Les **arnaques** aux faux fournisseurs

par Olivier Wajnsztok,
Directeur associé, AgileBuyer

LES PARTICULIERS NE SONT PAS LES SEULS À SUBIR DES ARNAQUES PAR LE BIAIS DE LEURS ACHATS. LES ENTREPRISES PEUVENT AUSSI EN FAIRE L'OBJET, ET LES SOMMES EN JEU PEUVENT ÊTRE CONSIDÉRABLES.

Si « l'arnaque au président » reste la plus connue et la plus spectaculaire, d'autres arnaques, plus simples, ciblant l'organisation achat et la comptabilité fournisseur existent aussi. Quelles sont-elles et comment s'en prémunir ?

La « Nigériane »

Le nom de ces arnaques vient du fait qu'elles sont souvent organisées à partir de pays de la côte ouest de l'Afrique. Ces arnaques surviennent souvent dans un contexte international, mettant en relation des entités basée dans différents pays et ainsi permettre de mettre à profit une communication plus limitée entre les acteurs.

Dans les faits, la manipulation est simple : l'entreprise arnaquée est contactée par un interlocuteur qui semble être un de ses fournisseurs étrangers. Ce dernier, basé dans un pays situé en Asie par exemple, va expliquer que sa société a changé de banque pour des questions de niveau de qualité de prestation ou de sécurité insuffisante. Les paiements sont donc maintenant à effectuer sur un nouveau compte, hébergé dans une banque allemande par exemple.

Suite à cela, les paramètres du vrai fournisseur sont modifiés dans l'ERP de l'entreprise arnaquée par son propre personnel. Le prochain paiement dû au fournisseur est logiquement envoyé sur le compte des fraudeurs, qui ne manque pas d'être vidé dès la réception du transfert.

Les fraudeurs ont rarement le niveau d'information suffisant pour cibler un transfert spécifique, mais avec un peu de chance, le prochain paiement est conséquent et peut atteindre des centaines de milliers d'Euros, voire beaucoup plus. La société Michelin en a fait les frais en 2014 à hauteur de 1,6 millions d'Euros. La même année le cabinet KPMG était escroqué de 7,6 millions d'Euros.

La fausse commande

Là, c'est plutôt le côté vente de l'entreprise qui en est victime. Cette pratique consiste à se faire passer pour une entreprise, le plus généralement connue et ayant pignon sur rue. Le but est d'agir en son nom pour effectuer une demande d'ouverture de compte client, pour ensuite émettre de faux bons de commandes. La clé étant d'induire en erreur des entreprises peu familières des procédures d'achat en vigueur dans la société usurpée. Une fois le bon de commande traité par le fournisseur abusé, il suffit de récupérer la marchandise à une adresse neutre ou un dépôt pouvant faire figure de centre de stockage. Le temps que le fournisseur se retourne vers la société « acheteuse » pour retard de paiement en présentant un numéro de commande inexistant, le lieu de livraison n'est plus utilisé par les fraudeurs depuis longtemps.

Les marchandises ciblées sont généralement des produits largement répandus et susceptibles d'être utilisés par tout type d'entreprise. La société ENGIE en a par exemple fait l'expérience en 2013 concernant des tentatives de création de compte fournisseur à son nom et de fausses commande pour du matériel informatique et bureautique.

Quelles politiques et procédures adopter ?

Si les escrocs parviennent à leurs fins, c'est qu'il existe des faiblesses dans le système, et que ces escrocs sont toujours inventifs pour les exploiter.

Paradoxalement, les procédures bancaires sont plus strictes pour les particuliers que pour les entreprises, alors que les montants concernés sont potentiellement bien plus importants. A titre d'exemple, un simple fax suffit parfois encore pour valider une transaction !

Les entreprises doivent donc mettre en place des procédures en interne et ne pas compter uniquement sur la vigilance des banques. Cela peut être des procédures simples, mais elles doivent être permanentes.

On peut par exemple mettre en place un système de double signature, dès que le virement dépasse une certaine somme, voire installer un logiciel bloquant toute transaction sans contre validation.

Instaurer une politique de méfiance peut suffire à contrer l'arnaque à la « Nigériane » : Toute modification dans l'ERP à la demande du fournisseur ne doit pas être exécutée par la comptabilité fournisseur sans que cette dernière ait demandé à l'acheteur en charge de ce fournisseur de vérifier en direct l'information auprès du concerné.

Il est plus difficile de protéger ses fournisseurs de fausses commandes envoyées en notre nom. Une fois le sujet identifié, la meilleure arme reste la communication rapide auprès du marché en publiant un appel général à la vigilance sur toute commande ou demande de création de compte fournisseur en provenance de votre entreprise ou de ses filiales

L'importance de l'humain

Après analyse des différentes menaces et des potentielles réponses pouvant y être données, on se rend compte que le facteur humain reste la pierre angulaire du système de défense d'une entreprise.

Les fraudes externes abordées précédemment représentent la grande majorité des tentatives, et sont toutes basées sur la manipulation humaine, à l'exception des fraudes informatiques (cyber attaques).

Mettre en place des procédures est indispensable, mais ces dernières sont au final appliquées par les employés. Les procédures ne fournissent pas de protection complète en soi, mais doivent être là pour permettre aux employés d'identifier les situations à risques, les doutes, et agir en conséquence.

L'étude Euler Hermes de Mai 2015, menée auprès de 184 personnes (dont 80% de Directeurs Administratifs et Financiers) indique d'ailleurs que 86% des tentatives déjouées l'ont été suite à des réactions humaines, et non pas par des procédures de contrôle interne ou des dispositifs techniques.

La sensibilisation des équipes doit donc être une priorité, et leur faire suivre des formations spécifiques peut également se révéler efficace, notamment afin de leur permettre d'établir une cartographie des risques de fraudes. Une fois les risques principaux identifiés, il est beaucoup plus facile d'orienter sa vigilance sur les failles principales.

> Si les escrocs parviennent à leurs fins, c'est qu'il existe des faiblesses dans le système

Cela étant dit, même avec les bonnes procédures en place et des employés informés et vigilants, les fraudeurs feront toujours preuve d'une grande inventivité et sont toujours aux aguets pour exploiter une faille potentielle. Les procédures en place et les formations suivies ne doivent pas créer de sentiment de sécurité excessif et la méfiance sera donc toujours la première arme de défense à disposition des sociétés.