Livre blanc

# LA SÉCURITÉ DES PAIEMENTS

Exalog

# En quelques mots

Depuis quelques années, de plus en plus d'entreprises de toutes tailles sont victimes de tentatives d'escroquerie sur les virements bancaires.

**Dans ce livre blanc, vous découvrirez quelles actions mettre en place pour réduire considérablement les risques liés à vos ordres de paiement.**

# SOMMAIRE

# 1

# LES RISQUES

# A Détournement de fonds

Lors de l'utilisation d'une application de gestion des paiements, une personne malveillante peut créer un compte bancaire pirate et effectuer ou faire effectuer des virements sur ce compte. Cette opération peut être effectuée par un utilisateur normal de l'application ou par une personne extérieure.

## Les risques de détournements par un utilisateur de l'application

### Réalisation d'une opération frauduleuse

Un utilisateur malveillant ayant accès à l'application peut effectuer lui-même des virements frauduleux. Si les droits ne sont pas correctement paramétrés, il peut enregistrer un faux compte bancaire, créer des ordres de paiements pour ce compte et les faire exécuter

### Altération de fichiers

Un utilisateur peut également altérer un fichier de virements s'il a accès aux répertoires dans lesquels le fichier transite (fichier de paie ou fichier de règlements issu de l'ERP de la société). Il peut créer ou remplacer un compte de destinataire. Cette modification sera difficile à repérer lors de la validation du fichier correspondant

## Les risques de détournements par une personne extérieure à la société

Souvent, l'escroc contacte la société en se faisant passer pour :

- **Un fournisseur**

L'escroc demande à la société de changer ses coordonnées bancaires pour le règlement de ses factures. Les nouvelles coordonnées correspondent à un compte qui sera utilisé pour détourner des fonds

- **Un faux assistant**

L'escroc peut appeler un utilisateur et lui demander d'effectuer un virement de « test » pour vérifier le bon fonctionnement de l'application. Il prétend travailler pour l'une des banques de la société, ou pour l'éditeur du logiciel de gestion des paiements

Les fonds détournés sont généralement transférés immédiatement sur une succession de comptes à l'étranger, ce qui rend la récupération des sommes détournées difficile.

- **Un dirigeant**

Une personne peut se faire passer pour un dirigeant de la société : prétextant une urgence ou une opération exceptionnelle (par exemple la nécessité de parer à un contrôle fiscal imminent ou de gérer une opération confidentielle à l'étranger) elle contacte les services comptables de l'entreprise et demande le virement d'une somme importante sur un compte qu'elle fait créer pour l'occasion

**Il s'agit généralement d'opérations très bien préparées : les escrocs se renseignent notamment sur les procédures internes, les noms des personnes et les habitudes de la société. Elles ciblent des exécutants en jouant sur leur respect de l'autorité et de la hiérarchie.**

Parfois, l'escroc ne contacte pas directement la société, mais pirate l'un de ses postes informatiques :

## Récupération d'identifiants

L'utilisateur de l'application de gestion des paiements installe sans le savoir un virus informatique sur son ordinateur (en cliquant sur une pièce jointe ou sur un lien d'un e-mail). Ce virus permet au pirate d'analyser l'ensemble des actions que l'utilisateur réalise sur son poste, et de capturer ce qu'il saisit sur son clavier. Le pirate parvient alors à se procurer les codes d'accès de l'utilisateur, qu'il utilisera pour réaliser des actions frauduleuses

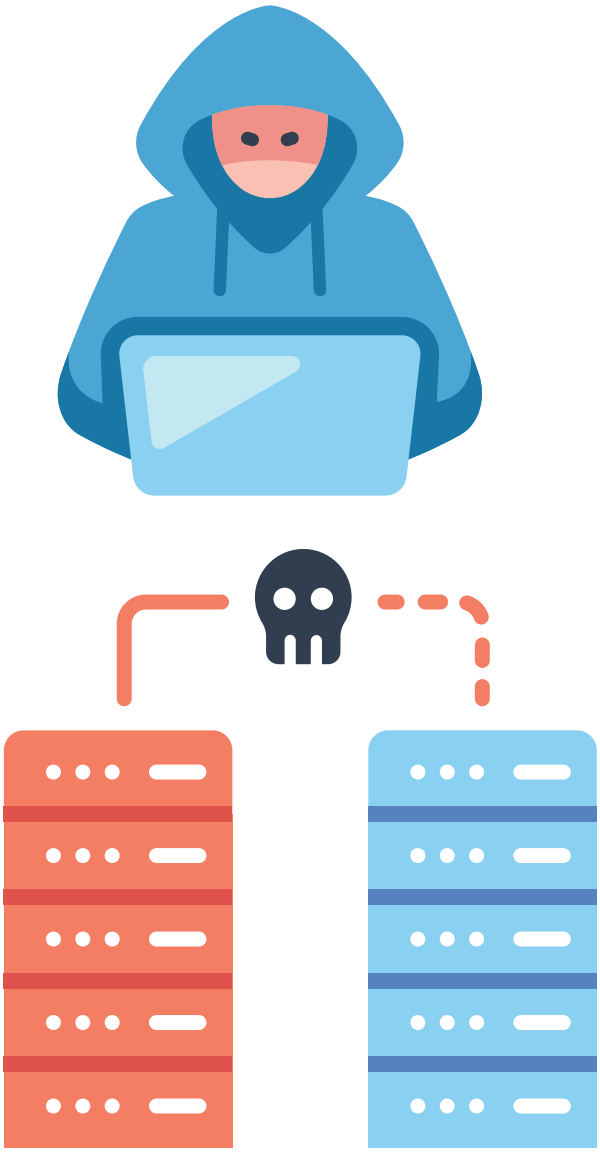
## Prise de contrôle à distance

Un virus informatique peut également permettre à un escroc de prendre le contrôle à distance de l'ordinateur de l'utilisateur. Le pirate peut ensuite se connecter à l'application de gestion des paiements et réaliser des opérations frauduleuses au nom de l'utilisateur

# B Divulgation d'informations confidentielles

**Un salarié en poste ou un ancien salarié peut potentiellement accéder à des données confidentielles, dans le but de :**

- Fournir à des entreprises concurrentes des informations telles que la liste des fournisseurs et clients de la société, ou la situation de sa trésorerie (solde des comptes)
- Révéler en interne les montants de salaires, dividendes ou jetons de présence



# C Indisponibilité du système de paiements

**Des actions de destruction de données peuvent être effectuées par un salarié en poste, un ancien salarié, une société concurrente ou encore un pirate informatique, et peuvent entraîner une indisponibilité du système de paiements.**

L'intention ici est de nuire à la société visée en paralysant son système de trésorerie via des actions telles que :

- Supprimer des données dans l'application
- Empêcher les accès utilisateurs
- Empêcher la communication avec les banques

Les conséquences de telles actions peuvent être industrielles, lorsqu'un fournisseur non payé décide d'arrêter sa production ou d'annuler une livraison. Elles peuvent aussi être sociales quand le non-paiement des salaires entraîne des mouvements sociaux dans l'entreprise.

2

# LES ACTIONS PRÉVENTIVES

# A Organisation

## 1. Définir une politique de sécurité de l'entreprise

**La sécurité des paiements doit idéalement s'inscrire dans un projet plus vaste de politique de sécurité de l'entreprise, dont le but est de protéger les biens et les services de l'entreprise.**

La politique de sécurité doit couvrir :

- Les données de l'entreprise, des applications et des systèmes d'exploitation
- Les télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- Les infrastructures matérielles : salles sécurisées, postes de travail, etc.

La mise en œuvre de cette politique comporte les étapes suivantes :

1. Identifier les données sensibles de l'entreprise, et les classer par ordre de criticité
2. Recenser et classer les risques pesant sur ces données
3. Analyser les procédures déjà en place
4. Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés

Après avoir élaboré une politique de sécurité qui réponde aux menaces identifiées, il est indispensable de diffuser ces informations à l'ensemble des collaborateurs. Toutes les personnes travaillant dans l'entreprise sans exception doivent être sensibilisées.

Il faut également s'assurer que la politique de ressources humaines de l'entreprise s'inscrive bien dans la politique de sécurité définie. Cela passe par exemple par des mesures de contrôle lors des recrutements (pièce d'identité, diplômes, extraits de casier judiciaire, etc.). Il faut aussi prévoir des procédures de création et de suppression de droits pour les salariés, sur tous les accès informatiques et physiques.

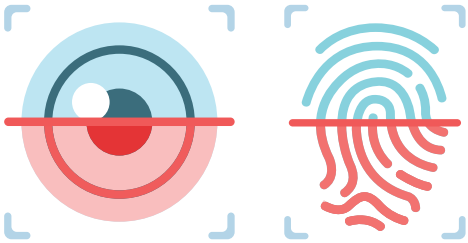
# 2. Définir les procédures de traitement des paiements

**En parallèle du travail sur la politique de sécurité de l'entreprise, il convient de définir les procédures de traitement des paiements. Celles-ci concernent : les accès, la ségrégation et l'automatisation des tâches, les droits et limites.**

## Accès

L'accès à l'application de gestion des paiements doit respecter les règles d'authentification forte dictées par la **Directive européenne sur les Services de Paiements 2** (DSP2). L'authentification de l'utilisateur doit ainsi combiner au moins 2 facteurs parmi les 3 suivants :

- Quelque chose que l'utilisateur connait : comme par exemple un mot de passe
- Quelque chose que l'utilisateur possède : il s'agit d'un élément matériel non mémorisable, comme une clé USB FIDO, une carte à puce, ou encore une carte de sécurité comprenant plusieurs codes
- Quelque chose que l'utilisateur est : tels qu'une empreinte digitale, l'iris de son œil ; ce sont des facteurs biométriques



Dans le cadre de la stratégie d'authentification à deux facteurs, **la clé FIDO** sécurisée peut être utilisée comme second facteur d'authentification et constitue une alternative simple à la saisie d'un code issu d'une carte à codes de sécurité. La logistique de sa mise à disposition aux collaborateurs est plus simple qu'un certificat : aucune configuration n'est requise et il n'est pas nécessaire de la renouveler. La même clé peut également être utilisée pour s'authentifier à plusieurs applications (Google, Gmail, Facebook, etc.). Enfin, la clé FIDO est un moyen abordable de sécurisation d'accès car elle coûte moins de 20 euros.

**RAPPEL**

Chaque personne physique utilisatrice d'un logiciel de gestion des paiements doit disposer de ses identifiants de connexion personnels et uniques.

**L'identification biométrique peut quant à elle être utilisée comme premier ou second facteur d'authentification, et se substitue alors à des moyens plus contraignants, comme le mot de passe ou la carte à codes de sécurité. Son utilisation rend l'authentification simple et rapide.**

Si vous continuez de vous connecter par code d'accès et mot de passe, il est recommandé d'apporter une attention particulière aux mots de passe, en :

- Imposant la saisie de caractères spéciaux, de chiffres et de lettres, et d'au moins 8 caractères
- Bloquant la connexion après 3 tentatives échouées
- Définissant une période de validité, qui oblige les utilisateurs à renouveler leur mot de passe régulièrement, par exemple tous les 3 mois.

Enfin, il est également conseillé de mettre en place une limitation d'accès en fonction de l'adresse IP de l'utilisateur. L'application de gestion des paiements empêchera alors la connexion aux ordinateurs avec une adresse IP inconnue.

## Ségrégation des tâches

Une seule et même personne ne doit pas être en mesure de créer et d'envoyer un paiement. Il convient donc de multiplier les acteurs impliqués dans les processus de création et de validation des ordres de paiements et des bénéficiaires, en **dissociant leurs rôles**.

**L'administrateur doit répondre aux questions suivantes, en s'assurant que les différentes tâches sont attribuées à des utilisateurs distincts.**

- Qui est habilité à enregistrer des comptes bancaires ?
- Qui est habilité à préparer des ordres de virements ?
- Qui est habilité à les valider ?
- Qui est habilité à les envoyer ?
- Qui est habilité à enregistrer des données telles que les comptes bancaires, les profils utilisateurs, les destinataires ?
- Qui est habilité à modifier ces données ?
- Qui est habilité à les supprimer ?
- Qui est habilité à valider les modifications de données ?

Lorsque plusieurs personnes sont impliquées dans la validation de données ou d'ordres, on parle du principe des 4/6 yeux. Ce contrôle permet d'éviter par exemple :

- La création d'un « faux » profil utilisateur dont une personne malveillante pourrait se servir pour effectuer des opérations frauduleuses
- La création d'un compte de destinataire qui n'est en réalité pas lié à la société
- La suppression non autorisée de données

## Droits et limites

**La sécurité des paiements doit passer par la définition des droits de chaque utilisateur. Ces droits peuvent être limités à la consultation de données, à certaines actions ou à la validation.**

- ### Limitation de consultation

Il s'agit ici de permettre la visualisation d'un contenu spécifique (détail d'ordres de virements par exemple) à certains utilisateurs seulement. Cela peut passer par des restrictions d'accès à des données ou par le chiffrement de fichiers. On prévient ainsi la divulgation d'informations confidentielles en interne ou à une entreprise concurrente. En particulier, pour les virements de salaires, il convient de mettre en place un système de protection qui permettent aux acteurs de la chaîne de paiement de visualiser uniquement le montant total de la remise, et non pas le détail des ordres

- ### Limitation par action

On peut limiter les actions autorisées pour chaque utilisateur par :

- Société (pour un groupe)
- Compte bancaire
- Montant
- Type d'ordre


- ### Validation

Pour les utilisateurs disposant de droits de validation, la signature numérique est le moyen le plus sécurisé d'autoriser l'envoi d'ordres bancaires. Elle garantit l'intégrité d'un document numérique et permet de connaître clairement son signataire. L'utilisateur disposant de la clé privée liée à un certificat électronique est le seul à pouvoir l'apposer, ce qui empêche toute personne malveillante d'usurper son identité et de valider des opérations non autorisées. La signature numérique garantit en outre que le document n'a pas été modifié entre sa signature et sa réception par la banque. Conjointement à l'utilisation de la signature numérique, il est conseillé de mettre en place un workflow de validation des paiements dans l'application de gestion des paiements. Cela permettra ainsi de structurer les étapes de validation d'une remise de paiements et de soumettre cette remise à la signature numérique d'une ou de plusieurs personnes avant de pouvoir l'envoyer en banque. La sécurité des paiements est ainsi renforcée avec une double, voire triple vérification de la remise de paiements.

Un autre moyen de réduire les risques de fraude bancaire est d'automatiser le traitement des paiements. Certaines tâches, comme la vérification des coordonnées bancaires d'un fournisseur ou l'autorisation d'un virement vers un pays étranger, sont souvent effectuées manuellement. Non seulement, ces tâches sont chronophages, mais elles augmentent les risques d'erreur et de fraude qui restent très présents.

## Automatisation des tâches

**L'application de gestion des paiements doit offrir plusieurs solutions pour automatiser le traitement des paiements pour éviter au maximum les interventions humaines, automatiser des contrôles, et renforcer ainsi la sécurité des paiements.**

### • Vérification que l'IBAN n'est pas frauduleux

Que ce soit pour les comptes des particuliers ou ceux des professionnels, le contrôle de l'IBAN permet non seulement d'avaliser les opérations de transferts de fonds, mais également de s'assurer que l'argent sera bien envoyé sur le bon compte.
La vérification de l'IBAN intervient à plusieurs étapes et de manière récurrente : lorsqu'un nouvel IBAN est saisi, ou qu'un virement ou un prélèvement est créé ou effectué.
L'application de gestion des paiements permet d'automatiser cette tâche de vérification et de mieux sécuriser les opérations d'envoi ou de réception d'argent de compte à compte. Les risques de fraude aux coordonnées bancaires sont ainsi réduits. Cette fonction de contrôle d'IBAN peut se faire par l'application ou par un tiers qui renverra le résultat du contrôle dans l'application de paiements.

### • Listes blanches

L'application doit permettre de pouvoir paramétrer des listes blanches de pays autorisés pour les virements. Cette liste a pour but de bloquer les virements frauduleux vers des pays non autorisés.
Aussi lors de la saisie de vos paiements, il vous est possible d'ajouter une pièce justificative (facture) sous forme de fichier ou bien d'un lien vers un logiciel externe comme par exemple un logiciel de gestion électronique de documents. Dans ce cas, il faut que votre logiciel de paiements vous permette de paramétrer une liste blanche pour définir les liens internet ou ftp/ftps autorisés. Cette liste a pour but de protéger l'entreprise contre les risques d'intrusion dans ses systèmes d'informations. En effet, ces liens peuvent être utilisés comme des points d'entrée pour récupérer

des données et construire une fraude bancaire, comme l'usurpation d'identité.

- ## Chiffrement et signature

Dans une automatisation complète des flux, les paiements proviennent de l'ERP comptable, sont mis automatiquement dans le workflow de validation et envoyés en banque après que le nombre de validation ait été atteint. Pour sécuriser encore davantage vos flux, les remises qui sortent de vos ERP peuvent être chiffrées et signées, ce qui assure la confidentialité et l'intégrité du fichier entre les 2 systèmes. Personne ne peut modifier la remise entre l'ERP et le logiciel de trésorerie. Exemple de solution : chiffrement et signature PGP.

# B Sensibilisation et formation

## 1. Sensibiliser les utilisateurs aux risques

**Les collaborateurs les plus exposés à une tentative de fraude sont les trésoriers, les comptables, et de manière générale les utilisateurs agissant sur les moyens de paiement. Afin de prévenir au mieux les risques, il convient de sensibiliser et de former ces utilisateurs.**

Les collaborateurs doivent être à tout moment conscients que l'entreprise peut être la cible de tentatives d'escroquerie comme le détournement de fonds, la divulgation d'informations ou la suppression de données. C'est pourquoi il est important de :

- Expliquer aux collaborateurs les différents types de risques encourus, présenter des exemples concrets d'escroquerie ou de tentative d'escroquerie et les conséquences concrètes (montants détournés, impacts sur l'image et la réputation de la société)
- Rappeler aux utilisateurs qu'il ne faut en aucun cas déroger aux procédures
- Leur demander d'être vigilants notamment lorsqu'une situation sort de l'ordinaire, comme par exemple la demande de modification de coordonnées bancaires d'un fournisseur

Les fraudeurs prétextent souvent l'urgence et la discrétion afin de pousser leur interlocuteur à effectuer une opération de virement, et ce en dépit des règles de sécurité fixées par l'entreprise, ou du simple bon sens. Les demandes de règlements urgents faites la veille d'un week-end sont ainsi très répandues, car elles empêchent les victimes de réagir rapidement.
Les escrocs peuvent utiliser l'intimidation, l'empathie ou encore la flatterie afin d'amener leur interlocuteur à transmettre un ordre de paiement : les collaborateurs doivent savoir reconnaitre ces comportements et s'en méfier.

# 2. Former les utilisateurs

**L'objectif pour les utilisateurs est de connaître les procédures de paiement mises en place et de savoir utiliser à bon escient les outils de sécurité mis à leur disposition.**

Il faut ainsi expliquer et détailler :

- **Les procédures de paiement à respecter :**
  - Saisie en ligne
  - Importation de fichier
  - Mise en workflow
  - Validation/signature
  - Envoi de remise à la banque
  - Validation éventuelle après envoi (lorsque la validation se fait sur le site web de la banque par exemple)
- **Le rôle des acteurs impliqués dans la chaîne de paiement :**
  - Qui saisit les ordres ?
  - Qui crée les bénéficiaires ?
  - Qui valide les ordres ?
  - Qui signe numériquement les ordres ?
  - Qui réalise l'envoi à la banque ?
- **Les procédures de contact des banques et leurs interlocuteurs**

  Ainsi, les utilisateurs seront vigilants s'ils sont contactés par un interlocuteur ou via une procédure inconnus. Il faut également qu'ils soient en mesure de contacter la banque pour vérification, signalement, ou tout problème relatif aux moyens de paiements
- **Les règles de gestions des incidents**

  Les utilisateurs doivent savoir qui contacter dans et en dehors de l'entreprise, et de quelle manière, afin de réagir au plus vite en cas de tentative de fraude

**En cas de fraude avérée, il convient de prévoir une procédure spécifique à suivre, et de la communiquer aux utilisateurs :**

- Informer les personnes désignées dans l'entreprise
- Prévenir l'établissement bancaire
- Déposer plainte auprès du commissariat de police
- Recueillir les traces des actions frauduleuses et les adresses IP utilisées (via le service informatique)

- ## Les méthodes de gestion des absences et des congés

  Les règles de sécurité doivent tenir compte des périodes de congés ou d'absence, et détailler les procédures à respecter dans ces situations particulières et identifier les personnes à contacter en remplacement

La formation est un travail continu : il faut systématiquement former les nouveaux collaborateurs et informer les utilisateurs habituels chaque fois que les procédures ou les outils de sécurité évoluent.

# 3. Principales règles à respecter

**Voici des règles incontournables à faire respecter par tous les collaborateurs.**

- **Identifiants et mots de passe :**
  Ne jamais communiquer ses accès à une tierce personne (même à un collègue), afin d'éviter qu'une personne malveillante utilise ces accès pour effectuer des opérations non autorisées

- **E-mails et pièces jointes :**
  Ne pas cliquer sur les pièces jointes ou les liens d'e-mails dont l'expéditeur est inconnu. Cela pourrait permettre à un malware d'être installé sur le poste de l'utilisateur, afin qu'un pirate informatique en prenne le contrôle ou récupère des informations de saisie (comme un mot de passe)

- **Conversations téléphoniques :**
  Ne jamais agir au téléphone, et ne pas effectuer des actions demandées par une personne dont l'identité n'a pu être vérifiée

- **Communication interne :**
  Informer sa hiérarchie si un interlocuteur demande la réalisation une opération exceptionnelle dans l'urgence et/ou dans la plus grande discrétion

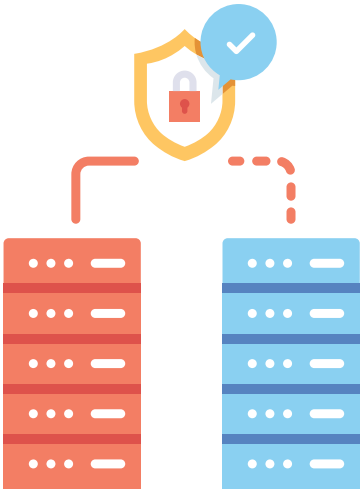
- **Réseaux sociaux :**
  Ne jamais diffuser d'informations sensibles sur les réseaux sociaux professionnels et personnels

# C Sécurisation des environnements de travail

**Il est nécessaire de sécuriser l'environnement de travail des utilisateurs en mettant en place un dispositif de sécurité informatique :**

- Installation et mise à jour automatique d'anti-virus et d'anti-malwares sur les postes des utilisateurs

- Obligation pour un utilisateur de passer par un administrateur pour installer un programme ou un logiciel. Cela peut éviter l'installation involontaire d'un outil malveillant (type Phishing) conçu par exemple pour récupérer des identifiants de connexion à une application



- Mise en place d'un système de sauvegarde et de restauration complet des postes de travail

- Sécurisation de l'accès à Internet par la mise en place d'un proxy sur le réseau de l'entreprise. Celui-ci bloque l'accès aux sites considérés comme risqués ou indésirables, répertoriés dans des listes noires publiques disponibles gratuitement

Nous vous recommandons fortement d'élaborer une charte informatique. Celle-ci définit les règles d'utilisation des outils informatiques que tous les collaborateurs doivent respecter.

3

# LES AUDITS ET CONTRÔLES

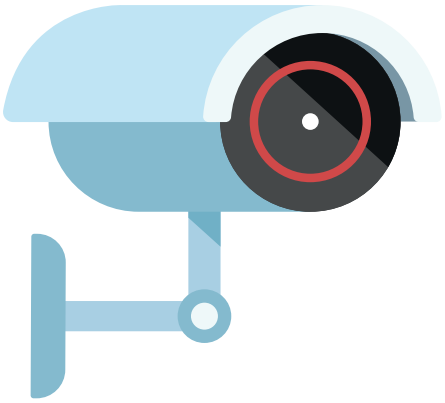
**L'efficacité des contrôles dépend de la qualité des traces. La traçabilité doit donc être préalablement mise en place sur l'ensemble des outils et infrastructures utilisés par l'entreprise :**

- Traces sur les connexions aux serveurs depuis des ordinateurs locaux ou des ordinateurs distants (réseau VPN)
- Traces sur les accès aux serveurs partagés et sur toutes les actions effectuées sur les serveurs contenant des données sensibles
- Traces sur les réseaux : détection de blocages réseaux, inspections réseaux permettant de repérer des fichiers ou programmes potentiellement malicieux
- Traces sur les données récoltées par tous les anti-virus installés sur les postes des collaborateurs
- Traces sur les envois et réceptions d'e-mails (heures, adresses e-mails de l'envoyeur et du destinataire)
- Traces sur les sites web consultés par les collaborateurs afin de repérer les sites potentiellement dangereux (risque de téléchargement d'un logiciel malveillant par exemple)

# A Contrôle du respect des procédures

## 1. Contrôle des paramétrages

**Il s'agit ici de vérifier que les paramétrages de l'application de gestion des paiements sont bien en adéquation avec la politique de sécurité mise en place :**



- Les accès à l'application sont-ils correctement protégés (complexité des mots de passe, blocage au bout d'un certain nombre de tentatives de connexion, restriction d'accès en fonction de l'adresse IP d'origine, etc.) ?
- La ségrégation des rôles entre les collaborateurs est-elle bien établie ?
- La création/modification/suppression de données dans l'application requiert-elle bien une validation d'un administrateur ou d'un superviseur de sécurité ?
- L'accès à des données confidentielles est-il restreint à certains utilisateurs désignés ?
- Les étapes des processus de validation des paiements respectent-elles bien les procédures définies

## 2. Utilisation des traces

Vos collaborateurs peuvent être amenés à effectuer bon nombre d'opérations sur un outil de traitement de paiements : exécution de virements, consultation de relevés de compte, ajout/modification/suppression de données comme les profils utilisateurs, comptes émetteurs, destinataires, etc. C'est pourquoi il est important de garder une trace de toutes ces opérations et des informations associées (utilisateurs ayant effectué l'opération, date et heure, type d'action, description précise de l'action effectuée, etc.) afin de vérifier la conformité des opérations effectuées avec les procédures internes mises en place.

# 3. Contrôles aléatoires sur les paiements réels

**Parallèlement aux audits internes réguliers et programmés, mettre en place des contrôles aléatoires est une bonne manière de vérifier « en temps réel » le respect des procédures de sécurité.**

Cela permet notamment de vérifier si un paiement est bien traité selon un workflow de validation défini, ou encore de voir si la ségrégation des rôles est bien respectée (la personne qui crée des ordres de paiements n'est pas celle qui les valide par exemple).

# B Vérification du fonctionnement des outils de sécurité

**Des audits internes réguliers doivent permettre de vérifier l'adéquation des modes de fonctionnement des outils avec la politique de sécurité de l'entreprise.**

## Les contrôles sur les environnements de travail

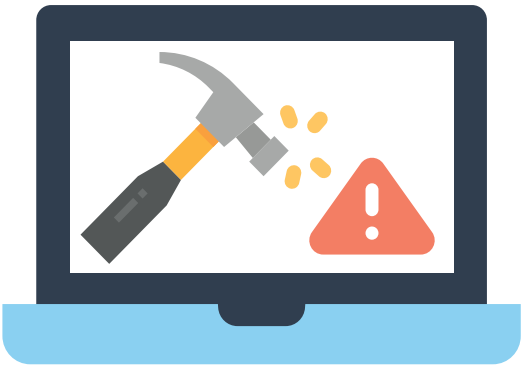
- Vérifier la présence et le bon fonctionnement des anti-virus/anti-malware sur l'intégralité des postes de travail de l'entreprise
- Vérifier le bon fonctionnement des sauvegardes intégrales de système d'information
- Tester la restauration de sauvegarde complète des serveurs, postes de travail et PC portables
- Tester les mécanismes de sauvegarde et de restauration des boites aux lettres individuelles, courriels et pièces jointes

## Les contrôles sur les systèmes de gestion des paiements

- Vérifier le bon fonctionnement des mécanismes de protection des accès (par exemple, s'assurer qu'une application de gestion des paiements se bloque au bout d'un certain nombre de tentatives échouées)
- Vérifier le bon fonctionnement des workflows automatiques paramétrés pour le traitement de certains paiements
- Vérifier le bon fonctionnement des mécanismes de cryptage de fichiers sensibles
- Vérifier le bon fonctionnement des mécanismes de restrictions d'accès à certaines données ou certaines fonctionnalités

# C Tests de résistance

**Un test de résistance vise à soumettre un produit, une entité ou un système à des conditions d'utilisation extrêmes, ou à des attaques, afin de tester sa stabilité. Cette technique peut servir à identifier des failles dans le système de sécurité mis en place, mesurer l'impact de chaque vulnérabilité sur la sécurité du système d'information, et définir un plan d'action pour leur prise en compte.**



Dans le cas précis de la gestion des paiements via un logiciel ou une application web, les exemples de tests suivants peuvent être réalisés :

- Création d'un faux compte de destinataire qui n'est pas lié à la société et qui pourrait potentiellement servir à détourner des fonds : le but ici est de voir si la création du compte est validée ou non
- Création d'un faux compte utilisateur dont l'instigateur pourrait se servir pour masquer sa véritable identité et se connecter à l'application pour commettre des actions frauduleuses
- Tests de pénétration : vous pouvez faire appel à une société spécialisée afin de vérifier la résistance de l'application aux intrusions extérieures

# CONCLUSION

**En résumé, voici un rappel des étapes à suivre pour garantir la sécurité de vos paiements :**

- **Identifier le niveau actuel de sécurité des paiements, les données sensibles de l'entreprise, les menaces pesant sur son activité et leurs conséquences**
- **Définir une politique de sécurité en élaborant des procédures de traitement des paiements claires et précises**
- **Sensibiliser et former les utilisateurs aux bonnes pratiques et aux règles de sécurité à respecter**
- **Sécuriser les environnements de travail des collaborateurs**
- **Effectuer des audits/contrôles afin de s'assurer du bon respect des procédures mises en place pour détecter d'éventuelles failles dans la gestion des paiements**

Ce livre blanc vous est proposé par Exalog,
éditeur de logiciels de gestion des paiements et de la trésorerie

**www.exalog.com** **contact@exalog.com**