Sécurité économique territoriale

Auvergne - Rhône-Alpes

Focus sur les escroqueries aux faux ordres de virements internationaux

Réalisées par téléphone ou par courriel, les escroqueries aux faux ordres de virement internationaux touchent les entreprises de toute taille et de tous les secteurs.

Très habiles et œuvrant souvent depuis l'étranger, les escrocs utilisent des techniques dites ***d'ingénierie sociale*** pour recueillir un maximum de renseignements sur l'entreprise et ses salariés en consultant les sources ouvertes (*internet, sites de l'entreprise, réseaux sociaux, ...*).

Une fois cette phase achevée, ils passent à celle du contact. Pour parvenir à leurs fins, ils se servent des ressorts psychologiques de base (*flatterie, peur, menaces, ...*) pour isoler leurs victimes et les contraindre à effectuer les actions demandées. L'argent indûment obtenu est ensuite transféré sur des comptes domiciliés à l'étranger (*Moyen Orient et/ou Asie*).

Trois grandes variantes de ce type de détournement d'actifs financiers ont été recensées :

- L'escroquerie dite au faux président : un individu se fait passer pour un des dirigeants, un avocat, un membre de l'autorité des marchés financiers, auprès d'un des collaborateurs en vue d'obtenir de lui un virement urgent concernant une opération confidentielle (*rachat de société par exemple*).

- L'escroquerie aux coordonnées bancaires : l'escroc fait croire à un changement de domiciliation bancaire d'un fournisseur, d'un client ou de tout autre partenaire de l'entreprise. Il envoie un relevé d'identité bancaire mentionnant les nouvelles coordonnées par courriel, avec des caractéristiques d'adresse de messagerie très proches de celles de l'interlocuteur habituel.

- L'escroquerie par moyen informatique : un individu se faisant passer pour un technicien de la banque tente d'obtenir du service comptabilité de l'entreprise l'exécution d'un « *virement test* », via l'installation de logiciels malveillants permettant la récupération informations ou la prise en main à distance de l'ordinateur.

Ce type d'atteinte pourrait être facilement déjoué si des mesures simples étaient appliquées, à savoir :

- Sensibiliser régulièrement les collaborateurs,
- Mettre en place une procédure écrite claire concernant l'exécution des virements,
- Communiquer en interne sur cette procédure,
- Porter une attention particulière sur les informations diffusées en dehors de l'entreprise,
- Vérifier systématiquement la légitimité de toute demande faite hors du cadre habituel,
- Sécuriser les installations informatiques, (*mise à jour des logiciels, sauvegardes quotidiennes, mise en œuvre d'une charte d'utilisation du matériel informatique, d'internet et des réseaux sociaux,…*).

En cette période de crise économique, ces « *attaques* » peuvent entraîner de graves conséquences sur la pérennité des sociétés et le devenir de leurs salariés. Plusieurs entreprises ont été placées en liquidation judiciaire, des comptables ont sombré dans la dépression et quelqu'uns ont même mis fin à leurs jours.

En vue d'alerter et conseiller les dirigeants, une plaquette de sensibilisation et 3 messages d'attention ont été édités par la cellule intelligence économique de la région de gendarmerie Auvergne – Rhône-Alpes. (***documents téléchargeables en cliquant directement sur l'image correspondante***).


Escroqueries aux virements : Comment s'en prémunir ?


Sécurité économique territoriale
Rhône-Alpes
MESSAGE D'ATTENTION
Alerte


Sécurité économique territoriale
Rhône-Alpes
ALERTE
MESSAGE D'ATTENTION


Sécurité économique territoriale
Rhône-Alpes
MESSAGE D'ATTENTION
Alerte