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.

FAUX ORDRES DE VIREMENTS INTERNATIONAUX (FOVI)

Les FOVI : Les Faux Ordres de Virements Internationaux nommés également "arnaques aux présidents" consistent, au moyen de manœuvres frauduleuses, à obtenir de la part d'une entreprise victime un virement bancaire indu sur des comptes étrangers et portant généralement sur des sommes importantes.

DE QUOI PARLE T-ON ?

En forte recrudescence, les FOVI existent depuis de nombreuses années. Leurs auteurs recourent à des modes opératoires parfois sophistiqués auprès, généralement, du service comptable de l'entreprise victime via les vecteurs principaux suivants :
- Faux tests informatiques.
- Usurpation d'identité (directeur).
- Action directe auprès de la banque détentrice des comptes.
- Utilisation d'un logiciel espion (cheval de Troie).

Explications :

Les FOVI sont des escroqueries réalisées principalement par téléphone et concernent toutes les entreprises.
Les escrocs collectent en amont un maximum de renseignements sur l'entreprise victime à l'aide des réseaux sociaux, des vecteurs de communication de l'entreprise, d'Internet, mais aussi depuis quelques mois en utilisant des virus informatiques (chevaux de Troie).
L'ensemble des informations récoltées (données bancaires, organigramme société, projets, etc.) associé à un ton persuasif (clé de voûte de l'opération) permettent, en prétextant une opération urgente, d'obtenir des virements bancaires internationaux.
Cette escroquerie est réalisée grâce à des méthodes très élaborées qui reposent essentiellement sur la manipulation d'interlocuteurs (chef comptable, secrétaire direction, etc.) susceptible de déclencher des ordres de virements dans un cadre habituel ou à la suite de négociations imprévues. En effet, pour asseoir sa crédibilité et usurper une fonction, l'escroc apportera des détails précis sur l'entreprise et son PDG.
C'est ce que l'on nomme une attaque d'ingénierie sociale.

Précautions :

Quelque règles simples permettent de se prémunir contre ce type d'attaque mais aussi décourageront les escrocs :
- Utiliser des logiciels originaux et à jour sur le réseau informatique et les ordinateurs de l'entreprise.
- Protéger ses ordinateurs par un antivirus performant et à jour.
- Ne pas mettre d'informations stratégiques sur le site Internet de l'entreprise.
- Sensibiliser l'ensemble des personnels sur ce type d'escroquerie.
- Alerter les personnels sur l'importance de ne pas divulguer sur les réseaux sociaux des informations concernant l'entreprise.
- Instaurer un protocole de virements bancaires connus uniquement des responsables (banque, chef entreprise, comptable). Créer des mots d'authentification pour réaliser ces virements.
- Exclure les paiements de fin de semaine afin de pouvoir réagir rapidement auprès des banques en cas d'attaque avérée et réalisée par les escrocs.
- Accroître la vigilance lors des périodes scolaires et des remplacements de titulaires de postes par des stagiaires (comptabilité, standardiste, etc.)

Réactions :

Que faire en cas de doute d'attaque ou si l'escroquerie a pu se réaliser ?
- Prévenir immédiatement la banque pour arrêter la transaction et rapatrier les fonds.
- Déposer plainte auprès des services de police ou gendarmerie.

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