Région de gendarmerie Nouvelle-Aquitaine
Antenne Sécurité Économique et Protection des Entreprises de la formation administrative de Poitou-Charentes
Groupement de gendarmerie départementale de la Vienne.

Alerte

ESCROQUERIE PAR « FAUX TECHNICIEN »

Récemment, le comptable d'une PME est contacté par un individu se présentant comme technicien de maintenance de la banque gérant les comptes de la société. Celui-ci invoque la migration en cours vers une nouvelle version du site web de la banque et indique qu'à cet effet quelques manipulations informatiques sont nécessaires sur le poste dédié à la comptabilité. L'employé s'exécute et le jour même un virement de plus de 170 000 € à destination d'un pays balte est réalisé à son insu. Plusieurs autres affaires similaires ont d'ores et déjà été recensées.

DE QUOI PARLE T-ON ?

Déjà utilisée à de nombreuses reprises en 2013 et 2014, lors du passage aux normes européennes de paiement SEPA, l'escroquerie réalisée par un individu se présentant comme technicien de maintenance d'une banque revient sur le devant de la scène. Variante de l'escroquerie dite au faux virement, elle est particulièrement simple à réaliser et ne nécessite que peu de moyens techniques. Lors du contact, l'escroc invoque une quelconque opération de maintenance (mise à jour serveur, maintenance du site de la banque, etc.) et invite le comptable à se rendre sur un site internet via une URL communiquée. Un programme se télécharge alors automatiquement. Par la suite, il est demandé au salarié de se connecter sur le site de la banque gérant les comptes de la société en rentrant son identifiant et son mot de passe, puis de réaliser diverses manipulations telle que la navigation dans les différents onglets de l'interface. A l'issue, l'escroc indique que le site de la banque sera indisponible durant quelques jours puis met un terme à la communication. A aucun moment le comptable ne s'est rendu compte que le programme malveillant téléchargé avait permis à l'attaquant de prendre le contrôle à distance de son ordinateur. Par contre, quelques temps après, il constatera qu'un virement a été effectué à son insu.

QUE FAIRE ?

Les potentielles victimes peuvent facilement éviter de tomber dans le piège en respectant les procédures édictées en interne et en appliquant quelques mesures de bon sens :

En amont **:**

- Sensibiliser régulièrement les équipes financières et comptables ainsi que tout salarié exerçant une fonction dite de « filtre » (secrétaire, assistant de direction, standardiste). En effet, ces personnels sont susceptibles d'être contactés par l'escroc lors de la phase préparatoire de recueil d'informations ou durant l'escroquerie en elle-même.

- En ce qui concerne l'informatique, proscrire l'accès aux ordinateurs en mode « administrateur». Créer des comptes « utilisateurs » avec des privilèges correspondant aux besoins réels des postes occupés. Toute installation de programme ou d'exécutable sur les machines de l'entreprise ne peut et ne doit être réalisée que par un responsable informatique.

Durant la phase contact **:**

- En cas de doute et surtout avant de débuter toute opération demandée par l'appelant, contactez immédiatement votre hiérarchie ainsi que votre organisme bancaire pour vérifier ses dires. Le standard téléphonique de l'entreprise ayant également pu être piraté (dans le but de router les appels vers un complice), privilégier le contact depuis un téléphone portable.

Important **:**

- Dans le cas où le comptable ou le responsable financier aurait commencé à télécharger un quelconque programme, isoler immédiatement l'ordinateur utilisé en le déconnectant du réseau.
Cette simple opération empêchera l'escroc de pouvoir prendre la main à distance sur le PC à l'insu de l'utilisateur réel.

AU MOINDRE DOUTE, ALERTEZ IMMÉDIATEMENT LES FORCES DE L'ORDRE