SERVICE
AFFAIRES

IMPORTANT : PRÉVENTION DE LA FRAUDE VIA SYSTÈME TÉLÉPHONIQUE (PBX)

Chère cliente,
Cher client,

En raison d'une recrudescence de fraudes sur les systèmes téléphoniques (PBX) visant les entreprises canadiennes, nous souhaitons vous sensibiliser aux méthodes d'infiltration utilisées par les fraudeurs et vous informer de la conséquence principale d'une telle fraude. Par la même occasion, nous désirons vous rappeler les mesures de sécurité recommandées en matière de configuration de système téléphonique.

LE FONCTIONNEMENT D'UN SYSTÈME TÉLÉPHONIQUE

Le PBX est un commutateur d'entreprise qui permet de gérer les communications internes et externes. Les systèmes téléphoniques fonctionnent de la même façon que les serveurs informatiques, qu'on utilise conjointement à des systèmes d'exploitation connus, mais ils sont dotés d'une application de téléphonie. En matière de sécurité, les systèmes téléphoniques sont soumis aux mêmes contraintes que les serveurs informatiques.

DE QUELLE FAÇON LES FRAUDEURS S'INFILTRENT-ILS?

Les fraudeurs accèdent généralement à votre système téléphonique en devinant, grâce à diverses techniques, les mots de passe de vos boîtes vocales. De l'extérieur de votre entreprise, ils arrivent ainsi à activer sur votre système téléphonique des fonctions de renvoi d'appel vers des numéros de téléphone à l'extérieur du pays. En effet, les renvois d'appel sont fréquemment faits vers des numéros à l'étranger, dans des pays où le tarif à la minute est très élevé. Les fraudeurs opèrent généralement la nuit, les weekends ou durant une période de congé, pour que leur intrusion soit plus difficilement détectée. Notez que les systèmes téléphoniques IP, connectés à Internet, peuvent aussi être la cible de fraudes.

LA CONSÉQUENCE PRINCIPALE D'UNE FRAUDE TÉLÉPHONIQUE : LA SURFACTURATION

La surfacturation découlant de nombreux appels outre-mer est la conséquence la plus fréquente d'une fraude téléphonique. Nous vous rappelons que vous êtes responsable de payer la totalité des appels qui ont été effectués à partir de votre système téléphonique ou qui ont été acceptés (p. ex. appels à frais virés) et portés à votre numéro de téléphone, et ce, même si vous avez fait preuve de diligence raisonnable dans l'application des mesures de sécurité mises en place. La fraude téléphonique est un crime. Si vous croyez avoir été victime de fraude, nous vous suggérons de porter plainte auprès des autorités locales.

COMMENT LIMITER LES RISQUES DE FRAUDE?

Voici quelques mesures de sécurité recommandées afin de protéger votre système téléphonique. Cette liste n'est pas exhaustive. Elle n'est donnée qu'à titre informatif.

- Éviter les mots de passe faciles à deviner, tels que les numéros de téléphone, les numéros de poste, les séquences simples (12345678), et les chiffres consécutifs ou répétitifs (00000000).
- Modifier le plus rapidement possible les mots de passe par défaut fournis lors de l'installation d'un nouvel équipement ou de la création de boîtes vocales.
- Modifier régulièrement les mots de passe (p. ex. tous les 60 jours).
- Retirer ou restreindre toutes les fonctions non essentielles, notamment celles qui permettent d'effectuer des appels vers l'extérieur à partir de votre système : conférences téléphoniques, appels à partir de la boîte vocale, utilisation du service du téléphoniste (0+), etc.

- Limiter l'accès au système téléphonique au personnel autorisé, même pendant les heures ouvrables de l'entreprise ou durant les vacances.
- Ne jamais publier les numéros de téléphone donnant directement accès au système (accès direct au système, ADAS).
- Limiter ou bloquer les appels sortants en dehors des heures d'ouverture de l'entreprise via votre système téléphonique.
- Éliminer toutes les boîtes vocales non assignées ou non utilisées.
- Demander à l'installateur du système téléphonique d'effectuer régulièrement les mises à jour nécessaires de votre équipement.
- Faire régulièrement un audit de votre système téléphonique afin de réexaminer sa configuration et son niveau de sécurité.
- Inciter les membres de votre entreprise à adopter de bonnes pratiques en intégrant la sécurité des systèmes téléphoniques à votre politique relative à la sécurité des systèmes d'information.
- Installer un pare-feu devant l'autocommutateur pour filtrer les adresses IP entrantes.
- Souscrire une assurance contre la perte financière causée par une fraude téléphonique.

COMMUNIQUEZ AVEC VOTRE FOURNISSEUR D'ÉQUIPEMENT TÉLÉPHONIQUE

Nous vous rappelons que vous êtes responsable de protéger votre équipement téléphonique. Demandez à votre fournisseur*, qui assure le soutien et la gestion de votre équipement téléphonique, d'appliquer les configurations et les normes de sécurité adéquates.

Nous espérons que ces quelques conseils aideront votre entreprise à mieux se protéger contre les fraudes téléphoniques.

* Veuillez noter que Vidéotron n'est pas un fournisseur d'équipement téléphonique et que les propos de cette lettre sont à titre indicatifs seulement.