Cybercriminalité: privés et PME, vous êtes la cible!

Cyberrisques: une menace majeure pour chacun

A la maison, dans la rue, au bureau, en vacances, nous ne sommes nulle part à l'abri des cyberrisques. Dans nos habitats, les objets connectés sont pléthore et peuvent être la cible d'attaques informatiques. Sans oublier les ordinateurs, tablettes ou téléphones qui sont autant de risques d'intrusion chez vous. Pour entrer dans les foyers privés ou dans les secrets des entreprises, les intrus n'utilisent plus uniquement la porte ou une fenêtre.

Dans nos logements, la domotique nous facilite la vie, mais constitue également un terrain idéal pour les cybercriminels. Un individu malintentionné peut prendre contrôle à distance de caméras de surveillance afin de préparer un cambriolage. Ou alors il peut être à l'affût d'images privées compromettantes. Selon le type de système d'accès, un pirate pourrait également vous empêcher de rentrer chez vous ou parvenir à pénétrer lui-même dans votre maison. Dans ce cas, l'identification par la voix est une solution contre les risques d'intrusion.

GROS PLAN

PME, sauvegardez correctement vos données!

Une perte de données est vite arrivée. Hormis les actes criminels, elle peut également résulter d'une défaillance technique, d'une erreur de manipulation ou d'un incendie. Il est donc indispensable de sauvegarder vos données régulièrement.

- Conservez les supports de données en lieu sûr et élaborez un concept de sauvegarde complet.
- Assurez-vous de la réussite des sauvegardes et appliquez le principe «deux précautions valent mieux qu'une».
- Vérifiez régulièrement l'intégralité et la lisibilité des sauvegardes.
- Confiez la sauvegarde à un partenaire de confiance ou faites-la vous-même.
- Actualisez régulièrement votre concept de sauvegarde et planifiez des sauvegardes régulières, au moins une fois par semaine, idéalement une fois par jour.
- Conservez les sauvegardes en dehors de l'entreprise.

LA MOBILIÈRE

Il n'est pas rare que des criminels s'immiscent dans des ordinateurs pour y dérober des données clients sensibles.

LA MOBILIÈRE

Steven Wyss, conseiller en assurances et prévoyance.

Les acteurs de l'immobilier, une cible potentielle

Une PME sur trois a déjà été victime d'une cyberattaque. Malgré cela, les PME ne se protègent pas suffisamment contre les cyberrisques. Les entreprises qui ont déjà été victimes d'une cyberattaque sont plus enclines à renforcer les mesures de protection; elles savent que leurs activités peuvent être paralysées d'un coup . Pour les autres, sous-estimer les dangers leur fait courir des risques.

Les menaces sont variées. Il n'est pas rare, malheureusement, que des criminels s'immiscent dans des ordinateurs pour y dérober des données clients sensibles, telles que des références de carte de crédit, des numéros de téléphone ou des adresses e-mail.

Les professionnels de l'immobilier sont des cibles de choix: ils détiennent des données sensibles sur les bâtiments qu'ils ont en gestion, comme les codes d'accès de serrures électroniques ou l'électricité contrôlée à distance, qui sont deux exemples de systèmes facilement accessibles pour des initiés du piratage informatique. Ils sont également en possession d'informations aussi précieuses que confidentielles sur leur clientèle, qui sont par définition intéressantes pour les pirates.

Point faible des PME: l'humain

Pour se protéger, les mesures ne manquent pas, mais un scanner antivirus ou un pare-feu ne résout pas tout. Le plus grand facteur de risque est, reste l'humain. De nombreuses PME ne sont pas encore assez bien informées sur le thème des cyberrisques. En matière de cybersécurité, l'individu, donc chaque membre d'une équipe, constitue un point d'entrée. Il est important que les PME, quelle que soit leur taille, sensibilisent leur personnel et prennent conscience que leur modèle d'affaire est dépendant d'une infrastructure informatique en état de marche. Une panne due à une intrusion intempestive peut entraîner des conséquences dramatiques.

Le bon sens, un allié précieux

Que ce soit en ligne ou hors ligne, le bon sens est toujours le meilleur conseiller. Lorsque vous quittez votre maison, vous fermez à clef. En outre, vous faites attention à la qualité de la serrure. En ligne aussi, il faut être vigilant et ne pas ouvrir sa porte au premier venu. Installez un logiciel antivirus et mettez-le à jour régulièrement, tout comme votre système d'exploitation. Ne transmettez aucune information personnelle à des personnes que vous ne connaissez pas. Il est recommandé d'utiliser des mots de passe différents pour chaque compte sur Internet. En cas de piratage, il faut impérativement le changer. Il vaut mieux qu'il soit long avec au moins huit caractères et comprenant deux caractères spéciaux. Si vous avez de la peine à tous les mémoriser, utilisez un gestionnaire de mots de passe sécurisé. Vérifiez régulièrement vos relevés bancaires et relevés de carte de crédit.

En 2023, l'assurance cyberprotection est devenue vitale tant pour les privés que pour les entreprises. Renseignez-vous! ■

STEVEN WYSS
Conseiller en assurances et prévoyance
Agence générale La Mobilière Genève

GROS PLAN

Soudain des messages racistes sont diffusés en votre nom...

- **Fraude lors de paiements ou de transactions en ligne**
  Une personne attend un colis. Elle reçoit un faux e-mail d'un transporteur la priant de verser un supplément pour la livraison. Elle communique les données de sa carte de crédit, que les escrocs utilisent à deux reprises pour des transactions.
- **Perte de données**
  Tout à coup, l'ordinateur ne reconnaît plus son disque dur. Le serveur réseau (NAS) utilisé pour les sauvegardes des photos de famille et d'autres données a soudain rendu l'âme. Pendant qu'il rechargeait, le laptop a explosé.
- **Atteinte à la personnalité**
  Un utilisateur s'est fait pirater son profil Facebook et des messages racistes sont diffusés en son nom, au vu de tous sur le réseau social.
- **Violation des droits d'auteur**
  Une bande de copains a tourné une vidéo et l'a postée sur YouTube. Un beau jour, une des personnes constate que cette vidéo est utilisée par un site de commerce en ligne à des fins publicitaires. Cette personne est aisément reconnaissable sur la vidéo et n'a jamais donné son consentement à son utilisation.