GCA Cybersecurity Toolkit™ *For Small Business*

Boîte à outils de cybersécurité pour petites entreprises de la GCA

Bienvenue

Dear Colleague:

Cher(e) collègue,

Internet fait aujourd'hui partie intégrante des activités de la plupart des entreprises. La sécurisation de l'écosystème numérique de votre entreprise doit faire partie de votre fonctionnement. Une cyberattaque peut avoir des conséquences dévastatrices, notamment des pertes financières, le vol d'informations sensibles, des chaînes d'approvisionnement compromises, et plus encore.

Vous avez beaucoup d'autres préoccupations et responsabilités, et nous avons travaillé pour vous fournir une ressource que vous pourrez utiliser concrètement afin de répondre à vos besoins en cybersécurité. La boîte à outils de cybersécurité de la Global Cyber Alliance (GCA) pour les petites entreprises fournit des outils gratuits et efficaces permettant de réduire votre cyberrisque. Les outils sont soigneusement sélectionnés et organisés pour faciliter la recherche et la mise en œuvre d'étapes importantes qui aideront à protéger votre entreprise contre les cybermenaces. Nous avons inclus des vidéos ainsi qu'un forum communautaire où vous pouvez trouver du soutien et obtenir des réponses aux questions de vos pairs et experts en sécurité. La boîte à outils est conçue pour vous, et non pour une petite entreprise hypothétique avec des experts en cybersécurité sur le personnel et un budget important.

Le Manuel de la boîte à outils de cybersécurité pour petites entreprises de la GCA est un document qui accompagne la boîte à outils afin de vous guider lors de son utilisation. Vous pouvez télécharger le manuel dans son intégralité, ou chapitre par chapitre, au fur et à mesure de la mise en œuvre des actions recommandées dans la boîte à outils. Ce guide vous permet de travailler à votre propre rythme pour agir et sera un document de référence pratique lorsque vous en aurez besoin.

Ces ressources seront régulièrement mises à jour avec les contributions d'utilisateurs, d'experts du secteur et de partenaires à travers le monde.

Nous espérons que vous profiterez de la boîte à outils et du manuel pour commencer à améliorer votre cybersécurité dès aujourd'hui!

Cordialement,

Philip Reitinger
Président et PDG

Table des matières

Chapitres du manuel

Identifier vos appareils et applications

Quel problème cette boîte à outils résout-elle?

L'identification de vos appareils et applicatinos est la première étape pour améliorer la sécurité, tout simplement parce que vous ne pouvez pas protéger quelque chose dont vous ignorez la présence. N'oubliez pas que de nombreuses cyberattaques et violations de données sont causées par des ordinateurs portables ou d'autres appareils perdus ou volés, par un accès non autorisé aux comptes et par des vulnérabilités logicielles non corrigées. En identifiant quels ordinateurs, appareils et logiciels vous avez (c'est-à-dire en connaissant vos actifs), vous comprendrez mieux les risques potentiels, ce qui vous permettra de prendre des décisions éclairées et de mettre en œuvre des mesures pour réduire ces risques.

- Connaissez-vous le nombre d'ordinateurs portables et d'appareils mobiles détenus par votre entreprise, savez-vous qui y a accès et quels sont les logiciels et applications qu'ils contiennent ?

- Savez-vous quel âge ont vos ordinateurs et quand vous avez mis à jour leur sécurité pour la dernière fois ?

- Avez-vous des systèmes ou des appareils connectés à Internet (tels que des caméras de sécurité ou des contrôles des bâtiments) qui sont également connectés à votre réseau d'entreprise ?

Ces actifs pourraient offrir une voie vers votre environnement d'entreprise qu'un pirate pourrait utiliser pour voler ou corrompre vos données. Il est clair qu'il est important de savoir quels sont les appareils et les systèmes dont vous disposez. Certains de vos actifs sont plus essentiels aux opérations de l'entreprise que d'autres, et le fait d'avoir un inventaire complet et à jour vous aide à établir des priorités sur ce qui doit être protégé et à quel niveau.

Qu'est-ce que cette boîte à outils vous aidera à accomplir?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux:

- ✔ **Comment effectuer un inventaire de vos données et systèmes**
- ✔ **Quels appareils et applications sont essentiels pour le fonctionnement de votre entreprise**

Comment utiliser la boîte à outils

Utilisez les outils de la ***boîte à outils Identifier vos appareils et applications*** pour vous aider à identifier tous vos appareils (y compris les ordinateurs de bureau, les ordinateurs portables, les smartphones et les imprimantes) et les applications (par exemple, les e-mails, logiciels, navigateurs et sites Web) afin que vous puissiez prendre des mesures pour les sécuriser.

Cet inventaire servira de guide et de liste de contrôle à mesure que vous utiliserez les autres boîtes à outils. 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.

Téléchargez les outils à partir du site Web et notez les dates de réalisation. Profitez également de l'occasion pour planifier un examen régulier afin de vous assurer que toutes vos informations sont à jour.

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considérer

1.1 Identifier vos appareils

Lors de la création d'un inventaire, il est important de tenir compte de tout ce qui est présent dans votre environnement.

Cela inclut des éléments tels que les ordinateurs de bureau, les ordinateurs portables, les smartphones, les imprimantes, les caméras de vidéosurveillance, les PoS, les appareils IoT et les routeurs.

De nombreux appareils IoT grand public n'ont pas, ou très peu, de sécurité intégrée, c'est pourquoi vous devez vérifier s'il serait possible de les séparer du reste de votre réseau ou de les supprimer complètement.

Les équipements plus anciens peuvent être hors garantie et ne plus être protégés contre de nouvelles vulnérabilités, mais ils sont importants pour le fonctionnement de votre entreprise. Ceux-ci doivent être identifiés comme faisant partie de votre inventaire et un plan doit être élaboré pour remplacer, mettre à niveau ou restreindre leur utilisation.

De nombreux appareils tels que les routeurs, la vidéosurveillance et les imprimantes sont parfois oubliés lorsque l'on pense à l'environnement informatique, mais tout ce qui a une connexion à Internet ou au réseau local doit être pris en considération lorsque vous faites votre inventaire d'actifs, parce que ces connexions mènent souvent aisément à votre entreprise.

Identifiez où les données sensibles et critiques métier sont conservées, que ce soit sur des appareils autonomes connectés au réseau ou dans le cloud. Il se peut que des niveaux supplémentaires de

protection soient envisagés pour ces appareils, mais la première étape consiste à documenter où tout est conservé.

1.2 Identifier vos applications

Identifiez toutes vos applications, y compris les applications professionnelles, les comptes en ligne pour lesquels vous utilisez votre adresse e-mail professionnelle et les autres applications auxquelles vous accédez localement ou à distance via vos appareils.

Il est important d'inclure toutes les applications et les comptes, sans oublier ceux que vous n'utilisez plus, car vous êtes peu susceptible de mettre à jour les logiciels qu'ils contiennent. S'ils ne vous sont plus utiles, supprimez ou fermez les comptes. Un ancien compte en ligne peut contenir certaines de vos informations personnelles, et si l'entreprise pour laquelle vous avez initialement défini ce compte est victime d'une attaque, vos données pourraient être affectées.

Vous trouverez des informations, du soutien et des conseils supplémentaires pendant la mise en œuvre dans la **catégorie Identifier vos appareils et applications** sur le Forum communautaire de la GCA.

Liens Identifier vos appareils et applications:

Boîte à outils: ***outils Identifier vos appareils et applications***
https://gcatoolkit.org/fr/petites-entreprises/identifier-vos-appareils-et-applications

Forum communautaire: **Catégorie Identifier vos appareils et applications**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/know-what-you-have/

Le forum dans d'autres langues
https://community.globalcyberalliance.org/t/language-support-on-the-forum-de-es-fr-id/

Mettre à jour vos défenses

Quel problème cet outil résout-il?

Les cybercriminels recherchent des faiblesses et des défauts (connus sous le nom de vulnérabilités) qui peuvent être utilisés pour accéder aux systèmes ou diffuser des logiciels malveillants. Les acteurs malveillants pourraient avoir accès aux comptes financiers de votre entreprise, aux données de vos clients, et bien plus encore. Vous pouvez vous protéger contre cela en mettant à jour vos défenses (c'est-à-dire en veillant à ce que vos systèmes, appareils et données soient toujours à jour). 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 ».

Cette boîte à outils répond à la nécessité d'appliquer ces correctifs en temps opportun, y compris la configuration des systèmes afin qu'ils puissent être appliqués automatiquement dans la mesure du possible. En outre, il est important de se rendre compte qu'avec le temps, de nombreux systèmes sont ajoutés, adaptés ou reconfigurés, ce qui peut conduire à l'introduction de faiblesses qui pourraient être exploitées par les cybercriminels. Une autre question à garder à l'esprit est de savoir si un fournisseur tiers a accès aux données dans vos systèmes. Il est important de tenir des dossiers à jour ; cela vous permet de gérer les mises à jour nécessaires pour veiller à ce que les correctifs les plus actuels soient appliqués à vos systèmes, appareils et applications.

Qu'est-ce que cette boîte à outils vous aidera à accomplir?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux comment:

- ✔ **Vérifier que vous exécutez la dernière version du logiciel sur votre appareil**
- ✔ **Définir vos appareils pour accepter et appliquer automatiquement les mises à jour de sécurité**
- ✔ **Implémenter des paramètres de configuration sécurisés pour les appareils mobiles, les navigateurs Web et les systèmes d'exploitation**

Comment utiliser la boîte à outils

Utilisez les outils de la ***boîte à outils Mettre à jour vos défenses*** pour vous assurer que vos appareils et applications sont configurés avec les derniers correctifs de sécurité appliqués et avec les niveaux de sécurité appropriés pour le type de données qu'ils contiennent. Si vous avez créé un inventaire dans la boîte à outils Identifier vos appareils et applications, utilisez-le comme guide et liste de contrôle pour vous assurer que tous vos appareils sont mis à jour et sont configurés de façon à accepter automatiquement les mises à jour de sécurité.

Une fois que vous avez terminé la boîte à outils Mettre à jour vos défenses, mettez à jour votre liste de vérification de sécurité et définissez un rappel pour répéter ce processus périodiquement afin qu'il devienne routinier.

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considerer

2.1 Mettre à jour vos appareils et applications

Lorsqu'une solution, ou un correctif, est développé(e) et mis(e) à disposition pour une vulnérabilité connue, il est important que tous les utilisateurs de ce système ou de cette application l'appliquent immédiatement - idéalement automatiquement parce que jusqu'à ce que cela soit fait, ils sont exposés à des attaques via cette vulnérabilité.

Vérifiez chaque appareil et application et configurez-les pour des mises à jour automatiques. Nous avons fourni une liste des systèmes et applications les plus courants, mais pour ceux qui ne sont pas couverts dans cette boîte à outils, vérifiez les instructions ou les pages de support correspondant à l'appareil ou à l'application. Cochez chaque élément de votre liste au fur et à mesure, chaque fois que vous ajoutez un nouvel appareil ou une nouvelle application à votre entreprise.

Souvent, les paramètres les plus sécurisés ne sont pas fournis comme configuration de sécurité par défaut dès le départ pour vos appareils ou applications, car la facilité d'utilisation et la commodité sont prioritaires sur la sécurité. Par conséquent, vous devez vérifier s'il y a des configurations de sécurité recommandées par le fabricant pour vos appareils et applications et les implémenter.

Tous les appareils qui ne sont plus pris en charge doivent être supprimés, car ils risqueront toujours d'être compromis en raison d'une faiblesse nouvellement découverte. Si cela n'est pas possible, ils doivent être isolés des autres appareils et leur utilisation doit être limitée à des fonctions d'entreprise spécifiques seulement.

Les outils de cette boîte à outils proposent des conseils de configuration pour les systèmes courants afin d'appliquer automatiquement les mises à jour. Consultez ces conseils pour tous vos appareils et systèmes afin de vous assurer qu'ils sont configurés en conséquence.

2.2 Chiffrer vos données

Si votre réseau informatique est victime d'une violation, il est fort probable que le pirate cherchera à voler des informations sensibles ou confidentielles, qu'il pourra utiliser pour son propre gain financier ou politique. En cryptant les données stockées sur votre disque dur, il est beaucoup plus difficile pour les criminels de faire usage de ces données, car ils devront les décrypter avant qu'elles ne soient utilisables.

Le chiffrement est le processus par lequel les données sont converties d'une forme lisible (texte en clair) en une forme codée (texte chiffré). Ce codage est conçu pour être inintelligible, sauf par les parties qui possèdent la ou les clés permettant d'inverser le processus de codage. Le chiffrement permet de stocker et de transmettre des données de manière confidentielle. Il permet également de prouver que ces données proviennent de la personne qui prétend les avoir envoyées.

Ces outils vous permettent de chiffrer les fichiers stockés sur votre disque dur. Si votre système d'exploitation n'est pas inclus dans la boîte à outils ici, d'autres options peuvent être disponibles via le fabricant de l'équipement ou d'autres offres de sécurité disponibles dans le commerce.

2.3 Sécuriser vos sites Web

Pour de nombreuses entreprises, le site Web est essentiel au fonctionnement de l'entreprise. Son utilisation peut inclure la circulation d'informations sensibles à travers la chaîne d'approvisionnement ou il peut être la principale plateforme de négociation sur laquelle votre entreprise repose. Si des pirates accèdent au site Web, ils peuvent intercepter ou voler des données, modifier son contenu,

l'infecter avec des logiciels malveillants ou prendre le contrôle des opérations. N'importe laquelle de ces actions pourrait avoir un impact dévastateur sur la capacité de votre entreprise à fonctionner.

Ici, vous trouverez des outils susceptibles d'être utilisés pour effectuer des vérifications régulières sur votre site Web (connues sous le nom de scans) afin d'identifier les vulnérabilités et les faiblesses potentielles. Veillez à ce que les problèmes identifiés soient évalués par le personnel compétent en informatique et à ce que des mesures appropriées soient prises.
Les sous-catégories de boîtes à outils fournissent des instructions et des outils pour les systèmes couramment utilisés. Pour d'autres systèmes, recherchez de l'aide via le site Web du fournisseur ou demandez conseil sur le forum communautaire de la GCA, **dans la catégorie Mettre à jour vos défenses** ou **auprès de la communauté des petites entreprises**.

Liens Mettre à jour vos défenses:

Boîte à outils: ***outils Mettre à jour vos défenses***
https://gcatoolkit.org/fr/petites-entreprises/mettre-a-jour-vos-defenses/

Forum communautaire: **catégorie Mettre à jour vos défenses**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/update-your-defences/

Communauté des petites entreprises
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Éviter l'emploi de mots de passe simples

Quel problème cette boîte à outils résout-elle ?

Les mots de passe sont une première ligne de défense pour protéger vos comptes et données (tels que les e-mails, les dossiers du personnel ou les bases de données des clients).

Malheureusement, les mots de passe sont souvent une cible facile pour les cybercriminels, et les violations de données liées au piratage se produisent souvent en raison de mots de passe faibles. Les attaquants ont de nombreuses façons d'essayer d'accéder à vos mots de passe, de l'utilisation de craqueurs de mots de passe facilement accessibles (c'est-à-dire des programmes qui testent en boucle des combinaisons couramment utilisées) à l'utilisation sur d'autres sites populaires d'un nom d'utilisateur et d'un mot de passe obtenus à partir d'un compte ayant subi une violation. Ces techniques requièrent peu de capacités techniques, sont rapides, entièrement automatisées, et sont

facilement accessibles à ceux qui savent où les chercher sur Internet. Le problème pour les petites et moyennes entreprises est que bon nombre d'entre elles n'ont pas de politique de mot de passe, ou si elles en ont élaboré une, elles ne l'appliquent pas strictement.

Il est donc essentiel d'avoir des mots de passe forts pour protéger vos données. Mais vous devez également aller plus loin en mettant en œuvre l'authentification à deux facteurs ou multifacteur (2FA).

2FA nécessite plusieurs informations d'identification, ce qui rend beaucoup plus difficile l'accès à vos comptes pour un attaquant.

Avec 2FA, un utilisateur a besoin des éléments suivants:

- Quelque chose que vous connaissez, comme un mot de passe;
- Quelque chose que vous avez, comme un jeton (Google Authenticator, Authy, Okta, RSA, etc) ou un code de vérification envoyé sur votre téléphone ; ou
- Quelque chose que vous êtes, comme votre empreinte digitale ou votre visage (biométrie).

Cette boîte à outils vous permet de créer des mots de passe plus forts et uniques pour chacun de vos comptes et vous montre comment configurer l'authentification 2FA. Il s'agit de deux des étapes importantes de la protection de l'accès à vos comptes et données.

Qu'est-ce que cette boîte à outils vous aidera à accomplir?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux comment:

✔ **Créer un mot de passe fort**
✔ **Tester vos comptes pour voir s'ils ont été compromis**
✔ **Configurer l'authentification 2FA pour les comptes en ligne les plus courants**

Comment utiliser la boîte à outils

Utilisez les outils de la ***boîte à outils Éviter l'emploi de mots de passe simples*** pour vous assurer que vos appareils et applications sont configurés avec des mots de passe forts et l'authentification 2FA. Si vous avez créé un inventaire dans Identifier vos appareils et applications, utilisez-le comme guide et liste de contrôle pour vous assurer que vous l'avez mis en œuvre dans tous vos comptes.

Une fois que vous avez terminé la boîte à outils Éviter l'emploi de mots de passe simples, mettez à jour votre liste de vérification de sécurité et définissez un rappel pour répéter ce processus périodiquement afin qu'il devienne routineer

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considérer

3.1 Mots de passe forts

L'une des méthodes les plus courantes que les criminels utiliseront pour accéder à vos comptes, à votre réseau et à vos informations est de se connecter en utilisant votre identité. Il est vraiment important que vous:

- Utilisiez un mot de passe unique et fort (ou phrase de passe) pour chacun de vos comptes.
- Utilisiez des lettres, des chiffres et des caractères spéciaux pour garantir un mot de passe fort.
- Changiez votre mot de passe immédiatement si vous avez été victime d'une fuite de données.
- Gardiez vos mots de passe privés et en sécurité.
- Ne réutilisiez jamais un mot de passe.
- Ne cliquiez jamais sur un lien dans un e-mail vous disant «il est temps de réinitialiser votre mot de passe »; accédiez toujours au site Web du compte via le navigateur Web.
- Évitiez de vous connecter aux comptes via le Wi-Fi public.

La réutilisation du même mot de passe pour plusieurs comptes implique que si un criminel met la main sur l'un de vos mots de passe, il a facilement accès à tous vos comptes. Les détails du nom d'utilisateur et du mot de passe peuvent être vendus en ligne par des criminels qui les ont volés lors d'une cyberattaque et être réutilisés jusqu'à ce que le mot de passe soit modifié. L'évolution rapide de la technologie signifie qu'un ordinateur portable moderne bon marché peut rapidement tester en boucle toutes les combinaisons pour travailler sur de courts mots de passe simples.

Vous devez mettre en place une politique de mot de passe qui sera comprise et respectée par tout le personnel et tous les sous-traitants qui ont accès à vos systèmes. Certains systèmes et applications vous permettent de demander un mot de passe respectant obligatoirement des critères minimum. Pensez à vérifier vos paramètres de sécurité pour voir si cette configuration est possible pour vous.

Vous pouvez utiliser les outils de Mots de passe forts pour en savoir plus sur les mots de passe et vérifier si votre adresse e-mail a été volée lors d'une fuite de données. Si c'est le cas, changez immédiatement votre mot de passe et ne le réutilisez jamais.

N'oubliez pas non plus de vérifier les paramètres de mot de passe sur les routeurs, imprimantes et autres équipements connectés à votre réseau. Ceux-ci peuvent facilement être oubliés et sont généralement fournis avec des mots de passe simples par défaut. Passez en revue l'inventaire que vous avez créé dans Identifier vos appareils et applications, et cochez-les au fur et à mesure!

3.2 Outils pour la double authentification

L'authentification à deux facteurs (2FA) fournit une deuxième ligne de défense importante au-delà des mots de passe pour protéger les comptes contre tout accès non autorisé. Il existe un certain nombre

de méthodes d'authentification différentes qui peuvent être utilisées pour la 2FA. Ceux-ci vont d'un code unique envoyé par SMS à votre téléphone mobile, un jeton matériel que vous transportez, une empreinte digitale ou la reconnaissance faciale.

Les outils de la 2FA contiennent des ressources téléchargeables qui fournissent des méthodes d'authentification acceptées pour de nombreux comptes courants.

Lors de la mise en œuvre des outils et des conseils de la boîte à outils Éviter l'emploi de mots de passe simples, examinez également les autorisations dont dispose chaque utilisateur lors de l'accès à des applications liées à l'entreprise. Envisagez de limiter l'accès uniquement à ceux qui en ont besoin et dans la mesure où leur rôle l'exige.

3.3 Gérer vos mots de passe

Les gestionnaires de mots de passe sont un moyen de garder tous vos mots de passe ensemble en toute sécurité, sans avoir besoin de se souvenir de chacun individuellement. Cela signifie que vous n'avez qu'à mémoriser un mot de passe chaque fois que vous souhaitez vous connecter à l'un des comptes dont le mot de passe est stocké dans le gestionnaire de mots de passe. Les gestionnaires de mots de passe sont plus faciles à utiliser. Toutefois, cela signifie également que si le gestionnaire de mots de passe est compromis, l'attaquant aura accès à tous les mots de passe.

Vous trouverez des informations, du soutien et des conseils supplémentaires pendant la mise en œuvre dans la **catégorie Éviter l'emploi de mots de passe simples** sur le Forum communautaire de la GCA.

Liens Éviter l'emploi de mots de passe simples:

Boîte à outils: ***outils Éviter l'emploi de mots de passe simples***
https://gcatoolkit.org/fr/petites-entreprises/eviter-lemploi-de-mots-de-passe-simples

Forum communautaire: **catégorie Éviter l'emploi de mots de passe simples**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/beyond-simple-passwords/

Prévenir le hameçonnage et les logiciels malveillants

Quel problème cette boîte à outils résout-elle?

Chaque année, de nombreuses petites entreprises sont victimes de logiciels malveillants coûteux et d'attaques de hameçonnage. Lorsqu'un utilisateur clique sur un site Web infecté par un logiciel malveillant ou ouvre une pièce jointe infectée dans un e-mail de hameçonnage, le résultat peut être supprimé ou modifié des fichiers, des applications modifiées ou des fonctions système désactivées.

Les logiciels malveillants sont tout logiciel conçu pour causer des dommages et/ou un accès non autorisé aux appareils ou aux réseaux. Les e-mails de hameçonnage incitent l'utilisateur à penser qu'il a affaire à une entité digne de confiance afin que l'attaquant puisse bénéficier d'un accès non autorisé à du contenu privé, sensible ou limité, ou encre à de l'argent. L'attaquant utilisera toutes les méthodes possibles pour que son e-mail semble authentique et attirant, afin que l'utilisateur clique dessus ou l'ouvre. Les e-mails peuvent ressembler à ceux qui viennent d'une personne que vous connaissez, ils peuvent imiter les logos et le format des e-mails d'entreprises bien connues, ou ils peuvent se référer à des actualités récentes ou un travail que vous venez d'effectuer.

Selon certaines estimations, plus de 90 % des cyberattaques commencent par un e-mail de hameçonnage. Si vous cliquez sur le lien ou ouvrez la pièce jointe dans un e-mail de hameçonnage, vous pouvez déclencher n'importe quel nombre d'activités mises en place par l'attaquant et susceptibles d'inclure le vol de vos données, la création d'un itinéraire secret (connu sous le nom de porte dérobée) dans votre ordinateur pour une utilisation ultérieure, l'installation d'un type de logiciel malveillant à travers lequel l'attaquant vous verrouille hors de vos données et vous demande de payer une rançon pour l'accès (connu sous le nom ransomware), ou le téléchargement d'un autre type de logiciel malveillant qui permet à l'attaquant de voir ce que vous tapez, par exemple les mots de passe ou les numéros de compte (connu sous le nom de logiciel-espion).

Les conséquences du hameçonnage et des attaques de logiciels malveillants sont graves pour les petites entreprises. Les effets peuvent inclure la perte ou les dommages aux données, la perte de revenus si votre entreprise est fermée lors d'une attaque, les dépenses engagées pour réparer/remplacer l'équipement, les coûts pour aviser les clients d'une violation, ainsi que la perte de réputation et les poursuites potentielles.

La ***boîte à outils Prévenir le hameçonnage et les logiciels malveillants*** vous aidera à réduire les risques en renforçant votre résilience aux attaques. Sont inclus des outils pour vous empêcher d'aller vers des sites Web infectés, des logiciels antivirus pour aider à prévenir les virus et autres logiciels malveillants d'entrer dans vos systèmes, et des bloqueurs d'annonces pour éviter les publicités en ligne susceptibles de transporter des virus.

Qu’est-ce que cette boîte à outils vous aidera à accomplir ?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux:

- ✔ **Comment un logiciel antivirus protège vos systèmes et vos données**
- ✔ **Comment installer un logiciel antivirus sur votre système**
- ✔ **Les publicités numériques et les risques qu’elles posent**
- ✔ **Comment installer un bloqueur d’annonces pour bloquer les annonces, vidéos et autres contenus indésirables**
- ✔ **Ce que signifie DNS et pourquoi c'est important**
- ✔ **Comment fonctionne la sécurité DNS et les types d’attaques qu’elle permet de réduire**
- ✔ **Comment installer Quad9 sur vos appareils et ordinateurs Android**

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considerer

Les outils ont été soigneusement choisis en fonction de normes mondiales reconnues, et ils ne sont présentés ici dans aucun ordre particulier ou priorité recommandée.

4.1 Antivirus

Il est important d’utiliser des antivirus en temps réel, car ils vérifient les virus au moment où ils se produisent et peuvent ainsi les éliminer avant qu’ils ne puissent causer des dommages. De plus, les antivirus sont mis à jour parallèlement au développement de la protection contre les nouveaux virus.

4.2 Bloqueurs de publicités

Certaines publicités ou messages en ligne qui apparaissent lors de la navigation sur un site Web sont utiles ; toutefois, d’autres peuvent contenir du code malveillant et risquent d'infecter votre ordinateur avec des logiciels malveillants si vous cliquez sur l’annonce. Un bloqueur d’annonces peut être utilisé pour empêcher l’apparition de publicités sur les pages Web, ce qui offre une protection supplémentaire lors de la navigation.

4.3 Sécurité DNS

La sécurité DNS utilise le système de noms de domaine (qui est l’équivalent Internet d’un annuaire téléphonique) pour traduire le nom de site Web texte (nom de domaine) d’un utilisateur dans le navigateur en un ensemble unique de nombres (adresse IP), que les ordinateurs comprennent.

Un grand nombre d'attaquants tentent d'utiliser des noms de domaine de site web similaires pour faire croire aux victimes qu'elles se connectent à un site légitime. Ces sites peuvent ressembler au vrai nom du site Web, mais une inspection plus approfondie peut révéler des différences.

Ainsi, par exemple, l'URL légitime d'une entreprise peut ressembler à « www.mygreatwidgets.com », tandis que l'URL factice pourrait ressembler à « www.rnygreatwidgets.com ».

Les pare-feu DNS, qui constituent un type de sécurité DNS, peuvent aider à prévenir les virus et les attaques de hameçonnage, car ils vérifient si l'adresse IP du site Web demandé est connue pour abriter du code malveillant. Le cas échéant, l'accès à ce site sera bloqué. Les utilisateurs peuvent implémenter des services de filtrage DNS sur leurs systèmes à l'aide des outils de cette sous-catégorie pour empêcher l'accès à des sites Web malveillants connus.

Les sous-catégories de boîtes à outils fournissent des outils pour les systèmes couramment utilisés. Pour bénéficier d'une aide, effectuez des recherches ou posez des questions sur le Forum communautaire de la GCA, **dans la catégorie Prévenir le hameçonnage et les logiciels malveillants** ou auprès de **la communauté des petites entreprises**.

Liens Prévenir le hameçonnage et les logiciels malveillants:

Boîte à outils: ***outils Prévenir le hameçonnage et les logiciels malveillants***
https://gcatoolkit.org/fr/petites-entreprises/prevenir-lhameconnage-et-les-logiciels-malveillants/

Forum communautaire: catégorie Prévenir le hameçonnage et les logiciels malveillants
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/prevent-phishing-and-viruses/

Communauté des petites entreprises
https://community.globalcyberalliance.org/c/community-discussions/small-business-community/

Sauvegarder et récupérer

Quel problème cette boîte à outils résout-elle?

La perte ou la corruption de données peut être due à une cyberattaque (comme ransomware) ou par une défaillance ou un vol d'équipement, une erreur humaine, des dommages accidentels, un incendie ou une inondation. Quelle que soit la cause, l'impact de la perte de données ou des temps d'arrêt de l'équipement peut avoir un impact sérieux sur la productivité et la rentabilité de votre entreprise.

Une sauvegarde est une copie de vos données, stockées à un emplacement différent des données

d’origine, qui peut vous aider à récupérer vos informations après une attaque ou une perte de données. Le fait d’avoir des sauvegardes régulières sur et hors ligne facilitera une récupération plus rapide de la perte de données ou de la corruption des données. Les deux sont importantes car les sauvegardes en ligne sont définies pour sauvegarder automatiquement sur un réseau, tandis que les sauvegardes hors connexion nécessitent le branchement puis la suppression d’un périphérique externe (par exemple, un USB ou un disque dur) pour le stockage physique ailleurs (ce qui permet également de se prémunir contre la sauvegarde par inadvertance des données déjà corrompues).

Qu’est-ce que cette boîte à outils vous aidera à accomplir?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux:

- ✔ **Pourquoi les sauvegardes sont importantes pour votre entreprise, en particulier dans le cadre de la récupération d’une attaque de ransomware**
- ✔ **Comment activer la sauvegarde complète sur votre ordinateur Windows ou Mac**

Comment utiliser la boîte à outils

Utilisez les outils de la ***boîte à outils Sauvegarde et récupération*** pour vous assurer que vos systèmes sont régulièrement sauvegardés, à un niveau et une fréquence appropriés au type de données conservées.

Quelles données sauvegarder ? Cela dépend de vos informations et du risque présenté par leur perte. Si vous avez créé un inventaire dans la boîte à outils Identifier vos appareils et applications, utilisez-le comme guide et liste de contrôle et mettez-le à jour au fur et à mesure.

Une fois que vous avez terminé la mise à jour de la boîte à outils Sauvegarde et récupération, mettez à jour votre liste de vérification de sécurité et définissez un rappel pour un examen périodique afin de vous assurer que votre stratégie reste appropriée pour votre entreprise.

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considérer

Un ransomware est une méthode d’attaque qui est devenue un problème sérieux pour les petites entreprises. Un ransomware est un type de logiciel malveillant qui infecte les ordinateurs et bloque l’accès aux données. L’auteur exige le paiement, parfois sous forme de cryptomonnaie (c’est-à-dire, sous forme de bitcoins qui sont moins faciles à retracer que les transferts traditionnels), en promettant que les données seront restaurées une fois la rançon reçue. Grâce aux sauvegardes de vos données, vous avez la garantie de pouvoir accéder à vos informations si vous êtes victime de ransomware.

5.1 Sauvegarder les systèmes d'exploitation

Le fait d'avoir une stratégie de sauvegarde solide qui inclut des sauvegardes en ligne et hors ligne facilite la récupération plus rapide des pertes de données ou de la corruption des données.

- Les différents jeux de données que vous détenez doivent être classés dans l'inventaire (reportez-vous à la boîte à outils Identifier vos appareils et applications pour aider à créer un inventaire).
- Envisagez l'utilisation du chiffrement pour les informations sensibles (reportez-vous à la boîte à outils Mettre à jour vos défenses pour plus d'informations sur le chiffrement).
- Mettez en œuvre une approche sensée pour sauvegarder chaque ensemble de données après avoir tenu compte de l'« impact d'une perte » pour chacun d'eux. L'impact de la perte peut affecteur la réputation ou les finances, ou avoir un impact d'ordre juridique.

Dans la sous-catégorie Sauvegarder les systèmes d'exploitation, vous trouverez des instructions pour les sauvegardes sur les systèmes d'exploitation courants. Si le vôtre n'est pas inclus, recherchez de l'aide via le site Web de votre fournisseur ou posez une question dans la **catégorie Sauvegarde et récupération** sur le Forum communautaire de la GCA.

Assurez-vous également d'avoir un plan de récupération après sinistre, qui vous permet de récupérer les systèmes critiques à la suite d'une catastrophe (en cas de catastrophe accidentelle ou naturelle). L'utilisation d'un plan permet de minimiser le temps de récupération et les dommages causés aux systèmes, protège contre les responsabilités potentielles et peut également améliorer la sécurité. Il existe de nombreux modèles et guides pour l'élaboration d'un plan disponible en ligne. Veillez à le tenir à jour et à réaliser des scénarios fictifs pour exercer le plan, et vous assurer que tout le monde sait comment le mettre en œuvre.

Liens Sauvegarde et récupération:

Boîte à outils: ***outils Sauvegarde et récupération***
https://gcatoolkit.org/fr/petites-entreprises/sauvegarder-et-recuperer/

Forum communautaire: **catégorie Sauvegarde et récupération**
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/back-up-and-recover/

Protéger vos e-mails et votre réputation

Quel problème cette boîte à outils résout-elle?

Les e-mails sont souvent utilisés comme point de départ d'une cyberattaque. Il est extrêmement rapide et peu coûteux d'envoyer des milliers d'e-mails à des destinataires peu méfiants dans l'espoir que certains d'entre eux croient qu'ils sont authentiques et cliquent sur le lien du site web malveillant ou téléchargent la pièce jointe dangereuse.

L'une des techniques utilisées par les cybercriminels consiste à faire croire que l'e-mail a été envoyé d'une source légitime, comme votre institution financière, un client, un partenaire d'affaires ou une autre organisation familière. L'une de ces techniques est connue sous le nom d'usurpation de domaine de messagerie. Dans ce cas de figure, l'adresse e-mail « usurpée » utilisée est exactement la même que la véritable adresse, ce qui donne l'impression que le message a effectivement été envoyé par cette organisation, et donne au destinataire peu de raisons de soupçonner une fraude.

Si votre domaine de messagerie d'entreprise (la partie de votre adresse e-mail après le « @ ») est compromise, cela peut avoir de graves conséquences pour vous, vos clients et la chaîne d'approvisionnement. Si ce destinataire de l'e-mail a agi sur l'e-mail parce qu'il croyait sincèrement qu'il venait de vous, cela peut entraîner une infection de son système informatique par une certaine forme de logiciels malveillants ou de ransomware. Le criminel serait également en mesure de prendre le contrôle de vos systèmes et de trafiquer vos coordonnées bancaires, de sorte que les clients effectuent des paiements sur d'autres comptes en pensant qu'il s'agit du vôtre.

La boîte à outils Protéger vos e-mails et votre réputation fournit des conseils et des outils pour vous protéger contre ce type de menace, notamment en vous guidant au cours de l'utilisation d'une norme de messagerie connue sous le nom de DMARC (Domain-based Authentication, Reporting, and Conformance, authentification, reporting et conformité basés sur le domaine). DMARC est un moyen efficace d'empêcher les spammeurs et les hameçonneurs d'utiliser les domaines de l'entreprise pour mener des cyberattaques dangereuses. Elle permet de vérifier que l'expéditeur d'un e-mail a le droit d'utiliser votre domaine de messagerie et d'envoyer des e-mails.

Les attaquants peuvent également configurer des sites Web « similaires ». Par exemple, le véritable domaine « BestBusiness.com » peut être usurpé en utilisant la forme « BestBusiness.com » ou « BestBusiness.net » pour inciter les clients ou les utilisateurs à les visiter.

Si vos domaines de messagerie ou de site Web sont usurpés, cela pourrait endommager votre réputation et votre marque, ainsi que nuire à vos clients. L'utilisation des outils de Protéger vos e-mails et votre réputation permet d'identifier et de prévenir l'usurpation d'identité.

Qu’est-ce que cette boîte à outils vous aidera à accomplir?

Après avoir suivi les étapes de cette boîte à outils, vous comprendrez mieux:

- ✔ **Ce que signifie le DMARC, pourquoi il est important et quelles attaques il atténue**
- ✔ **Le guide de configuration de DMARC de la GCA**
- ✔ **Comment vérifier votre propre domaine de messagerie pour voir si DMARC est activé**

Comment utiliser la boîte à outils

Utilisez les outils de la ***boîte à outils Protéger vos e-mails et votre réputation*** pour vous assurer que votre entreprise est protégée contre l’usurpation de domaine de messagerie par la mise en œuvre de DMARC et identifier les domaines potentiels de sites Web similaires.

Mettez à jour votre liste de vérification de sécurité une fois qu'elle est terminée et encouragez vos clients et votre chaîne d’approvisionnement qui utilisent leur propre domaine à faire de même, car l’efficacité de DMARC dépend à la fois de l’expéditeur et du récepteur l'ayant mis en œuvre.

Navigation dans les sous-catégories de boîtes à outils et informations supplémentaires à considerer

6.1 Mettre en place DMARC

Utilisez les outils de cette sous-catégorie pour en savoir plus sur DMARC, vérifiez si votre domaine de messagerie est protégé par DMARC et, dans l’affirmative, à quel niveau.

6.2 Comprendre les rapports DMARC

Une fois qu’une stratégie DMARC aura été configurée sur votre domaine de messagerie, vous commencerez à recevoir des rapports indiquant comment votre domaine de messagerie est utilisé. Ceux-ci peuvent être difficiles à comprendre dans leur format brut.

Les outils de la sous-catégorie Comprendre les rapports DMARC aident à fournir une interprétation et une identification plus rapide des activités frauduleuses. Cela vous permet de passer en toute confiance du niveau de stratégie « aucun » à « quarantaine », puis au plus haut niveau « rejet ». Il est également important de tenir compte de toute organisation ou service de messagerie autorisé à envoyer des e-mails en votre nom, tels que les services de marketing par e-mail, et de vérifier s’ils ont mis en œuvre DMARC.

Ce n’est que lorsque votre domaine de messagerie a atteint le niveau « rejet » que vous bénéficiez pleinement de DMARC.

6.3 Protection des marques commerciales

Les fraudeurs peuvent enregistrer des domaines qui ressemblent beaucoup à votre propre domaine dans l'espoir que les gens cliqueront sur leur site. Utilisez ces outils pour identifier les domaines qui tentent d'imiter le vôtre, ainsi que les domaines qui contiennent du hameçonnage ou des contenus malveillants ciblant votre domaine.

Pour obtenir un soutien supplémentaire lors de la mise en œuvre de DMARC, consultez le **Forum de DMARC** ou **la catégorie Protéger vos e-mails et votre réputation** dans le Forum communautaire de la GCA.

Liens Protéger vos e-mails et votre réputation:

Boîte à outil: ***outils Protéger vos e-mails et votre réputation***
https://gcatoolkit.org/fr/petites-entreprises/proteger-vos-emails-et-votre-reputation/

Forum communautaire: Forum de DMARC
https://community.globalcyberalliance.org/c/dmarc/

Catégorie Protéger vos e-mails et votre réputation
https://community.globalcyberalliance.org/c/cybersecurity-toolbox/protect-your-email-and-reputation

Glossaire des termes

Glossaire de certains termes couramment utilisés relatifs à la cybersécurité. Certains de ces termes ont été inclus dans les chapitres du Manuel de la cybersécurité de la GCA pour les petites entreprises, tandis que d'autres sont fournis à titre d'informations supplémentaires si vous souhaitez explorer davantage ces concepts par vous-même.

compte Se réfère généralement à l'accès à un système informatique ou un service en ligne, nécessitant généralement un mot de passe pour entrer.

adversaire Une personne, un groupe, une organisation ou un gouvernement qui mène ou a l'intention de mener des activités préjudiciables.

antivirus Logiciel conçu pour détecter, arrêter et supprimer les virus et autres types de logiciels malveillants.

application (appli) Programme conçu pour effectuer des tâches spécifiques. Appli fait souvent référence aux programmes téléchargés sur les appareils mobiles.

actif Une personne, une structure, une installation, de l'information et des dossiers, des systèmes et des ressources en technologie de l'information, du matériel, des processus, des relations ou une réputation qui a de la valeur. Tout ce qui est utile et qui contribue à la réussite de quelque chose (par exemple une mission organisationnelle) est considéré comme un élément de valeur ou une propriétés auquel/à laquelle une valeur peut être attribuée.

attaque Tentative d'accès non autorisé aux services, aux ressources ou aux informations d'un système, ou toute tentative de compromission de l'intégrité du système. Acte intentionnel de contournement d'un ou plusieurs services de sécurité ou contrôles d'un système d'information.

signature d'attaque Modèle caractéristique ou distinctif qui peut être recherché ou qui peut être utilisé afin d'établir un lien avec des attaques précédemment identifiées.

surface d'attaque Ensemble de façons dont un adversaire peut entrer dans un système et potentiellement causer des dommages. Caractéristiques d'un système d'information qui permettent à un adversaire de sonder, d'attaquer ou de maintenir sa présence dans le système d'information.

attaquant Acteur malveillant qui cherche à exploiter les systèmes informatiques avec l'intention de changer, détruire, voler ou désactiver leurs informations, puis d'exploiter le résultat.

authentification Processus de vérification de la véritable identité d'une personne qui tente d'accéder à un ordinateur ou à un service en ligne. Concerne également la source et l'intégrité des données, de l'utilisateur, du processus ou de l'appareil.

porte dérobée Moyen secret pour les cybercriminels d'accéder à un système informatique sans y être autorisé.

sauvegarde Copie de vos données, stockées à un emplacement différent des données d'origine, qui peut vous aider à récupérer vos informations après une attaque ou une perte de données.

sauvegarder Faire une copie des données stockées sur un ordinateur ou un serveur afin de réduire l'impact potentiel d'une défaillance ou d'une perte.

bot Ordinateur ou appareil connecté à Internet qui a été secrètement compromis avec du code malveillant pour effectuer des activités sous la commande et le contrôle d'un administrateur distant.

botnet Réseau d'appareils infectés (bots), connectés à Internet, utilisé pour commettre des cyberattaques coordonnées à l'insu de leur propriétaire.

violation Incident au cours duquel les données, les systèmes informatiques ou les réseaux sont accessibles ou affectés de manière non autorisée.

attaque de force brute Utilisation d'une puissance de calcul pour entrer automatiquement un grand nombre de combinaison de valeurs, généralement afin de découvrir les mots de passe et d'accéder aux systèmes.

bogue Défaut, défaillance, faille ou imperfection inattendue et relativement mineure dans un système ou un appareil d'information.

configuration Disposition des composants logiciels et matériels d'un système informatique ou d'un appareil.

configuration Processus de configuration d'un logiciel ou d'un appareil pour un ordinateur, un système ou une tâche spécifique.

cyberattaque Tentative malveillante de nuire, de perturber ou d'accéder sans y être autorisé à des systèmes informatiques, des réseaux ou des appareils, par des moyens cybernétiques.

cyberincident Le plus souvent, une violation des règles de sécurité d'un système ou d'un service. Tentatives d'accès non autorisé à un système et/ou aux données, utilisation non autorisée de systèmes pour le traitement ou le stockage de données, modifications d'un logiciel ou d'un matériel de firmware de systèmes sans le consentement des propriétaires du système, perturbation malveillante et/ou déni de service.

cybersécurité Protection des appareils, des services et des réseaux (et des informations qu'ils contiennent) contre le vol ou les dommages.

cryptomonnaie Argent numérique. La cryptomonnaie est stockée dans un portefeuille numérique (en ligne, sur votre ordinateur ou sur d'autres matériels). En règle générale, la cryptomonnaie n'est pas soutenue par un gouvernement, et elle ne bénéficie donc pas des mêmes protections que l'argent stocké dans une banque.

attaque par dictionnaire Type d'attaque de *force brute dans* laquelle l'attaquant utilise des mots de dictionnaire, des phrases ou des mots de passe courants connus comme des suppositions.

empreinte numérique Empreinte d'informations numériques laissées derrière elle par l'activité en ligne d'un utilisateur.

refus de service (DoS) Attaque dans laquelle les utilisateurs légitimes se voient refuser l'accès aux services informatiques (ou aux ressources), généralement en raison d'un surcharge de demandes sur le service.

appareil Une partie de matériel informatique conçue pour une fonction spécifique. Il s'agit notamment des ordinateurs portables, téléphones mobiles ou imprimantes.

DMARC Signifie Domain-Based Message Authentication, Reporting and Conformance (Authentification des messages basée sur un domaine, génération de rapports et conformité). DMARC est un mécanisme qui permet aux expéditeurs et aux récepteurs de surveiller et d'améliorer la protection de leur domaine contre les e-mails frauduleux.

usurpation de domaine de courrier électronique Technique utilisée par les cybercriminels dans le cadre de laquelle l'adresse e-mail « usurpée » utilisé est exactement la même que la véritable adresse, ce qui donne l'impression d'un envoi par l'organisation concernée.

chiffrement Convertir des données dans une forme qui ne peut pas être facilement comprise par des personnes non autorisées.

pare-feu Périphérique matériel/logiciel ou programme logiciel qui limite le trafic réseau selon un ensemble de règles déterminant les accès autorisés ou non.

pirate Personne qui viole la sécurité informatique pour des raisons malveillantes, pour recevoir des félicitations ou pour un gain personnel

matériel Un ordinateur, ses composants et son équipement connexe. Le matériel comprend des disques durs, des circuits intégrés, des écrans d'affichage, des câbles, des modems, des haut-parleurs et des imprimantes.

menace intérieure (interne) Personne ou un groupe de personnes ayant accès et/ou une connaissance privilégiée d'une entreprise, d'une organisation ou d'une société, et qui pourrait présenter un risque potentiel en enfreignant les politiques de sécurité dans l'intention d'entraîner un préjudice.

Internet des objets (IoT) Désigne la capacité des objets du quotidien (plutôt que des ordinateurs et des appareils) à se connecter à Internet. Les bouilloires, les réfrigérateurs et les téléviseurs en sont des exemples.

intrusion Acte non autorisé de contournement des mécanismes de sécurité d'un réseau ou d'un système d'information.

système de détection d'intrusion (IDS) Programme ou appareil utilisé pour détecter qu'un attaquant a accédé ou a tenté d'accéder aux ressources informatiques sans en avoir l'autorisation.

système de détection d'intrusion (IPS) Système qui bloque également les accès non autorisés lorsqu'ils sont détectés.

enregistreur de frappes Logiciel ou matériel qui suit les frappes et les événements du clavier, généralement en secret, pour surveiller les actions de l'utilisateur d'un système d'information.

malvertising Utilisation de la publicité en ligne comme méthode de livraison de logiciels malveillants.

logiciel malveillant Expression qui inclut les virus, les chevaux de Troie, les vers ou tout code ou contenu pouvant avoir un impact négatif sur les organisations ou les personnes. Logiciel destiné à infiltrer et endommager ou désactiver les ordinateurs.

atténuation L'application d'une ou de plusieurs mesures visant à réduire la probabilité d'un événement indésirable et/ou à en diminuer les conséquences.

réseau Deux ordinateurs ou plus liés afin de partager des ressources.

menace extérieure (externe) Une personne ou un groupe de personnes externes à une organisation qui ne sont pas autorisées à accéder à ses biens et qui présentent un risque potentiel pour l'organisation et ses biens.

mot de passe Une chaîne de caractères (lettres, nombres et autres symboles) utilisée pour authentifier une identité ou vérifier l'autorisation d'accès.

craqueurs de mots de passe Programmes conçus pour deviner un mot de passe, souvent en testant des combinaisons couramment utilisées ou en utilisant un nom d'utilisateur et un mot de passe obtenus à partir d'un compte qui a été piraté.

gestionnaires de mots de passe Programmes qui permettent aux utilisateurs de générer, stocker et gérer les mots de passe dans un seul emplacement en toute sécurité.

correction Application de mises à jour au firmware ou au logiciel pour améliorer la sécurité et/ou les fonctionnalités.

pentest (test de pénétration) Test autorisé d'un réseau informatique ou d'un système conçu pour rechercher les faiblesses de sécurité afin qu'elles puissent être corrigées.

Informations d'identification personnelle / Informations personnellement identifiables (PII) Les informations qui permettent de déduire directement ou indirectement l'identité d'une personne.

pharming Attaque contre l'infrastructure réseau qui entraîne la redirection d'un utilisateur vers un site web illégitime malgré la saisie de l'utilisateur dans l'adresse correcte.

phishing E-mails de masse non ciblés envoyés à de nombreuses personnes demandant des informations sensibles (comme les coordonnées bancaires) ou les encourageant à visiter un faux site Web. Uneforme numérique d'ingénierie sociale pour tromper les individus en leur fournissant des informations sensibles.

message en clair Informations non chiffrées.

serveur proxy Serveur qui agit comme intermédiaire entre les utilisateurs et d'autres serveurs, et qui valide les demandes des utilisateurs.

ransomware Logiciel malveillant qui rend les données ou les systèmes inutilisables jusqu'à ce que la victime effectue un paiement.

récupération Activités après un incident ou un événement visant à rétablir les services et les opérations essentiels à court et moyen terme, et à rétablir pleinement toutes les capacités à plus long terme.

résilience Capacité de s'adapter aux conditions changeantes et de se préparer, de résister et de se remettre rapidement des perturbations.

restaurer Récupération des données à la suite d'une défaillance ou d'une perte informatique.

évaluation des risques Processus d'identification, d'analyse et d'évaluation des risques ainsi que des préjudices potentiels afin d'informer les priorités, d'élaborer ou de comparer les actions et d'éclairer la prise de décisions.

informations de sécurité et gestion d'événements (SIEM) Processus dans lequel les informations réseau sont regroupées, triées et corrélées afin de détecter les activités suspectes.

smishing Hameçonnage par SMS - Messages texte de masse envoyés aux utilisateurs en leur demandant des informations sensibles (par exemple, des coordonnées bancaires) ou en les encourageant à visiter un faux site Web.

signature Tendance reconnaissable et distinctive. Les types de signatures incluent: signature d'attaque, signature numérique, signature électronique.

ingénierie sociale Manipuler les gens pour qu'ils effectuent des actions spécifiques ou divulguent des informations qui sont utiles à un attaquant.

logiciel Se réfère aux programmes qui dirigent le fonctionnement d'un ordinateur ou le traitement des données électroniques.

spam Abus des systèmes de messagerie électronique pour envoyer sans discrimination des messages non sollicités en grande quantité.

spear-phishing Forme plus ciblée d'hameçonnage, où l'e-mail est conçu de façon à faire croire qu'il est envoyé par une personne connue du destinataire et/ou en qui il a confiance.

spoofing Usurpation de l'adresse d'envoi d'une transmission pour obtenir l'entrée illégale [non autorisée] dans un système sécurisé. Se faire passer pour, escroquer, tricher et imiter sont des formes de spoofing.

logiciel espion Programme malveillant qui transmet des informations sur les activités d'un utilisateur d'ordinateur à une partie externe.

chaîne d'approvisionnement Système d'organisations, de personnes, d'activités, d'informations et de ressources, pour la création et le déplacement de produits, y compris les composants et/ou les services des fournisseurs jusqu'à leurs clients.

système Désigne généralement un système d'un ou de plusieurs ordinateurs ou appareils qui entrent, introduisent, traitent et stockent des données et des informations.

administrateur système (admin) Personne qui installe, configure, dépanner et entretient les configurations du serveur (matériel et logiciel) pour assurer leur confidentialité, leur intégrité et leur disponibilité ; gère également les comptes, les pare-feu et les correctifs ; responsable du contrôle d'accès, des mots de passe, de la création et de l'administration de comptes.

menace Quelque chose qui pourrait causer du tort à un système ou à une organisation.

acteur de menace Une personne, un groupe, une organisation ou un gouvernement qui mène ou a l'intention de mener des activités préjudiciables.

cheval de Troie Programme informatique qui se fait passer pour un logiciel légitime, mais avec une fonction cachée qui est utilisée pour pirater l'ordinateur de la victime. Un type de programme malveillant.

double authentification (2FA) Utilisation de deux composants différents pour vérifier l'identité revendiquée par un utilisateur. Également connue sous le nom d'authentification multifacteur.

réseau privé virtuel (VPN) Réseau crypté souvent créé pour permettre des connexions sécurisées pour les utilisateurs distants, par exemple dans une organisation dont les bureaux sont situés à plusieurs endroits.

virus Programme informatique qui peut se répliquer, infecter un ordinateur sans autorisation ou connaissance de l'utilisateur, puis se propager ou se diffuser sur un autre ordinateur. Un type de programme malveillant.

vulnérabilité Faiblesse, ou défaut, dans un logiciel, un système ou un processus. Un attaquant peut chercher à exploiter une vulnérabilité pour obtenir un accès non autorisé à un système.

whaling Attaques de hameçonnage hautement ciblées (sous l'apparence d'e-mails légitimes) qui s'adressent aux cadres supérieurs.

ver Programme autonome, auto-propageant et indépendant qui utilise des mécanismes de réseautage pour se propager. Un type de programme malveillant.

Définitions compilées à partir des ressources produites par:

British Standards Institute

https://www.bsigroup.com/en-GB/Cyber-Security/Glossary-of-cyber-security-terms/

National Cyber Security Centre (NCSC -ROYAUME-UNI)
https://www.ncsc.gov.uk/information/ncsc-glossary

National Initiative for Cybersecurity Careers and Studies (NICCS - États-Unis)
https://niccs.us-cert.gov/about-niccs/cybersecurity-glossary

Ressources supplémentaires:

Australian Cyber Security Centre Glossary
https://www.cyber.gov.au/acsc/view-all-content/glossary

Connaissances mondiales
https://www.globalknowledge.com/us-en/topics/cybersecurity/glossary-of-terms/

SANS Institute Glossary of Security Terms
https://www.sans.org/security-resources/glossary-of-terms/