LES LOGICIELS DE GESTION DES PAIEMENTS : DES OUTILS HAUTEMENT SÉCURISÉS

Alors que la généralisation du télétravail a provoqué une véritable recrudescence des cyberattaques, la sécurisation des paiements et de la trésorerie des entreprises est aujourd'hui une priorité absolue. Pour comprendre le phénomène, rencontre avec Madame Stéphanie Bombart, dirigeante de la société Exalog : éditeur de logiciels de gestion des paiements et de la trésorerie.

Stéphanie Bombart

Informations Entreprise : Lorsque l'on parle de fraudes aux virements de quels volumes parle-t-on ?

Stéphanie Bombart : Selon l'étude d'Euler Hermes et l'Association nationale des Directeurs Financiers et de Contrôle de Gestion (DFCG), en 2021 1 entreprise sur 4 a subi une fraude, et 33% des entreprises victimes de fraude ont subi un préjudice supérieur à 10K € (14% ont subi un préjudice supérieur à 100K €). Un phénomène d'ailleurs accentué suite à la généralisation du télétravail. Si la sécurité des paiements est un enjeu important des entreprises, elle est notre priorité première chez Exalog : tous nos logiciels doivent être 100% sécurisés pour faire face aux risques de cyber attaques.

IE : Dans un monde marqué par les cyberattaques, comment empêcher les fraudes aux virements ? Quel est l'avantage de mettre en place un outil de gestion des paiements et de la trésorerie ?

Stéphanie Bombart : Dès qu'une entreprise travaille avec plusieurs banques, elle a tout intérêt à disposer d'un logiciel capable de se connecter à ses banques, pour pouvoir émettre des paiements rapidement et facilement avec un niveau de sécurité maximal. Or, encore trop de sociétés vont sur le site web de leurs multiples banques pour leurs paiements, avec des procédures de validation hétérogènes ! Un outil unique comme Exabanque (pour les PME) ou Allmybanks (pour les ETI et grands comptes) permet de centraliser les informations bancaires ainsi que la base de données fournisseurs et d'homogénéiser les procédures de validation et d'envoi des paiements aux banques. L'entreprise peut ainsi gagner en efficacité et maîtriser au mieux la sécurité de ses paiements.

Par ailleurs, notre solution Allmybanks propose la connectivité plug and play au réseau mondial bancaire sécurisé SWIFT. Le but ? Pour les groupes internationaux de faire des paiements sécurisés partout dans le monde. Tous les logiciels ne proposent pas cette possibilité, l'audit pour être opérateur SWIFT étant extrêmement complexe et poussé sur la sécurité.

Les outils de gestion des paiements ont aussi l'avantage de s'interfacer avec les ERP pour l'automatisation et la sécurisation des flux.

Enfin, nos applications permettent aussi à une entreprise de récupérer en automatique ses relevés de comptes, pour avoir une visibilité immédiate de sa trésorerie et d'en optimiser la gestion (prévisions, codification des flux, fonctions de centralisation du cash...). Or beaucoup d'entreprises utilisent encore Excel pour le suivi de leur trésorerie. Une situation qui se révèle inadaptée au regard de la complexité des données gérées, des risques d'erreur, ou encore des problématiques de maintenabilité et de pérennité dans le temps.

IE : La sécurité des paiements passe donc par une plateforme sécurisée. Comment assurez-vous la sécurité de vos logiciels ?

Stéphanie Bombart : Nos applications Exabanque et Allmybanks, sont fournies en mode SaaS. Elles sont accessibles avec un simple navigateur, sans aucune installation technique sur les postes des utilisateurs ou des serveurs du client.

Comme nos logiciels sont en mode SaaS, c'est Exalog qui s'occupe de toute la sécurité, des infrastructures, de la sauvegarde, de la disponibilité des données. Nous sommes d'ailleurs certifiés ISAE 3402 pour la qualité et la sécurité de nos procédures de mode SaaS. Et nous avons en moyenne un audit de sécurité par mois !

Toutes les données de nos clients (12 000 sociétés utilisatrices) sont hébergées en France, dans des data centers hautement sécurisés certifiés ISO 27001 (plus haut niveau de sécurité dans l'hébergement des données). Les informations les plus sensibles de nos clients sont cryptées. L'accès à nos logiciels est verrouillé par au moins deux facteurs d'authentification. Nous contrôlons également la localisation de l'utilisateur (adresse IP). Dès que l'utilisateur se connecte depuis une localisation autre que sa localisation habituelle, un code de sécurité lui est envoyé pour s'assurer que c'est bien lui qui tente de se connecter : un dispositif extrêmement efficace.

IE : De ce postulat, quelles procédures mettre en place dans le logiciel ?

Stéphanie Bombart : Si la fraude peut venir d'un hacker qui essaye de trouver une faille technique ou de se connecter, elle peut aussi venir de l'intérieur. La ségrégation des tâches est donc importante. Une seule et unique personne ne doit pas être en mesure d'effectuer tout le flux de paiement : saisir le fournisseur, créer le paiement, le signer, l'envoyer en banque… c'est une organisation à mettre en place qui se traduit en habilitations dans nos applications. Autre outil : l'activation du principe des 4 yeux ; c'est-à-dire la validation par un superviseur de l'ajout ou de la modification de fournisseurs, d'utilisateurs, de sociétés par un utilisateur. Il est également possible de paramétrer une liste blanche de pays vers lesquels les paiements sont autorisés. Le but est de bloquer tout paiement frauduleux vers un pays non autorisé. Enfin pour assurer une sécurité maximale des paiements, il convient de paramétrer des workflows de validation qui peuvent dépendre des montants engagés, et de signer les paiements avec la signature numérique ; un procédé qui réduit considérablement le risque de fraude ! Car les banques vérifient systématiquement ces signatures personnelles et infalsifiables. De plus, la signature numérique garantit que le fichier reçu par la banque est identique à celui signé par le signataire.

Le dernier aspect de la sécurisation des paiements est le STP : Straight through processing, tendre vers une automatisation complète pour plus de sécurité. Le but est que toutes les données validées en comptabilité ne soient plus modifiées, et qu'il n'y ait aucune intervention manuelle. Les paiements qui proviennent de l'ERP sont ainsi mis automatiquement dans le workflow de validation du logiciel de paiements, et envoyés en automatique à la banque après que le nombre de validations ait été atteint.

IE : La sensibilisation des utilisateurs sur le risque de fraude apparaît également primordiale ?

Stéphanie Bombart : Oui, toute la difficulté repose sur le fait d'évangéliser les organisations sur ces questions, et notamment pour ce qui concerne les bonnes pratiques de sécurité appliquées aux paiements à l'heure où les fraudes et les cyberattaques constituent une menace majeure. Aujourd'hui, les entreprises en prennent peu à peu la mesure car certaines d'entre elles ont été attaquées.

Il faut également sensibiliser de manière régulière les utilisateurs aux risques de fraude en donnant des exemples et des conséquences concrètes, typiquement : être vigilant quand une situation sort de l'ordinaire, ne jamais agir au téléphone, ne pas donner ses informations personnelles. Nous-même, en tant qu'éditeur de logiciels de paiements, nous informons régulièrement nos clients des procédures nécessaires à déployer pour assurer la sécurité de leurs paiements.

IE : Quelles sont les dernières innovations du marché en termes de sécurisation des flux ?

Stéphanie Bombart : Tout d'abord, des innovations d'authentification par la biométrie et la clé USB FIDO. FIDO est une alliance qui regroupe les grands acteurs de l'informatique comme Google, Microsoft, Intel… qui développent des normes d'authentification pour éviter le recours massif aux mots de passe. Exalog fait partie des 1ers éditeurs de logiciels de cash management à avoir proposé la connexion par authentification biométrique (l'empreinte ou visage) et par la clé USB FIDO comme 2ème facteur. L'intérêt de la clé FIDO est qu'elle n'est pas chère, elle est plug and play (pas de certificat à gérer), et devient un standard international compatible avec de nombreuses applications. Vous pouvez l'utiliser pour vous connecter à votre application de paiements mais aussi à gmail, facebook, wordpress… Ces nouveaux modes d'authentification FIDO rendent l'authentification plus simple et plus fluide tout en assurant le même niveau de sécurité.

Autre innovation, les plateformes de contrôle automatique des coordonnées bancaires des tiers (Trustpair et SiS id) pour éviter les fraudes aux virements. Exabanque et Allmybanks sont connectées en natif avec ces plateformes.

Enfin, la clé de signature numérique se dématérialise. La signature numérique sera possible sans clé USB, pour éviter les problèmes logistiques de distribution ou informatiques. Bientôt, elle permettra aussi de signer numériquement les paiements, directement sur mobile !

Comme vous le voyez la sécurisation des flux et des données est un sujet stratégique, c'est pourquoi nos logiciels évoluent en permanence pour offrir de nouveaux outils pour fluidifier et sécuriser le travail de gestion des paiements et de la trésorerie.