MINISTÈRE
DE L'INTÉRIEUR
Liberté
Égalité
Fraternité

Direction centrale de la sécurité publique
Direction départementale de la sécurité publique de Seine-et-Marne

Circonscription d'Agglomération de Melun Val de Seine

POLICE NATIONALE

La Police Nationale vous informe :

La cybersécurité pour les TPE/PME/ COMMERCANTS – enjeux et solutions

Le numérique occupe aujourd'hui une place prépondérante dans le fonctionnement des entreprises quelle que soit leur taille – y compris pour les plus petites d'entre elles. Cette situation suscite un intérêt toujours croissant des cybercriminels. Mais quels sont exactement les risques pour les TPE, PME et Commerçants, comment y faire face ? Cybermalveillance.gouv.fr vous livre toutes les clés pour assurer sa cybersécurité en entreprise.

L'intensification des usages numériques et la recrudescence des cybermenaces

Que ce soit pour des usages personnels ou professionnels, le numérique occupe aujourd'hui une place majeure, et même souvent incontournable, dans le fonctionnement de notre société. Ordinateurs, tablettes, smartphones, objets connectés font maintenant partie de notre quotidien pour communiquer, s'informer, s'amuser, acheter, vendre, payer et même faire ses démarches administratives. Pour les particuliers comme pour les entreprises, cette tendance s'est encore accentuée avec la crise sanitaire qui a vu s'intensifier le télétravail et les achats en ligne.

Mais **cette ultra connexion par Internet et la dématérialisation des échanges représentent également un vaste champ d'opportunités pour les cybercriminels**. Le cliché du hacker adolescent doué et isolé qui cherchait à pirater un réseau informatique depuis sa chambre juste pour montrer qu'il en était capable est aujourd'hui quasiment révolu. **Aujourd'hui, les pirates**

cherchent principalement à exercer leur activité pour gagner beaucoup d'argent, et s'organisent sur le «darknet», l'Internet des cybercriminels, pour se spécialiser et travailler en équipe afin de maximiser leurs profits.

Les cyberattaques et les cyber-escroqueries se sont intensifiées au fil des ans. Comme le démontre l'actualité, des grandes entreprises aux plus petites, des administrations aux collectivités locales, des hôpitaux aux particuliers en passant par des associations… Tous les acteurs de la société en sont quotidiennement victimes et peuvent en subir le préjudice.

Les petites entreprises particulièrement vulnérables aux cyberattaques

Les plus petites entreprises sont souvent peu conscientes des risques et ne prennent pas forcément les mesures nécessaires pour se protéger, car elles pensent souvent, à tort, que leur taille ou leur activité ne sont pas assez significatives pour intéresser des cybercriminels. En réalité, c'est tout le contraire: les cybercriminels ont bien compris que toute entreprise, quelle que soit sa taille, constitue une valeur marchande, que ce soit à travers une trésorerie potentielle ou des informations qu'elle détient. Les petites entreprises sont d'autant plus faciles à pirater qu'elles sont souvent moins protégées.

Pour une TPE ou PME, les conséquences d'une cyberattaque peuvent s'avérer très importantes et parfois même désastreuses: perte immédiate d'argent suite à une fraude au virement, perte d'exploitation ou arrêt de l'activité, suite à une attaque par rançongiciel, qui prendra en otage les données de l'entreprise contre une rançon. Toute cyberattaque a un coût direct et indirect pour l'entreprise qui en est victime. C'est évidemment le coût non planifié de remise en état du système attaqué et de reconstitution, lorsque c'est possible, des informations détruites, comme les fichiers clients, les contrats, la facturation ou la comptabilité, etc. Mais c'est également un coût lié à la réputation de l'entreprise et à la perte de confiance des salariés, des clients, des fournisseurs et même des investisseurs qui peut avoir de sérieuses incidences dans la durée en termes de chiffre d'affaires ou de développement de l'entreprise. Souvent fragiles financièrement, certaines petites entreprises victimes de cyberattaques se voient contraintes de cesser leur activité. De plus, la responsabilité juridique civile et pénale du dirigeant peut même parfois être engagée en cas de manquements à ses obligations de protection de ses systèmes informatiques et des informations à caractère personnel détenues par son entreprise.

Mais l'informatique, et a fortiori, la cybersécurité, est rarement le cœur de métier des petites et moyennes entreprises. Par où commencer pour éviter ces risques ?

Comment renforcer la cybersécurité de son entreprise ?

Pour prendre en compte le risque, **la première chose à faire est l'inventaire de ses systèmes numériques et des informations auxquels ils permettent d'accéder** en répondant aux questions : «Que se passerait-il si ces informations étaient volées ou détruites et quelles sont les mesures qui sont prises pour l'empêcher ?». Cet inventaire vous permettra de recenser les systèmes les plus critiques de l'entreprise et leurs lacunes de sécurité pour **prioriser les actions à conduire**.

Ensuite, **assurez-vous que des mesures de cybersécurité élémentaires sont bien respectées**, comme l'utilisation de mots de passe différents et complexes pour chaque service (messagerie, cloud, site Internet, réseaux sociaux, banque en ligne, logiciels métiers…) afin d'éviter que le piratage d'un accès ne permette d'en pirater d'autres; que vos données les plus sensibles sont bien régulièrement sauvegardées et déconnectées de votre réseau afin d'éviter qu'elles ne soient détruites en cas d'attaque; que vos ordinateurs, smartphones, tablettes, serveurs sont bien mis à jour de leurs correctifs de sécurité, et que vous maîtrisez bien les connexions extérieures à votre réseau comme pour le télétravail, la télémaintenance, ou l'interconnexion avec des clients ou fournisseurs… En vous assurant que vous n'ouvrez pas plus d'accès que ce qui est strictement indispensable au bon fonctionnement de votre activité et que ces accès soient suffisamment sécurisés. **Plus vous ouvrez de portes, plus vous risquez de voir entrer quelqu'un d'indésirable et malveillant, a fortiori si les portes sont sécurisées par un simple verrou.**

Enfin, **faites-vous accompagner par des spécialistes reconnus en cybersécurité**. Comme en médecine, il ne viendrait à l'idée de personne de s'adresser à un cardiologue lorsqu'on a la vue qui baisse. Il en va de même pour l'informatique qui regroupe de nombreuses spécialités différentes. **Un prestataire spécialisé en cybersécurité vous accompagnera pour construire votre plan d'action et en suivre la mise en œuvre en appui de votre service informatique et de vos prestataires d'infogérance,** si vous en disposez. En cas d'attaque, il vous apportera ses compétences spécifiques pour vous aider à en limiter les effets. **Mais comment trouver ce type de prestataire spécialisé et s'assurer de ses compétences ?**

ExpertCyber: un label gage de qualité, d'expertise et de confiance en cybersécurité

C'est pour répondre à cette question que Cybermalveillance.gouv.fr a créé avec l'AFNOR et des organisations professionnelles **le label ExpertCyber**. Ce label atteste des compétences et de la qualité de service de prestataires spécialisés au profit des TPE et PME. Pour être mis en contact avec ces prestataires labellisés, rendez-vous sur le site Cybermalveillance.gouv.fr et décrivez sommairement votre besoin pour que les professionnels ExpertCyber soient sollicités en fonction de leurs compétences et proximité géographique.

Vous trouverez également sur Cybermalveillance.gouv.fr de nombreuses ressources sur les bonnes pratiques de cybersécurité, les principales menaces et les moyens de s'en protéger ou d'y faire face.

Si les cybercriminels sont ingénieux et compétents, sachez qu'ils sont aussi pressés de gagner beaucoup d'argent en faisant le moins d'efforts possible. Si vous attaquer leur demande trop de temps et de moyens au regard du bénéfice qu'ils peuvent en espérer, ils passeront leur route et chercheront une victime plus facile. **Le coût de votre sécurisation pour obtenir votre juste niveau de sécurisation afin d'éviter une cyberattaque sera toujours bien inférieur au coût que pourra représenter une telle attaque pour votre entreprise.**

Source: Cybermalveillance.gouv.fr janv. 2023