LA PROXIMITÉ INFORMATIQUE

LIVRE BLANC

Comment sécuriser votre système d'information contre les cyberattaques

INTRODUCTION

Equifax, Yahoo, LinkedIn, Renault, Marriott, Microsoft, Axa, Robinhood… Ce ne sont que quelques noms d'entreprises qui ont été victimes de cyberattaques au cours des dernières années. Or, si on parle beaucoup des grands groupes, toutes les entreprises et organisations sont concernées. Les ETI, PME et TPE sont aussi la cible régulière des hackers en raison de la faiblesse supposée des défenses portées par des ressources technologiques limitées.

Et si on y ajoute les institutions publiques, les collectivités territoriales et les établissements de santé, il n'a jamais été aussi urgent de renforcer sa cybersécurité. **187 incidents subis par des collectivités territoriales, soit 10 par mois en moyenne, ont été déclarés à l'Anssi entre janvier 2022 et juin 2023.**

La cybercriminalité n'est pas une menace nouvelle : c'est en 1955 que l'on voit la première apparition du mot « hacking » au MIT, aux États-Unis.

Toutefois, c'est bien plus tard, à partir des années 90 que le rythme s'accélère fortement dans une société qui s'informatise de plus en plus.

Ainsi, en 1994, le piratage du système informatique de la Citibank à New York fait disparaître 10 millions de dollars des comptes de la banque.

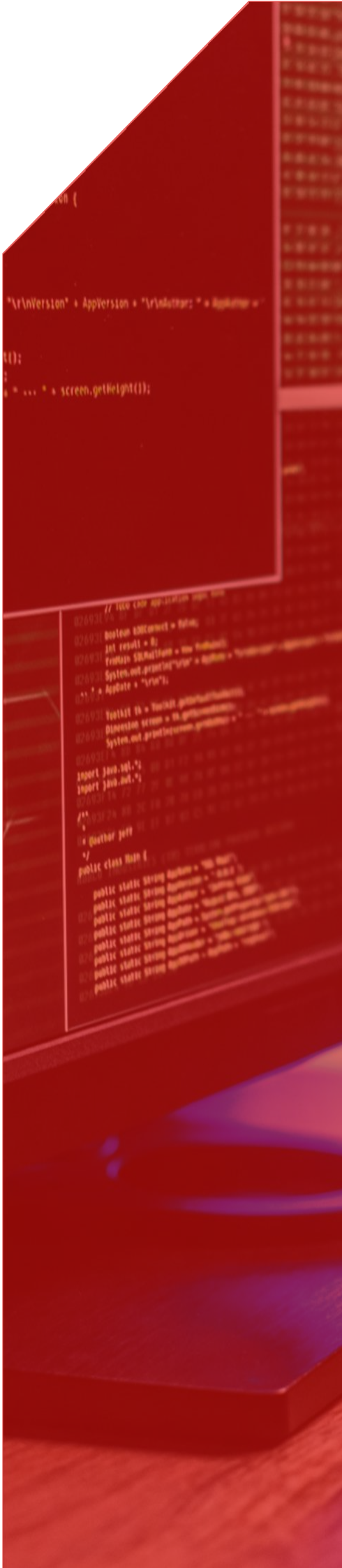
En 2013, 30 000 sites web sont piratés chaque jour. Aujourd'hui, une cyberattaque se **produit toutes les 39 secondes** à travers le monde et en 2021, les attaques par ransomware ont enregistré **une augmentation de 102%** par rapport à l'année précédente.

Dans ce contexte, les questions de cybersécurité ne sont pas des questions ou des sujets techniques.

Ce sont des sujets business, car une attaque peut mettre à mal une entreprise mal préparée : perte de fichiers, perte de clients, perte de confiance... se relever d'une attaque a des effets importants sur la pérennité d'une organisation, en particulier dans le contexte lié aux évolutions du monde du travail :

La transition accélérée au télétravail

Les organisations ont déployé des solutions pour **permettre l'accès à distance aux services et applications informatiques**, sans toujours bien prendre en compte la question de la cybersécurité.



Une sensibilisation et des formations limitées

Les collaborateurs, **n'ont pas toujours les bons réflexes ou les connaissances** pour parer les tentatives d'hameçonnage ou les fichiers et liens dangereux.

Une professionnalisation des attaques

Avec des moyens de plus en plus importants, en particulier envers les entreprises évoluant dans **des secteurs sensibles comme la communication, les médias, la finance, la défense, l'aéronautique, la construction, etc.**

Une mobilité omniprésente

Ouvre de nouvelles opportunités pour les pirates via des attaques utilisant des applications mobiles vérolées ou des accès Wi-Fi corrompus.

L'usage massif de solutions cloud

Et en particulier de logiciels qui ne sont pas toujours aussi protégés ou perfectionnés qu'ils devraient l'être.

Une sécurité qui n'est pas toujours la priorité des TPE, PME et collectivités

Qui sont de plus en plus ciblées par les pirates en raison des ressources et des systèmes de sécurité moins robustes que les grandes organisations.

Ce livre blanc vous donnera donc les clés et les enjeux pour mieux comprendre les questions de cybersécurité, son impact sur votre activité quotidienne, et l'importance d'être bien accompagné pour y faire face.

Bonne lecture !

01.

Les risques, les enjeux et les impacts des cyberattaques pour votre organisation

Pour le cabinet PWC la pénurie mondiale d'ingénieurs en cybersécurité se monte jusqu'à 3,5 millions. La crise sanitaire a amplifié le sujet de la cybersécurité, car **40% des dirigeants français observent une intensification des interactions entre les équipes de sécurité et les dirigeants d'entreprise.**

La sécurisation de votre système d'information est donc une question stratégique qui nécessite une réponse adaptée. Et la première étape consiste à mieux comprendre les menaces existantes.

LE SHADOW IT

Quelle que soit le taux de travail à distance dans votre organisation, **tous vos collaborateurs utilisent de nombreuses applications dans leur quotidien.** Ils s'attendent d'ailleurs à retrouver ces usages dans le cadre de leurs missions de travail avec une conséquence directe : si l'entreprise ne fournit pas les outils dont ils ont besoin ou si les logiciels en place sont trop complexes, mal pensés ou inadaptés, ils vont les chercher eux-mêmes.

C'est ainsi que l'on voit des commerciaux échanger des informations sur WhatsApp, des comptables travailler avec des documents Google depuis un compte personnel, des marketeurs tester des logiciels d'emailing ou d'automatisation avec des données de clients ou de prospects en dehors de tout cadre précis, etc. Toutes ces pratiques peuvent sembler anecdotiques. Mais en réalité, **elles créent toutes un nouveau point d'entrée, des échanges de données non sécurisés, non contrôlés et la création de canaux de communication officieux et parallèles qui échappent à tout contrôle.**

LE RANSOMWARE (OU RANÇONGICIEL)

C'est un logiciel qui chiffre les fichiers d'un ordinateur et qui nécessite le paiement d'une rançon (généralement via une cryptomonnaie comme le bitcoin) pour le déverrouillage. Un simple clic sur un lien vérolé ou un fichier infecté peut **mener à l'installation du ransomware à l'insu de l'utilisateur.** Une fois installé et déployé, il peut contaminer toutes les machines connectées au réseau et **paralyser le système informatique d'une société.**

Résultat : impossible de se servir de son ordinateur et d'accéder à son fichier client ou ses documents. Pire : la perte des données engendre aussi une perte ou un chiffrement des jeux des sauvegardes en raison de la capillarité du réseau informatique. La situation est alors critique et peut remettre en question la viabilité de l'organisation.

L'ADVANCED PERSISTENT THREAT

L'Advanced Persistent Threat (APT - ou « menace persistante avancée ») est une **approche qui implique des infiltrations longues et discrètes à travers le réseau pour récupérer des documents ou des données confidentielles ciblées**. L'APT peut cibler toute organisation, en particulier si elles sont des sous-traitantes ou partenaires de groupes ayant une importance stratégique, ou si elles sont détentrices d'un savoir-faire, d'un brevet ou d'une technologie en particulier.

Les pirates utilisent l'APT en lien avec une stratégie de social engineering afin de collecter des informations personnelles sur des plateformes publiques ou des réseaux sociaux pour crédibiliser leur stratégie.

LE PHISHING

Le phishing (ou hameçonnage en français) reste une menace courante, bien que très connue. Le principe est simple : vous recevez un e-mail qui semble venir, par exemple, de votre banque ou de votre fournisseur d'accès internet, vous demandant de vous identifier pour régler un problème urgent. Le lien renvoie vers un site en tout point semblable au site officiel, mais appartenant au pirate **qui récupère alors vos identifiants**. Ces e-mails peuvent être envoyés en masse ou de manière très ciblée suite à un précédent vol de données, ce qui augmente le taux de conversion des victimes pour les pirates.

Pour faire monter la pression et inciter les utilisateurs à partager leurs identifiants ou données personnelles, les pirates ajoutent très souvent une contrainte de temps. Ils peuvent ainsi dire qu'une amende devra être payée sous 3 jours, ou 24 heures si l'utilisateur ciblé ne se connecte pas pour annuler.

On peut aussi ranger dans cette catégorie, les pirates qui se font passer pour un directeur ou un manager et qui prétendent être en réunion avec un client très important.

Ils ne peuvent pas être dérangés et auraient besoin d'une carte cadeau afin de la faire parvenir à ce client dans les plus brefs délais. Dans les pires des cas, ce faux directeur peut aussi insister auprès de son comptable pour envoyer un virement dans une banque à l'étranger sous différents prétextes. Ces demandes urgentes peuvent avoir des conséquences importantes et il est essentiel de savoir les détecter et s'en protéger.

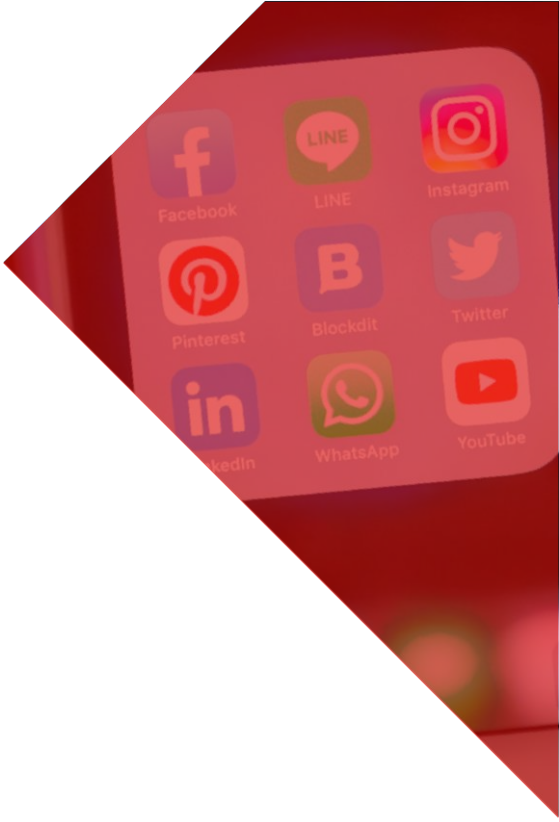
LES RÉSEAUX WI-FI PUBLICS

Les réseaux Wi-Fi publics sont très pratiques dans un café, un hôtel, une gare ou un aéroport. Pourtant, c'est aussi **un vrai danger pour la sécurité et la confidentialité de vos données.** En effet, pour un pirate expérimenté, un réseau Wi-Fi public est un terrain de jeu idéal grâce à deux techniques faciles à mettre en place :

La technique du jumeau maléfique : le pirate installe son propre hotspot Wi-Fi public à partir d'un ordinateur connecté à internet qu'il nomme soigneusement afin de tromper les utilisateurs. Vous êtes à l'hôtel du château ? Il suffit de créer un réseau intitulé « Hotelchateau_wifi » pour que les utilisateurs s'y connectent en toute confiance. Même chose pour votre entreprise ABC. Un réseau «ABC_invités » peut sembler suffisamment légitime pour que vos clients, partenaires et fournisseurs puissent s'y connecter lorsqu'ils vous rendent visite. Une fois connecté, tout ce qui s'y passe devient transparent pour le pirate qui peut récupérer la liste des sites visités, des numéros de carte bancaire, des mots de passe et une grande quantité de données personnelles.

La technique du « Man-in-the-middle » : le pirate s'introduit sur un réseau Wi-Fi puis intercepte toutes les communications qui transitent. L'ensemble des interactions entrantes et sortantes passe alors par le pirate qui est invisible pour les utilisateurs, mais qui surveille tout.

LES APPLICATIONS MOBILES



Selon une étude de NowSecure portant sur plus de 400 000 applications disponibles sur le Google Play Store, **11% des applications font fuiter des informations sensibles et 25% ont au moins un risque de sécurité important.** Sans compter que la moitié des applications - y compris les plus populaires - envoient des données à une ou plusieurs régies publicitaires pouvant inclure les numéros de téléphone, les numéros IMEI, la liste des appels et les emplacements géographiques. Dans certains cas, une application peut même prendre le contrôle de votre téléphone et accéder à vos renseignements confidentiels comme vos mots de passe, vos photos et vos informations bancaires.

Un pirate peut aussi exécuter des failles dites « zéro day » qui n'ont pas encore été corrigées et qui sont très dangereuses. C'est ainsi que le PDG d'Amazon **aurait été piraté par les services saoudiens à partir d'une conversation WhatsApp.** Les applications mobiles, même si elles sont légitimes, peuvent donc aussi ouvrir la porte aux pirates. Une fois dans un mobile, les pirates n'ont plus qu'à se servir : accès aux données stockées sur le téléphone, lancement d'un programme vérolé, surveillance de l'utilisation du téléphone, interception des données de communication et de géolocalisation, accès au micro ou à la caméra, etc.

02.

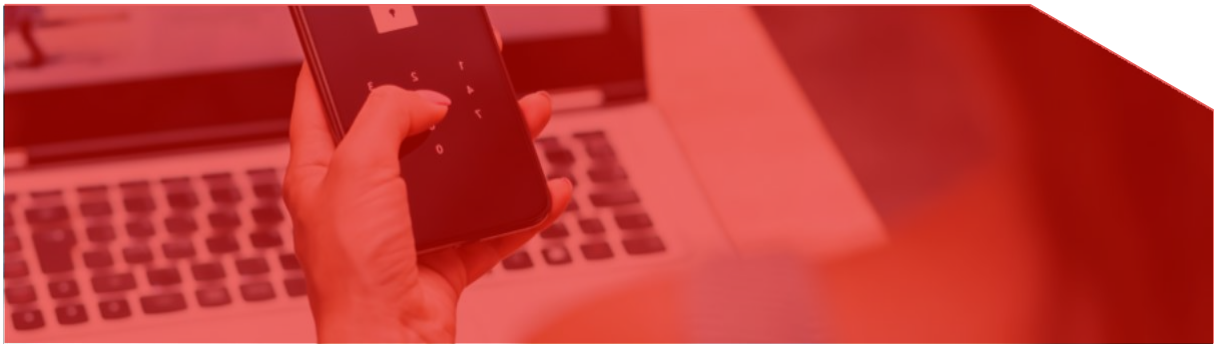
Les bonnes pratiques pour votre organisation

Une étude de l'institut Ponemon financée par IBM a pris le temps de s'intéresser aux menaces informatiques, pays par pays.

En France, le risque numérique se répartit de la façon suivante :

- **Attaques criminelles (ciblées ou opportunistes)** : 50% des cas.
- **Problème technique ou défaillance du système informatique ou logiciel** : 19% des cas.
- **Erreur humaine** : 31% des cas.

Clic sur un lien inadéquat, non-respect des mises à jour logicielles, mots de passe simples et identiques pour tous les comptes… Si les raisons qui peuvent mettre en danger le système d'information d'une organisation sont nombreuses, l'utilisateur est toujours impliqué dans la chaîne d'actions qui précède une attaque. Qu'il s'agisse de négligences, de manque d'intérêt ou de temps, ne pas impliquer les utilisateurs peut avoir des conséquences importantes.



METTRE EN PLACE UNE CHARTE INFORMATIQUE D'ENTREPRISE

C'est un document qui repose sur les mêmes principes qu'un règlement intérieur avec des règles à suivre et des bons comportements à adopter en matière d'informatique et de cybersécurité.

C’est aussi un contrat moral qui lie les collaborateurs à leur organisation afin de mettre en place des procédures adaptées pour l’utilisation des matériels et logiciels.

L’objectif est de déterminer ce qui est accepté, toléré et interdit. Quelques exemples :

Il est **accepté** et **attendu** qu’un collaborateur utilise son ordinateur professionnel à des fins professionnelles en demandant explicitement une autorisation pour installer tout nouveau logiciel métier.

Il est **toléré** de connecter un ordinateur professionnel à un réseau Wi-Fi personnel en télétravail à condition de passer par un VPN.

Il est **interdit** de communiquer avec des clients ou fournisseurs avec des outils non approuvés par la DSI, du type WhatsApp ou Messenger.

Sans une charte pour fixer des objectifs clairs et des cas d’usages en matière de cybersécurité, la responsabilité des initiatives de gouvernance de la sécurité sera probablement indéfinie au sein de l’entreprise. Cela veut dire que les salariés seront les seuls juges de ce qu’ils veulent ou peuvent faire. La charte vient cadrer le tout pour garantir que le développement et la gestion de vos politiques de sécurité répondent à une vision claire et précise.

SENSIBILISER LES COLLABORATEURS

La formation est indispensable pour sensibiliser ses collaborateurs. C'est une mission qui peut d'ailleurs nécessiter le travail d'un designer pédagogique, afin de créer des parcours d'apprentissage personnalisés, adaptés aux fonctions et aux rôles des salariés.

Ces formations doivent être régulières, non techniques dans la majorité des cas, et illustrées avec de nombreux exemples concrets.

Sur le plan organisationnel, le blended learning qui comprend **un mix de formations en présentiel et en ligne est une option qui fonctionne bien.** Une plateforme d'apprentissage peut ainsi intégrer un système de quiz et de vérification des acquis, ainsi que des sessions de vidéo à la demande visionnables selon les contraintes des équipes. Il est important de garder en mémoire que la formation doit être récurrente.

Deux heures de sensibilisation à l'arrivée d'un nouveau collaborateur ne seront pas utiles si les messages, bonnes pratiques et conseils en matière d'hygiène numérique ne sont pas répétés régulièrement.

Sensibiliser et former ses collaborateurs est indispensable pour protéger son entreprise des menaces informatiques. Personne n'a envie d'être accusé de négligence en cas de problème. Sécuriser ses actifs est loin d'être une simple charge opérationnelle. C'est un investissement qui protège votre activité, votre rentabilité, vos salariés et votre réputation.

FOURNIR LES BONS OUTILS POUR LE NOMADISME ET LE TÉLÉTRAVAIL

Le travail à distance et en mode hybride s'est largement démocratisé suite à la pandémie de COVID-19.

Il est donc indispensable de fournir aux équipes les bons outils pour **travailler dans tous les environnements et dans tous les contextes, comme :**

- **Les outils de protection** : on y retrouve les antivirus, l'EDR (Endpoint Detection and Response), la détection du phishing, le chiffrage de données, le MDM (Mobile Device Management), etc.
- **Des outils d'accessibilité** : c'est notamment le cas des gestionnaires de mots de passe, les VPN pour se connecter sur des réseaux sécurisés, l'authentification renforcée à l'aide des solutions multifactorielles, certains outils de surveillance selon la politique de l'entreprise, etc.
- **Des outils de connectivité et de productivité** : des solutions de messagerie, de téléphonie virtuelle (VoIP), des applications professionnelles selon les métiers, des plateformes de cloud et de transfert de fichiers, etc..

Pour tous ces outils, il existe **des solutions de protection qui doivent être déployées**. Ainsi, un message sur Slack, un PDF sur Google Drive, ou un document Word sur Sharepoint, par exemple, seront protégés pour éviter tout risque.

SÉCURISER LES OUTILS D'ENTREPRISE

Il ne peut y avoir de cybersécurité sans une équipe de professionnels et d'experts, que ce soit en interne, ou en service managé avec un prestataire tiers.

Son rôle consiste à gérer la stratégie IT de l'organisation, à **s'assurer que tout est conforme aux règles en vigueur, à gérer les mises à jour** (OS, programmes, antivirus, etc.), à **surveiller le réseau**, et à **mettre en place un plan de continuité** en cas de défaillance grave.

Disposer d'un centre opérationnel en cybersécurité (SOC), est **un atout indispensable dans la détection préemptive des cyberattaques.** Utilisant les dernières techniques de détection, souvent épaulées par l'intelligence artificielle, des équipes d'experts analysent et anticipent les attaques complexes qui échappent souvent à la détection traditionnelle des protections antivirus. Un centre opérationnel en cybersécurité permet également d'apporter une réponse efficace dans la gestion d'un incident, lorsqu'il s'agit d'isoler l'attaque et de mener des investigations pour corriger les éventuelles failles exploitées dans attaque.

De plus, le cœur du réacteur est lié à la supervision informatique et au support. Si un collaborateur a un problème avec un logiciel qui l'empêche de travailler**, il ne doit pas attendre 48 heures pour avoir une réponse.** C'est la même chose avec les questions de cybersécurité. Pour savoir si un e-mail est légitime ou si on peut ouvrir une pièce jointe envoyée par un nouveau fournisseur ou un client, le service desk doit pouvoir intervenir rapidement.

Pour simplifier ce travail, et aller au-delà, un outil de supervision est souvent indispensable, car les systèmes d'information sont de plus en plus complexes. Cela permet de faciliter le suivi de performance de l'ensemble des applications, qui pourront rapidement être intégrées, analysées et optimisées, quel que soit le département de l'entreprise. L'objectif reste bien sûr de prévenir les indisponibilités, gérer les priorités d'intervention ou encore pouvoir réagir rapidement en cas de problème.

A titre d'exemple, si toutes les équipes doivent passer au télétravail en trois jours, il sera indispensable de pouvoir s'assurer en priorité de la disponibilité des applications à distance.

Gartner prévoit d'ailleurs que dans les prochaines années, **40 % des grandes entreprises combineront le big data et le machine learning pour renforcer ou remplacer partiellement la supervision**. L'intelligence artificielle aidera également à automatiser certaines tâches chronophages ou sans valeur ajoutée (génération de ticket, consolidation de tableaux de bord...) pour l'amélioration de la disponibilité de l'IT afin que l'entreprise se concentre sur son core business.

NE PAS ÉGLIGER LE MOBILE

Un nombre croissant de professionnels dépendent de l'usage de smartphones et tablettes pour travailler, lorsqu'ils sont en déplacement, sur un salon, en rendez-vous extérieur, ou parfois, en télétravail. Le mobile est un point d'entrée important pour les pirates. Déployer un outil de MDM (Mobile Device Management) pour les téléphones et tablettes professionnels permet de limiter les risques et de mieux sécuriser ces terminaux.

Une solution de MDM permet à la DSI de savoir combien de téléphones sont opérationnels, à qui sont-ils assignés, où sont-ils, quels sont les usages, etc. Elle peut **aussi limiter certaines utilisations comme le téléchargement d'applications non autorisées.** Son objectif est d'harmoniser et de sécuriser des terminaux en s'assurant que **tous les collaborateurs aient des applications à jour** et que leurs appareils soient correctement paramétrés, tout en appliquant des politiques visant protéger les données sensibles de l'entreprise. Un MDM peut aussi imposer l'utilisation d'un code de déverrouillage et le chiffrement global ou ciblé du contenu. De plus, en cas de perte ou de vol, vous pouvez aussi désactiver l'appareil à distance, protégeant ainsi vos données confidentielles.

ÊTRE BIEN ENTOURÉ

La sécurisation de votre système d'information est un travail d'équipe. Parce que vous n'avez pas toutes les expertises en interne et que votre temps est consacré à de nombreux sujets stratégiques, choisir un prestataire pour vous accompagner dans la mise en place de ces bonnes pratiques est indispensable.

Il doit ainsi intervenir sur la partie conseil et accompagnement, afin de réaliser des audits, de comprendre la culture de l'entreprise, **les outils utilisés et les risques encourus**. Chaque système d'information est unique et les risques et failles peuvent prendre différentes formes. Sans audit approfondi, il est impossible de fournir des recommandations adaptées.

Votre prestataire doit donc être en mesure de comprendre tous les systèmes d'informations de l'entreprise, allant jusqu'aux CMS des sites internet ou des plateformes sur lesquelles transitent des données personnelles, comme les outils de marketing, de paiement, de logistique, etc. Il faut également prendre en considération tous les outils connectés, qu'ils soient personnels ou professionnels (ordinateurs, téléphones, tablettes, mais aussi clés USB, solutions de cloud publiques ou privées, etc.).

CONCLUSION

La cybersécurité n'est pas une dépense opérationnelle. C'est un investissement. Imaginez que vous arrivez au bureau le lundi matin et découvrez une fuite massive de données personnelles et certains ordinateurs sont bloqués par un ransomware. La semaine démarre mal…

Les conséquences financières et organisationnelles sont immenses en cas de cyberattaques. Une étude réalisée par Deloitte a mis en lumière les impacts qui vont bien au-delà de ce que vous pouvez penser :

Les coûts directs à prévoir :

- Honoraires d'avocats et frais de justice.
- Mise en conformité réglementaire.
- Enquêtes techniques.
- Sécurisation des données post-incident.
- Relations publiques.
- Amélioration des dispositifs de cybersécurité.
- Perte de temps productif.

Les coûts indirects cachés, souvent ignorés, mais bien présents :

- Augmentation des primes d'assurance.
- Perte de contrats clients.
- Dépréciation de la valeur de marque.
- Perte de propriété intellectuelle.
- Perte de confiance des parties prenantes.
- Impacts liés à la perturbation de l'activité.
- Arrêt de travail des collaborateurs.

Le coût d'une solution complète de cyberdéfense est sans commune mesure avec le coût engendré par une attaque. Si la technique est importante, il ne faut pas non plus négliger l'impact sur le moral des collaborateurs, leur confiance, et la culture de l'entreprise. L'organisation a un devoir de protection vis-à-vis de ses collaborateurs. La cybersécurité fait aussi partie de ce devoir.

XEFI

LA PROXIMITÉ INFORMATIQUE

www.xefi.com