Lexique

www.sharp.fr

SHARP
Be Original.

Plan d'action

Appareils protégés

Toujours être vigilant!

Le langage complexe de la sécurité simplifié

La cybercriminalité peut prendre de nombreuses formes différentes pour les entreprises connectées.
Comprendre à quoi ressemble une attaque, comment elle peut se matérialiser et quelles implications elle peut avoir sur votre entreprise ne doit pas être sous-estimé.

Mais pour de nombreuses petites et moyennes entreprises (PME), lutter contre la menace n'est pas la première étape. Pour véritablement vous protéger contre les cybermenaces, vous devez comprendre le véritable sens de tout ce jargon.

Pour permettre une meilleure compréhension, nous en avons décrypté une partie pour vous.

Sécurité du réseau

Le cadenas d'acier qui protège vos informations

De la même manière que vous enfermez vos biens les plus précieux dans un coffre-fort ou que vous attachez votre vélo à un mur, la sécurité du réseau protège les informations sensibles de votre entreprise.

Essentielle sur tout réseau d'entreprise, vos mesures de sécurité doit inclure un système de détection d'intrusion (IDS), conçu pour surveiller et identifier les menaces potentielles, les activités suspectes, et les tentatives d'accès non autorisées sur les appareils connectés, tels que les ordinateurs portables et les imprimantes.

Pertes de données

Un peu comme si quelqu'un vous volait votre portefeuille dans le train

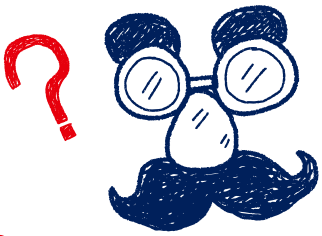
Vous ne savez peut-être pas toujours que cela s'est produit jusqu'à ce qu'il soit entre de mauvaises mains. Une fuite de données se produit lorsque des informations sensibles, qu'elles appartiennent à l'entreprise ou à un client, sont volées par des personnes malveillante (cybercriminels). Cela peut se produire à l'insu de l'entreprise ou sans son autorisation. Une fuite de données peut finalement entraîner une perte de confiance de la part des clients ou des utilisateurs, une atteinte à la réputation de la marque et même des amendes coûteuses.

Phishing, vishing et smishing

En gros : un hacker déguisé en votre patron, client, meilleur ami ou magasin de vêtements

Ces types d'attaques ne sont pas toujours évidents à l'œil nu, mais ils sont courants. En fait, environ 90 % des cyberattaques commencent par du phishing (e-mail), tandis que le taux d'attaques par smishing (SMS) et par vishing (appel vocal) est également en augmentation. Nous avons tous vu ces e-mails sournois apparaître dans notre dossier indésirable. Le phishing, le smishing et le vishing sont des cyberattaques qui incitent les utilisateurs à cliquer sur des e-mails, à répondre à des messages, ou répondre à des appels qu'ils jugent légitimes.

Si l'attaque réussit, les employés seront alors incités, sans le savoir, à fournir des informations sensibles telles que le mot de passe de leur réseau.



Malware

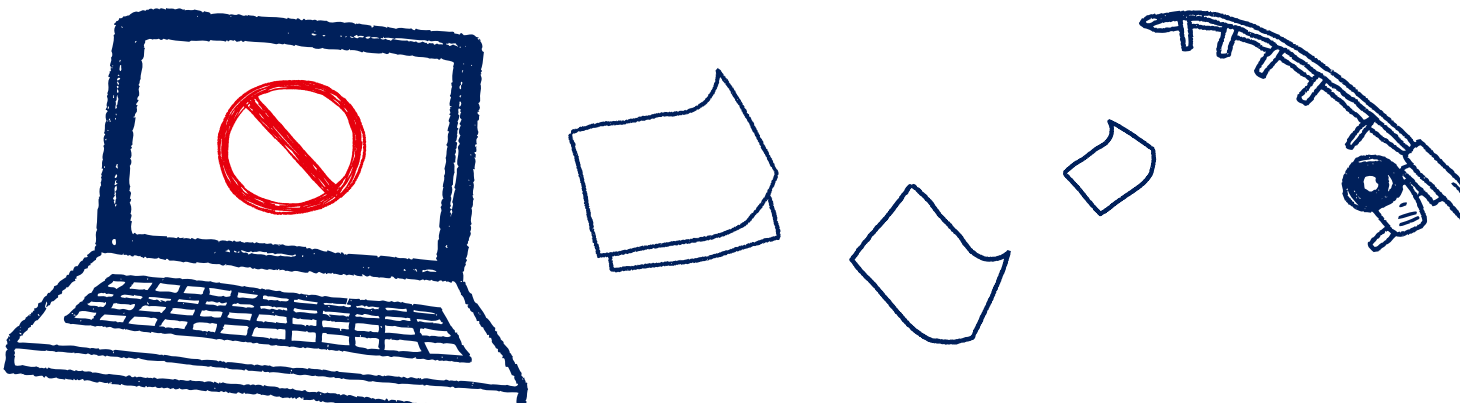
Le genre de logiciel malveillant, conçut uniquement avec de mauvaise intentions

« Malware » est l'abréviation de logiciel malveillant. Il s'agit d'un logiciel conçu par des cybercriminels pour endommager les systèmes réseau de votre entreprise et vous empêcher de les utiliser. Après avoir ouvert un e-mail de phishing, cliqué sur un lien suspect ou accédé à un site Web déjà compromis, des logiciels malveillants peuvent infiltrer votre système. Une fois cela fait, les informations stockées sur votre réseau peuvent être exposées aux pirates informatiques, entraînant une escalade des

Ransomware

Vos données prises en ôtages

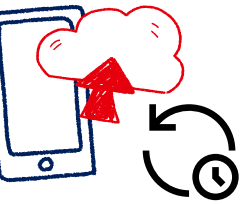
Forme de malware, le ransomware est utilisé par les cybercriminels pour bloquer l'accès aux informations commerciales critiques en les chiffrant (en code). Chaque type d'entreprise connectée possède des données, depuis les dossiers financiers jusqu'aux résultats des tests des patients et aux documents juridiques confidentiels. Y avoir accès est crucial pour le fonctionnement d'une entreprise. Cependant, une fois que le ransomware a infiltré votre réseau, votre entreprise peut perdre cet accès. Pour le récupérer, des rançons (des frais coûteux) doivent souvent être versées au pirate informatique qui a perpétré l'attaque.



Sécurité des points d'accès

Avant tout, assurez-vous que tous vos appareils sont aussi sécurisés que votre ordinateur de bureau

Votre défense numérique ne commence et ne se termine pas avec votre ordinateur. La sécurité des points finaux fait référence au processus consistant à garantir tous vos « points finaux » ; des tablettes aux smartphones et autres appareils connectés à Internet (comme votre imprimante de bureau), disposent d'une protection partagée. Ceux-ci doivent être gérés et surveillés de manière centralisée pour garantir une vision réaliste de votre posture en matière de cybersécurité.



Gestion des patchs

Pensez à mettre à jour le système d'exploitation de votre téléphone

Nous avons probablement tous rencontré ces mises à jour logicielles sur nos téléphones : « mettre à jour maintenant vers Windows 10 » ou « installer iOS 9 999 ». Cependant, ces mises à jour constituent une mesure de sécurité cruciale. La gestion des correctifs est le processus d'application de mises à jour aux logiciels, pilotes et micrologiciels pour protéger les vulnérabilités du réseau. Cela implique de surveiller la conformité, de gérer les applications utilisées par votre entreprise et de garantir que vos systèmes fonctionnent à leur plein potentiel.

Rester en sécurité

Bien que complexe, la compréhension du langage de la cybersécurité est aujourd'hui importante pour toute entreprise connectée.

Parallèlement, Sharp propose une gamme complète de services et de solutions de cybersécurité sur mesure, vous permettant de gérer plus facilement les risques.

Visitez le Real World Security hub

Cryptage

Imaginez toutes vos données, mélangé dans un sac de scrabblea

Comment empêcher quelqu'un de lire un message secret ? Vous mélangez les mots, les lettres et les chiffres. C'est essentiellement ce que fait le cryptage. Il code le « texte brut » – vos données sensibles – en « texte chiffré », ce qui le rend illisible pour toute personne ne disposant pas d'une « clé de déchiffrement », c'est-à-dire le mot de passe que vous utilisez pour accéder à un réseau sans fil sécurisé. Dans une entreprise, le cryptage doit être appliqué à tous les appareils, comme votre téléphone et votre ordinateur portable, afin que le contenu stocké sur chacun ne puisse pas être lu en cas de perte ou de vol de

Réponse aux incidents

Votre plan d'action pour repousser une attaque

Quelle est la première étape lorsque votre entreprise est compromise par une cyberattaque ? Une réponse aux incidents (RI) est l'approche systématique adoptée par les organisations qui souhaitent planifier la manière de répondre et de gérer efficacement les incidents de cybersécurité. Ne pas avoir mis en place une solide approche RI lorsqu'une menace fait surface peut empêcher votre entreprise de la combattre – et est essentielle pour maintenir l'intégrité, la confidentialité et la disponibilité des données commerciales sensibles.