE CONFIGURATION

L'appareil se connecte régulièrement au serveur. La configuration n'est plus celle que le service informatique a définie.

- [ ] Les réglages de certains appareils peuvent avoir été modifiés à notre insu depuis leur inscription.
- [ ] Pour détecter les changements de configuration, nous procédons à des vérifications périodiques de l'inventaire, au lieu d'effectuer une surveillance en continu.
- [ ] Nous n'avons pas de processus automatisé pour corriger un appareil qui s'est écarté de la configuration prévue.

2.

APPAREILS NON MIS À JOUR

La plupart des appareils sont à jour. Ce sont les exceptions qui créent le risque.

- [ ] Nous ne pouvons pas vérifier que tous les appareils du parc ont bien reçu un correctif sans intervention manuelle.
- [ ] Il arrive que des appareils hors ligne ou connectés à d'autres réseaux manquent des cycles de mise à jour.
- [ ] Il est difficile de déterminer depuis combien de temps un appareil utilise une version obsolète du système d'exploitation.

3.

LES MENACES QUI ÉCHAPPENT À LA MDM

Un appareil peut être inscrit, avoir tous ses voyants au vert, mais être la victime d'une compromission active.

- [ ] Nous ne disposons pas d'outils dédiés à la sécurité des points de terminaison en dehors de notre solution MDM sur notre parc de Mac.
- [ ] Nos outils actuels ne permettent pas de détecter les signaux comportementaux, les processus suspects, ni les indicateurs de compromission.
- [ ] Nous ne serions pas informés si une menace active était présente sur un appareil qui apparaît conforme dans notre tableau de bord MDM.

4.

EXPIRATION DES ACCÈS

Les droits d'accès accordés par le passé persistent souvent après un changement de rôle.

- [ ] Les autorisations ne sont pas toujours actualisées lorsqu'un employé change de poste ou quitte l'entreprise.
- [ ] L'accès aux appareils ne s'adapte pas automatiquement lorsque le statut d'un utilisateur change.
- [ ] Il arrive que d'anciens prestataires ou des salariés réaffectés aient encore accès à des ressources dont ils n'ont plus besoin.

5.

FRAGMENTATION DES OUTILS

Le risque émerge dans les fissures qui séparent les outils.

- [ ] Les outils de gestion, d'identité et de sécurité sont déconnectés.
- [ ] Un appareil signalé comme non conforme par la MDM pourrait franchir notre couche d'identité sans être bloqué.
- [ ] La détection d'un incident de sécurité sur un point de terminaison ne déclenche pas automatiquement une réaction dans notre plateforme de gestion.

Pourquoi ces lacunes passent souvent inaperçues

Ces failles se cachent derrière des états apparemment normaux : « inscrit », « connecté » et « actif ». Elles déclenchent rarement des alertes. Le plus souvent, elles sont révélées par un audit, un incident ou un contrôle de sécurité.

Votre résultat

0 à 3 → **Exposition limitée**

Peu de signes de failles cachées, même s'il subsiste peut-être certains angles morts.

4 à 8 → **Présence d'angles morts**

Certaines lacunes peuvent être présentes sans qu'il y ait de signes avant-coureurs évidents.

9 à 15 → **Plusieurs lacunes cachées**

Plusieurs types de risque peuvent affecter des appareils qui semblent conformes et en bon état.

Ces failles ne déclenchent pas d'alertes.
Elles se manifestent sous forme d'incidents.

« Combler le fossé : la sécurité sur macOS » dresse l'inventaire des lacunes qui échappent à vos outils actuels et vous explique comment les combler.

jamf

www.jamf.com/fr/

Téléchargez le livre blanc