Le risque cyber pour les TPE/PME : plus qu'une réalité, une urgence

Christophe HERAULT
Directeur Innovation - Pôle SMB
Docaposte

La cybersécurité est aujourd'hui un enjeu crucial pour toutes les entreprises, quelle que soit leur taille. En 2022, une entreprise française sur deux a été victime d'une cyberattaque. Et les TPE/PME sont souvent les plus vulnérables face aux attaques informatiques, car elles disposent de moins de ressources pour se protéger.

Tous les secteurs sont concernés y compris le secteur public, comme en témoignent les récentes cyberattaques contre les mairies de Lille, Angers, ou encore des hôpitaux à Brest, Bourg-en-Bresse ou Corbeil-Essonnes.

Les cyberattaques peuvent avoir des conséquences désastreuses pour les TPE/PME. En effet, elles peuvent entraîner la perte de données sensibles, des pertes financières, une interruption de l'activité, une perte de crédibilité et une diminution de la confiance des clients. Les conséquences peuvent être encore plus graves si l'entreprise est confrontée à une violation de la confidentialité des données de ses clients.

Des chiffres parlants et alarmants

Selon le rapport "Les enjeux de la cybersécurité pour les PME" publié par la CPME en 2020, 43% des PME françaises ont été victimes d'au moins une attaque informatique en 2019.

Toujours selon ce rapport, les attaques les plus courantes sont les attaques par phishing (31%), les attaques par ransomware (17%) et les attaques par déni de service (9%).

Le coût moyen d'une attaque informatique pour une PME est estimé à environ 75 000 euros, selon une étude réalisée par Hiscox en 2019. Selon le baromètre de la sécurité des entreprises en France publié par CESIN en 2020, 45% des entreprises françaises ont subi une attaque informatique en 2019, et 23% d'entre elles ont subi une perte financière suite à cette attaque.

Sécuriser la donnée, une priorité

Comme toute matière première, les données font envie !

Elles peuvent être la cible de captation, de détention malveillante, voire de vol. Les modes opératoires des cybercriminels consistent le plus souvent à demander une rançon après avoir verrouillé ou volé des données et à les revendre sur le « dark web » au plus offrant. Pour cela, la technique du « phishing » (hameçonnage) par mail est la plus répandue auprès des particuliers, les entreprises étant plutôt victimes de « ransomware » (attaque contre paiement d'une rançon).

S'organiser et anticiper

L'organisation et l'anticipation sont majeures afin de se protéger contre les cyberattaques. Les TPE/PME doivent mettre en place des mesures de sécurité efficaces. La première étape consiste à sensibiliser les employés aux risques de sécurité informatique et à leur apprendre à adopter des pratiques de sécurité appropriées.

Les TPE/PME doivent également investir dans des solutions de sécurité telles que des pares-feux, des antivirus, des logiciels de chiffrement et des sauvegardes de données.

Le cycle de la cybersécurité détermine 3 phases distinctes :

- Prévenir
- Protéger
- Restaurer

Prévenir

La première phase, la prévention, consiste à mettre en place des mesures pour anticiper les risques de cybersécurité. Cela inclut la sensibilisation des employés aux bonnes pratiques de sécurité informatique, la mise en place de politiques de sécurité claires, la formation des équipes pour détecter les menaces potentielles, la surveillance des systèmes informatiques pour détecter les comportements suspects et l'identification des vulnérabilités des systèmes et des réseaux.

Protéger

La deuxième phase, la protection, vise à mettre en place des mesures pour protéger les systèmes informatiques et les données contre les attaques. Cela peut inclure l'utilisation de logiciels de sécurité tels que des pares-feux, des antivirus, des logiciels de chiffrement et des sauvegardes de données régulières. Il est également important de s'assurer que les logiciels et les systèmes sont régulièrement mis à jour avec les derniers correctifs de sécurité pour réduire les risques d'exploitation de vulnérabilités connues.

Restaurer

La troisième phase, la restauration, consiste à réagir en cas d'incident de cybersécurité. Cela peut inclure la mise en place d'un plan d'urgence pour gérer les incidents de sécurité, la restauration des systèmes et des données après une attaque et la mise en place de mesures pour éviter que l'incident ne se reproduise.

En somme, le cycle de la cybersécurité est un processus continu qui nécessite une attention constante et des mesures proactives pour protéger les systèmes et les données contre les menaces de cybersécurité.

Se préparer à réagir : un impératif

Enfin, les TPE/PME doivent se préparer à réagir en cas d'attaque informatique. Il est important de mettre en place un plan d'urgence et de former les employés pour qu'ils sachent quoi faire en cas de violation de la sécurité. Les TPE/PME doivent également envisager de souscrire une assurance cyber-risque pour se protéger contre les pertes financières liées à une violation de la sécurité.

Conclusion

Les TPE/PME doivent prendre les mesures nécessaires pour se protéger contre les cyberattaques.

La cybersécurité ne doit pas être considérée comme une dépense inutile, mais comme un investissement dans la protection de l'entreprise et de ses clients. Les TPE/PME qui adoptent des pratiques de sécurité informatique efficaces peuvent renforcer leur crédibilité, améliorer leur réputation et protéger leur avenir.

Autant d'enjeux pour lesquels Docaposte, filiale numérique du Groupe La Poste et acteur central de la confiance numérique, peut répondre.