Meilleures pratiques de sécurité

Dans le monde connecté d'aujourd'hui, les équipements suscitent tout naturellement des questions et des inquiétudes. Le principal est d'en prendre conscience, puis d'appliquer les mesures de bon sens qui s'imposent. Utilisez cette liste de contrôle comme outil de planification.

1. Prise en charge précoce

Prévoyez les technologies à venir, et la manière de les protéger.

2. Protection des données

Utilisez des connexions cryptées et authentifiées chaque fois que possible.

3. Contrôle des services

Pensez à désactiver les services technologiques que vous ne comptez pas utiliser.

4. Changement de mots de passe

En utilisant les mots de passe par défaut, vous offrez aux pirates une porte d'accès facile à vos équipements. **Activez les mots de passe de l'interface utilisateur.**

5. Gestion à distance

Profitez d'un système de gestion à distance sécurisé pour mettre rapidement à jour les paramètres. Plus les équipements, les solutions et les systèmes utilisent longtemps des paramètres obsolètes, plus ils deviennent une cible de choix.

6. Journalisation des activités

Utilisez les journaux d'activité et d'audit au maximum pour détecter tout comportement suspect.

7. Besoin d'information

Ne confiez les calendriers et plans de mise à jour qu'à ceux qui en ont besoin. Plus les employés sont nombreux à connaître les plans de mise à jour, plus les risques de violation de sécurité augmentent.

8. Surveillance des équipements hors de portée

Surveillez en permanence votre système pour identifier les équipements « hors de portée ». Si vous soupçonnez le retrait d'un équipement, supprimez ses identifiants de connexion jusqu'à confirmation de son emplacement.

9. Mise à jour simplifiée

Choisissez des équipements faciles à mettre à jour tout au long de leur cycle de vie, afin de respecter les nouvelles normes. Vérifiez que les systèmes de mise à jour empêchent la falsification des fichiers de mise à jour.

10. Mise au rebut des équipements

Planifiez la mise au rebut d'un équipement en supprimant les paramètres système de l'entreprise, en effaçant les comptes d'utilisateur et les identifiants de connexion de l'appareil et en vérifiant que les systèmes existants ne sont pas programmés pour rechercher des unités hors service.

11. Confidentialité, intégrité et disponibilité

Pensez toujours à assurer la confidentialité, l'intégrité et la disponibilité à tous les stades du cycle de vie d'un équipement.

12. Planification en continu

La mise à jour des mesures de sécurité doit être une priorité de tous les instants. La planification de la sécurité n'a rien de ponctuel.

Le saviez-vous ?

360 000 $

Le cryptage réduit en moyenne de **360 000 $** les coûts liés à la violation des données ; c'est le meilleur moyen de contrecarrer le piratage.[1]

81 %

L'utilisation de mots de passe volés ou faibles est à l'origine de **81 %** des violations de données par piratage.[2]

1,2 million $

Les entreprises capables de mettre en place des cellules de crise et de tester des plans d'intervention réduisent de plus de 1,2 million $ **le coût d'une attaque.**[3]

38 %

38 % des entreprises ont déclaré des incidents de sécurité dus à leurs équipements.[4]

40 %

40 % estiment que les cyber-attaques justifient une sécurisation accrue des appareils mobiles.

197 jours

Il faut à une entreprise en moyenne 197 jours pour se rendre compte qu'une violation de données a eu lieu.[5]

[1] Cost of a Data Breach Report 2019, IBM Security • [2] 2017 Verizon Data Breach Investigations Report, IBM Security • [3] Cost of a Data Breach Report 2019 • [4] Carbon Black Incident Response Threat Report, Novembre 2018 • [5] 2018 and 2019 Cost of Data Breach, Ponemon Institute