Livre Blanc

Conseils pratiques pour limiter la fraude relative à vos flux financiers

mercuria
la logique de gestion

Bonjour,

Depuis plusieurs années, les entreprises sont de plus en plus la cible de fraudes au sens large du terme. La dématérialisation des flux, la réduction des délais et coûts, l'importance du web sont notamment des explications à l'émergence d'escroqueries au sein des services financiers. Bien évidemment, la fraude la plus connue est celle dite du « président » mais il en existe bien d'autres moins connues ou soupçonnées.

D'origine interne ou externe, ces fraudes, dont le nombre reporté par les entreprises ne cesse d'augmenter d'années en années, coûtent des millions d'€uros chaque année ! Chacun d'entre nous connaît bien évidemment cette thématique et se dit avoir mis en place des procédures ou systèmes pour ne pas être touché par ces « attaques ».

Cependant, au-delà de la mise en place d'éléments de sécurité, la vraie question à se poser n'est pas « Qu'est-ce que j'ai mis en place pour éviter la fraude ? » mais « **Jusqu'à quand les moyens mis en place vont pouvoir me défendre des attaques ?** ».

L'objectif de ce livre blanc n'est pas de lister l'ensemble des fraudes existantes ou à venir, bien connues de nous tous (fraude au président, demande d'un faux ordre de virement papier, falsification de courriers électroniques…) mais de vous **permettre d'avoir une vision la plus large des risques liés aux flux financiers** et vous proposer des **solutions concrètes de diminution du risque au sein de votre entreprise**.

Bonne découverte !

Service Communication MERCURIA

Des données sensibles manipulées par de nombreuses personnes, source de danger !

Les collaborateurs des services administratifs et financiers sont amenés à manipuler des données délicates : IBAN, numéros de compte internes et/ou ceux de vos fournisseurs, pouvoirs bancaires, ordres de virements…

Bien évidemment, au-delà d'une clause de confidentialité souvent liée au contrat de travail, il est difficile, voire impossible, de crypter toutes ces données ou limiter leur accès car elles font partie du quotidien de vos équipes. Sans pour autant être dans un climat de « psychose », différents niveaux de sécurité peuvent être mis en place simplement.

1. Renforcer votre gestion des droits d'accès et automatiser votre chaîne de flux

Souvent mise en place au sein des entreprises, il est nécessaire de revoir la gestion de vos accès aux applications de gestion et d'imposer régulièrement des changements de mot de passe. En effet, il est fréquent lors de l'arrivée d'un stagiaire, d'un CDD de ne pas créer de mots de passe et de lui laisser le sien pendant la durée de la mission sans pour autant le modifier après.

Une **finesse des droits d'accès** est possible dans certains logiciels au niveau de la consultation, de la création, de la modification, par pays, par montant, par profil, limité dans le temps…

Au-delà des droits, **automatiser la totalité des tâches de la chaîne de traitement** d'un flux financier est un enjeu majeur. Par exemple, à la génération d'un règlement fournisseur de votre système d'information, le fichier est pris en charge sans délai. Il est crypté, transmis pour validation et envoyé à la banque sans qu'aucune manipulation ne soit possible. Votre chaîne est donc **100% automatisée et sécurisée**.

2. Dissocier les acteurs d'un flux financier et mettre en place un processus de tâches

Confier, malgré une honnêteté totale, l'intégralité du processus d'un virement par exemple, est source de risques plus importants pour vous. Il est effectivement conseillé de **dissocier les acteurs** : un collaborateur a les droits de créer un compte par exemple, un autre complète, prépare l'ordre de virement en lui-même et une tierce personne va le valider avant de l'envoyer aux banques. Vous limitez ainsi le risque de fraude en dispatchant les tâches sur plusieurs collaborateurs. La mise en place d'une note expliquant ce processus au sein de votre société et partagée entre les services est nécessaire. De plus, il convient de décrire dans cette **note de procédure**, le processus en cas d'absence d'un membre de la chaîne de validation ou de **gestion des demandes exceptionnelles** pour éviter notamment la « fraude au président ». La mise en place d'une signature électronique (cf. paragraphe ci-dessous) peut vous aider à fiabiliser ce point.

3. Mettre en place un système de signature électronique

Les banques sont de plus en plus « frileuses » pour recevoir des confirmations de virement par fax car cela entraîne chez elles du temps homme de traitement (refacturé souvent cher). Au-delà du coût, ce processus n'est pas sécurisé car une imitation de signature peut se faire facilement.

Autre alternative, aller sur chaque site de vos banques pour effectuer ces transactions, récupérer ou déposer un fichier avec des mots de passe différents par banque… Ceci implique souvent, chez vous, une multitude de mots de passe, des procédures différentes et des niveaux de sécurité aléatoires d'un site à l'autre notamment liés au dépôt de fichiers.

La mise en place d'une **signature électronique** est simple. Il s'agit de signer de manière électronique vos fichiers de flux financiers avant de les envoyer aux banques. Muni d'une clef « Token » qui sert pour toutes vos banques (certificat unique), vous pouvez ainsi crypter les fichiers et les signer de manière électronique et sécurisée. Vous pouvez même mettre en place des **doubles signatures** selon un certain niveau de montant par exemple. Ainsi, tout est sous contrôle et validé via une clef « Token » unique par signataire.

Si vous ne souhaitez pas mettre en place une signature externe (envoi vers les banques), vous pouvez utiliser le système de signature électronique en interne uniquement pour la validation de fichiers au sein même de votre entreprise.

La dématérialisation totale de vos flux grâce à la signature électronique vous permet ainsi de **simplifier et sécuriser votre processus de validation et d'envoi de fichiers financiers**.

4. Palier au rôle de la banque qui a évolué : vérifier vos prélèvements

Depuis le passage au SEPA, la banque n'assure plus le rôle de contrôle sur vos prélèvements. Auparavant, avant toute demande de prélèvement sur vos comptes bancaires, chacune de vos banques vérifiait la présence d'une autorisation de prélèvement… Aujourd'hui, ce rôle et responsabilité incombent à votre entreprise. Il est de la **responsabilité du débité (votre entreprise) de vérifier les éléments bancaires du débiteur** : l'ICS (identifiant créditeur), le numéro de compte et le numéro de mandat entre autre…

Une solution sécurisée consiste à récupérer l'avis de prélèvement mis à disposition par votre banque 2 jours avant l'échéance. Le travail de vérification et de contrôle consiste à croiser les tiers de cet avis avec un référentiel des tiers crypté autorisés à prélever sur votre compte.

Vous êtes ainsi capable d'anticiper toute anomalie et pouvez agir avant la tentative de fraude.

Souvent réalisée manuellement cette opération est longue et fastidieuse, l'automatiser vous permet de **viabiliser 100% de vos prélèvements** et vous laisse le temps **d'alerter vos banques en cas de fraude**.

5. Veiller à la bonne réception et traitement de ces derniers au-delà de l'envoi des fichiers

Envoyer un fichier à vos banques via votre outil de communication bancaire est simple et peut être effectué facilement par un tiers. De nouveaux services peuvent sécuriser vos flux car au-delà de l'envoi, le PSR (Payment Status Report) et l'ARA (Accusé Réception Applicatif) vous permettent d'**interpréter vos retours bancaires**. Vous pouvez envisager de recevoir un **accusé de réception des fichiers** adressés à vos banques ainsi que la **confirmation du traitement** (bien traité ou traité en partie avec le détail des erreurs).

Ce retour de la banque vous permet de **vérifier à la réception et à la bonne exécution de vos ordres bancaires**.

6. Contrôler l'intégrité de vos coordonnées bancaires

La modification d'un IBAN est simple dans un outil comptable et peut, selon vos volumes, ne pas être identifiée rapidement. Il peut être nécessaire de mettre en place une base de données cryptée de vos tiers en y associant leurs IBAN. A chaque demande de virement, un outil va aller **comparer et vérifier si des écarts** sont présents entre la base cryptée et sauvegardée et votre ERP ou outil comptable. Vous serez ainsi alerté par mail en cas d'anomalie : création ou modification d'un IBAN, discordance entre le nom du tiers et son numéro de compte, création d'un compte tiers déjà existant…

7. Instaurer un rapprochement bancaire automatique journalier

Le pointage des écritures bancaires et des règlements est capital en fin de processus. En effet, il permet de pouvoir identifier des fraudes (souvent sur des petits montants d'ailleurs qui ne sont pas soumis à des processus de validation en amont). La **finesse du paramétrage de votre outil de rapprochement bancaire comptable** (rapprochement de plusieurs écritures ensemble…) et l'**automatisation** de ce dernier peuvent vous permettre de réduire vos risques de fraude et d'être alerté rapidement sur des anomalies concernant l'ensemble de vos flux financiers (prélèvements, virements, chèques, CB…).

8. Sensibiliser les équipes en internes et expliquer votre processus de contrôle

Au-delà de l'ensemble des processus et outils de contrôle que vous pouvez mettre en place, une **sensibilisation de vos équipes** à votre démarche de sécurité financière est capitale. Chaque acteur doit comprendre, mesurer le risque et adhérer aux procédures internes. Vous pouvez également mettre en place des **audits internes ou externes** sur le respect des procédures et communiquer sur les résultats, axes de progression… au sein de votre entreprise.

Pour plus d'informations sur la sécurité de vos flux financiers, contactez-nous !

mercuria
la logique de gestion

5 rue de la Toscane

44240 La Chapelle sur Erdre

T. 02 40 49 16 49

F. 02 40 49 11 56

mercuria@mercuria.fr

www.mercuria.fr