Document d'information, Boîte à outils de cybersécurité de la GCA : Identifier vos appareils et applications

Il est vraiment important de comprendre vos appareils et applications, car vous ne pouvez pas les protéger si vous ne les connaissez pas. En identifiant vos appareils et applications :

- vous comprenez les risques potentiels, vous permettant ainsi de faire quelque chose pour y remédier ;
- vous savez que vous n'éliminerez jamais tous les risques, mais que vous pouvez les réduire ;
- vous avez une meilleure « cyber hygiène » et sensibilisation, ce qui peut réduire de 80 % votre exposition aux menaces fréquentes.

La cybersécurité est un voyage et non une destination. Alors commencez à l'instaurer dans votre routine quotidienne.

Liste de contrôle : Identifier vos appareils et applications

Créez un inventaire :

- Qu'y a-t-il dans votre environnement informatique ?
  - *Vos appareils : ordinateurs de bureau, serveurs, ordinateurs portables, smartphones, tablettes, POS, IdO, CCTV, etc.*
  - *Vos applications : Microsoft Office, Adobe, applications POS, Chrome, etc.*
  - *Vos comptes en ligne : e-mail, Amazon, iCloud, Facebook, banque, cartes de crédit, etc.*

- Qu'est-ce qui est accessible sur Internet ou sur votre réseau interne ?
  - *Un appareil de l'IdO qui partage votre réseau interne, mais qui peut être contrôlé sur Internet pourrait présenter un risque.*
  - *Un ancien appareil qui n'est plus utilisé et qui n'est pas protégé, mais qui est toujours allumé, peut être exposé à une attaque.*
  - *Tout appareil qui utilise encore un mot de passe par défaut que vous n'avez pas changé est un moyen d'accès courant (par exemple un système CCTV avec un simple mot de passe admin/admin ou un ancien routeur).*
  - *Un ancien compte en ligne que vous n'utilisez pas, mais qui conserve vos données, peut subir une violation et vous mettre (ainsi que d'autres appareils connectés) en danger.*
  - *Les logiciels de votre ordinateur que vous n'utilisez plus ou n'entretenez plus, mais que vous n'avez pas supprimés peuvent être ciblés.*

- Quel niveau d'accès est nécessaire pour assurer une fonctionnalité habituelle ?
    - L'accès a-t-il été supprimé pour ceux qui n'en ont plus besoin ?
        - *Des relations ont-elles pris fin avec des entrepreneurs tiers ?*
        - *Des entreprises de la chaîne d'approvisionnement qui n'existent plus ?*
        - *Des employés qui ont quitté l'organisation, qui ont changé de rôle ou qui sont en congé prolongé ?*
    - Les systèmes et applications qui ne sont plus pertinents ou utilisés ont-ils été supprimés ?
    - Limiter le nombre d'utilisateurs ayant des privilèges d'administration. L'accès au niveau administrateur doit être réservé aux administrateurs et non aux utilisateurs quotidiens des systèmes ou des applications.

- Restreindre l'accès aux systèmes et aux applications afin de réduire potentiellement les dommages provenant :
    - de menaces internes intentionnelles et accidentelles causées par :
        - *l'action délibérée d'un employé mécontent ;*
        - *un employé victime de chantage dans le but d'accéder à des renseignements confidentiels ;*
        - *l'impact et les conséquences de l'ouverture d'un e-mail d'hameçonnage ;*
        - *la suppression accidentelle ou corruption de données.*

Pendant l'inventaire, examinez également si les exigences relatives aux mots de passe forts sont applicables et si la double authentification (2FA) est activée. (La 2FA est une couche supplémentaire de protection pour vos mots de passe.)

- Créez des réseaux séparés et limitez les droits d'accès (admin/utilisateur/aucun) afin que les informations sensibles soient plus difficiles d'accès et que les systèmes clés ne se trouvent pas sur le même réseau que les appareils moins sécurisés, réduisant ainsi l'impact d'une attaque car :
    - la sécurité de nombreux appareils IdO grand public est très peu, voire pas du tout intégrée ;
    - les équipements plus anciens peuvent être hors garantie et ne plus être protégés contre de nouvelles vulnérabilités ;
    - des tiers ayant des droits d'accès au réseau offrent un accès aux attaquants :
        - *Si des tiers ont accès à votre réseau, ont-ils une politique en place pour imposer le changement de mot de passe au moment du départ du personnel clé ?*

- Assurez-vous de tenir votre inventaire à jour régulièrement, y compris chaque fois que vous ajoutez ou supprimez de nouveaux équipements, comptes ou de nouvelles données critiques.

Utilisez les outils de la boîte à outils « Identifier vos appareils et applications » pour vous aider ou pour développer un système alternatif qui vous convient.

https://gcatoolkit.org/fr/petites-entreprises/identifier-vos-appareils-et-applications/