
HubSpot

# Comment assurer la cybersécurité de votre entreprise ?

# Table des matières

# Introduction

**La digitalisation des entreprises, qui a connu une véritable explosion à la suite de la crise sanitaire, a engendré de nombreux bouleversements pour les professionnels.**

Ces derniers se sont retrouvés dans l'obligation pratiquement immédiate d'adapter leur activité à un nouveau mode de fonctionnement virtuel et cette transition vers le numérique n'a pas toujours été réalisée de manière sécurisée. Les sociétés sont donc rapidement devenues une cible de choix pour les pirates informatiques, en raison de leur méconnaissance des règles de bases de la cybersécurité.

Le nombre d'entreprises françaises touchées par des cyberattaques affiche une constante augmentation depuis des années, il semble donc plus que jamais primordial de mettre en place une stratégie de protection des données efficace. Il existe plusieurs réflexes et outils pour mettre en place et renforcer facilement sa cybersécurité en tant que professionnel.

Chapitre 1

# Quels risques cyber pour les entreprises françaises actuelles ?

# Quels risques cyber pour les entreprises françaises actuelles ?

## Une menace qui plane sur les grands groupes comme sur les petites entreprises

**Il existe plusieurs analyses sérieuses démontrant l'importance du risque représenté par les cyberattaques pour les entreprises.** D'après une étude menée par **Opinionway** pour le CESIN, Club des Experts de la Sécurité Informatique et du Numérique, **54 %** des entreprises françaises en auraient été victimes en 2021. Un chiffre en constante augmentation depuis des années, qui justifie que l'ensemble des professionnels fassent de la **cybersécurité** une véritable priorité. Désormais, comme les experts de ce domaine le rappellent souvent, la question à se poser n'est plus « *vais-je un jour subir une cyberattaque ?* » mais bel et bien « *quand vais-je subir une cyberattaque ?* ».

Si les grands groupes restent des cibles privilégiées pour les pirates informatiques, aussi appelés hackers, les PME et TPE se révèlent tout aussi concernées par cette menace permanente. En effet, les grandes entreprises possédant plus de moyens ont immédiatement réagi face à ces attaques et ont vite considéré la cybersécurité comme un enjeu stratégique majeur. Les plus petites structures, souvent moins conscientes et informées des risques, manquent encore parfois de temps, de moyens et d'informations pour se prémunir de ce risque alors que la menace de cyberattaques plane également sur elles. La plus petite TPE dispose forcément de données confidentielles comme des coordonnées bancaires, des références client ou encore des exemplaires de contrats, dont le vol par des pirates informatiques peut s'avérer extrêmement préjudiciable.

## Les conséquences d’une cyberattaque pour une entreprise

**Les cyberattaques concernent toutes les entreprises, peu importe leur taille, et peuvent engendrer des conséquences financières, mais aussi juridiques et sociales, dramatiques.**

Il existe une multitude d’attaques différentes, les plus populaires restant les rançongiciels, aussi connus sous le nom de ransomwares. Payer la rançon demandée ne garantit absolument pas de récupérer les données dérobées, qui sont bien souvent revendues au marché noir ou à la concurrence immédiatement, mais génère une perte d’argent conséquente. En effet, ce type d’attaque empêche l’entreprise d’accéder à ses informations, outils et postes de travail : en plus de perdre le montant de la rançon, elle perd aussi son temps de travail. Il s’agit précisément de l’objectif de certaines cyberattaques, qui ne demandent pas d’argent de manière directe mais paralysent la société. Le groupe français Saint Gobain a, par exemple, perdu 220 millions d’euros de chiffre d’affaires en 2017 à cause d’une attaque depuis sa branche située en Ukraine.

En plus de ces conséquences financières parfois irréparables, les cyberattaques impactent également la réputation des professionnels et peuvent engendrer de sérieux problèmes juridiques. Le vol de données par une tierce personne reste en effet considéré comme une fuite de données de la part de l’entreprise, censée garantir la sécurité de ces informations par une politique RGPD. Les sanctions applicables peuvent atteindre 20 millions d’euros ou 4 % du chiffre d’affaires. En décembre 2021, par exemple, la CNIL, Commission Nationale de l’Informatique et des Libertés, a imposé à l’entreprise Slimpay une amende de 180 000 € pour protection insuffisante des données de ses clients.

Se protéger contre les attaques informatiques représente donc une nécessité pour l’ensemble des professionnels et implique avant tout de connaître les différents modes opératoires des hackers.

Chapitre 2

# 3 formes de cyberattaques fréquentes en entreprise

# 3 formes de cyberattaques fréquentes en entreprise

## L’hameçonnage ou phishing

Il existe de nombreuses manières, pour les pirates informatiques, de récupérer et de dérober des données pour les revendre. **L’attaque la plus basique, à laquelle tous les individus possédant une boîte mail peuvent être confrontés, reste sans doute l’hameçonnage, aussi appelé phishing.** Il s’agit, pour les hackers, d’amener les victimes à cliquer sur un lien internet, par exemple, qui les redirige vers un site sur lequel ils renseignent des données personnelles ou relatives à la société, dans un contexte professionnel. Pour persuader les utilisateurs de mordre à l’hameçon, les malfaiteurs se font très souvent passer pour un client, un concurrent ou encore une institution officielle. Ce type d’attaque conduit souvent à une usurpation d’identité.

## Les rançongiciels ou ransomwares

Comme leur nom l'indique, les rançongiciels empêchent les utilisateurs d'accéder à leurs données et demandent le paiement d'une rançon pour les rendre à nouveau disponibles. **En pratique, le pirate crypte les données de sa victime pour lui interdire l'accès et lui réclame souvent une rançon en cryptomonnaie à une échéance précise, jouant ainsi sur le sentiment d'urgence et de panique.** Ces attaques concernent en premier lieu les entreprises, susceptibles de céder au chantage rapidement par peur de voir leur activité couler de manière rapide. La plus importante attaque de ce type reste WannaCry, qui, en 2017, a touché plus de 250 000 ordinateurs à travers le monde et a notamment impacté des sociétés comme FedEx, Nissan ou encore Hitachi. Même si la victime décide de payer la rançon, les pirates détruisent ou revendent les informations volées sans jamais les rendre, ce qui laisse l'entreprise en bien mauvaise posture.

## Le déni de service, DDOS

**L'attaque DDOS, qui signifie *Distributed Denial Of Service*, correspond à un déni de service, c'est-à-dire que les hackers rendent un site ou un service inaccessible en saturant son serveur avec de très nombreuses requêtes.** Cette sollicitation excessive provoque une panne ou une exécution très dégradée du service. Un site marchand victime de ce type d'attaque peut vite se retrouver en grande difficulté car un DDOS interrompt de manière instantanée les ventes en ligne sur le site. Une fois que celui-ci s'avère complètement bloqué, les pirates peuvent alors dérober les données présentes sur le serveur.

Chapitre 3

# Solutions pour garantir la cybersécurité de son entreprise

# Solutions pour garantir la cybersécurité de son entreprise

## Sensibiliser ses collaborateurs et nommer un responsable cybersécurité

**Dans leur grande majorité, les cyberattaques ne peuvent avoir lieu que parce qu'un utilisateur s'est montré négligeant ou naïf mais surtout, mal informé.**
De très nombreux logiciels malveillants s'infiltrent dans les systèmes car un collaborateur a cliqué, sans le soupçonner, sur une pièce-jointe corrompue ou sur un lien douteux. La première chose à faire pour réduire le risque de cyberattaque consiste donc à sensibiliser les membres des équipes.

**À cette fin, la plateforme nationale Cybermalveillance.gouv.fr a développé un kit de sensibilisation destiné aux professionnels.** Il paraît notamment avisé d'organiser des réunions de présentation des risques et des bonnes pratiques à suivre et de les rappeler dans les bureaux sur divers supports de communication écrits, afin que chacun les garde bien présents à l'esprit.

Par ailleurs, proposer des formations à ses collaborateurs leur assure de maîtriser tous les enjeux de la cybersécurité de manière encore plus approfondie et de désigner un responsable en interne. **Un référent cybersécurité ou RSSI, Responsable de la Sécurité des Systèmes et de l'Information, représente, pour une entreprise, un réel atout** car cette personne a précisément pour rôle de procéder à l'analyse des risques et de définir les meilleures stratégies de protection à développer.

## Installer des antivirus et pare-feu sur les postes informatiques et effectuer les mises à jour logiciel régulièrement

L'un des premiers outils à mettre en place pour lutter contre l'installation de virus ou de logiciels malveillants sur les postes informatiques de la société consiste à **les équiper d'antivirus.** Ces outils représentent la première ligne de défense contre les attaques extérieures et protègent les ordinateurs connectés à internet contre les menaces. Ils possèdent une base de données répertoriant l'ensemble des menaces informatiques connues afin de mieux les détecter et d'empêcher leur intrusion dans l'ordinateur.

Les cyberattaques évoluent de manière quasiment quotidienne, il s'avère donc extrêmement important de mettre à jour la base de données des logiciels antivirus pour que ceux-ci actualisent leurs informations et puissent combattre toutes les attaques, même les plus sophistiquées. La plupart des antivirus se mettent à jour de façon automatique et programment des analyses automatiques de l'ordinateur en profondeur, activer ces fonctionnalités permet donc de bénéficier d'une protection de base sans y penser.
En plus de passer au crible les fichiers présents sur le poste, certains antivirus proposent des prestations supplémentaires comme l'ajout de pare-feu, de filtrage web ou encore de sécurisation renforcée lors de transactions bancaires. Le pare-feu se présente comme un prolongement de l'antivirus et contrôle l'ensemble du trafic sur le poste et bloque les éléments indésirables.

## Encourager les utilisateurs à choisir des mots de passe efficaces

L'une des cyberattaques les plus basiques consiste, pour un hacker, à tout simplement tenter sa chance en entrant un mot de passe extrêmement simple tel que « motdepasse », « azerty » ou encore « 123456 ». **Il s'agit de l'attaque dite « en force brute ».** Une variante de cette technique se trouve aussi dans **l'ingénierie sociale** : l'attaquant essaie, en guise de mot de passe, les prénoms ou les dates de naissance des proches de sa victime. **L'utilisation de mots de passe trop simples à deviner ou identiques d'un service à l'autre constitue donc un sérieux danger pour les entreprises à plus ou moins long terme.**

**Parmi les bonnes pratiques à mettre en place, il est notamment conseillé de créer des mots de passe uniques pour chaque utilisateur, et différents pour chaque application.** Ces mots de passe doivent également s'avérer complexes, c'est-à-dire présenter une certaine longueur, d'au moins 8 caractères, et inclure des caractères spéciaux, des lettres en majuscules ainsi que des chiffres. Plus un mot de passe se révèle compliqué à deviner, plus un pirate aura du mal à le trouver et à s'infiltrer dans le système. Il convient également de les changer tous les 3 mois afin de rendre les accès encore plus difficiles. Les **gestionnaires de mots de passe** représentent d'ailleurs de formidables outils pour renforcer la sécurité de ces données. Ceux-ci permettent de stocker l'ensemble des mots de passe d'un utilisateur de façon cryptée et protègent ainsi toutes ces informations sans que l'utilisateur n'ait besoin de les mémoriser.

## Privilégier l'authentification à deux facteurs

**L'authentification à deux facteurs implique non pas un, mais deux moyens de se connecter à une application ou à un service. Il peut s'agir, par exemple, d'entrer un mot de passe puis de valider une notification reçue par SMS, sur le téléphone.**
Les institutions bancaires recourent très souvent à ce type de méthodes pour garantir la sécurité des paiements en ligne. L'authentification multi facteurs complexifie l'accès au service et ralentit les pirates, ce qui peut se révéler d'une importance cruciale.

## Effectuer des sauvegardes externes régulièrement

**Sauvegarder l'ensemble de ses données de manière séparée garantit de conserver une copie de toutes les informations nécessaires au maintien de son activité en cas d'attaque.** Stocker tous ses fichiers tels que des documents, tableurs, messages, informations confidentielles ou contrats sur un cloud sécurisé ou un disque dur externe permet de ne pas redouter la cessation d'activité en cas de système paralysé. Il existe d'ailleurs des outils réalisant des sauvegardes automatiques de toutes les données présentes sur un poste informatique sur un support extérieur sécurisé. L'essentiel reste de conserver ces sauvegardes en dehors de leur emplacement initial pour éviter qu'elles ne soient également corrompues en cas de problème.

## Restreindre au maximum l'accès au réseau et aux documents sensibles

Réserver l'accès de certains documents confidentiels à un nombre limité de personnes paraît logique. **Afin d'éviter toute intrusion ou vol de données sensibles, mieux vaut mettre en place un système d'authentification renforcé associé à une politique de certificats de droits d'accès**. Ainsi, seules les personnes autorisées peuvent consulter certains documents où se rendre dans les zones sensibles d'un bâtiment. Ces certificats doivent aussi faire l'objet de révisions régulières, pour restreindre encore plus l'accès aux seuls individus concernés.

**Les réseaux Wi-Fi peuvent aussi être réservés aux seuls collaborateurs de l'entreprise.** Il est possible de prévoir un réseau privé pour ces derniers, accessible uniquement depuis certains postes informatiques et nécessitant une identification forte pour y accéder, et un autre, public, pour les visiteurs. Ainsi, les données ne peuvent se croiser et les potentiels pirates sur le site ne peuvent accéder au réseau interne. Il faut alors masquer le réseau Wi-Fi interne pour les appareils des visiteurs en cachant son SSID, *Service Set Identifier*, et attribuer un mot de passe complexe à son routeur.


## Utiliser un VPN

Un **VPN**, Virtual Private Network constitue un réseau privé protégeant toute l'activité des utilisateurs sur internet. Ces outils cryptent l'ensemble des activités réalisées en **ligne depuis un poste informatique et masquent les adresses IP de leurs abonnés.** De ce fait, la navigation se déroule de manière totalement confidentielle, sécurisée et intraçable. Il s'agit d'un bon moyen de renforcer la sécurité sur les postes de collaborateurs effectuant du télétravail et utilisant des réseaux Wi-Fi pas forcément sécurisés.

**De plus en plus d'entreprises subissent des cyberattaques chaque année et celles-ci peuvent avoir de graves conséquences, tant sur le plan financier que juridique, et impacte également la réputation des sociétés de manière très négative. Il existe heureusement beaucoup de gestes et d'outils faciles à mettre en place pour se prémunir des attaques : complexification des mots de passe, sensibilisation en interne, restrictions d'accès aux réseaux et documents sensibles ou encore utilisation de VPN.**

HubSpot

**Logiciel marketing**

Rassemblez tous vos outils
et vos données marketing
au même endroit

**Demander une démonstration**