CYBERATTAQUES : comment se protéger ?

DÉCOUVREZ LES BONNES PRATIQUES

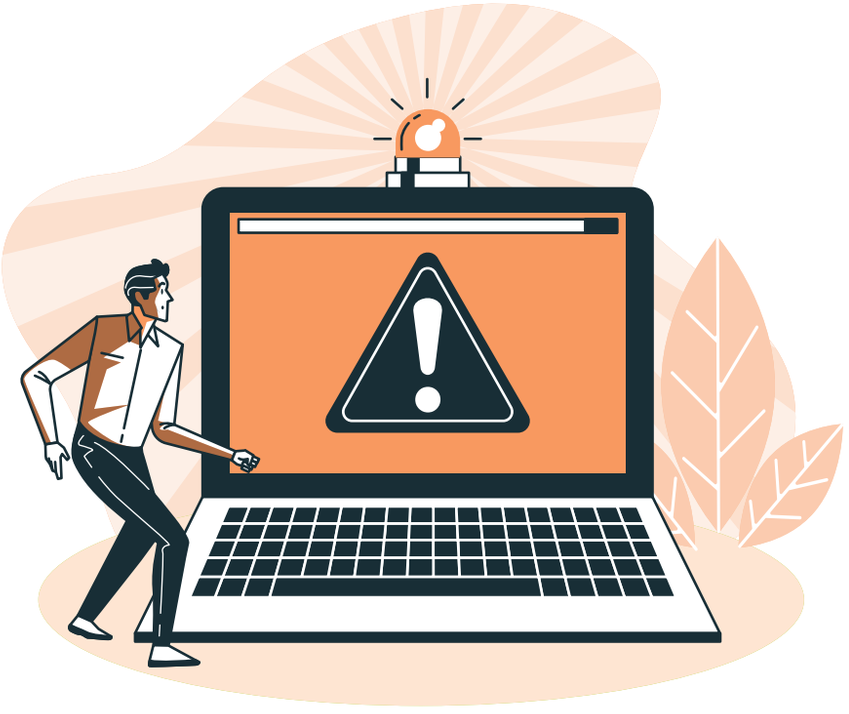
LIVRE BLANC

Quelles sont les bonnes pratiques à suivre pour faire face à une cyberattaque ?

Les cyberattaques se multiplient, toujours plus sophistiquées, impactant chaque jour des millions d'entreprises à travers le monde. Quel que soit le secteur d'activités concerné, le risque zéro n'existe pas. Toute entreprise, indépendamment de sa taille ou de son chiffre d'affaires, sera confrontée un jour à une attaque, si ce n'est déjà fait. La cybercriminalité prend des formes diverses et sert des intérêts variés : appât du gain, vol de données, cyber espionnage, volonté de nuire à l'image d'une entreprise ou institution… Pour le moment, seulement 39 % des entreprises se disent être suffisamment préparées pour faire face, si besoin, à une cyberattaque de grande ampleur. [1]

Si l'aspect technologique, la capacité des entreprises à protéger leurs outils, joue évidemment un rôle clé dans la lutte contre cette menace, le cyber-risque le plus répandu reste à ce jour l'humain : dans 43 % des cas, c'est la négligence ou l'erreur de manipulation ou de configuration d'un salarié qui a rendu possible la cyberattaque. [1] **L'email s'impose d'ailleurs comme une porte d'entrée privilégiée par les cybercriminels** : de nombreuses entreprises ne protègent pas suffisamment leur messagerie ou n'informent pas assez leurs salariés sur les risques potentiels, alors qu'il s'agit du premier vecteur de cyberattaque et d'un élément essentiel à sécuriser.

Il est impossible d'empêcher des cybercriminels de chercher à nuire à votre entreprise, mais en adoptant les bonnes pratiques et en connaissant les éléments les plus vulnérables de votre structure pour les protéger efficacement, vous pouvez les empêcher d'atteindre leur objectif. Dans ce livre blanc, nous vous expliquons quelles sont les cyberattaques les plus courantes, leurs impacts sur votre entreprise et les solutions pour vous protéger et limiter les risques. Nous vous donnons également toutes les solutions pour bien réagir en cas de cyberattaque et en limiter les conséquences.



SOMMAIRE

1

ÉTAT DES LIEUX DE LA CYBERCRIMINALITÉ

Cybercriminalité : chiffres clés et enjeux

La cybercriminalité se distingue de la criminalité traditionnelle par les outils utilisés : ici, tout passe par l'informatique. La généralisation de l'utilisation d'Internet par tous les secteurs de l'économie, les réseaux sociaux, mais aussi l'utilisation massive de l'email par les entreprises, ont grandement facilité son expansion.

Elle se développe sous deux formes principales :

- **L'atteinte aux biens :** le piratage informatique, le cyber-espionnage, les fraudes liées aux paiements en ligne
- **L'atteinte aux personnes :** la diffusion de données, photos ou vidéos portant atteinte à des personnes

Les particuliers ne sont pas les seuls à être visés par des cyberattaques. **D'après le baromètre de la cybersécurité des entreprises publié en janvier 2020 par le CESIN, 65 % des entreprises déclarent avoir constaté au moins une cyberattaque au cours des 12 derniers mois**. Si 55 % d'entre elles ont constaté que le nombre d'attaques sur leur entreprise était stable, 40 % estiment qu'il est en augmentation par rapport à l'année précédente. [1]

Autre chiffre tout aussi inquiétant : en France en 2019, plus de 79 % des entreprises ont été victimes de cyberattaques. [1] Contrairement à certains a priori, les plus touchées ne sont pas les grandes entreprises, mais les ETI (Entreprises de Taille Intermédiaire). [4]

Le baromètre de la cybersécurité des entreprises dévoile également les cyberattaques principales constatées par les entreprises :

Le *phishing*

79%

Il s'agit d'une technique permettant de récupérer des données privées, généralement mise en place via l'envoi massif d'emails à de nombreux destinataires.

Le *spearphishing*, ou arnaque au président

47%

Les cybercriminels se font passer pour le président d'une société auprès de ses employés. Là encore, l'email est le canal le plus utilisé. La principale différence avec le phishing est le degré de personnalisation de l'attaque.

L'exploitation d'une vulnérabilité

43%

Il s'agit de repérer une faille dans le système d'information pour s'y infiltrer. Cela est généralement lié à un système.

Les tentatives de connexion

40%

Cette technique consiste à rendre inaccessible un site en le saturant de connexions.

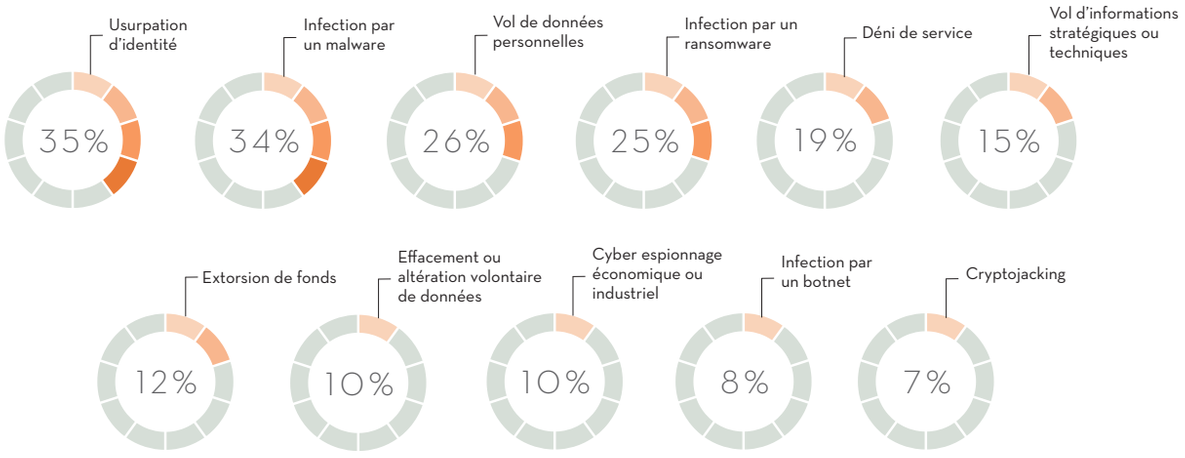
L'exploitation d'un défaut de configuration

29%

Des outils mal configurés ou non mis à jour représentent une véritable porte ouverte pour les cyberattaques.

Ces cyberattaques servent des objectifs précis. Il est important de les connaître pour comprendre que toute entreprise, indépendamment de sa taille ou de son secteur d'activités, peut être visée.

Une analyse des conséquences constatées par les entreprises met en lumière les objectifs les plus fréquents :



Les pirates cherchent donc à extorquer des fonds ou des informations (ransomwares, extorsion, cryptojacking), s'infiltrer dans les systèmes (usurpation d'identité, espionnage), ou simplement causer des dégâts à leur cible.

Dans plus de la moitié des cas, un impact négatif a été constaté par les entreprises victimes d'une cyberattaque. Les effets principaux observés sont :

01	27%	La production se trouve perturbée pendant une période significative
02	17%	Le site web de l'entreprise devient indisponible
03	9%	Une perte de chiffre d'affaires
04	8%	Des retards sur la livraison auprès des clients
05	7%	Un arrêt total ou partiel de la production
06	5%	Une mauvaise image pour l'entreprise

Ces effets peuvent rapidement se cumuler et ont une incidence directe sur le chiffre d'affaires et la réputation de l'entreprise. Par exemple, une attaque par déni de service réussie aura un gros impact sur un site d'e-commerce : les clients ne peuvent plus y accéder, ils ne passent donc aucune commande et la production est à l'arrêt. Quant aux commandes déjà passées, elles prennent du retard. De façon plus générale, le vol de données ou l'infection par un malware peuvent avoir des conséquences très graves pour toutes les entreprises, en les exposant à une rançon et en paralysant leurs systèmes. **Un simple email d'apparence anodine peut ainsi entraîner des réactions en chaîne aux conséquences désastreuses pour une entreprise.**

Cyberattaques : objectifs et risques

Les cyberattaques prennent des formes variées, mais comme nous l'avons vu précédemment, certaines sont plus utilisées que d'autres. C'est le cas du ransomware, du phishing et du spearphishing.

RANSOMWARE : LE PRENEUR D'OTAGE

Un ransomware est un logiciel de rançon. Une fois introduit dans votre système, **il restreint l'accès à toutes vos données en les chiffrant ou en verrouillant votre ordinateur**. Le cybercriminel lèvera la restriction uniquement en échange du paiement d'une rançon. C'est là l'objectif principal du hacker avec cette technique : obtenir de l'argent.

Ce logiciel peut s'infiltrer sur un ordinateur lorsqu'une personne de l'entreprise visite un site web suspect ou utilise un service cloud, mais l'email reste la voie privilégiée. Dans ce cas, le cybercriminel envoie un simple email à l'apparence rassurante et contenant une pièce jointe qui est en fait le ransomware.

Le ransomware est une attaque particulièrement stressante pour les victimes, soit parce que les données bloquées sont sensibles, soit parce que le logiciel, par son action, rend impossible la poursuite du travail. Bien souvent, ces deux effets vont de pair. Pour s'en sortir, la meilleure solution est de supprimer ce logiciel en utilisant des outils adaptés ou en faisant appel à un expert.

Céder au chantage et payer la rançon est une possibilité, mais ce n'est pas recommandé : **le cybercriminel peut encaisser l'argent sans déverrouiller vos données. Il peut également conserver une copie des données et les utiliser de manière frauduleuse, ou tout simplement recommencer ensuite, sachant désormais que vous êtes prêt à payer.**

Les hackers, selon leur objectif de gain et le ransomware utilisé, peuvent opérer de deux manières différentes :

- Diffuser le ransomware vers le plus grand nombre possible d'entreprises, sans tenir compte de leur taille ou de leur secteur d'activités. Ici, il s'agit de viser large pour obtenir un maximum de retours, quitte à extorquer de plus petites sommes.
- Cibler précisément des secteurs sensibles, dont les banques et assurances et le domaine de la santé. Les cibles sont moins nombreuses et les sommes demandées généralement plus grandes, au vu du caractère sensible des données visées.

Toute entreprise peut ainsi se retrouver visée par une telle attaque, c'est pourquoi il est indispensable de protéger au maximum ses outils, et plus particulièrement sa messagerie.

PHISHING : LE VOLEUR DE DONNÉES

Le phishing, aussi appelé hameçonnage en français, **consiste à voler des données personnelles, comme des identifiants de connexion ou des moyens de paiement**. La méthode la plus utilisée est l'envoi d'emails, dans lesquels les cybercriminels se font passer pour une entreprise ou un organisme de confiance, comme la CAF, le centre des impôts, une banque ou un opérateur de téléphonie. Ces emails sont conçus pour paraître crédibles (reprise des logos, présence des mentions légales…).

Pour faire réagir la victime et l'encourager à cliquer sur le lien indiqué, deux méthodes sont utilisées :

- La peur : par exemple, un email informant la cible qu'un paiement a été rejeté et qu'une procédure de saisie va être demandée, qu'un de ses comptes sur les réseaux sociaux a été bloqué ou encore pour la remercier d'un achat onéreux qu'elle viendrait d'effectuer. C'est une astuce psychologique connue qu'exploitent les hackers : face à une annonce suffisamment stressante, les victimes font preuve de moins de discernement et sont plus susceptibles de se tourner vers la solution la plus rapide et simple pour régler le problème. Ici, il s'agira de cliquer sur le lien indiqué par les cybercriminels et de fournir les données demandées.
- L'appât du gain : l'email annonce un remboursement en attente, un gain à un jeu ou un héritage au bénéfice de leur cible. Généralement, la somme promise est soit suffisamment petite pour paraître crédible (quelques centaines d'euros), soit suffisamment importante pour que la cible se laisser appâter.

Dans tous les cas, lorsque la personne clique sur le lien donné, elle est redirigée vers un site qui imite celui de l'organisme ou de l'entreprise citée. Elle sera alors invitée à donner des informations personnelles pour achever la procédure. Les cybercriminels peuvent ainsi les récupérer.

Si l'arnaque est connue, elle continue de faire des victimes. Les cybercriminels envoient des emails de plus en plus sophistiqués et crédibles, provenant d'adresses qui, en apparence, semblent officielles. **Les sites dont ils usurpent l'identité paraissent eux aussi parfaitement officiels.**

Les cybercriminels peuvent viser différents types de données personnelles, selon leur objectif, comme :

- Les identifiants et mots de passe, pour s'infiltrer dans les systèmes et réaliser des usurpations d'identité,
- Les coordonnées bancaires pour voler des fonds,
- Les informations personnelles (nom, prénom, numéro de sécurité sociale, scan des pièces d'identité…) pour alimenter un réseau de faux papiers ou utiliser les informations à des fins frauduleuses.

Cette méthode cible tous les types de profils, du particulier à l'entreprise. Elle repose avant tout sur l'humain. Ici, pas besoin de s'infiltrer dans une forteresse ultra sécurisée, tout le monde est susceptible de recevoir l'email, de cliquer sur le lien et de remplir le formulaire. À moins, bien sûr, d'être parfaitement informé sur ces arnaques et/ou de sécuriser sa messagerie pour filtrer automatiquement ce type d'emails.

SPEARPHISHING : L'ATTAQUE CIBLÉE

Le spearphishing repose sur le même principe que le phishing, seule la manière de procéder change :

- Dans le cas du phishing, les cybercriminels visent des centaines ou milliers de personnes à la fois. Ils utilisent donc des emails plus génériques, ce qui explique qu'ils se font généralement passer pour des organismes connus, cela augmente les chances que des personnes mordent à l'hameçon.
- Dans le cas du spearphishing, une seule personne précise est visée. Pour piéger la victime, **le cybercriminel se fait passer pour une personne de son entourage personnel ou professionnel**, ce qui implique des recherches en amont pour étudier la cible. Il peut s'agir de recherches sur le web ou les réseaux sociaux, mais aussi d'informations collectées via un vol de données.

Pour mener à bien leur opération, les hackers vont collecter un grand nombre de données, non seulement sur la victime, mais aussi sur la personne dont ils vont usurper l'identité. Par exemple, un employé d'une entreprise recevra un email semblant provenir d'un supérieur et demandant de réaliser un virement sur un compte bancaire. Le hacker aura pris soin de créer une adresse email au nom du supérieur hiérarchique et aura choisi de l'envoyer à un moment où ce dernier est absent et peut effectivement avoir besoin de ce service. Des éléments personnels pourront aussi être ajoutés pour apporter plus de crédibilité à l'ensemble, en fonction des informations qu'auront pu collecter les hackers. Tout est fait pour que la victime ne se méfie pas.

L'email est là encore une voie privilégiée par les cybercriminels, mais ils peuvent également procéder par SMS ou en utilisant un faux site web.

Cette attaque peut concerner un virement frauduleux, mais pas seulement. Le hacker peut également demander à la victime d'ouvrir une pièce jointe corrompue ou de se rendre sur un site web malveillant. Il en profitera alors pour s'insérer dans le système et en prendre le contrôle. Il aura ensuite carte blanche : vol d'informations sensibles, espionnage industriel, détournement de fonds ou même altération des données. Le spearphishing demande plus de travail et de recherches de la part des cybercriminels, leur objectif est donc à la hauteur de cet effort. C'est pourquoi ils ciblent plus particulièrement les grandes entreprises, les organisations majeures (banques, santé, armée…) et les personnes influentes.

Les conséquences peuvent être considérables. Si le coût du phishing se compte en dizaine de millions d'euros chaque année, celui du spearphishing, qui fait pourtant moins de victimes, se chiffre en milliards : en un an, le spearphishing a coûté 25 fois plus que le phishing aux USA. **Il est donc essentiel de bien protéger la messagerie de l'entreprise et de sensibiliser les salariés à ce type de cyberattaque.**

RECOMMANDATIONS ET BONNES PRATIQUES

Comment se protéger des cyberattaques ?

La cybercriminalité se déploie massivement et concerne désormais tout le monde : les particuliers, mais plus encore les organisations et entreprises de petite, moyenne ou grande envergure. Le risque zéro n'existe pour personne.

Il existe des solutions pour réagir en cas de cyberattaque, mais dans la majorité des cas, le mal est déjà fait (perte de chiffre d'affaires, répercussion sur l'image de marque...). C'est pourquoi il est essentiel de tout mettre en œuvre pour agir en amont en sécurisant vos outils. Si vous ne pouvez pas empêcher des hackers de chercher à vous nuire, vous pouvez les empêcher d'atteindre leur objectif.

La sécurité ne passe pas uniquement par la mise en place de technologies et de solutions de sécurité, mais aussi par la vigilance et la formation humaine. Dans cette partie, vous découvrirez comment vous protéger des cyberattaques, quelles barrières mettre en place et quelles sont les bonnes pratiques à adopter pour sécuriser votre entreprise. En suivant ces recommandations, vous deviendrez une entreprise cyber-résiliente.

BARRIÈRES TECHNOLOGIQUES : quelles technos pour quel niveau de sécurité ?

Sécuriser un seul élément ne suffit pas : la moindre faille peut être exploitée par des cybercriminels. Pour vous protéger efficacement, il est nécessaire de prendre en compte l'ensemble des interfaces de votre SI.

Sécuriser votre messagerie

Les statistiques montrent que l'email reste une voie d'accès privilégiée, il est donc indispensable de sécuriser votre messagerie.

Pour se prémunir de ce type d'attaques, la meilleure solution est d'opter pour un système anti-spam et anti-virus capable d'authentifier les expéditeurs et de classifier les principaux types de menaces véhiculées par l'email (au premier rang desquels les tentatives de phishing, de spearphishing, et les ransomwares).

Les solutions les plus efficaces combinent un ensemble de technologies analysant la provenance des emails reçus, l'authenticité des expéditeurs, et les messages eux-mêmes pour détecter les pièces jointes vérolées, les liens malveillants, et les messages au contenu suspect. La combinaison de technologies d'Intelligence Artificielle, d'analyse de liens au moment du clic, et de sensibilisation des utilisateurs au phishing permet de se protéger au mieux contre les principaux vecteurs de menaces informatiques.

Les solutions modernes impliquent de plus en plus les utilisateurs, en mettant en avant cette couche de sécurité avec des interfaces et des outils de sensibilisation pour faire de l'intelligence humaine une brique de sécurité supplémentaire, au lieu de percevoir uniquement les utilisateurs comme une vulnérabilité.

Protéger votre parc informatique

Adopter un antivirus capable de protéger à la fois votre parc informatique et l'ensemble de vos serveurs est essentiel. N'oubliez pas d'installer un pare-feu : cet outil simple à mettre en place constitue une barrière indispensable. Il vous permet de définir clairement les types de contenus et de communication autorisés sur le réseau, et vous autorise une configuration précise selon vos critères de sécurité.

Installer un proxy et un VPN

Un proxy vous permet de contrôler les menaces provenant de la navigation web de vos employés. En visitant des sites dangereux, un employé imprudent et peu protégé peut télécharger des fichiers dangereux qui pourront infecter votre système d'information. De plus, si vous avez des employés en télétravail ou sur des sites distants, un VPN vous permettra de faire passer leurs connexions par votre réseau interne et donc de bénéficier des mesures de protection que vous avez mises en place.

BARRIÈRES HUMAINES :
prévention, information et formation utilisateur

Prévention, information et formation sont les trois piliers d'une véritable cybersécurité. Utiliser les outils les plus puissants ne sera jamais suffisant si vos salariés ne sont pas sensibilisés et impliqués face aux risques de cyberattaques : à travers l'envoi d'emails frauduleux, ce sont eux que ciblent les cybercriminels en priorité, car ils savent que l'erreur humaine demeure la plus simple des failles à exploiter pour atteindre une entreprise.

Il est essentiel de les informer et de les former pour qu'ils soient eux-mêmes acteurs de votre sécurité. Selon le baromètre de la cybersécurité des entreprises, les salariés sont globalement sensibilisés aux cyber-risques (74%). Le problème majeur est autre : seulement la moitié d'entre eux respecterait les recommandations.

Vous devez donc agir sur plusieurs points :

01

Sensibiliser et informer les salariés

Expliquer à ses salariés quelles sont les cyberattaques les plus courantes, comment les repérer et les éviter, mais aussi quels sont les risques qui pèsent sur l'entreprise.

02

Former et/ou proposer des formations

La formation peut se faire grâce à des vidéos, des conférences ou des ateliers dédiés. Les salariés apprendront les bons gestes à adopter et ils découvriront également comment exploiter les outils mis en place pour sécuriser au mieux leurs emails et outils de travail. Cette formation devra être renouvelée chaque fois que nécessaire, les techniques de cyberattaque et les outils pour s'en prémunir étant amenés à évoluer régulièrement. Il existe aussi des solutions permettant de simuler des attaques (notamment de phishing) en conditions réelles pour que vos employés soient plus familiers avec les modes opératoires des pirates informatiques.

03

Rappeler et répéter

Utilisez les moyens à votre disposition pour encourager les salariés à respecter les consignes données. Il peut s'agir d'une campagne d'affichage, de rappels réguliers des bonnes pratiques, de tests en interne pour vérifier qu'ils suivent bien vos consignes...

BONNES PRATIQUES À ADOPTER AU QUOTIDIEN

La cybercriminalité ne se repose jamais. Pour se protéger, il faut se montrer attentif au quotidien, en adoptant les bonnes pratiques :

01

Utiliser des mots de passe forts et les changer régulièrement.

02

Effectuer des tests en envoyant un email frauduleux à différents salariés (y compris parmi les cadres) pour vérifier comment ils y réagissent.

03

Réaliser toutes les mises à jour logicielles au fur et à mesure : de nombreuses mises à jour visent à réparer des failles de sécurité, c'est pourquoi vous ne devez jamais tarder à les installer.

04

Limiter l'accès aux données sensibles : chaque salarié ne devrait avoir accès qu'aux données indispensables à l'exécution de ses missions. Il est essentiel de définir clairement qui a accès à quoi et de protéger ces accès.

05

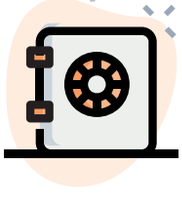
Tester les processus de sécurité : peu importe les outils utilisés pour protéger votre parc informatique et vos réseaux, vous devez les tester régulièrement pour vous assurer qu'ils sont efficaces.

06

Orchestrer la sauvegarde de données : vos données sont précieuses, vous devez les protéger au mieux. Pour cela, il faut adopter une solution de sauvegarde efficace, capable de planifier régulièrement des sauvegardes automatiques et de les stocker dans des espaces sécurisés.

07

Penser aux appareils mobiles : smartphones, tablettes, ordinateurs portables... les salariés les utilisent quotidiennement, aussi bien au travail, qu'à leur domicile ou en déplacement. Vous devez donc vous assurer qu'ils sont bien protégés et que les salariés sont aussi vigilants avec ces appareils qu'avec leur ordinateur de bureau. Il s'agira, par exemple, de les informer sur les risques d'utiliser le Wi-Fi public ou d'insérer des clés USB non sécurisées dans ces appareils.



Victime d’une cyberattaque : comment réagir ?

Prévenir est l’idéal, mais parfois, les outils efficaces et les bonnes pratiques ont été mises en place trop tard, ou de manière insuffisante. Si vous constatez une cyberattaque contre votre entreprise, vous devez garder la tête froide et adopter la bonne attitude.

LES SIGNES QUI DOIVENT VOUS ALERTER

De nombreux signes peuvent vous indiquer que vous êtes, potentiellement, victime d’une cyberattaque. Voici les plus fréquents :

La connexion internet est ralentie.

Des fichiers ont disparu.

La boîte d’envoi de la messagerie contient des emails que vous n’avez pas envoyés.

Vous recevez des emails suspects, par exemple, des messages qui vous informent de la non-délivrance d’emails que vous n’avez pas envoyés.

Votre antivirus et/ou vos logiciels de sécurité ont été désactivés sans intervention de votre part.

Des anomalies sont constatées dans les procédures de paiement ou de commande.

Lors de la navigation sur internet, des fenêtres pop-up s’ouvrent en nombre.

Votre site internet connaît un pic d’activité soudain, sans aucune raison logique ou, à l’inverse, sa fréquentation a chuté brutalement.

Des fichiers ont été créés ou modifiés sans intervention de votre part ou du salarié concerné.

Un ou plusieurs ordinateurs ne démarrent plus, ne répondent plus ou fonctionnent anormalement.

Des services que vous n’avez pas autorisés sont ouverts.

Des logiciels que vous n’avez pas installés sont présents sur les postes de travail.

Les mots de passe ont été réinitialisés, vous n’avez plus accès aux services concernés.

Des comptes ont été créés, modifiés ou détruits sans autorisation.

Certains signes peuvent paraître anodins, de même que d’autres peuvent n’avoir aucun lien avec des hackers, mais il convient, dans tous les cas, de vous montrer vigilant et de réagir immédiatement.

NE PAS PANIQUER, MAIS INTERVENIR IMMÉDIATEMENT

En cas de cyberattaque suspectée, vous devez réagir vite, mais sans précipitation. Des décisions trop hâtives pourraient entraîner des dommages plus grands comme des perte de données.

Cependant, nous conseillons d'isoler du réseau tous les postes infectés pour éviter une propagation, notamment pour les ransomware.

La première chose à faire est d'analyser la situation : quels éléments ont été infectés et quelles en sont les conséquences ? Organisez une cellule de cybercrise avec le responsable de la sécurité et tous les collaborateurs clés afin de déterminer le scénario d'attaque et définir un plan d'action.

Il faudra également identifier les ressources à protéger, évaluer les suites judiciaires et réfléchir à la communication à adopter si l'information d'une cyberattaque a fuité.

Pour limiter les conséquences de la cyberattaque, vous pouvez :

- Mettre à jour les logiciels.
- Changer tous les mots de passe.
- Tenter un nettoyage à l'aide d'un antivirus.
- Restaurer une sauvegarde.

S'il s'agit d'une attaque de type chantage, il ne faut pas céder : comme nous l'avons vu dans la première partie, les risques que le hacker ne tienne pas parole ou recommence sont particulièrement élevés. Qu'il s'agisse de cliquer sur un lien, appeler un numéro ou directement faire un virement, ne prenez aucun risque et demandez de l'aide.

DEMANDER DE L'AIDE

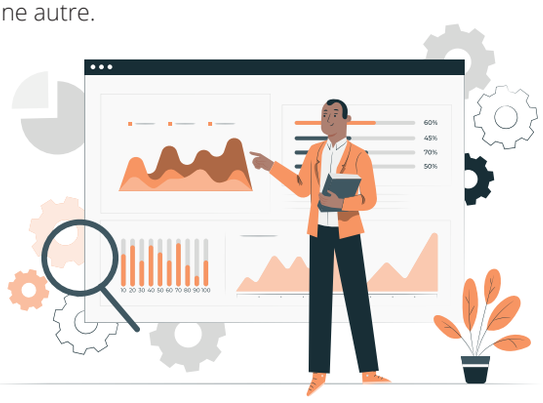
Dans certains cas, il est possible de régler seul le problème en interne, notamment lorsque l'entreprise dispose d'un service informatique efficace. Si l'attaque est trop importante ou que vous ne disposez pas des ressources internes pour y faire face, il est recommandé de faire appel à un expert de la cybersécurité.

Il saura identifier le type d'attaque et mettre en place des actions pour la stopper ou en limiter l'impact.

RETOUR À LA NORMALE : mise en place d'outils de sécurité pour empêcher de futures attaques

La cyberattaque vous a permis de comprendre que votre entreprise présente des failles de sécurité. Ces failles ne doivent pas être considérées comme uniques : par exemple, ce n'est pas parce qu'un hacker a privilégié l'email pour vous attaquer que seule votre messagerie est faillible. C'est, au contraire, l'occasion idéale pour revoir toute votre stratégie de cybersécurité : réaliser un audit pour identifier toutes les failles potentielles, adopter de nouveaux outils de sécurité plus performants, informer et former vos salariés...

Vous n'avez pas pu empêcher cette cyberattaque, mais vous pourrez ainsi limiter les risques d'en subir une autre.



LE FUTUR DES CYBERATTAQUES : ANTICIPATION ET PRÉVENTION

Les cybercriminels se montrent toujours plus ingénieux : s'il faut craindre l'arrivée de nouveaux types d'attaques, **il ne faut pas négliger non plus les méthodes déjà anciennes et qui se perfectionnent de plus en plus**. Plus que jamais, les entreprises doivent se montrer vigilantes et adopter des solutions efficaces et durables pour se protéger.

Des cyberattaques de plus en plus sophistiquées

Le phishing fait figure de classique. Bien que largement connu, il continue pourtant à faire de nombreuses victimes. Les cybercriminels apprennent de leurs erreurs et améliorent sans cesse leurs techniques pour produire **des emails toujours plus crédibles**. Il est déjà difficile pour les salariés d'identifier les emails frauduleux, malgré les efforts des entreprises pour les sensibiliser et informer. C'est pourquoi il est nécessaire de sécuriser la messagerie avec des outils fiables, capables de repérer les emails frauduleux et de les filtrer automatiquement.

Il en va de même avec le ransomware qui représente déjà une menace et qui va continuer à se déployer ces prochaines années. D'une part, les techniques s'affinent sans cesse pour piéger des victimes et contourner les systèmes de sécurité. Et d'autre part, les cybercriminels visent de plus en plus d'entreprises avec cette méthode.

Les réseaux sont eux aussi de plus en plus exploités par les cybercriminels. Ils représentent à la fois une porte d'entrée idéale vers les entreprises, mais aussi un plan B très intéressant lorsque l'entreprise ciblée ne peut pas être atteinte directement. Les attaques par rebond vont ainsi se multiplier, d'autant plus avec le déploiement de la 5G qui va impliquer un remaniement des réseaux à grande échelle. D'après une étude de Forrester pour Hiscox, 68 % des entreprises françaises interrogées ont été victimes d'une attaque par rebond en 2018, et ce n'est qu'un début (2). Pour se protéger, les entreprises doivent non seulement sécuriser parfaitement leurs réseaux, mais aussi s'assurer que leurs protections restent efficaces dans le temps.

Une autre menace, plus pernicieuse, s'invite déjà chez les particuliers et les entreprises : **les objets connectés et le cloud** (les espaces de stockage en ligne). C'est véritablement le futur des cyberattaques, une aubaine pour les cybercriminels !

Pour bien comprendre l'ampleur du phénomène, il faut savoir que **89% des entreprises utilisent le cloud pour stocker une partie de leurs données** et 55 % le font avec le cloud public. Malheureusement, 46 % des salariés n'en maîtrisent pas l'utilisation ! [1] Ajoutons à cela que les clouds publics sont rarement sécurisés convenablement.

Quant aux objets connectés, s'ils nous rendent de nombreux services, ils représentent également une opportunité parfaite pour la cybercriminalité :

- Un rapport de Zscaler, entreprise spécialisée dans la sécurité des réseaux informatiques, indique que pas moins de 91,5 % des données qui transitent par des dispositifs IoT dans les réseaux d'entreprise ne sont pas chiffrées. Ce manque de chiffrement les rend particulièrement vulnérables à ces cyberattaques. [3]
- La majorité des organismes de santé, des fabricants d'objets connectés (IoT) et des entreprises qui exploitent des IoT ont déjà subi une cyberattaque sur leurs IoT au cours des 12 derniers mois. [5]

Des menaces liées à l'Intelligence Artificielle

Les tendances technologiques actuelles montrent une évolution rapide des capacités des algorithmes d'Intelligence Artificielle. Ceux-ci deviennent plus perfectionnés, mais aussi beaucoup plus faciles à mettre en œuvre, ce qui fait craindre la possibilité croissante de leur utilisation pour industrialiser des attaques informatiques.

En particulier, nous avons identifié **trois types d'algorithmes** ayant une application directe dans le cadre de tentatives de phishing par d'autres canaux que l'email :

01

La génération automatique de texte

Les programmes modernes sont capables de générer des textes très proches de ceux écrits par un humain, et sont capables de prendre en compte un contexte, comme on peut le tester en direct sur le site https://inferkit.com. Des pirates pourraient utiliser ce genre d'algorithmes pour faire des vagues massives d'emails, tous différents les uns des autres, mais tous pertinents. On peut même imaginer des emails personnalisés à partir d'informations récupérées sur les employés, par exemple au travers des réseaux sociaux.

02

Les robots capables d'avoir des conversations téléphoniques

Les avancées d'entreprises comme Google montrent des algorithmes capables de tromper un humain dans une conversation téléphonique, dans des contextes de plus en plus complexes. Cela peut ouvrir la voie à des tentatives de phishing par téléphone.

03

Le DeepFake

C'est-à-dire le fait de remplacer un visage dans une vidéo par celui d'une autre personne. Là encore, les applications sont pour le moment limitées, mais la technologie évolue rapidement et pourrait être utilisée dans le cadre d'usurpations d'identité à travers des appels vidéo.

Quelles solutions pour se protéger efficacement et durablement ?

Comme nous l'avons vu, la porte d'entrée principale pour les cybercriminels est la messagerie, c'est donc un élément clé à protéger. Pourtant, il n'est pas réaliste d'exiger des salariés qu'ils gèrent seuls ce problème : **ils reçoivent sans cesse de nombreux emails, bien trop pour leur accorder à tous le même degré de vigilance**. Quand bien même vos employés seraient particulièrement informés et attentifs sur les risques de cyberattaque, les cybercriminels inventent sans cesse de nouveaux stratagèmes pour les piéger. La gestion de la messagerie, avec en plus la prise en compte des risques liés aux emails frauduleux, génère pour les salariés du **stress et une perte de productivité**. Il est plus que jamais nécessaire d'utiliser des outils réellement efficaces pour sécuriser totalement la messagerie et soulager les employés.

C'est pourquoi la meilleure protection viendra de la combinaison d'une solution technologique et de la sensibilisation des employés.

La solution Mailinblack Protect répond aux besoins précis des entreprises via une solution clé en main qui combine le meilleur de la technologie au service de votre sécurité. Cette **solution innovante repose à la fois sur l'intelligence artificielle et l'intelligence humaine**, ainsi que sur un modèle de DeepLearning puissant et propriétaire. C'est une protection à 360°, qui inclut anti-spam, anti-phishing, anti-malware et anti-spearphishing. Outre la sécurité optimale assurée par cette solution, elle offre également un **gain de temps réel pour les salariés** : les emails sont automatiquement triés, les messages frauduleux, publicitaires et autres newsletters laissent la place aux seuls emails professionnels. En moyenne, le volume d'emails est ainsi réduit de 70 %.

De plus, la société Mailinblack propose des **campagnes de simulation de phishing** permettant à ses clients de former ses employés en conditions réelles. En plus de **mesurer leur vulnérabilité face à ce type d'attaques**, les entreprises qui mettent en place ce type de démarches peuvent observer la progression de leurs employés au fil des campagnes et faire d'eux une véritable couche de protection supplémentaire.

LE MOT DE LA FIN

Les entreprises représentent une cible privilégiée pour les cybercriminels, toujours plus inventifs et ingénieux. Les conséquences de leurs attaques sont dramatiques : perte de chiffre d'affaires, arrêt de la production, image de marque dégradée… Dans de nombreux cas, la cyberattaque entraîne même la fermeture des entreprises visées. L'email demeure la voie royale pour ces criminels, mais bien d'autres menaces existent et se développent, portées par le déploiement des nouvelles technologies.

Il est indispensable de savoir comment réagir en cas de cyberattaque, mais le mieux sera toujours d'éviter tout simplement d'être attaqué. Les entreprises doivent devenir cyberrésilientes, en mettant en place des barrières technologiques, comme une solution pour sécuriser la messagerie, et en informant et formant leurs employés. C'est ainsi qu'elles pourront limiter les risques et développer sereinement leur activité.

Description de l'entreprise

Mailinblack est une **société française** qui dédie ses compétences humaines et ses ressources technologiques à la sécurité des entreprises. Nous nous investissons chaque jour à vos côtés pour vous apporter des **solutions innovantes et efficaces**, dans une véritable démarche sociétale et dans une relation basée sur l'écoute, l'échange et le partage. Notre solution sur mesure Mailinblack Protect est compatible avec tous les serveurs de messagerie et permet de répondre aux besoins spécifiques de chaque client. Notre équipe accompagne **depuis 15 ans** des entreprises issues de secteurs variés et les aide à sécuriser leur messagerie au quotidien, non seulement en leur fournissant des outils performants, mais aussi en leur proposant des conseils et des formations. Nos valeurs, notre expertise et notre engagement, mais aussi la confiance qu'ont placée en nous déjà **plus de 10 000 clients**, nous ont permis de nous positionner comme leader en France des technologies propriétaires.

Sources

(1) Baromètre de la cybersécurité des entreprises, Vague 5 – Janvier 2020 :
https://www.cesin.fr/uploads/files/BJ20433%20-%20Barom%C3%A8tre%20du%20CESIN%20vague%205%20-Vdef.pdf

(2) Étude de Forrester pour Hiscox :
https://www.hiscox.co.uk/cyberreadiness

(3) Rapport Zscaler :
https://www.lemondeinformatique.fr/actualites/lire-plus-de-90-des-donnees-iot-en-entreprise-ne-sont-pas-chiffrees-75397.html

(4) Silicon.fr :
https://www.silicon.fr/avis-expert/2020-la-france-championne-des-cyberattaques

(5) GlobalSign :
https://www.globalsign.fr/fr/blog/previsions-2020/

CONTACTEZ-NOUS

contact@mailinblack.com

+33 (0)4 88 60 07 80

www.mailinblack.com

4 place Sadi Carnot, 13002 Marseille