9 MESURES VISANT À RENFORCER
LA CONFIDENTIALITÉ DES ÉQUIPEMENTS ET DES DONNÉES

Réduisez les risques associés aux imprimantes code à barres thermiques

CONFIDENTIALITÉ

Appliquez le modèle CIA (Confidentiality, Integrity, Availability) à l'ensemble du parc

INTÉGRITÉ

1 CHIFFREZ TOUTES LES CONNEXIONS

Utilisez des solutions de chiffrement et d'identification, même si les équipements sont connectés à un réseau Ethernet ou ne manipulent pas directement d'informations stratégiques.

2 APPLIQUEZ LA ROTATION DES DONNÉES DE CONNEXION

Faites tourner les mots de passe utilisateur, les clés et les données de connexion à vos équipements, tâche qui sera considérablement simplifiée si vous utilisez une solution de gestion centralisée des appareils.

3 PROTÉGEZ LES ACCÈS

Ne privilégiez pas la convivialité aux dépens de la sécurité. Faites obstacle à une utilisation inappropriée des équipements en protégeant les accès et en activant un système de saisie des mots de passe simple sur le panneau de commande.

4 SURVEILLEZ LES MÉTHODES DE COMMUNICATION

Envisagez de mettre hors service les services réseau inutilisés, notamment FTP, SNMP et SMTP, qui vous exposent à des risques.

5 CONTRÔLEZ LES SOLUTIONS DE GESTION À DISTANCE DES ÉQUIPEMENTS

Si les solutions de gestion à distance améliorent considérablement la productivité, les accès et les autorisations doivent toutefois faire l'objet d'un contrôle rigoureux.

DISPONIBILITÉ

6 EFFECTUEZ DES MISES À JOUR RÉGULIÈRES ET CONFIDENTIELLES

Ne communiquez les calendriers de mise à jour qu'en cas de nécessité absolue.

7 ASSUREZ LE SUIVI DES ÉQUIPEMENTS

En utilisant d'emblée un schéma d'affectation de nom et une solution de gestion qui vous permettent de suivre les équipements, vous identifiez rapidement ceux qui présentent un risque de perte ou de vol, et dont il faudra, le cas échéant, désactiver les données de connexion.

8 TENEZ COMPTE DE LA LONGUEUR DU CYCLE DE VIE DES ÉQUIPEMENTS

En ce qui concerne les équipements dont la durée de vie peut atteindre 10 ans, sélectionnez un système d'exploitation qui peut être mis à jour régulièrement pour assurer l'application des nouvelles normes. Lors des mises à jour, utilisez les signatures numériques pour ne pas entraver l'« intégrité » du SE.

9 SÉCURISEZ LE RETRAIT DES ÉQUIPEMENTS

Lors du retrait d'un équipement, supprimez les fichiers et paramètres correspondants, désactivez les données de connexion et les comptes utilisateur associés, et vérifiez qu'aucun de vos systèmes n'est codé en dur pour continuellement rechercher ou tenter d'utiliser l'appareil.

Pour découvrir l'impact considérable de Link-OS en matière de protection des imprimantes code à barres et des données, rendez-vous sur www.zebra.com/linkos.

ZEBRA