pérenne IT

PME et sécurité informatique
Par où commencer ?

Perenne-it.fr

SOMMAIRE

Introduction

La transformation digitale ne s'est pas arrêtée aux grandes entreprises, elle concerne aujourd'hui tout autant les PME et les TPE. Dans le même temps, le nombre de cyberattaques ne fait que croitre et touche aujourd'hui toutes les entreprises.

69 % *

Des victimes de cyberattaques sont des PME / TPE

→ En parrallèle de ce chiffre, le nombre de cyberattaques augmente d'année en année, et les petites et moyennes entreprises sont désormais en première ligne.

* Source : rapport d'activité CNIL 2021

La cybersécurité : une problématique majeure

Les chiffres le confirment : **les cyberattaques sont de plus en plus nombreuses**. Fort de ce constat, les dirigeants de petites et moyennes entreprises ne peuvent plus ignorer les questions de cybersécurité.

→ Quel budget investir ?

Les conséquences financières d'une cyberattaque sont souvent bien plus élevés que les investissements consentis pour s'en protéger. Mais comment définir son budget ?

→ Dois-je avoir un prestataire ?

Il est judicieux que des ressources internes soient allouées à la cybersécurité, mais peut-on pour autant se passer d'un prestataire pour garantir la fiabilité des mesures de sécurité ?

→ Peut-on garantir une sécurité totale ?

Malgré ces mesures, il est impossible de garantir que le risque d'incident n'existe plus. Que faut-il alors faire pour limiter les dégats si on incident venait tout de même à se produire ?

→ Démarche ponctuelle ou continue ?

La sécurité informatique est-elle seulement une affaire de mise en place d'outils techniques, ou bien s'agit-il d'une démarche plus globale devant être ajustée en permanence ?

Sécurité informatique : quel investissement ?

Trop souvent, les organisations perçoivent la cybersécurité comme une dépense, qu'il faut donc limiter au maximum. Or, il faut la considérer comme un investissement. Internet et la digitalisation généralisée des données sont des instruments incontournables pour le développement des entreprises, et ils permettent aussi de réduire les coûts. Cependant l'information numérisée représente une richesse croissante qu'il convient aussi de protéger à sa juste valeur.

Investir pour prévoir les risques

La cybersécurité doit d'emblée être intégrée à tout processus de traitement des données afin d'en assurer la protection de façon optimale. Contrairement aux coûts élevés des incidents de cybersécurités, ces coûts peuvent être contrôlés et planifiés. Le chef d'entreprise doit mettre en place les moyens suivants :

- Déterminer les impacts en termes financiers et mettre en face les investissements adaptés
- Informer les salariés de leurs droits et obligations au moyen d'une charte informatique.
- Organiser une surveillance du réseau informatique de l'entreprise en respectant les droits des salariés.
- Mettre l'entreprise en conformité avec la législation relative à la protection des données à caractère personnel (RGPD).
- Elaborer et formaliser un plan de continuité informatique en cas de sinistre.
- Prévoir des moyens de traçabilité et de conservation des connexions réseau.

32 000 € *

Le coût financier moyen d'une cyberattaque pour une PME.

- De nombreuses PME et TPE sont obligés d'interrompre leur activité après une cyberattaque, et certaines d'entres elles n'y survivent pas. 20 % des entreprises perdent même plus de 100 000 €

*** Source : rapport 2022 Cybersecurity Census Report**

Pourquoi commencer par un audit ?

Par nature, les risques et menaces de sécurité ne sont pas visibles et lorsqu'ils se matérialisent il est trop tard. L'audit de sécurité informatique permet de mettre en évidence la situation réelle afin de porter ses efforts à bon escient.

Les objectifs de l'audit

L'audit de sécurité va permettre de travailler sur les axes suivants :

- Technique
- Humain
- Organisationnel

Il va également mettre en exergue les vulnérabilités organisationnelles et/ou techniques, et fournir une évaluation globale, au travers du référentiel utilisé.

Élaborer un plan d'action

A l'issue de l'audit il sera possible d'élaborer un plan d'actions à plus ou moins long terme avec des points de contrôle réguliers, selon une fréquence à définir et selon les vulnérabilités identifiées et les impacts potentiels.

53 % *

La part des cyberattaques causées par l'exploitation d'une faille de sécurité.

→ Identifier ces failles de sécurité au préalable réduit fortement le risque de subir un incident.

*** Source : Baromètre de la CESIN**

Quelles ressources pour la sécurité informatique?

Les grandes entreprises disposent d'équipes dédiées et la charge de la sécurité informatique revient au RSSI (responsable de la sécurité du système d'information). Sauf rares exceptions les PME ne peuvent pas se permettre d'avoir de ressources dédiées à cette tâche.

60% *

Des violations de données ont entrainé des hausses de prix répercutées sur les clients.

→ Faire appel à un prestataire informatique limite le risque d'incident.

Quel rôle pour les prestataires spécialisés ?

Pour les TPE et les PME, il est préférable de recourir à une prestation de service externalisée qui permet de bénéficier d'une expertise à la demande, proportionnée aux besoins et aux moyens disponibles pour assurer la sécurité de l'entreprise, sans pour autant abandonner le contrôle et les arbitrages qui restent une prérogative interne.

Les missions du prestataire informatique

- Définir une politique de sécurité de la donnée et des accès aux données
- Identifier les risques et anticiper les menaces, assurer la continuité de service en cas de sinistre
- Mettre en œuvre et administrer les solutions de sécurité
- Sensibiliser les collaborateurs et dirigeants
- Vérifier régulièrement et corriger si nécessaire
- Fournir des métriques intelligibles aux dirigeants,

*** Source : Baromètre de la CESIN**

La sécurité informatique : un sujet strictement technique ?

On pense trop souvent que la sécurité informatique se résume à l'acquisition ou la mise en place d'outils techniques. Or il s'agit avant tout d'une démarche d'organisation basée sur les enjeux, les risques et les menaces. Bien qu'indispensables, les outils techniques ne sont qu'un instrument parmi d'autres au service d'une démarche de sécurité ; trop souvent mal paramétrés ou non mis à jour ils représentent une protection illusoire.

La PSSI : première étape

La sécurisation des systèmes d'information commence par la mise en œuvre d'une politique de sécurité des systèmes d'information (PSSI). Partant des enjeux business, des risques et des menaces la PSSI fixe le curseur de la sécurité (ni trop ni trop peu) et elle décrit les outils humains, organisationnels et techniques au service de la stratégie de sécurité. La PSSI doit être maintenue à jour en fonction des évolutions de l'entreprise, des technologies et de des menaces, ainsi que l'ensemble des procédures qu'elle comporte.

Dans un second temps : la mise en place d'outils techniques

Les outils techniques sont au service de la PSSI, leur paramétrage et leur utilisation décrits dans les procédures de la PSSI, mais ils ne constituent qu'une fraction du dispositif qui comporte aussi une dimension légale, RH, etc..

53 %*

Des entreprises françaises ont été attaquées en 2021.

→ Un chiffre en hausse par rapport aux années précédentes.

*** Source : Baromètre de la cybersécurité en entreprise CESIN 2022**

Comment anticiper un incident informatique ?

Malgré la mise en place de mesures de sécurité, un incident est malheureusement toujours possible. L'anticipation est la meilleure stratégie pour éviter que les conséquences perturbent, voire stoppent votre activité. Ces mesures d'anticipation ne visent pas seulement à éviter les incidents, mais à amoindrir l'impact de ces derniers.

83 % *

Des PME ne sont pas préparées à se remettre des dommages financiers d'une cyberattaque.

→ Les incidents informatiques majeurs impliquent des conséquences importantes qui doivent être anticipées

Des mesures d'anticipations

→ Sauvegardes régulières

Réaliser des **sauvegardes régulières** et s'assurer de la recouvrabilité des données en faisant des **tests de restauration**. Dupliquer les sauvegardes sur un autre site ou encore sur un autre type de média.

→ Supervision du SI

La supervision du SI est la solution idéale pour anticiper les problèmes informatiques. **Le monitoring** surveille en continu votre infrastructure pour détecter les activités jugées inhabituelles ou suspectes.

→ PCA et PRA.

- Un PRA (**plan de reprise d'activité**) permet de restaurer rapidement vos données si elles ont été volées ou perdues. Un PRA est indispensable pour redémarrer au plus vite l'activité.
- Le PCA (**plan de continuité d'activité**), permet à l'entreprise de continuer son activité, même en cas d'incident ou de crise majeur. Il définit toutes les mesures d'urgence à prendre en cas de crise.

→ L'assurance Cybersécurité

Les assurances et notamment les assurances Cyber permettent de réduire l'impact d'un sinistre et de mieux y faire face dans l'urgence. Elles peuvent couvrir une partie des dommages, limiter votre responsabilité, inclure le recours à une société spécialisée pour gérer le sinistre et revenir au plus vite à la normale.

*** Source : Etude Accenture**

La sécurité informatique : démarche ponctuelle ou permanante ?

Une fois que la politique de sécurité de l'entreprise a été définie, que des dispositifs techniques ont été mis en place, et qu'un plan de secours a été établi, on pourrait imaginer que la question de la sécurité informatique est réglée. Or, comme tous les processus clé de l'entreprise la sécurité de son système d'information doit être suivie et évoluer en permanence pour rester adaptée aux enjeux et besoins.

Une démarche évolutive

La sécurité informatique est une démarche qui doit être ajustée en permanence.

- Parce que les techniques d'attaques évoluent et se développent sans cesse.
- Parce que l'organisation de l'entreprise, son système d'information évoluent.
- En raison des mouvements de personnel
- Les technologies et règlementations évoluent en permanence.

Il ne s'agit pas forcément d'un immense travail : organiser un à deux comités de sécurité par an avec les acteurs et professionels permet de suivre et d'ajuster régulièrement le dispositif de sécurit.

35 % *

Des attaques menées en 2021 provenaient de méthodes inconnues.

- Avant la pandémie de Covid-19, ce chiffre était de 20 %. La sécurité se doit d'être ajustée en permanence pour prévenir ces attaques.

*** Source : Cynet Report Covid19 cyberattack analysis**

Conclusion

L’avis de l’expert

Philippe Bougoin, directeur technique chez Pérenne’IT

“ **La sécurité informatique doit être considérée comme un enjeu pour toute entreprise**, TPE/PME comprise. Les entreprises sont de plus en plus dépendantes de la technologie et les attaques informatiques sont de plus en plus sophistiquées. Par conséquent, il est essentiel que les entreprises prennent **des mesures proactives** pour protéger leurs systèmes informatiques et leurs données.

Avant tout, il est important que les entreprises aient des **politiques et des procédures claires** en place pour la gestion de la sécurité informatique.

Cela peut inclure des politiques sur l'utilisation acceptable des ordinateurs, des moyens d’authentification des utilisateurs, des protocoles de sécurité pour le travail à distance, des contrôles pour l'accès aux données sensibles et **des mesures à prendre en cas de cyberattaque**.

Il est important que les entreprises **travaillent avec un professionnel de la sécurité adapté à leur taille et leurs enjeux business**. Les coûts associés à la sécurité informatique seront toujours moins élevés que les coûts associés à un sinistre qui peut parfois entrainer la fermeture de l’entreprise. **Ils doivent être évalués comme une assurance destinée à protéger les actifs de l'entreprise.** ”

En savoir plus ?

Vous souhaitez des informations complémentaires sur notre approche, nous consulter pour une question ou un projet ?

NOUS CONTACTER

NOS SERVICES