6.5. Prévenir la fraude à la facture et la cyberfraude : comment être sur ses gardes ?

Fraude à la facture, cyberfraude, phishing, « arnaque au CEO », … Une entreprise sur cinq en est victime chaque année. Evitez de tomber dans le piège !

CYBERFRAUDE - ARNAQUE AU CEO

Le mot « cybercriminalité » ne vise pas toujours les pirates informatiques astucieux : leurs méthodes de travail sont souvent étonnamment simples. Un certain nombre d'entreprises ont récemment été confrontées à l' « **arnaque au CEO ».** Il s'agit d'une escroquerie qui a pour objectif de voler de l'argent à une entreprise en usurpant l'identité de l'un de ses dirigeants, administrateur délégué, directeur financier, etc.

Avec l'adresse mail d'un chef d'entreprise - *ou une adresse très ressemblante* - les escrocs demandent à la comptabilité d'effectuer un versement d'argent rapidement, et dans le plus grand des secrets. Sous la menace de l'urgence, le personnel comptable tombe très vite dans le panneau, et se rend compte après coup de l'arnaque dont il a été victime. La situation actuelle ou le télétravail est généralisé rend d'autant plus aisé le recours à de telles pratiques.

D'après le Centre for Cyber Security Belgium *(le Centre Belge pour la Cybersécurité),* de plus en plus de signalements de ce type sont enregistrés, bien que les entreprises qui en sont victimes ne s'en vantent généralement pas. Petit ou grand, tout le monde peut tomber dans le piège. Ainsi, la filiale Benelux de la maison de champagne Vranken-Pommery s'est faite extorquer 800.000 euros en 2015 par le biais d'une arnaque au CEO.

COMMENT PRÉVENIR UNE ARNAQUE PU CEO ?

- N'ouvrez pas d'hyperliens ou de pièces jointes de courriels suspects : adresse électronique douteuse, nom de domaine étranger, erreurs linguistiques inhabituelles dans le courriel ?
- Évitez les vulnérabilités de votre environnement informatique : installez toujours les mises à jour de sécurité les plus récentes.
- Maintenez un contrôle d'accès strict : ne partagez jamais vos mots de passe, changez-les régulièrement.
- Prévoyez des mécanismes de sécurité : tels que des limites de paiement pour le personnel ou une procédure de double approbation pour les paiements de montant élevé.
- Sensibilisez vos collaborateurs aux risques de sécurité et à la façon de faire face à des situations suspectes.

L'arnaque au CEO n'étant liée ni à un problème technique, ni à un problème de sécurité informatique, son succès ou son échec dépendra uniquement de la manière dont les collaborateurs auront été sensibilisés (ou pas) et appliqueront - ou non, les procédures internes. L'arnaque au CEO est donc, avant tout, un problème humain.

FRAUDE À LA FACTURE

Les entreprises sont également de plus en plus confrontées à des **factures falsifiées :** factures fantômes, factures falsifiées, fausses factures concernant l'enregistrement d'une marque ou d'un nom de domaine ou l'application du RGPD, ... Toutes ces pratiques sont assez courantes.

Votre entreprise passe une commande de fournitures et reçoit une facture de son fournisseur. Vous réglez la facture de bonne foi mais recevez un avertissement quelques jours plus tard. Vous avez sans doute été victime d'une **facture falsifiée :** des escrocs ont intercepté la facture de votre fournisseur et ont adapté le numéro de compte, et les coordonnées de contact, avant de vous transmettre la facture « falsifiée ». En effectuant votre versement, vous payez en fait vos escrocs.

Le SPF Économie a récemment invité les entreprises à la vigilance contre **la fraude à la facture autour du règlement général sur** la **protection des données** *(« RGPD »). A* ce propos, des dizaines de signalements ont déjà été reçus, impliquant principalement deux organisations *« GDPR Organisation »* et *« Les documents BE ».* Les entreprises reçoivent une lettre ou un e-mail les invitant à effectuer un paiement à ces organisations inconnues, soi-disant responsables de l'application du RGPD.

En septembre dernier, c'est le SPF Finances qui mettait en garde les citoyens contre **les e-mails frauduleux** invitant les destinataires à rembourser une dette fiscale en cliquant sur le bouton « MyMinfin », soi-disant à la demande du SPF Finances.

COMMENT PRÉVENIR UNE FRAUDE À LA FACTURE ?

- Vérifiez l'adresse mail de l'expéditeur et comparez-là à celle envers laquelle vous effectuez vos échanges habituel*lement (exemple : l'adresse mail du SPF Finance est toujours « xxx@minfin.fed.be »).*

- Comparez toujours le numéro de compte figurant sur la facture avec le numéro de compte figurant sur le bon de commande.

- Soyez vigilant s'il s'agit d'un nouveau contractant ou si une facture mentionne un nouveau numéro de compte. Conservez les données et le numéro de compte de vos fournisseurs même si vous payez par e-banking.

- En cas de doute, attendez pour payer et contactez d'abord l'expéditeur et/ou votre conseiller juridique.

- Soyez vigilant lorsque les dates d'émission et de réception diffèrent d'une semaine (ou plus) : il s'agit du laps de temps requis par les escrocs pour falsifier la facture.

- Sensibilisez vos collaborateurs aux risques de sécurité et à la façon de faire face à des situations suspectes.

VOUS AVEZ TOUT DE MÊME PAYÉ UNE FACTURE FALSIFIÉE ?

Prenez contact avec votre conseiller juridique au plus vite afin de signaler l'incident et de tenter d'obtenir le remboursement du montant versé.

Joachim Colot
Senior Specialist
DELOITTE PRIVATE

AIHE REVUE NR. 230 OCTOBRE-NOVEMBRE 2020