Le guide de base de la cybersécurité pour les professionnels par SilentGuard

Bonjour et merci d'avoir téléchargé ce guide ! Ce que vous avez fait fait est une première étape essentielle : Réaliser l'importance de protéger ses données numériques et prendre des actions concrètes comme télécharger ce livret !

Nous allons voir ici de manière simple et intuitive comment nous allons pouvoir renforcer votre sécurité en ligne. Dans ce livret nous allons donc aborder des conseils directement liés à la cyber sécurité pour les entreprises, et ensuite à la préservation de votre vie professionnelle numérique. Bonne lecture !

En 2021, le cybercrime a coûté 6 000 milliards de dollars américains, un coût qui va passer à 10 500 milliards de dollars vers 2025, avec un risque d'être attaqué qui augmente de plus en plus également. La mise en place d'un système de cybersécurité solide est donc vitale.

1. La cybersécurité de l'entreprise:

a. Pourquoi la cybersécurité est importante pour une entreprise ?

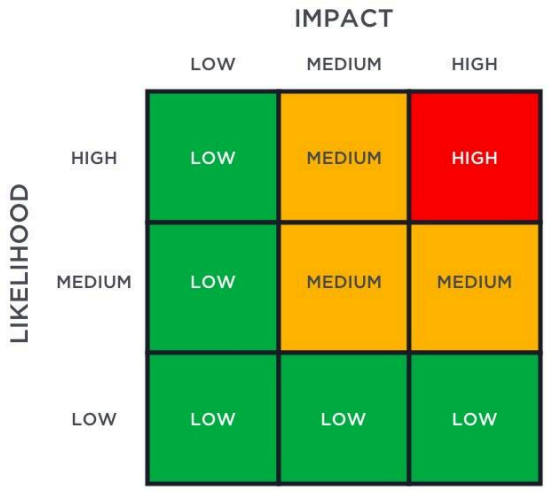
Les entreprises quelles qu'elles soient sont exposées à de très nombreuses menaces. Les comptes peuvent être piratés, les employés peuvent être victimes de hameçonnage (aussi connu comme phishing). Les entreprises peuvent aussi être victimes de rançongiciels (des logiciels qui demandent des rançons pour libérer les systèmes informatiques), mais aussi de différentes fraudes, comme les fraudes aux virements, aux faux conseillers bancaires, au faux support technique. Les données peuvent être volées, le site Internet peut être attaqué (l'apparence serait modifiée, le fonctionnement du site serait arrêté). Enfin, les entreprises peuvent être victimes de virus et de piratages informatiques, et des dommages divers peuvent être portés aux systèmes informatiques. Cela a pour conséquences entre autres la paralysie de l'entreprise, des opportunités commerciales qui sont manquées, une perte de productivité, une baisse de confiance envers l'entreprise ou encore la diffusion des données volées. Cette dernière est l'une des conséquences les plus connues. On retrouve par exemple la diffusion des données de Strava, une application de fitness qui a rendu public la localisation de soldats, de gardes du corps d'hommes politiques, ou encore d'équipages de sous-marins de la marine française. Il y a aussi eu le piratage des données du site Ashley Madison qui était un site de rencontre permettant à des personnes mariées d'avoir des affaires avec un anonymat complet. Ce piratage a exposé environ 37 millions de personnes infidèles.

b. A quoi ressemble la cybersécurité pour une entreprise ?

La cybersécurité entre les professionnels et les particuliers est différente, elle doit être bien plus complexe. Cette cybersécurité implique de nombreux aspects. Elle doit protéger les différentes ressources de l'entreprise, que ce soit celles présentes sur le site de l'entreprise, mais aussi celles qui sont dans le Cloud et le réseau. Il faut aussi s'intéresser à la fiabilité des fournisseurs tiers de l'entreprise, et des sous-traitants. L'environnement de risque doit être compris, des contrôles d'accès pour les bâtiments et les fichiers doivent être mis en place. Les différentes vulnérabilités et menaces qui existent déjà doivent être prises en compte. Qui plus est, il faut sauvegarder les données, les protéger ainsi que les autres ressources par rapport à des accès non autorisés et à des fuites. Enfin, il faut mettre en place des plans de correction en cas de problèmes.

Pour résumer, il y a un besoin de mesurer les différents risques liés à la cybersécurité et son absence, de mesurer les potentiels pertes et préjudices, comme le vol de propriété intellectuelle, la perte d'argent, l'endommagement de la réputation de l'entreprise…

Pour mesurer ces risques, il faut suivre différentes étapes. D'abord, les différentes ressources doivent être identifiées, et leur priorité doit être définie. Les ressources avec la priorité la plus importante sont celles qui impliquent le plus de risques si elles sont perdues, exposées ou encore endommagées. Il faut ensuite identifier les vulnérabilités, c'est-à-dire les différents points faibles des systèmes qui permettraient à quelqu'un de s'infiltrer. Ensuite, la probabilité des potentiels incidents de sécurité est à évaluer. L'impact de la menace, ie les dommages qui peuvent être causés, doivent être calculés, et il en est de même pour le risque. Finalement, les différentes corrections à apporter au système de cybersécurité actuel sont à planifier.

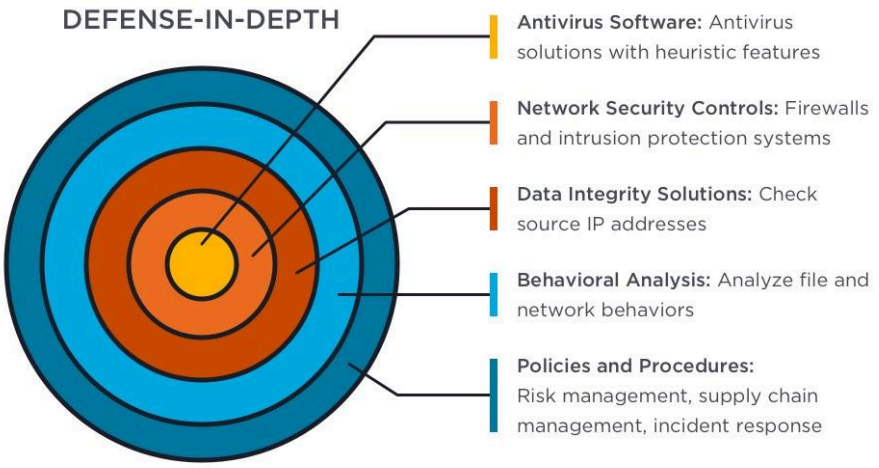


c. Les éléments à mettre en place au sein de l'entreprise en elle-même

Il n'y a pas d'outil de cybersécurité qui soit capable de protéger une entreprise de tous les risques, de toutes les attaques qui peuvent être portées. Il est donc nécessaire d'adopter une approche de défense en profondeur (DEP). Cette approche implique plusieurs couches de protection. Ainsi, si l'une de ces couches venait à tomber, les autres couches resteraient complètement fonctionnelles. Cette approche contient donc plusieurs éléments: un logiciel antivirus, des contrôles de sécurité du réseau, des solutions d'intégrité des données, des analyses comportementales et enfin des stratégies et procédures.

L'antivirus a pour fonction de rechercher et de signaler les activités suspectes sur le système. Les contrôles de sécurité du réseau comprennent les pare-feu et des

systèmes de protection contre les intrusions, qui permettent d'identifier les différentes menaces pour la sécurité, mais aussi de les bloquer à partir des règles de sécurité établies par l'entreprise. Les solutions d'intégrité des données examinent les adresses IP afin de déterminer si la source des fichiers reçus est connue et de confiance. Les analyses comportementales permettent une analyse du comportement des fichiers et des réseaux en utilisant comme standard des comportements "normaux" prédéfinis par l'entreprise, pour pouvoir envoyer des alertes, et/ou effectuer des actions automatiquement pour bloquer la violation du système informatique, ou encore empêcher de la poursuivre. Enfin, les stratégies et procédures sont celles de gestion des risques, de gestion de la chaîne logistique, de réponses aux incidents, …



Mais comment mettre en œuvre cette version de la cybersécurité ? Après tout, le cybercrime subit des changements constants, il faut donc rester sur ses gardes, et mettre à jour les mesures de sécurité régulièrement. Pour se faire, l'entreprise a besoin de suivre une approche systématique. Il faut commencer par analyser les risques, ce qui implique de rester au courant des risques critiques qui peuvent affecter l'entreprise, et donc d'intervenir de la bonne façon pour pouvoir diminuer l'impact potentiel de ces risques. Ensuite, il est nécessaire de faire l'inventaire des ressources, et d'en effectuer la gestion, pour savoir ce que l'entreprise à, pour savoir ce qui est risqué. L'inventaire à effectuer ensuite est celui des vulnérabilités, ce qui permet de savoir quels sont les points faibles, pour pouvoir y faire attention. Suivant cet inventaire, il est nécessaire de déployer la gestion des accès et des identités, pour pouvoir contrôler l'accès aux différents services, aux systèmes, et aux données. Sécuriser ces données est l'étape suivante, car l'ensemble des données doivent être protégées des accès et des utilisations non autorisés. L'étape suivante est la gestion des incidents, c'est-à-dire bien s'occuper de réduire l'impact des différents accidents. Après, vient la sécurité de la chaîne

logistique, où on identifie les potentiels risques des réseaux tiers, comme les différents sous-traitants. Enfin, il faut former les différents salariés, leur apprendre la bonne conduite concernant la cybersécurité.

2. Protéger ses données sur Internet:

a. Comment se protéger sur le net: les comptes et les données

L'entreprise n'est pas la seule à pouvoir prendre des mesures pour protéger les données sensibles, l'employé aussi le peut. Les premières précautions concernent les comptes et les données. Le mot de passe est quelque chose que chaque compte demande. Il faut donc, en créant un nouveau mot de passe, éviter d'utiliser des mots de passe évidents, comme des noms, des prénoms ou des dates de naissances, la vôtre ou ceux d'être chers. De même, il faut privilégier des mots de passe complexes, à savoir écrit avec des majuscules et des minuscules, des chiffres, et des caractères spéciaux. Il est bon également de ne pas utiliser plusieurs fois le même mot de passe, ni les communiquer à d'autres personnes. Enfin, enregistrer ses mots de passe dans un gestionnaire de mots de passe est utile, de même que l'activation de la double authentification. Pour finir, il faut aller dans les paramètres de confidentialité, et activer la fonction permettant de ne pas autoriser le partage de données, et de vérifier qu'il soit bien activé. Il est après tout possible de voir si ce paramètre à été changé sans prévenir.

Pour ce qui est de la connexion aux différentes applications, il vaut mieux privilégier éviter de se connecter à ses comptes professionnels sur des appareils qui n'ont pas été fournis par le service informatique de l'entreprise. Si c'est vraiment nécessaire, alors pensez bien à vous déconnecter des comptes. Enfin, si un compte ou une application n'est plus utilisé, alors il faut penser à les désinstaller. Finalement, il faut donner une priorité en se se connectant aux comptes utilisateurs plutôt qu'aux comptes administrateurs, car s'ils sont pirater, alors toutes les données sont accessibles.

Pour empêcher la perte de données si cela arrive, alors il faut penser à sauvegarder ses données. Pour se faire, il faut utiliser des endroits sûrs, comme des clés USB, des cartes SD, des disques durs en physique, mais aussi le Cloud et le réseau de l'entreprise. Pour chaque option de stockage, il est plus prudent de leur attribuer des utilisations spécifiques, pour éviter la contamination entre les différents moyens de stockage en cas de piratage. Lorsqu'une sauvegarde est effectuée, il

faut faire attention à bien chiffrer ses données. Enfin, il faut attribuer correctement les niveaux d'accès, à savoir les permissions d'accès, les permissions de modifications, entre autres,, mais aussi bien verrouiller les accès des documents confidentiels.

b. Comment se protéger sur le net: les systèmes informatiques

Les systèmes informatiques sont à protéger aussi. Il faut impérativement savoir quels sont les différents systèmes informatiques disponibles, comme les ordinateurs et les téléphones. De plus, il faut faire l'inventaire des différentes applications et logiciels, afin de savoir où on a un compte, et à quoi on est potentiellement toujours connecté. De plus, quand une nouvelle application est à télécharger, il faut toujours penser à passer par les sites et les magasins officiels des applications, afin de télécharger la bonne version, et pas une contaminée par un virus ou un cheval de Troie. Il en est de même pour les mises à jour des systèmes d'exploitation et des applications, qui sont à effectuer dès que possible et, encore une fois, toujours depuis les sites officiels des éditeurs.

De plus, pour protéger les systèmes, il faut bien utiliser les antivirus et les pare-feu, et bien les mettre à jour. De plus, il faut bien faire attention à ne pas utiliser de clés USB ou de disques durs inconnus? Cliquer sur les liens ou sur les pièces jointes douteuses n'est aussi pas conseillé. Pour vérifier la légitimité des liens est à vérifier, notamment en passant la souris dessus, et en vérifiant les extensions des pièces jointes étranges. Pour ce qui est des mails et SMS suspects, il ne faut pas y répondre, mais contacter l'envoyeur par d'autres moyens. Enfin, il faut bien utiliser des filtres contre le hameçonnage, et les filtres anti-spam, des navigateurs Internet. Il s'agit d'une fonction qui permet d'avertir l'utilisateur au cas où.

c. Comment se protéger sur le net: autres protections à mettre en place

Ces protections ne sont pas les seules à devoir être mises en place, il y en a beaucoup d'autres. Il faut notamment faire attention au WiFi public. Ne pas se connecter aux réseaux publics est le plus prudent, et surtout ne pas les utiliser pour effectuer des opérations sensibles, comme remplir ses informations bancaires, effectuer des virements, entre autres. S'il est nécessaire d'utiliser ces réseaux, alors il est prudent d'utiliser un VPN pour se protéger. De plus, il est prudent de désactiver

les différentes connexions sans fil automatique, comme la connexion au WiFi, ou la connexion Bluetooth. Privilégier la connexion aux réseaux mobiles, comme la 4G et la 5G, des fournisseurs de service.

Enfin, il faut faire attention quand on fait partie d'une entreprise de bien séparer la vie personnelle et la vie professionnelle. Il faut donc ne pas se connecter aux réseaux professionnels en utilisant des équipements personnels, ou non fournis par le service informatique. De la même façon, il ne faut pas se connecter aux réseaux personnels avec des équipements professionnels, sans suivre les directives de l'entreprise liées au télétravail, comme l'utilisation d'un VPN. De plus, utiliser les adresses mails personnelles pour les affaires de l'entreprise est à éviter, de même que l'utilisation de mails professionnels pour les affaires personnelles. Enfin, il faut faire attention à ce que l'on publie sur les réseaux sociaux, faire attention à publier des données confidentielles notamment, ou publier quelque chose portant atteinte à la réputation de l'entreprise.

3. Le cas particulier du hameçonnage:

a. Qu'est-ce que le hameçonnage

Nous allons nous pencher plus particulièrement sur ce qui doit être fait dans le cas des mails de hameçonnage. Cette pratique, aussi connue sous le nom anglais de phishing, consiste à envoyer un mail ou SMS frauduleux qui cherche à pousser les personnes à qui ils sont envoyés à remettre ses données personnelles en se faisant passer pour quelqu'un de confiance et d'autorité, comme une banque, une entreprise connue, voir même le gouvernement.

Pour identifier les mails de hameçonnages, il y a divers moyens. Ils contiennent souvent des offres trop belles pour être vrai, et des objets de mails soit trop alléchants, soit trop alarmistes. L'apparence de ses mails est souvent suspecte, et remplie de fautes d'orthographes. Les pièces jointes sont aussi inattendues, et les adresses d'expéditions sont étranges, et les noms d'expéditeurs inhabituels. Il n'y a pas non plus de personnalisation en fonction de la personne recevant le mail, ces mails souvent étant envoyés en masse. Certaines demandes effectuées dans les mails sont inhabituelles, comme une demande d'envoi d'informations personnelles et/ou confidentielles. Il y a aussi souvent dans les mails des incitations à cliquer sur des liens, ou à télécharger des pièces jointes. Certains utilisent, pour imiter des adresses officielles, l'alphabet cyrillique, les "a" étant différents, même s'ils se ressemblent. Ces mails suspects peuvent aussi être accompagnés, à la réception, d'une notification de la messagerie ou de l'antivirus. Enfin, la plus simple façon de

les identifier, c’est encore de recevoir un mail d’une société ou d’un service dont vous n’utilisez pas les services, ou bien de recevoir les résultats d’un concours auxquels vous n’avez pas participé.

b. Comment se protéger du hameçonnage

Pour se protéger du hameçonnage, il y a plusieurs façons, qu’il vaut mieux utiliser de préférence les uns avec les autres. Pour commencer, ne pas communiquer d' informations sensibles par messagerie ou par téléphone. Par exemple, un conseiller bancaire ne demandera pas par téléphone vos informations bancaires. De plus, il faut toujours vérifier les différents liens. Notamment, il est possible de positionner le curseur de la souris sur le lien pour en voir un aperçu. Si le lien a été ouvert, alors vérifiez l’apparence du site, mais aussi l’adresse qui s’affiche dans le navigateur. Si possible, contacter directement l’organisme dont le mail prétend venir est également prudent. Enfin, pour prévenir de recevoir ses mails par rapport à ses comptes, il faut utiliser des mots de passe qui sont différents les uns des autres, qui ne sont pas évidents, comme un nom ou un prénom, et finalement un mot de passe complexe. Quand vous êtes connectés à vos comptes, alors vérifiez les dates et les heures des dernières connexions aux comptes, afin de vérifier si un accès illégitime a eu lieu. Enfin, activer la double authentification pour ses comptes est plus prudent.

c. Que faire en tant que victime de hameçonnage

Malgré toutes ces précautions, il est toujours possible de devenir victime de hameçonnage. Dans ce cas là, il est possible de contacter l’organisme concerné, à savoir celui dont le mail de hameçonnage prétendait venir. De plus, il vaut mieux agir immédiatement. Par exemple, vous pouvez immédiatement faire opposition aux moyens de paiement auprès de la banque. Il faut bien penser aussi à conserver toutes les preuves du hameçonnage, comme prendre des captures d’écran de tous les mails et les messages. Faire ça permet de rendre plus simple un dépôt de plainte, surtout s’il y a eu une usurpation d’identité, ou des débits bancaires frauduleux. Changer vos mots de passe immédiatement après avoir appris que vous avez été victime est aussi plus prudent. Enfin, il est prudent de signaler tous les messages et les sites douteux que vous rencontrez, notamment à Signal Spam, à Phishing Initiative, ou encore au 33 700 par SMS.

Conclusion :

Il existe de nombreuses menaces pour la sécurité des données des entreprises. Il est donc nécessaire de prendre les bonnes mesures de cybersécurité, que ce soit pour l'entreprise en général, ou pour les employés de manière individuelle.

Nous vous remercions pour avoir suivi ce livret, et espérons que vous pourrez les mettre en place autant que possible.

Sources :

https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/reseaux-sociaux
https://cyber.gouv.fr/bonnes-pratiques-protegez-vous
https://www.entreprises.cci-paris-idf.fr/web/pme/cybersecurite-des-entreprises-quelles-sont-les-reglementations-
https://www.francenum.gouv.fr/magazine-du-numerique/quelles-sont-les-principales-menaces-cyber-pour-les-entreprises-en-2023
https://www.entreprises.gouv.fr/priorites-et-actions/autonomie-strategique/soutenir-linnovation-dans-les-secteurs-strategiques-16
https://www.onelogin.com/fr-fr/learn/what-is-cyber-security
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/comment-reconnaitre-un-mail-de-phishing-ou-dhameconnage
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/hameconnage-phishing