Nouvelles de Security Awareness

L'infolettre sur la sensibilisation à la sécurité pour les personnes sensibilisées à la sécurité

Le problème de la cybercriminalité

Les 5 plus grandes menaces pour la sécurité

Tout ce que vous devez savoir sur la cybercriminalité

Comment ôter un octet à la cybercriminalité

TOUT CE QUE VOUS DEVEZ SAVOIR SUR LA CYBERCRIMINALITÉ

DE QUOI S'AGIT-IL?

On parle généralement de cybercriminalité lorsqu'on **utilise des ordinateurs et d'autres dispositifs connectés au réseau pour mener des activités illégales**. Quelques exemples : les attaques d'hameçonnage, le vol d'identité, le vol de données et la cyber-extorsion (comme les logiciels de rançon, qui cryptent vos données jusqu'au paiement d'une rançon).

EST-CE UN PROBLÈME FRÉQUENT?

Une recherche rapide sur Internet des « statistiques sur la cybercriminalité » nous donne accès à toutes sortes de statistiques effrayantes, par exemple : « il y a une cyber-attaque toutes les 39 secondes » ou « une personne sur cinq se fera voler les informations de sa carte de crédit cette année », etc. Si les statistiques peuvent parfois être trompeuses, il ne fait aucun doute que la **cybercriminalité est une industrie gigantesque qui continue à se développer chaque année**.

QUELS PEUVENT ÊTRE LES PRÉJUDICES CAUSÉS?

L'argent, comme pour la plupart des crimes, est le maître mot. La cybercriminalité peut engendrer des contraintes financières inimaginables pour les organisations de tous les secteurs. Elle peut également nuire gravement à la réputation d'une organisation auprès de ses clients et de ses partenaires commerciaux, ce qui peut parfois donner lieu à des poursuites judiciaires et à d'éventuels licenciements ou arrêts de travail. Pire encore, lorsque des ressources essentielles sont attaquées, comme les hôpitaux ou les réseaux électriques, la cybercriminalité menace des vies.

QUELLES SONT LES CIBLES?

À vrai dire, **la cybercriminalité vise chacun d'entre nous et toutes les organisations**. Les personnes très en vue, comme les célébrités ou les fonctionnaires d'état, ont généralement beaucoup plus à perdre qu'un citoyen ordinaire, et elles ont donc plus de valeur aux yeux des agresseurs. Mais les cybercriminels n'hésiteront pas à vous cibler également et à tenter d'accéder à votre compte bancaire ou à des informations confidentielles.

QUE POUVEZ-VOUS FAIRE FACE À CES MENACES?

Il n'y a pas besoin d'être un super-héros ou d'avoir des super-pouvoirs pour mettre fin à la cybercriminalité. **Il faut plutôt des « pare-feu » humains solides qui réfléchissent avant de cliquer, font preuve de bon sens et suivent toujours les politiques.** N'oubliez pas que si certains cybercriminels utilisent des méthodes sophistiquées pour percer les cyberdéfenses, la cybercriminalité est, en grande majorité, perpétrée en ciblant des humains chaque fois que cela est possible. Lorsque vous êtes au travail, en déplacement ou à la maison, gardez l'œil ouvert et l'oreille tendue, et contribuez à rendre le monde plus sûr.

LES 5 PLUS GRANDES MENACES POUR LA SÉCURITÉ

INGÉNIERIE SOCIALE

L'ingénierie sociale est l'art de manipuler, d'influencer et de tromper les humains à des fins néfastes. Les spécialistes de l'ingénierie sociale tentent de pirater vos émotions pour vous convaincre d'accomplir une action risquée comme cliquer sur un lien d'hameçonnage ou communiquer des informations sensibles par téléphone. Ces attaques constituent le fondement de la plupart des escroqueries et sont souvent la cause première des incidents de sécurité.

LOGICIEL DE RANÇON

Généralement diffusé par des attaques d'hameçonnage, le logiciel de rançon crypte les ordinateurs ou les données jusqu'à ce que la victime paie une rançon pour obtenir les clés de décryptage (ou réussit à restaurer les systèmes avec des sauvegardes non affectées). Cette attaque représente l'une des formes de cybercriminalité les plus répandues et les plus dangereuses, mettant parfois des vies en danger (lorsqu'elle frappe les hôpitaux) ou perturbant gravement la société (lorsqu'elle compromet des villes entières ou des services municipaux).

HAMEÇONNAGE

L'hameçonnage est la stratégie par défaut dans l'arsenal des cybercriminels. De nombreuses tentatives d'hameçonnage comportent des signaux d'alarme classiques, tels que des erreurs grammaticales ou un sentiment d'urgence, mais d'autres sont beaucoup plus sophistiquées (comme la fraude au PDG, dans laquelle l'agresseur prétend être votre patron et vous demande de transférer de l'argent). Les hameçonneurs vous ciblent également par le biais de messages textes (smishing ou hameçonnage par message texte) et d'appels téléphoniques réels (vishing ou hameçonnage par téléphone).

VULNÉRABILITÉS NON CORRIGÉES

Des systèmes et des dispositifs obsolètes laissent des portes dérobées ouvertes aux cybercriminels. C'est l'une des rares façons dont ils peuvent obtenir un accès non autorisé avec un minimum d'interaction humaine (comme dans le cas d'une personne cliquant sur un lien malveillant ou téléchargeant une pièce jointe). En permettant les mises à jour automatiques, vous fermez efficacement ces portes et améliorez la sécurité.

MENACES INTERNES

La triste réalité en matière de sécurité est que, si la plupart des attaques viennent de l'extérieur de l'organisation (comme dans le cas des pirates informatiques), la majorité des menaces à la sécurité viennent de l'intérieur de l'organisation. Si vous avez accès à nos systèmes, réseaux et données confidentielles, vous êtes une menace pour cet accès. Les failles de sécurité sont rendues possibles par une erreur humaine : cliquer sur un lien d'hameçonnage, envoyer accidentellement des données à la mauvaise partie, ne pas respecter les politiques, etc. C'est pourquoi nous nous concentrons sur la sensibilisation au bon sens et espérons construire une culture de « pare-feu humains » résistants qui donnent la priorité à la sécurité dans toutes leurs activités.

COMMENT ÔTER
UN OCTET À LA CYBERCRIMINALITÉ

Comme dans un octet de données. Vous comprenez? Parce qu'on parle de cybercriminalité et de sécurité numérique...

De toute façon, contrecarrer les cybercriminels n'est pas un processus très compliqué. Voyons comment vous pouvez prévenir la cybercriminalité dans trois phases importantes de la vie quotidienne : au travail, à la maison et en déplacement.

PRÉVENTION DE LA CYBERCRIMINALITÉ AU TRAVAIL

Commençons par le plus facile : **ne tombez pas dans le piège des attaques d'hameçonnage.** Vous pouvez les repérer en recherchant les signaux d'alarme classiques tels qu'une grammaire médiocre et une orthographe épouvantable, un sentiment d'urgence, un appel à cliquer ou à télécharger quelque chose, un langage menaçant et des promesses irréalistes.

Bien sûr, toutes les attaques d'hameçonnage sont loin de présenter ces signaux d'alerte. Vérifiez donc l'adresse de l'expéditeur. Passez la souris sur les liens pour afficher l'ensemble de l'URL. Méfiez-vous de toute demande de données sensibles ou d'argent. En cas de doute, ne cliquez pas, ne répondez pas, ne téléchargez rien. S'il semble venir d'une personne que vous connaissez, contactez cette personne et confirmez qu'elle a envoyé le message.

À part l'hameçonnage, gardez votre espace de travail organisé et verrouillez votre poste de travail lorsqu'il n'est pas utilisé. Veillez à bien fermer les portes derrière vous. Ne laissez jamais quelqu'un emprunter vos identifiants ou votre badge pour se connecter à un système ou entrer dans une zone sécurisée. Respectez toujours les politiques. Et signalez immédiatement les incidents de sécurité.

PRÉVENTION DE LA CYBERCRIMINALITÉ À LA MAISON

Commençons par le plus facile : ne tombez pas dans le piège des attaques d'hameçonnage (voir plus haut). Ensuite, nous vous conseillons d'élaborer une politique de sécurité pour votre foyer, semblable à celle que la plupart des organisations mettent en œuvre. Voici quelques mesures de sécurité à mettre en œuvre dans votre vie personnelle :

- *Protégez chaque compte et chaque appareil (y compris votre routeur) avec un mot de passe fort et unique.*
- *Activez les mises à jour automatiques dans la mesure du possible.*
- *Configurez les comptes des médias sociaux de manière à ce qu'ils soient entièrement privés et uniquement réservés aux « amis » que vous connaissez.*
- *Limitez ce que vous communiquez publiquement sur Internet.*
- *Configurez différents comptes d'utilisateur sur les appareils partagés et limitez l'accès des administrateurs.*
- *Si vous avez de jeunes enfants, pensez à utiliser un logiciel de surveillance parentale.*

PRÉVENTION DE LA CYBERCRIMINALITÉ SUR LES APPAREILS MOBILES

Lorsque vous êtes en déplacement, ne vous connectez jamais à un réseau public sans utiliser un réseau privé virtuel (RPV), qui crypte votre connexion et empêche le vol de données. Même lorsque vous utilisez un RPV, évitez de vous connecter à des comptes qui contiennent des données très sensibles.

Avant de télécharger une application ou un logiciel, faites des recherches sur les développeurs et n'installez qu'à partir de sources fiables. Les boutiques d'applications sont souvent la cible de cybercriminels qui tentent de diffuser des applications malveillantes qui se font souvent passer pour des versions légitimes.

Gardez l'œil sur vos appareils, et ne les laissez jamais sans surveillance. Pensez à activer les services « Trouver mon appareil », s'ils sont disponibles. Ceux-ci vous permettent de localiser votre téléphone via un deuxième appareil ou de le réinitialiser à distance aux valeurs par défaut (en supprimant tous vos renseignements personnels).