MATA I/O SECURE e-Link

UNE DÉMARCHE DE SÉCURITÉ GLOBALE

POUR LUTTER CONTRE LA FRAUDE AU VIREMENT

La fraude aux moyens de paiement touche toutes les entreprises, grands groupes ou PME et profite de l'hétérogénéité des systèmes qui constitue une zone de faille.

Les zones de faille se situent le plus souvent entre les applications de gestion de l'entreprise (ERP, comptabilité) et la banque car une campagne de règlement va donner lieu à la production de fichiers en clair qui seront envoyés à la banque au prix d'un certain nombre d'opérations manuelles.

La fraude peut également être le fruit d'une manipulation qui consiste à faire pression sur la bonne personne dans l'entreprise pour lui faire créer ou modifier un compte.

MATA I/O SECURE e-Link

POUR ÊTRE SÛR DE CE QU'ON SIGNE

- Réaliser toutes les opérations dans la même application
- Crypter les fichiers de règlement en sortie d'ERP pour éviter leur dépôt en clair
- Vérifier les comptes bancaires des tiers en les pointant avec une base référente sécurisée
- Intégrer le service bancaire SEPAmail Diamond pour contrôle automatique des IBAN
- Alerter les fondés de pouvoir des anomalies avant signature
- Signer ses ordres en EBICS TS, protocole reconnu par toutes les banques

S'ASSURER DE LA BONNE EXÉCUTION DES ORDRES BANCAIRES

- Tableau de bord global des flux
- Lecture des comptes rendus bancaires PSR et ARA
- Contrôle automatique des prélèvements au débit de vos comptes

UNE DÉMARCHE DE SÉCURITÉ GLOBALE

Parce que le niveau de sécurité se définit par la résistance du maillon le plus faible, **SECURE e-Link** traite l'ensemble des problématiques de sécurité de la chaîne de règlement par la création d'un espace de sécurité de l'ERP jusqu'à la banque.

MATA I/O SECURE e-Link :
un espace sécurisé et crypté qui va de votre ERP jusqu'aux banques.