LIVRE BLANC

CYBERSÉCURITÉ

CYBERSÉCURITÉ :

Les différentes méthodes et outils à mettre en place dans votre entreprise.

EQUADEX

DIGITAL FRIENDLY

EDITO

La sécurité informatique est un des sujets les plus complexes auxquels font face les entreprises et les organisations publiques. ***Les cybermenaces sont exponentielles*** et de plus en plus sophistiquées. (Malware, ransomware, phishing, attaque DDOS, attaque par force brute.)

Elles touchent sans distinction **les petites comme les grandes entreprises**, le secteur public autant que le privé. La cybersécurité est désormais considérée comme la ***priorité absolue*** pour près de 90% des responsables informatiques. Et notamment dans la sécurisation des accès à distance, puisque le développement du télétravail s'est accru depuis la crise sanitaire.

Afin de vous aider dans la mise en place ***des bonnes pratiques de cybersécurité***, nous avons rassemblé dans ce livre blanc nos conseils pour vous protéger et vous informer

SOMMAIRE

Quelques chiffres

QUELQUES CHIFFRES

80%

des entreprises **ont subi des attaques** contre leurs systèmes. (Etude Opinion Way)

des employés exercent des *activités professionnelles sur un appareil personnel. (Etude Gartner)*

60%

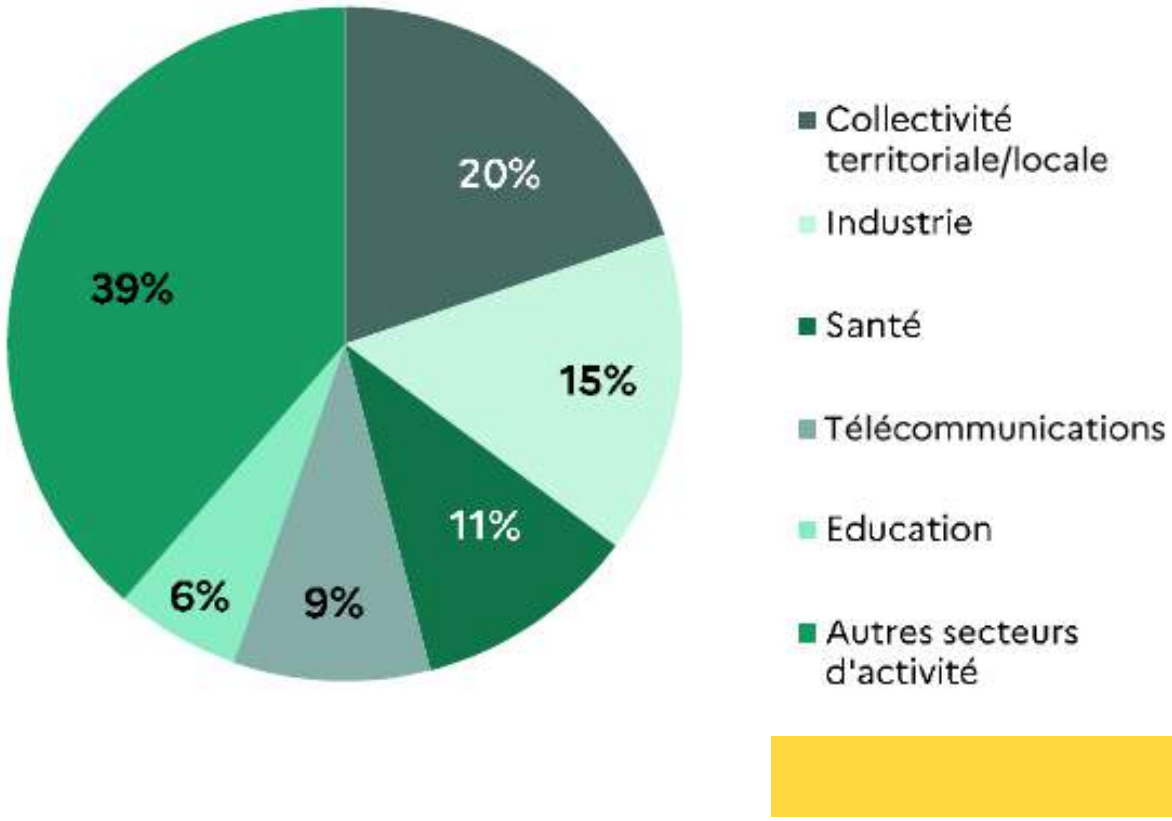
95%

L'erreur humaine est à l'origine de plus de 95% des violations de cybersécurité. (ETC Techsolutions)

des entreprises n'ont **pas de plan de réponse aux incidents de cybersécurité**. (IBM)

77%

QUELQUES CHIFFRES



- SECTEURS D'ACTIVITÉS TOUCHÉS PAR LES RANÇONGICIELS EN 2020 EN FRANCE (ANSSI)

Les solutions à mettre en place

LES SOLUTIONS À METTRE EN PLACE

Les sauvegardes

EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?

Effectuer des sauvegardes régulières permet une restauration rapide de votre activité en cas d'incident, notamment en **cas d'attaque par rançongiciel.**
Votre entreprise peut créer des sauvegardes de ses données importantes de nombreuses façons. Il est nécessaire d'**identifier les données** à sauvegarder. Pour identifier ces données vous devez avoir inventorié préalablement tout votre matériel, puis déterminer quelles données sont essentielles à la poursuite de votre activité. Il est par ailleurs recommandé d'employer plusieurs méthodes. Afin de garantir que les fichiers seront toujours disponibles en cas de nécessité.

La sauvegarde est un processus qui a pour but de *dupliquer et de mettre en sécurité les données* présentes dans un système informatique. On effectue une **copie des données** à un instant précis, puis on va les stocker dans un autre emplacement.

LES SOLUTIONS À METTRE EN PLACE

Les sauvegardes

EFFECTUEZ-VOUS DES SAUVEGARDES RÉGULIÈRES ?

Il existe différentes solutions de sauvegarde sur support physique comme ***l'enregistrement sur disques durs ou sur un NAS*** (Network Attached Storage), en data center, sur bandes magnétiques, etc...
La **sauvegarde en interne** de vos données est *primordiale*.

Cependant, elle n'est pas suffisante. Dans le cas d'un incident majeur dans le périmètre de votre site. Comme un sinistre, un virus sur votre réseau local par exemple vous perdez l'intégralité de vos données. En plus de conserver en local des sauvegardes à jour de vos fichiers et données. **Vous devez toujours stocker au moins une copie hors site.**
Il s'agit de garder à l'esprit que ces sauvegardes peuvent aussi être affectées par un rançongiciel. En effet, de plus en plus de cybercriminels cherchent à s'en prendre aux sauvegardes pour limiter les possibilités pour la victime de retrouver ses données et ainsi maximiser les chances qu'elle paie la rançon.

LES SOLUTIONS À METTRE EN PLACE

Les mises à jour

APPLIQUEZ-VOUS RÉGULIÈREMENT LES MISES À JOUR ?

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre ordinateur. Activez la mise à jour du système d'exploitation et de tous les logiciels utilisés, à chaque mise à disposition d'un correctif par leurs éditeurs._Cela est d'autant plus important pour tous les matériels exposés sur internet. Il est recommandé d'**activer les fonctions de mise à jour automatique.** Outre ces mises à jour régulières, des mises à jour hors calendrier peuvent survenir en cas de détection d'une vulnérabilité dont la criticité ne permet pas d'attendre plusieurs semaines pour le déploiement d'un correctif.

Ces mises à jour doivent être aussi appliquées dès que possible. Les **vulnérabilités non corrigées** des systèmes d'exploitation ou des logiciels présents sur le système d'information peuvent être **utilisées pour infecter le système** ou favoriser la propagation de l'infection.

Par habitude, par négligence ou par souci d'économies, il peut sembler tentant de conserver un matériel ou un logiciel au-delà de son « cycle de vie », c'est-à-dire après la période pendant laquelle son fabricant ou son éditeur garantit son maintien en conditions de sécurité. **Tout matériel ou logiciel qui ne peut plus être mis à jour doit être mis au rebut ou désinstallé.**

LES SOLUTIONS À METTRE EN PLACE

Les mots de passes robustes

AVEZ-VOUS IMPLANTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSES ROBUSTES ?

L'ANSSI recommande une longueur **minimum de 9 caractères** pour les services peu critiques et minimum **14 caractères** pour les services critiques (information personnelle, financière, possibilité d'impacter le fonctionnement de l'entreprise).

- Un mot de passe robuste comporte des capitales, des minuscules, des chiffres et des caractères spéciaux.
- Ces mots de passe ne doivent comporter **aucun élément personnel**.
- Il est possible d'avoir recours à une phrase de passe, elles sont souvent plus longues et plus simples à mémoriser
- Il faut des mots de passe **différents pour chaque service** nécessitant une authentification.

LES SOLUTIONS À METTRE EN PLACE

Les mots de passes robustes

AVEZ-VOUS IMPLANTÉ UNE POLITIQUE D'USAGE DE MOTS DE PASSES ROBUSTES ?

De nombreuses attaques sur Internet sont facilitées par l'utilisation de mots de passe trop simples ou réutilisés d'un service à l'autre. Les attaques contre des mots de passe peuvent être de différentes natures : **attaques par force brute** (la personne tente le plus grand nombre de combinaisons) ou **par dictionnaires** (elle tente les mdp les plus courants, qu'il s'agisse de noms communs ou de combinaisons simplistes). Ou de type **« ingénierie sociale »**, il teste alors des informations personnelles telles que les prénoms de vos proches ou les surnoms de vos animaux de compagnie, après les avoir récupérés sur les réseaux sociaux.

Il faut ajouter qu'une attaque contre les mots de passes peut ne pas avoir comme finalité de se limiter au service impacté, mais permettre une propagation de l'attaque au sein de l'entreprise ou à ses partenaires. Par exemple, votre courriel pourrait être utilisé par l'attaquant pour adresser des courriels malveillants vers vos contacts pro afin de les inciter à faire des actions dangereuses à leur insu.

LES SOLUTIONS À METTRE EN PLACE

Antivirus

UTILISEZ-VOUS DES ANTIVIRUS ?

Les antivirus sont très utiles à la protection des moyens informatiques : ils peuvent dans la majorité des cas empêcher une compromission et **éviter une attaque par rançongiciel**. Un antivirus doit être déployé sur tous les équipements, en priorité ceux connectés à Internet.
L'évolution d'un virus est très rapide, **des centaines de milliers de codes malveillants apparaissent chaque jour**. Sans la mise à jour fréquente du logiciel, la protection offerte par l'antivirus s'en trouve très rapidement plus restreinte. L'antivirus peut dans la majorité des cas, éviter le chiffrement de vos fichiers.

LES SOLUTIONS À METTRE EN PLACE

Les accès internet

CONTRÔLEZ-VOUS LES ACCÈS INTERNET ?

Les points d'accès Internet de votre entreprise, sont des failles dans laquelle un cybercriminel peut accéder au système d'informations. Privilégiez une approche de réseau privé virtuel (VPN) avec un unique point d'échange sécurisé avec Internet pour l'ensemble de l'entreprise.

Il est conseillé d'effectuer régulièrement des tests de vulnérabilités sur chacun de ces accès afin d'anticiper une attaque.

LES SOLUTIONS À METTRE EN PLACE

Pare-feu

AVEZ-VOUS ACTIVÉ UN PARE-FEU ?

Ce logiciel, installé sur l'ordinateur de l'utilisateur, **protège** principalement **contre des attaques provenant d'Internet.** Pour les entreprises disposant d'un système d'information d'entreprise, il permet également de ralentir ou limiter l'action d'un acteur malveillant ayant réussi à prendre le contrôle d'un des postes de travail.

Afin de pouvoir bloquer les cyberattaques, il est nécessaire d'avoir un **pare-feu et un proxy** pour protéger les connexions web. Par sa fonction de filtrage web, ce dernier vous permet de gérer les accès et de protéger votre réseau en premier lieu. Il est indispensable à votre infrastructure.

LES SOLUTIONS À METTRE EN PLACE

Vos collaborateurs

COMMENT INFORMEZ-VOUS VOS COLLABORATEURS ?

Informez et sensibilisez vos collaborateurs aux politiques de sécurité, les pratiques dangereuses des salariés sont principalement dues à **une méconnaissance des risques**. En étant conscient des risques et en sachant comment se défendre, nous contribuons tous à les réduire.
Une solution pour vérifier les bonnes pratiques de vos salaries ? Pour sensibiliser à la cybersécurité nous pouvons simuler des attaques. En **simulant un mailing frauduleux** vous pourrez voir la réaction de vos collaborateurs face à ces attaques. Et de ce fait, mettre en place ou non de nouvelles préconisations.
Cette sensibilisation peut également se décliner par le biais d'une charte informatique remise à chaque nouvel arrivant, qui détaille les usages numériques à respecter.

LES SOLUTIONS À METTRE EN PLACE

Vos collaborateurs

COMMENT INFORMEZ-VOUS VOS COLLABORATEURS ?

Il s'agit de **responsabiliser** les utilisateurs face à des menaces évolutives. Le plus souvent, l'attaque par rançongiciel commence par l'ouverture d'une pièce jointe piégée ou la consultation d'une page web malveillante. Ainsi, la formation des utilisateurs aux bonnes pratiques de sécurité numérique est une étape fondamentale pour lutter contre cette menace.

L'objectif est également de faire naître ou de renforcer certains réflexes chez les utilisateurs en les invitant à signaler au service informatique de l'organisation tout élément suspect.

Pour que l'accompagnement soit de longue durée, il ne faut cesser de communiquer, former et de sensibiliser. **Les mauvaises habitudes reviennent vite.**

Comment réagir en cas d'attaque ?

COMMENT REAGIR EN CAS D'ATTAQUE ?

Adapter les bons réflexes

Le premier réflexe est d'ouvrir **une main courante** permettant de tracer les actions et les évènements liés à l'incident. Ce document doit permettre à tout moment de renseigner les décideurs sur l'état d'avancement des actions entreprises.
Afin d'éviter une propagation du rançongiciel sur les autres équipements informatiques de l'entité, il est important de **déconnecter au plus tôt vos supports** de sauvegardes après vous être assurés qu'ils ne sont pas infectés et d'isoler les équipements infectés du SI en les déconnectant du réseau.

Une fois les programmes malveillants à l'origine de l'infection identifiés, il sera possible de rechercher dans les journaux du système d'information les éventuelles caractéristiques de ceux-ci. (exemple : URL utilisées pour communiquer avec l'infrastructure de l'attaquant, nom de fichier, objet du courrier électronique…).
Ces éléments pourront être utilisés sur les passerelles applicatives ou sur les équipements de filtrage pour éviter de nouvelles infections.

COMMENT REAGIR EN CAS D'ATTAQUE ?

Adapter les bons réflexes

En particulier, si une adresse IP est identifiée comme étant malveillante, il sera possible de mettre en place une règle au niveau des pares-feux. Si l'ensemble des fichiers d'une machine ont été chiffrés, son extinction électrique peut réduire les chances de retrouver dans la mémoire de l'équipement des éléments permettant de recouvrer les fichiers chiffrés. Si la machine infectée le permet, il est donc recommandé d'activer la mise en veille prolongée afin de faire cesser l'activité du programme malveillant tout en préservant la mémoire en vue d'une analyse ultérieure.

Afin de limiter la diffusion du rançongiciel et le chiffrement de données sur de nouvelles machines, il est préférable de **laisser éteints les équipements non démarrés.**

COMMENT REAGIR EN CAS D'ATTAQUE ?

Ne pas payer la rançon

Il est recommandé de ne **jamais payer la rançon.** Son paiement ne garantit pas l'obtention d'un moyen de déchiffrement. Il incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux. De plus, le paiement de la rançon **n'empêchera pas votre entité d'être à nouveau la cible de cybercriminels.**

Par ailleurs, l'expérience montre que l'obtention de la clé de déchiffrement ne permet pas toujours de reconstituer l'intégralité des fichiers chiffrés. En particulier, les fichiers modifiés par une application et chiffrés dans le même temps par le rançongiciel ont de fortes chances d'être corrompus.

COMMENT REAGIR EN CAS D'ATTAQUE ?

Ne pas payer la rançon

Le gouvernement a mis en place la plateforme cybermalveillance.gouv.fr. Après avoir réalisé un diagnostic en ligne, les victimes accèdent à des conseils personnalisés leur permettant de résoudre leur problème.

Les entreprises traitant des informations personnelles, relevant du Règlement général sur la protection des données personnelles (RGPD) sont soumises au respect des exigences de ce texte. En cas d'incident, elles sont également tenues d'informer la CNIL et leurs clients. Il est essentiel de porter plainte. En cas de rançon, ne pas la payer.

COMMENT REAGIR EN CAS D'ATTAQUE ?

Les conséquences pour mon entreprise

Elles sont de natures diverses. Les plus fréquentes sont **financières, de réputation ou d'image, de productivité, juridiques, pouvant entraîner des conséquences légales ou financières, humaines** (vitales ou handicapantes) dans le cas, par exemple, d'un sabotage.

QUELQUES HABITUDES À METTRE EN PLACE

- Ne pas ouvrir de pièces jointes provenant d'un inconnu.
- Ne **jamais communiquer d'informations personnelles.**
- Ne pas brancher sa clé USB personnelle sur un ordinateur professionnel.
- Si l'on reçoit une demande inhabituelle par email, n'hésitez pas à **demander validation** à votre supérieur.
- Vous pouvez faire passer le curseur de votre souris sur le lien reçu pour **vérifier la source**.

CONTACT

Nous pouvons vous accompagner et vous conseiller sur les aspects cybersécurité avec des solutions de protection, de sauvegarde, de sécurisation du réseau etc...

contact@equadex.net

ou par téléphone :
05 67 34 67 90