CPECF
expertise comptable

INFORMATION

FRAUDE ET CYBERCRIMINALITE

Soyez vigilant, la fraude en entreprise s'intensifie depuis 3 ans. La fraude s'attaque de plus en plus aux petites structures comme aux grandes entreprises. 3 entreprises sur 5 ont été touchées en 2016, avec des conséquences parfois irréversibles. Découvrez les bons réflexes à adopter et les actions à mettre en place.

LA FRAUDE PAR USURPATION D'IDENTITE EVOLUE

La fraude au virement fait des ravages en France et à l'international. Certaines grandes entreprises françaises subissent **jusqu'à 3 à 4 tentatives par jour.** Récemment une entreprise américaine a subi à Hong-Kong un préjudice de 47 millions de dollars !
En particulier, **la fraude au faux fournisseur – ou changement de RIB** – est redoutable pour les entreprises n'ayant pas renforcé leurs procédures.

Depuis 2015, les entreprises subissent également **des campagnes massives d'infection par logiciels malveillants,** envoyés par email. Plus de 35.000 PC sont ainsi infestés en France par le logiciel DRIDEX. Le logiciel prend la main sur le PC, initie des virements, et vole les listes de clients et fournisseurs de l'entreprise.

LES RISQUES ET PREJUDICES NE SONT PAS UNIQUEMENT FINANCIERS

Au-delà des préjudices financiers, ces fraudes causent des traumatismes humains, des licenciements, voire des faillites. Elles peuvent aussi **affecter gravement l'image de l'entreprise victime.**

LE VOL DE DONNEES EST UN RISQUE MAJEUR

Les informations que les entreprises détiennent sur leurs clients *(coordonnées, factures...)* sont précieuses. Les fraudeurs cherchent à voler ces données, par intrusion informatique, via logiciel malveillant, ou même par email et par téléphone (par exemple en usurpant l'identité d'un client).
Un vol de données peut avoir des conséquences dramatiques pour une entreprise *(particulièrement un grand facturier ou un grand bailleur)* : impayés massifs, dégradation d'image, risque commercial, ...

LA FRAUDE AU PRESIDENT

→ Un faux dirigeant exige de sa victime qu'elle envoie un virement confidentiel et urgent

LE TECHNICIEN BANCAIRE

→ Un faux technicien bancaire « aide » sa victime à faire un virement de test

LE CHANGEMENT DE RIB

→ Un faux fournisseur ou bailleur demande à sa victime de modifier ses coordonnées bancaires

PAR MALWARE ET PHISHING

→ Un malware, envoyé par email, affiche une fausse page pour voler votre code de validation

FRAUDE ET CYBERCRIMINALITE

(suite)

PROTEGER VOTRE ENTREPRISE

FORMATION ET SENSIBILISATION

Les fraudeurs exploitent toujours la faille humaine.

C'est pourquoi vous devez **sensibiliser et former vos collaborateurs.**

Les emails de sensibilisation ne suffisent pas : formez régulièrement toutes vos équipes *(comptabilité, trésorerie, achats, standardistes, nouveaux arrivants, intérimaires...)*, aux risques de fraude, aux risques cyber, et aux risques de vol d'information.

N'hésitez pas à **sensibiliser également vos clients et fournisseurs.**

SEPARATION DES ROLES ET PROTECTION DES BASES

Veillez à respecter **la séparation des rôles dans vos outils de comptabilité et de trésorerie.** Mettez en place des plafonds adaptés à votre activité, et limitez la trésorerie disponible. **Évitez les ordres de virements et les validations au format papier.**

Les **référentiels** contenant les coordonnées de vos clients et fournisseurs doivent être **protégés** *(contrôle d'accès et chiffrement).*

AUTHENTIFICATION DES CONTREPARTIES

Diffusez des **procédures écrites d'authentification des contreparties,** notamment pour les cas suivants :

- Fournisseur changeant de coordonnées bancaires ou téléphoniques,
- Toute personne demandant la réémission d'une facture, des informations sur vos outils, procédures ou coordonnées bancaires *(client, contrôleur des impôts, Banque de France, sondeur, etc.)*,
- Technicien souhaitant vous assister sur vos outils de trésorerie, vos terminaux de paiement électronique, etc.

CONTROLES

Faites **contrôler quotidiennement les virements émis,** en particulier les montants élevés à destination de pays étrangers. N'hésitez pas à exiger un document papier pour la validation de vos paiements. Faites réaliser des **audits et contrôles internes réguliers.**

GOUVERNANCE ANTI-FRAUDE

La lutte contre la fraude est un enjeu transverse, impliquant la trésorerie, la comptabilité, les achats, la DSI, les ressources humaines *(formations)*, le contrôle interne, etc. Montez une **gouvernance anti-fraude** pour améliorer continûment vos outils et procédures.

Travaillez également avec vos partenaires *(banques, éditeurs, assureurs...)*.

NOS SOLUTIONS POUR VOUS ACCOMPAGNER

1 DIAGNOSTIC PERSONNALISE

Notre équipe est à votre disposition pour réaliser un **diagnostic de prévention contre la fraude personnalisé,** vous permettant en quelques dizaines de minutes d'identifier des pistes d'amélioration.

2 FORMATION ET SENSIBILISATION

Pour vous aider à former vos équipes,
CPECF vous propose :

- ✔ Un accompagnement personnalisé
- ✔ Des brochures et kits de formation gratuits
- ✔ Des interventions auprès de vos équipes

→ POUR PLUS D'INFORMATIONS, CONTACTEZ-NOUS

Mise à jour au 30 janvier 2018