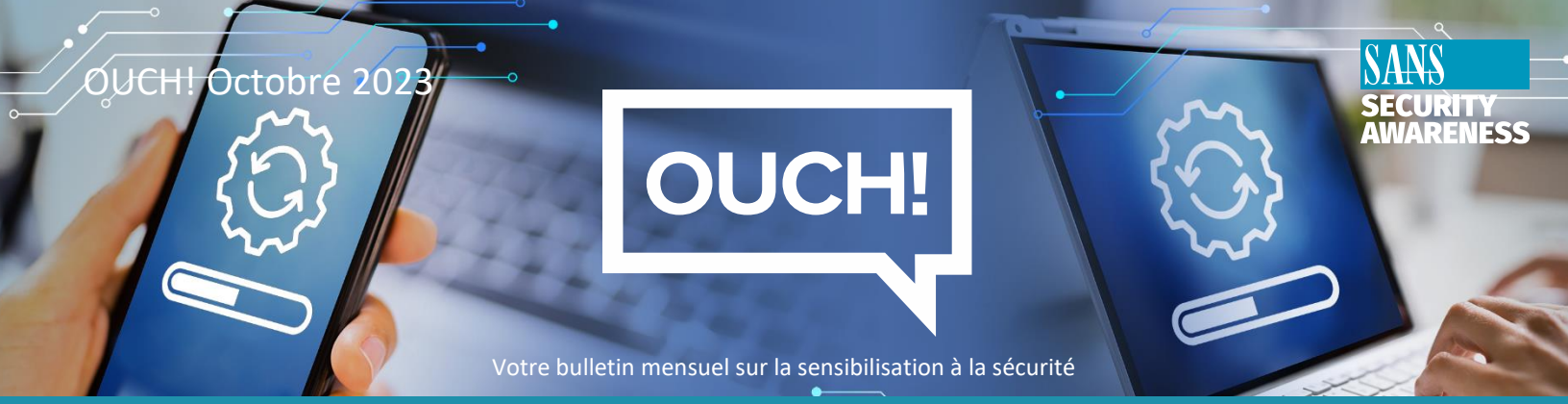

Le pouvoir de la mise à jour

Aperçu

Les cybercriminels recherchent constamment de nouvelles vulnérabilités dans les logiciels utilisés par vos appareils. Une vulnérabilité est une erreur ou une faiblesse dans la manière dont le logiciel a été développé. Ce logiciel peut faire fonctionner votre ordinateur portable, les applications mobiles de votre smartphone ou même le logiciel de votre thermostat. Les cyberattaquants profitent de ces vulnérabilités logicielles et les exploitent, ce qui leur permet de s'introduire à distance dans les systèmes, y compris ceux que vous utilisez. En même temps, les fournisseurs qui créent les appareils et les logiciels développent constamment de nouveaux correctifs pour ces vulnérabilités et les diffusent sous forme de mises à jour logicielles. L'un des meilleurs moyens de vous protéger est de vous assurer que les technologies que vous utilisez disposent toujours des dernières mises à jour. Ces mises à jour permettent non seulement de corriger les vulnérabilités connues, mais aussi d'ajouter de nouvelles fonctions de sécurité, ce qui rend le piratage de vos appareils beaucoup plus difficile pour les cyberattaquants.

Comment fonctionne la mise à jour

Lorsqu'une vulnérabilité logicielle est connue, le développeur ou le vendeur crée un correctif pour cette vulnérabilité (appelé « patch ») et diffuse la mise à jour au public. Votre système télécharge et installe alors cette mise à jour, qui corrige les vulnérabilités. Voici quelques exemples de logiciels que vous devez mettre à jour :

- Les systèmes d'exploitation de votre ordinateur portable (Microsoft Windows ou Apple macOS) ou de votre smartphone (Android ou iOS).
- L'équipement de réseau domestique, tel que votre routeur Internet ou vos points d'accès Wi-Fi, ou appareils domestiques intelligents, tels que thermostats, sonnettes, appareils électroménagers ou caméras de sécurité
- Les programmes qui s'exécutent sur vos appareils, tels que le navigateur web de votre ordinateur portable ou les applications mobiles de votre téléphone

C'est pourquoi, chaque fois que vous souhaitez acheter un nouvel appareil ou installer un nouveau programme informatique ou une nouvelle application mobile, vérifiez d'abord que le vendeur met activement à jour le programme ou l'appareil. Plus un logiciel reste longtemps sans mise à jour, plus il est susceptible de présenter des vulnérabilités que les cyber-attaquants peuvent exploiter. C'est pourquoi de nombreux fournisseurs, tels que Microsoft, publient automatiquement de nouveaux correctifs tous les mois. En outre, si vous n'utilisez plus un programme informatique, un logiciel ou une application mobile, supprimez-le de votre système. Moins vous avez de logiciels installés, moins vous avez de vulnérabilités potentielles et plus vous êtes en sécurité.

Enfin, si l'un de vos appareils ou l'une de vos applications sont anciens et ne sont plus pris en charge par le fournisseur, nous vous recommandons de les remplacer par des versions plus récentes qui sont activement mises à jour et prises en charge.

Comment mettre à jour

Il y a deux façons de mettre à jour vos systèmes.

1. **Manuellement (la méthode compliquée)** : Lorsqu'une mise à jour est disponible, vous la téléchargez et l'installez manuellement. Cela vous permet de mieux contrôler quand et comment les mises à jour sont installées. L'inconvénient des mises à jour manuelles est qu'elles demandent beaucoup plus de travail, car vous devez non seulement déterminer quand chacun de vos appareils ou programmes doit être mis à jour, mais vous devez également les mettre à jour manuellement, ce qui facilite les oublis.

2. **Automatiquement (la méthode facile)** : Vous activez la mise à jour automatique sur tous vos appareils, ce qui signifie que chaque fois qu'un nouveau correctif est publié, votre appareil le télécharge et l'installe automatiquement. L'avantage des mises à jour automatiques est que la plupart du travail est fait pour vous. L'inconvénient des mises à jour automatiques est que le programme mis à jour peut causer un problème, entraînant la perte de fonctionnalités ou de données. C'est rare pour les appareils personnels, mais ça peut se produire dans des environnements plus complexes, comme dans les grandes entreprises. Lorsque vous activez les mises à jour automatiques, vérifiez régulièrement votre système pour vous assurer que les mises à jour sont bien effectuées.

Nous vous recommandons vivement d'activer et d'utiliser la mise à jour automatique sur tous vos appareils personnels. Cela permet de s'assurer que toutes les technologies que vous utilisez, depuis votre smartphone et votre ordinateur portable jusqu'à votre moniteur pour bébé et vos serrures de porte, sont dotées des logiciels les plus récents. Des appareils et des logiciels mis à jour compliquent la tâche des cyberattaquants qui voudraient vous pirater, vous et vos systèmes.

Rédacteur Invité

Le docteur Janell Straach est membre du corps enseignant de l'université Rice où elle enseigne la cybersécurité et l'intelligence artificielle. Janell est présidente du conseil d'administration de Women In CyberSecurity (WiCyS). Vous pouvez contacter le Dr. Straach sur janell@wicys.org.

Ressources

Nettoyage de printemps du cyberespace numérique : https://www.sans.org/newsletters/ouch/digital-spring-cleaning-7-simple-steps/
Ai-je besoin d'un logiciel de sécurité ? : https://www.sans.org/newsletters/ouch/security-software/
Déclencheurs émotionnels - comment les cyber-attaquants vous piègent-ils ? : https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Traduit pour la communauté par : Juliette Busson