Les attaques FOVI (faux ordre de virement international) ou arnaque au président

« En 2019, **7 entreprises sur 10** ont subi une **tentative** de fraude, **27%** des entreprises ont été victimes d'**une fraude avérée**, 1/3 des entreprises a subi plus de cinq tentatives ». (source : enquête annuelle menée par le cabinet Euler Hermès France).

Les Ardennes ne sont pas épargnées par ce phénomène !

Les plus pratiquées sont les **fraudes au président**, les **faux fournisseurs**, viennent ensuite les **banques, avocats et les faux clients**. L'attaque peut également reposer sur une intrusion dans les systèmes informatiques et dans quelques rares cas, une aide interne est fournie.

Basée sur l'usurpation d'une identité, l'attaque s'appuie sur un **important travail de collecte de renseignements** sur des plateformes comme Facebook, LinkedIn, Infogreffe qui fournissent une **mine de renseignements exploitables** pour rendre l'attaque cohérente et crédible.

L'auteur mettra entre lui et sa victime un écran de fumée reposant sur l'**usage d'adresses fausses** (au libellé extrêmement proche) **ou usurpées**.

Il créera une structure juridique au **nom proche de partenaires réels de la victime** (banques, fournisseurs, clients) ainsi que le ou les comptes récipiendaires des virements qui peuvent être hors territoire national.

La **mise en échec d'attaques** de ce type repose principalement sur des **comportements humains** et un renforcement des **procédures internes**.

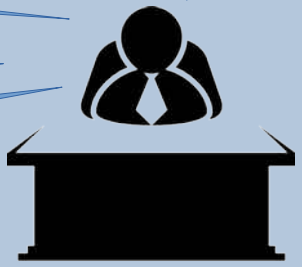
En amont les réflexions suivantes devront être menées par l'entreprise :

Quels **services** peuvent être souscrits auprès de ma **banque** pour sécuriser les virements ? (plafonds vers l'international, contre appel en cas de virement suspect)

Le **nombre d'employés habilités** à effectuer des virements est t-il strictement nécessaire ? Un employé doit-il pouvoir effectuer un virement sans validation hiérarchique ?

Une assurance contre le risque de cyber-escroquerie en particulier est-elle pertinente ?

Les collaborateurs sont-ils formés et sensibilisés sur les attaques d'ingénierie sociale et de Phishing ?



Groupe de prévention des cybermenaces – Gendarmerie des Ardennes
contact-covid-ggd08@gendarmerie.interieur.gouv.fr