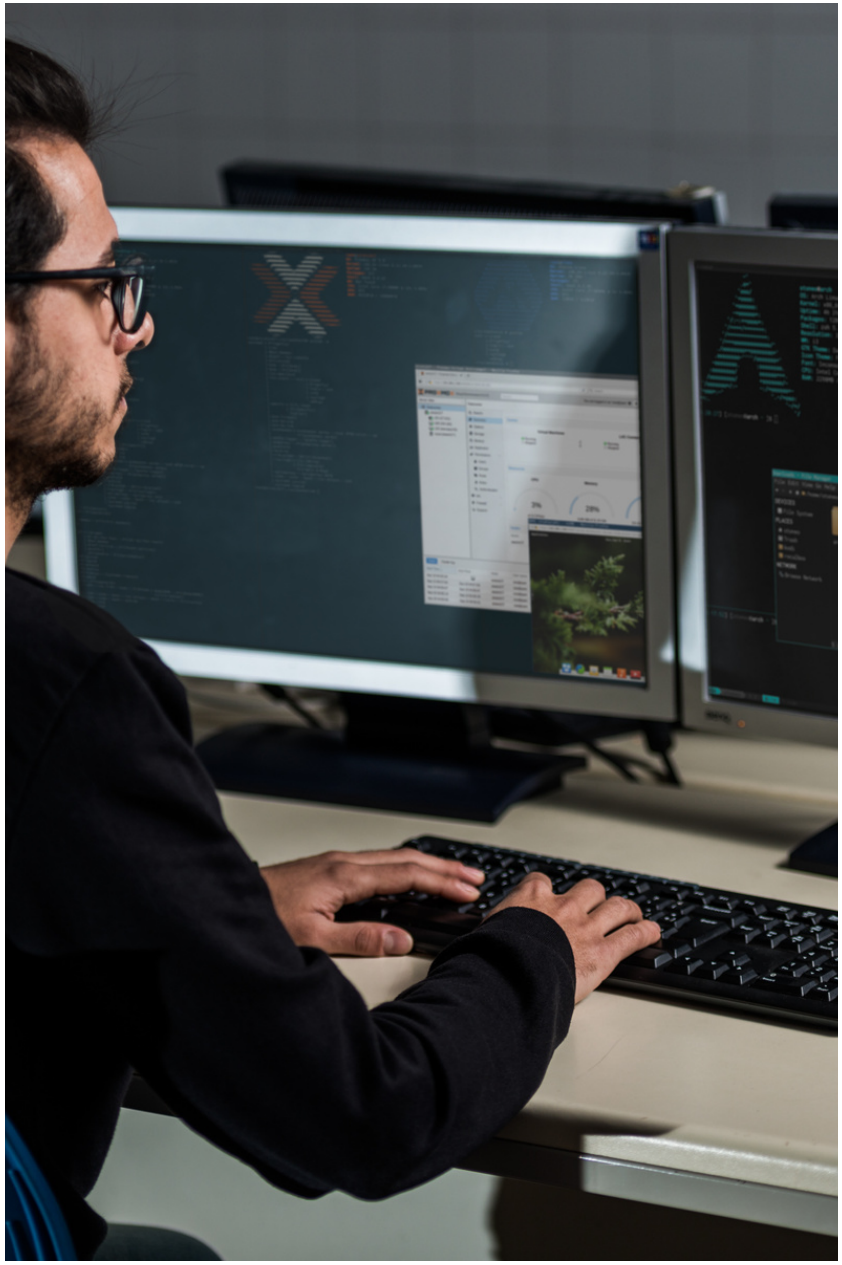
COMMENT MAÎTRISER LA SÉCURITÉ INFORMATIQUE DE VOTRE PME ?

INTRODUCTION

La gestion du risque numérique est devenue un enjeu stratégique pour toutes les entreprises. **En 2020, les cyberattaques ont atteint un taux record.** Face aux cas médiatiques retentissants, comme ceux de Meow ou de SolarWinds, des attaques moins spectaculaires ont fait partout sur le globe des centaines de milliers de victimes. La France n'est pas épargnée : selon l'Internet Crime Report 2020 du FBI, elle figure en 7ème place du Top 20 des pays les plus touchés par les cyberattaques.

L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) a révélé que les attaques sur notre territoire ont été 4 fois plus nombreuses en 2020 qu'en 2019. Ainsi, **90% des organisations françaises ont été victimes de cyberattaques l'année dernière** et, plus alarmant encore, 65% d'entre elles en ont subi plusieurs.

Le contexte sanitaire, qui a généralisé la mise en place du télétravail, souvent dans l'urgence et sans les mesures de sécurité ad hoc, a ouvert grand la porte aux pirates informatiques.



Mais de quoi parle-t-on exactement ? Définies comme des atteintes à des systèmes informatiques réalisées dans un but malveillant, les cyberattaques sont autant de menaces réelles qui exposent votre PME à des risques parfois extrêmement graves : perte financière, interruption des activités ou encore atteinte sérieuse à votre réputation.

Le manque de sensibilisation aux risques, les systèmes d'information mal maîtrisés, le non-respect des règles élémentaires de sécurité sont autant de failles que les pirates informatiques ne se privent pas d'exploiter. Et les PME, qui ne disposent souvent pas des connaissances et des moyens nécessaires pour se protéger, constituent une cible de choix. Trop souvent, les dirigeants ne se sentent pas réellement concernés. et quand ils le sont, il est souvent trop tard.

La cybersécurité est ainsi un enjeu majeur de la transformation digitale, dont peut dépendre la survie même de votre business.

C'est pourquoi nous allons vous aider à comprendre les risques concrets auxquels votre entreprise est exposée. Et parce que les cyberattaques ne sont pas une fatalité, nous vous allons dans ce guide, vous proposer les moyens efficaces pour maîtriser au mieux la sécurité informatique de votre PME.

LA CYBERSÉCURITÉ : UN ENJEU MAJEUR

DANS LA TRANSFORMATION NUMÉRIQUE

DES PME/ETI

Vous le savez : la transformation numérique est un phénomène mondial qui touche chacun d'entre nous. Particuliers, entreprises, administrations publiques, organisations privées : **personne n'y échappe**. Une révolution qui a profondément transformé le quotidien des entreprises. Qui peut aujourd'hui imaginer travailler sans Internet ni appareils connectés ?

Les interactions numériques permanentes entre collaborateurs, clients, fournisseurs ainsi que la multiplicité de nos outils informatiques ont fait entrer de plain-pied nos métiers dans le cyberespace... devenu le terrain de jeu de cybercriminels qui rivalisent d'ingéniosité pour en exploiter les faiblesses. Dès lors, toutes les entreprises sont potentiellement concernées par les cyberattaques, et parmi elles, **les PME et les ETI sont particulièrement exposées à la cybermenace**. Les réseaux informatiques des PME/PMI sont des cibles de choix car ils hébergent de plus en plus de données, et n'ont pas forcément pu bénéficier de soutien adapté en sécurité tout au long de leur transition.

Face à la multiplication des cyberattaques, il est devenu évident que chaque entreprise peut être touchée. Le débat ne se situant plus dans l'éventualité d'être attaqué ou pas, la cyber-sécurité n'est plus suffisante : la **cyber résilience** s'impose.

Il s'agit ici d'avoir conscience que l'attaque surviendra possiblement, de s'y préparer en mettant en place la meilleure défense possible pour ne pas perturber la continuité de vos affaires le cas échéant. En clair, être cyber résilient ne consiste pas à simplement sécuriser votre système d'information, mais à adapter votre politique de sécurité informatique quels que soient les événements, afin de vous relever rapidement en cas de difficultés et renforcer vos défenses existantes pour mieux répondre aux menaces futures.

L'amélioration continue est ainsi une notion clé de la cyber résilience. Face aux attaques dont vous serez —et avez peut-être déjà été — victime, votre organisation se doit d'être une organisation apprenante. Plus question de subir.

Il convient d'opter pour une approche intégrée et proactive de la sécurité numérique, afin de pouvoir en permanence identifier les incidents, s'en protéger et y répondre. Plutôt que d'attendre l'attaque, la cyber résilience vous permettra d'entrer d'ores et déjà en cyber-résistance.

QUELLES SONT LES CYBERATTAQUES

ET LES RISQUES QUI Y SONT RATTACHÉS ?

On sous-estime souvent les risques numériques. Si la grande cybercriminalité provient de réseaux organisés à dimension parfois internationale, un cyberattaquant isolé, un de vos clients, un ancien collaborateur ou un concurrent peut décider de s'en prendre à votre entreprise, de diverses façons.

Les portes d'entrée ? Votre système d'information, votre site web, tout votre matériel informatique connecté à Internet : ordinateurs, serveurs, imprimantes, smartphones ou encore tablettes. Vous vous demandez peut-être quelles sont les cyberattaques qui pourraient toucher votre entreprise ? Voici les trois plus fréquentes :

Le Phishing

Également connue sous le nom d'hameçonnage, cette technique consiste à envoyer un e-mail en se faisant passer pour quelqu'un d'autre, souvent une administration ou une entreprise existante, dans le but de soutirer des informations confidentielles (vous savez, comme ces faux emails de la CAF ou des Impôts qui vous demandent vos coordonnées bancaires).

Si vous pensez savoir détecter ces arnaques à coup sûr, dites-vous qu'à lui seul, le phishing représente plus du trois-quarts des cyberattaques subies par les entreprises...

Le Ransomware

Considéré, à juste titre, comme la principale menace cyber, un ransomware (ou rançongiciel) est un programme malveillant qui rend les données d'une entreprise inexploitable.

Bloquant les systèmes d'information pour demander des rançons, le ransomware provoque des dommages conséquents sur la production, la réputation et les finances des entreprises qui en sont victimes.

L'attaque DoS

Autrement appelée « attaque par déni de service », elles sont de plus en plus fréquentes et visent à rendre un site web indisponible en inondant le serveur de requêtes.

Les principales victimes de ce type d'attaque sont les sites d'e-commerce ou de service en ligne, dont elles paralysent totalement l'activité.

POURQUOI CES ATTAQUES ?

Les cybercriminels sont poussés par **l'appât du gain**, pour eux-mêmes ou pour le compte d'un client. Le côté ludique n'est pas à négliger : de nombreux hackers considèrent le piratage comme **une performance**, un exercice technique. La renommée joue également un rôle important : réussir un piratage spectaculaire qui fait la Une des médias leur assure une reconnaissance des autres attaquants. Enfin, il existe une cybercriminalité idéologique, qui **vise les entreprises en fonction de ce qu'elles représentent** ou des services qu'elles proposent.

ÇA N'ARRIVE PAS QU'AUX AUTRES !

En 2016, un transporteur des Landes a été victime d'un piratage via un mail infecté, qui a paralysé l'activité de ses 150 salariés en rendant inaccessibles les boîtes mails ou encore les feuilles de route des chauffeurs. Les pirates demandaient 5000€ en Bitcoin pour débloquer les données.

En 2017, des pirates informatiques ont totalement paralysé l'activité de Clermont Pièces, une PME du Puy-de-Dôme spécialisée dans les pièces d'électroménager. Les fichiers clients et le logiciel métier ont été verrouillés. Le gérant de la société a décidé de ne pas payer la rançon et a perdu tous accès à ses outils de travail. Il a été contraint de fermer son entreprise et de licencier ses huit salariés.

En 2019, une ETI de chaîne de magasins en région a été victime d'une attaque. L'ensemble de son réseau a été paralysé et ses données chiffrées par un ransomware. Pour les récupérer et reprendre son activité, la société a payé une rançon 150 000€ aux cybercriminels.

Ces entreprises font parties des rares PME/ETI qui ont communiqué sur les cyberattaques et les conséquences. Afin de préserver leur image, la grande majorité des entreprises préfère rester discrète sur les incidents dont elles ont été victimes.

DES RISQUES À NE PAS PRENDRE À LA LÉGÈRE

7 mois

Les cyberattaques ont donc des **conséquences très lourdes sur les entreprises**. Une paralysie de votre activité peut engendrer une perte financière conséquente, voire pour les PME les plus fragiles, un risque mortel. Selon l'ANSSI, **il faut en moyenne 7 mois à une entreprise pour détecter une violation de données,** et pas moins de 75 jours pour reprendre le cours normal de ses activités après une attaque... quand elle s'en relève.

Le coût moyen d'une cyberattaque pour une PME ou une ETI se situe en moyenne entre 300 000€ et 650 000€. Le piratage, le vol ou la destruction de données sont ainsi des menaces réelles à ne pas prendre à la légère : imaginez la perte de confiance de vos clients ou de vos fournisseurs s'ils savent que leurs données personnelles ont été exposées et sont à présent entre les mains de personnes malveillantes ?

Les risques judiciaires sont également présents, **la CNIL sanctionnant fortement tout manquement à la sécurisation des données des citoyens européens.** De fait, de nombreuses PME commencent à réaliser la potentielle gravité des cyberattaques qui visent leurs clients et leur réputation. Les risques financiers, l'atteinte à l'image et la perte de crédibilité ont un coût élevé qui peut être éviter en mettant en place une politique rigoureuse de gestion des risques numériques.

ÉVALUEZ-EN 4 ÉTAPES LA SÉCURITÉ INFORMATIQUE DE VOTRE PME

La mise en œuvre d'une stratégie de cybersécurité optimale commence nécessairement par l'analyse de votre environnement de travail et des mesures de sécurité existantes au sein de votre entreprise. Afin de savoir si votre PME est bien protégée contre les cyberattaques, suivez ces 4 étapes indispensables.

#1 Faites un état des lieux organisationnel et technique

Connaissez-vous l'infrastructure informatique de votre PME et savez-vous de quelle façon vos employés y ont accès ? Quels sont les outils, logiciels et appareils connectés que vos équipes utilisent ? Connaissez-vous l'ensemble de vos processus informatiques internes ?

Si ce n'est pas le cas, un état des lieux complet s'impose. Il vous permettra de détecter les portes d'entrée potentielles aux cyberattaques et d'anticiper le risque utilisateurs, tant il est vrai que les négligences humaines sont souvent à l'origine de la compromission.

#2 Évaluez les mesures de sécurité déjà mises en place

Afin de vérifier la vulnérabilité de vos serveurs, de votre réseau, de vos sites web, de vos postes de travail, réaliser un audit de sécurité est nécessaire.

Comment sont protégés vos sites Web ? Comment sont sécurisées vos données ? Les mots de passe de vos équipes sont-ils robustes ? Utilisez-vous un pare-feu ?

Faire le tour des mesures de sécurité existantes est indispensable pour évaluer si elles sont fiables ou si elles nécessitent des corrections. En fonction des ressources financières allouées à cette évaluation, il est possible de vérifier que les mesures fonctionnent par un diagnostic cyber ou par un test d'intrusion.

#3 Faites réaliser un audit de votre système informatique par des experts en cybersécurité

L'audit de votre système informatique est une étape technique qui nécessite d'être confiée à des professionnels. Il consiste en un diagnostic interne et externe du système d'information afin d'évaluer le niveau de criticité et le positionnement par rapport à d'autres entreprises. La simulation d'une attaque avec un test d'intrusion permettra d'identifier les failles de sécurité et corriger les vulnérabilités de votre système d'information.

#4 Déterminer et mesurer les risques liés à des failles de sécurité

Sur la base du rapport qui vous sera remis et des éventuelles failles critiques, ou non qui seront identifiées, vous déciderez du niveau de sécurité à atteindre pour votre entreprise et des priorités de correction des vulnérabilités. Vous faire accompagner par un expert est encore la meilleure solution pour mener à bien l'ensemble de ces 4 étapes et mettre en place une stratégie de sécurité informatique optimale.

CT-SQUARE : UNE ÉQUIPE EXTERNALISÉE QUI VOUS ACCOMPAGNE DANS LA PRÉVENTION ET LA GESTION DES CYBERATTAQUES

Une PME seule ne peut se doter de l'expertise et des outils nécessaires pour se protéger des cyberattaques. Aucun système d'information n'est infaillible, mais la prévention et la gestion du réseau permettent d'agir à temps pour éradiquer la menace et limiter les dommages pour l'entreprise.

Notre objectif ? Rendre la cybersécurité accessible et intelligible à tous afin d'aider les dirigeants et les équipes opérationnelles à prendre les bonnes décisions. CT-Square s'est appuyé sur son expérience des PME pour développer NOSCIT, une solution simple, automatisée et opérationnelle capable de détecter et de répondre aux cyberattaques.

Le professionnalisme et l'engagement de CT-Square ont été récompensés par la certification « Customer Satisfaction 2021 » délivrée par le label Indépendant Scorefact.

TOUT COMMENCE PAR LA PRÉVENTION

Le système de défense élaboré par les ingénieurs de CT-Square repose sur des sondes de sécurité placées sur votre réseau informatique. Conçues pour déceler des attaques, des anomalies ou des actions malveillantes, elles permettent aux experts de CT-Square de vous accompagner par des recommandations préventives.

Le but étant de renforcer la sécurité de votre PME de façon adaptée et continue pour faire face aux menaces cyber qui sont complexes, évolutives et de plus en plus destructrices et exigent un niveau d'expertise et un suivi particulièrement pointu.

NOUS GÉRONS LES ATTAQUES ET LES ENDIGUONS

La **surveillance du réseau 24h/7** par les sondes de sécurité vous permet de bénéficier d'une traque continue de la menace. Les experts du centre opérationnel de CT-Square traitent les alertes de sécurité avant de vous notifier si nécessaire.

En cas d'attaque avérée, la réponse est orchestrée par CT-Square et ses techniciens qui vous accompagnent dès le départ pour maîtriser l'incident puis éradiquer la menace. **Cette réactivité permet de limiter les dommages engendrés par l'attaque.**

CONCLUSION

Face à la menace réelle et sérieuse des cyberattaques qui touchent aujourd'hui la majorité des entreprises, il existe des solutions fiables pour prévenir les risques numériques et réagir rapidement en cas d'incident.

La cyber résilience, indispensable dans notre monde connecté et interdépendant, est d'ores et déjà une approche clé à adopter pour les PME, afin de tirer le meilleur parti des évolutions numériques sans en subir les inconvénients, et continuer à prospérer sereinement.

Et vous, êtes-vous suffisamment protégé contre les cyberattaques ? CT-Square reste à votre disposition pour tout accompagnement spécifique.

CONTACTEZ-NOUS

ct. square cybersecurity

ct-square.com
info@ct-square.com
3 rue de l'Arrivée
75015 Paris