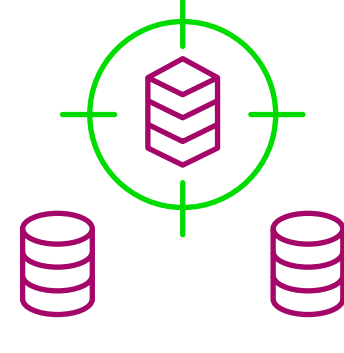


Comment sécuriser efficacement votre chaîne de paiement ?

En quelques années, la fraude aux paiements est devenue un véritable fléau pour les entreprises. Le nombre de cyber-attaques a progressé de 38 % dans le monde¹. D'où la nécessité pour les entreprises de se protéger. Voici, point par point, les étapes à mettre en place pour sécuriser votre chaîne de paiement.

Le risque financier lié à la fraude

L'explosion de la cybercriminalité fait porter un risque financier majeur sur les entreprises, il est donc vital pour elles, en interne comme en externe, de mettre en œuvre les moyens nécessaires pour diminuer ce risque.



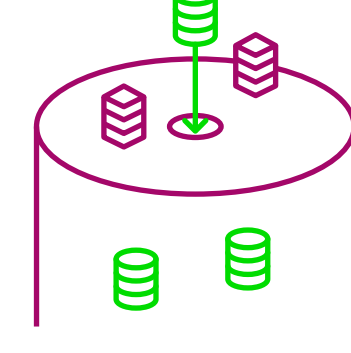
1

Identifier les zones de risques



2

Définir une politique de sécurité



3

Mettre en place des solutions

Les mécanismes d'alerte

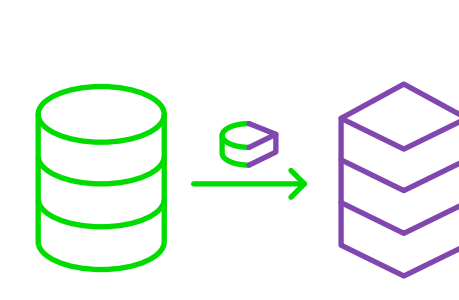
Pour anticiper et prévenir les risques, il est crucial de mettre en œuvre des mécanismes d'alerte sur des mouvements ou procédures suspects telles que :



Un transfert d'argent inhabituel, que ce soit en raison du motif ou du montant.



Une demande urgente d'argent couplée avec une demande de confidentialité.



Un transfert inhabituel vers des comptes bancaires étrangers.

Agir en amont et anticiper les risques

Certaines procédures internes sont essentielles à la protection contre la fraude. Pensez à :



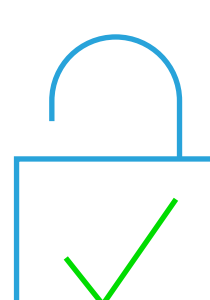
Prévenir plutôt que guérir

Sensibiliser en interne sur les risques de fraudes et informer des sanctions encourues.



Sécuriser les intégrations

Les process à risques comme les saisies manuelles ou les imports de fichiers doivent être sécurisés.



Sécuriser les process de signatures et de validation

Sensibiliser les valideurs et signataires sur les risques de ces process et leur donner les bons outils.

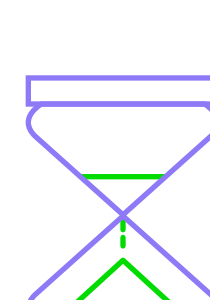


Sécuriser les transferts

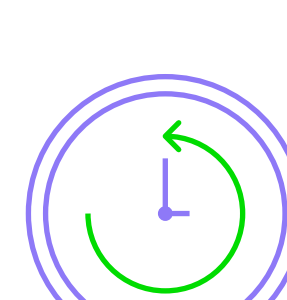
Tout ce qui relève du protocole bancaire doit être encadré par un processus stricte.

La sécurisation des flux avec les banques

La signature électronique comporte de nombreux avantages. Depuis 2000, elle a la même valeur légale que la signature manuscrite et permet :



un raccourcissement des délais de traitement des dossiers et de prises de décision



la suppression des délais et des coûts de traitement des courriers

La signature électronique s'inscrit dans un processus de contrôle et de traçabilité et permet la mise en place d'une chaîne décisionnelle sûre et de lutter contre la fraude.

Les salariés d'une entreprises doivent être informés des risques et formés aux règles de sécurité à respecter, mais aussi **mettre en place des protocoles strictes et rigoureux**, que ce soit en matière de transactions, de transferts ou de validation. **La prévention et l'anticipation des risques sont les maîtres mots** permettant une politique de sécurité efficace, rendant possible une baisse importante des risques de fraude au paiement.

Pour en savoir plus sur la sécurisation de vos flux financiers, contactez l'un de nos experts au :

0 825 007 017 Service 0,15 € / min + prix appel

en France.

+33 556 180 134

à l'export.

SOURCES

¹ Étude PwC, The Global State of Information Security Survey 2016, novembre 2015

sage

©2018 The Sage Group plc, ou ses partenaires. Tous droits réservés. Les marques, les logos et les noms des produits et services Sage mentionnés sont les marques appartenant à The Sage Group plc, ou à ses partenaires. Toutes les autres marques sont la propriété de leurs titulaires respectifs.