Privés et PME, cibles des pirates

Cybermenace: un seul clic suffit!

Être hors ligne fait définitivement partie du passé. Dans les maisons, 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.

Selon la Centrale d'enregistrement et d'analyse pour la sécurité et l'information MELANI, service de la Confédération, les corps de police cantonaux constatent une augmentation de la cybercriminalité liée au coronavirus.
Dans les maisons, la domotique nous facilite la vie, mais constitue également un terreau 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.

Les acteurs de l'immobilier, une cible potentielle

Une récente étude représentative réalisée par GFS Zurich a montré que le nombre de cyberattaques de PME avait considérablement progressé avec la pandémie, et notamment le télétravail. Une PME sur trois a subi une cyberattaque, contre une sur quatre en 2020.
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. D'une part, ils manipulent des données sensibles sur des bâtiments.

Denis Hostettler.

Par exemple les serrures électroniques, l'électricité contrôlée à distance, bref des systèmes qui peuvent être piratés. D'autre part, ils sont en possession d'informations précieuses sur leur clientèle. En effet, lors des transactions, ils collectent diverses informations privées, donc intéressantes pour les pirates.

La prudence comme première ligne de défense

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'affaires est dépendant d'une infrastructure informatique en état de marche. Une panne due à une intrusion intempestive peut entraîner des conséquences dramatiques.

Agir comme dans la «vraie» vie

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, ainsi que votre système d'exploitation. Ne transmettez aucune information personnelle à des gens 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 changer son mot de passe. Il vaut mieux avoir un long mot de passe, au moins huit caractères, avec deux caractères spéciaux. Si vous avez de la peine à mémoriser tous les mots de passe différents, utilisez un gestionnaire de mots de passe. Vérifiez régulièrement vos relevés bancaires et relevés de carte de crédit.
Enfin, l'assurance cyberprotection devient vitale, tant pour les privés que pour les entreprises. Des spécialistes sont là pour répondre à vos questions. ■

DENIS HOSTETTLER
Agent général La Mobilière
Genève