Document d'information, Boîte à outils de cybersécurité de la GCA : Mettre à jour vos défenses

Les cybercriminels sont constamment à la recherche de méthodes leur permettant d'accéder aux systèmes et aux données. L'une de ces méthodes consiste à détecter une faiblesse dans une configuration ou dans le code d'un développeur qui pourrait être reproduite sur l'ensemble de la base d'utilisateurs et exploitée à l'avantage du cybercriminel.

Les fabricants et les développeurs de logiciels publient régulièrement des mises à jour de leurs systèmes d'exploitation et applications afin de remédier aux faiblesses ou aux vulnérabilités découvertes récemment.

- Ces mises à jour sont généralement appelées « correctifs », et le processus est connu sous le nom de « mise à jour corrective ».

Il est vraiment important que les correctifs soient appliqués rapidement, et si possible automatiquement, pour éviter qu'ils ne soient utilisés dans une cyberattaque.

- L'attaque de ransomware WannaCry en mai 2017 qui a profité d'une faille identifiée dans le système d'exploitation Windows a eu des conséquences mondiales dévastatrices.
    - Elle ne ciblait pas des secteurs spécifiques, mais le type des appareils utilisés.
        - Elle a eu un impact sur les individus.
        - Elle a eu des répercussions sur les petites, moyennes et grandes entreprises.
        - Elle a eu des retombées dans les domaines de la police, de la santé, des transports, des télécommunications, des services bancaires, etc.
    - On estime qu'en 24 heures, plus de 230 000 systèmes informatiques ont été touchés dans 150 pays, avec des pertes évaluées en milliards de dollars.
- Des correctifs avaient été publiés par Microsoft en mars 2017 pour tous les appareils pris en charge.
    - Ceux qui n'avaient pas appliqué le correctif avant le début de l'attaque étaient en danger.
    - Ceux qui avaient appliqué le correctif (manuellement ou automatiquement) n'étaient pas en danger.
    - Ceux qui utilisaient Windows XP étaient en danger car Windows XP n'était plus mis à jour (le système d'exploitation était en « fin de vie », même si un correctif a rapidement été développé en raison de la gravité de WannaCry).

Fin de vie
Tous les appareils et systèmes d'exploitation ont une date de « fin de vie » après quoi ils ne sont plus entretenus ; le support cesse, aucun autre correctif n'est publié, et ils constituent un risque immédiat et permanent pour les vulnérabilités récemment découvertes. Cela peut également se produire si un fabricant cesse son activité et que personne ne reprend le développement de son ensemble de produits.

- Windows 7 est en fin de vie depuis janvier 2020.
- Windows XP est en fin de vie depuis avril 2014.
- *Les systèmes non pris en charge doivent être retirés du réseau, mis à niveau ou remplacés.*

Appareils IdO
L'augmentation du nombre d'appareils Internet des Objets (IdO), en particulier sur le marché des produits de consommation où les décisions d'achat sont souvent basées sur le prix, la facilité d'utilisation, la fonctionnalité et moins sur la sécurité, peut créer des points d'accès potentiels pour les attaquants. La plupart de ces appareils ayant des fonctionnalités de sécurité limitées et aucune possibilité de mise à jour corrective, en cas de faille, votre réseau resterait exposé aux attaques jusqu'à ce que l'appareil soit physiquement supprimé ou que des méthodes d'atténuation appropriées soient mises en œuvre. Les mesures préventives qui pourraient être prises pour éliminer ce risque seraient, le cas échéant, minimes.

Il est préférable de supprimer les anciennes applications qui ne sont plus utilisées et les équipements existants (anciens équipements qui ont été « adaptés » pour une utilisation sur un réseau ou sur Internet). Dans l'idéal, ces derniers devraient avoir été identifiés et supprimés/mis à jour lors de la mise en œuvre de la boîte à outils Identifier vos appareils et applications, en veillant à ce que les niveaux d'accès minimum pour la fonctionnalité habituelle soient appliqués.

En résumé :

- Les correctifs/mises à jour incluent des correctifs de sécurité importants qui permettent de se protéger contre les vulnérabilités découvertes récemment. Ils doivent être appliqués immédiatement à l'aide d'une option de mise à jour automatique dans l'idéal.
    - *Si vous n'installez pas les correctifs en temps opportun, vous mettez vos systèmes informatiques, et par conséquent votre organisation, en danger.*
- Supprimez les appareils qui ne peuvent pas faire l'objet d'une mise à jour corrective (c.-à-d. la plupart des appareils IdO grand public) et tous les appareils ou applications qui ne sont plus pris en charge, sans quoi ils peuvent mettre votre organisation en danger.
    - *Si l'appareil est nécessaire pour votre entreprise, isolez-le du mieux possible et interdisez tout accès à Internet et aux autres appareils.*
- Garantissez un niveau d'accès minimal pour les fonctionnalités habituelles et retirez immédiatement l'accès aux employés qui ont quitté l'organisation ou aux entreprises tierces qui ne fournissent plus de services (ou de clients).
- Assurez-vous que tous les logiciels et systèmes sont à jour, qu'ils ont fait l'objet de la mise à jour corrective la plus récente et qu'ils sont examinés régulièrement.

Utilisez les outils de la boîte à outils Mettre à jour vos défenses pour vous aider. Mettez en place une politique qui assure des examens réguliers de votre inventaire, de votre chaîne d'approvisionnement et de vos mises à jour.

https://gcatoolkit.org/smallbusiness/update-your-defenses/