

PAROLES D'EXPERTS

Facturation électronique : après la conformité, le défi de la sécurité

Depuis plusieurs années, la facture électronique est essentiellement abordée sous l'angle réglementaire. Pourtant, à mesure que la réforme se concrétise, une autre question s'impose : celle de la sécurité des données. Car derrière la dématérialisation des factures, ce sont désormais des flux d'informations financières, bancaires ou administratives qui circulent entre les organisations. Cette évolution ouvre de nouvelles opportunités, mais aussi de nouveaux risques.

 Ajouter La Gazette France à vos sources préférées



Loïc Helmstetter, Expert-comptable à Sarrebourg (c) Yzico

Là où les fraudeurs cherchaient autrefois à falsifier un document ou à usurper une identité de manière relativement grossière, ils disposent aujourd'hui d'outils beaucoup plus sophistiqués. Les campagnes de phishing sont personnalisées, les faux e-mails quasiment indiscernables des vrais et les tentatives d'usurpation s'appuient parfois sur l'actualité même de l'entreprise.

Dans ce contexte, la question n'est plus seulement de savoir si les systèmes sont sécurisés, mais si l'organisation est réellement préparée à faire face à ces nouveaux risques.

La facture électronique numérise bien plus que les factures

La réforme est souvent perçue comme un changement de format. Pourtant, son impact dépasse largement le simple remplacement d'un PDF par une facture électronique structurée. Les échanges reposeront désormais davantage sur des flux de données capables de circuler automatiquement entre différents systèmes, rendant les traitements plus automatisés et les informations plus facilement exploitables.

Cette nouvelle architecture présente de nombreux avantages :

→ Elle permet de fluidifier les processus, de réduire certaines tâches répétitives et d'améliorer la visibilité sur les flux financiers ;

→ Mais elle implique également une vigilance accrue sur la circulation et la protection des données.

La facture n'est plus seulement un justificatif comptable, elle devient un élément d'un écosystème numérique plus large, connecté aux systèmes de gestion, aux outils de comptabilité, aux plateformes d'échange et parfois aux solutions de paiement.

Plus de traçabilité ne signifie pas automatiquement moins de fraude

L'un des objectifs de la réforme est de renforcer la traçabilité des échanges. À juste titre, cette évolution est souvent présentée comme un facteur de sécurisation. Cependant, la traçabilité ne supprime pas à elle seule les risques de fraude. Elle en déplace parfois les frontières... Le paradoxe est simple : une facture peut être

conforme, correctement transmise et tracée, tout en donnant lieu à un paiement frauduleux si un fraudeur parvient à modifier des coordonnées bancaires ou à contourner les procédures de validation.

Prenons un exemple très concret : une entreprise reçoit une facture parfaitement conforme via son circuit habituel, le document est authentique et la transmission également. Entre-temps, un fraudeur a réussi à compromettre la messagerie du fournisseur et à transmettre de nouvelles coordonnées bancaires.

La facture est payée, les contrôles comptables sont respectés, mais les fonds sont virés vers un compte contrôlé par les fraudeurs. Le document n'était pas faux ; le paiement, lui, a été détourné.

Faux fournisseurs, changements frauduleux de RIB, compromission de messageries professionnelles ou usurpation d'identité figurent aujourd'hui parmi les principales menaces. Et l'intelligence artificielle renforce encore la crédibilité de ces attaques : les messages frauduleux peuvent désormais être parfaitement rédigés et adaptés au contexte de l'entreprise.

La frontière entre communication légitime et tentative de fraude devient alors plus difficile à identifier et la sécurisation des flux devient donc aussi importante que celle des documents.

L'humain reste le premier maillon de la sécurité

Les spécialistes de la cybersécurité partagent d'ailleurs un constat devenu récurrent : la majorité des fraudes réussies n'exploitent pas des failles inconnues ou particulièrement complexes. Elles exploitent des raccourcis du quotidien : un changement de RIB validé trop rapidement, une demande de paiement urgente que personne n'ose remettre en question, un mot de passe conservé dans un navigateur, une validation accordée parce qu'un message semble provenir d'un interlocuteur de confiance...

Autrement dit, les fraudeurs cherchent rarement à contourner les règles, ils cherchent plus souvent à contourner la vigilance.

Certaines mesures simples permettent déjà de réduire significativement les risques : l'authentification multifactorielle sur les outils sensibles, la vérification systématique des modifications de coordonnées bancaires, la revue régulière des droits d'accès ou

encore la mise en place de règles de validation adaptées aux paiements les plus sensibles.

Au-delà des procédures, la culture de vigilance devient un enjeu central : chaque collaborateur amené à traiter des données financières ou administratives participe désormais à la sécurité globale de l'organisation.

Une opportunité pour renforcer la gouvernance des données

La généralisation de la facture électronique conduit les entreprises à s'interroger davantage sur leur gouvernance des données : où les informations sont-elles hébergées, qui peut y accéder et comment réagir en cas d'incident ?

La donnée devient donc, progressivement, un actif stratégique au même titre que la trésorerie, les équipements ou le portefeuille clients. Sa protection ne relève donc plus uniquement des équipes informatiques, elle concerne désormais la direction, les fonctions financières, les responsables administratifs et l'ensemble des acteurs participant aux flux de l'entreprise.

Dans ce contexte, la conformité réglementaire n'est plus une finalité : elle constitue plutôt le point de départ d'une réflexion plus large sur la confiance, la maîtrise des flux et la résilience des organisations.

Une nouvelle responsabilité pour les entreprises

La facture électronique est souvent présentée comme un projet de conformité. En réalité, elle agit comme un révélateur beaucoup plus large. Elle oblige les entreprises à mieux connaître leurs flux, à revisiter leurs processus, à renforcer leur gouvernance des données et à développer une véritable culture de la vigilance.

Demain, la vraie question ne sera plus « sommes-nous conformes ? », elle sera : « sommes-nous capables de protéger nos flux et la confiance de nos partenaires ? ».

Par Loïc Helmstetter, Expert-comptable à Sarrebourg

La complexité devient un risque à part entière

La facture électronique repose sur un nouvel écosystème composé de plateformes, d'interconnexions, de flux automatisés et de multiples

intervenants. Pour les entreprises, cette richesse fonctionnelle constitue un progrès.

Mais elle crée également un nouvel enjeu : comprendre qui fait quoi et identifier les interlocuteurs légitimes. Les fraudeurs exploitent précisément cette période d'apprentissage. Faux e-mails de mise en conformité, demandes de validation d'accès, faux supports techniques ou fausses demandes de mise à jour de coordonnées bancaires utilisent tous le même levier : créer un sentiment d'urgence dans un univers encore nouveau pour de nombreuses entreprises.

Plus un environnement est complexe, plus il devient difficile de distinguer immédiatement le vrai du faux.