LE MOT DE LA SEMAINE

Escroquerie au Président

1094

De la nécessité de sensibiliser en interne contre les fraudes aux faux ordres de virement internationaux (FOVI)

LegalTag


LUDOVIC MALGRAIN, associé

JEAN-LOU SALHA Cabinet d'avocats White & Case LLP, département Contentieux pénal et règlementaire, Partenaire du Club des juristes

Comment peut-on encore expliquer que de nombreux groupes internationaux très structurés, aussi bien que des entreprises de taille plus modeste, continuent à être victimes d'ordres de virements internationaux frauduleux avec pour conséquence le transfert de fonds importants à l'étranger, alors même que le mode opératoire de cette fraude, qui évolue peu, est connu depuis plusieurs années, parfaitement identifié par les autorités judiciaires, régulièrement dénoncé par les services de police, l'Autorité des marchés financiers, les chambres de commerce et les établissements teneurs de compte ?

Cette fraude, commise systématiquement depuis l'étranger, coûte depuis 2010 aux entreprises et à leurs compagnies d'assurances plusieurs centaines de millions d'euros et enrichit des réseaux de criminalité très organisés jouant de la rapidité des transferts bancaires et des limites de la coopération judiciaire internationale, y compris au niveau européen, malgré les progrès liés à Eurojust.

La réponse s'impose comme une évidence : une sensibilisation insuffisante des équipes opérationnelles, à savoir de toutes les personnes susceptibles d'être sollicitées au sein des entreprises pour préparer, puis transmettre, les ordres de virement aux établissements bancaires chargés de leur traitement.

Certes, toute une série d'actions peut être menée avec efficacité dans les heures qui suivent la découverte de la fraude, afin d'obtenir le gel puis le retour des fonds.

Toutefois, ceci demeure au prix de procédures judiciaires coûteuses, longues, parfois aléatoires en fonction des juridictions concernées, alors même qu'une sensibilisation préalable des équipes ciblées par ces réseaux de criminalité permet de déjouer aujourd'hui efficacement cette escroquerie et demain d'autres types de manœuvres.

Le mode opératoire de cette escroquerie, souvent baptisée « escroquerie au Président », consiste systématiquement à cibler un employé du département Trésorerie, Comptabilité ou Finances de la société, au travers d'un contact téléphonique ou d'un e-mail prétendument adressé par le président, le directeur général, le directeur financier - celui qui dispose, pour le collaborateur ciblé, d'une autorité incontestable.

Cette usurpation d'identité donnera l'illusion à l'employé de recevoir un e-mail provenant du management.

Le motif du transfert apparaîtra dans les e-mails qui suivront, échangés souvent dans l'espace d'une journée : « OPA », « achat de société », « paiement d'un fournisseur »…

L'objet de la demande faite au collaborateur sera systématiquement de préparer un ordre de virement international à retourner par e-mail pour signature, puis à transmettre à la banque qui, tout en respectant ses procédures de contrôle, ne pourra pas détecter la fraude.

Pourtant, le fait de sensibiliser l'ensemble de la population « à risque » de l'entreprise sur les pratiques des fraudeurs et le comportement à adopter constitue le moyen le plus efficace de prévenir ces fraudes.

Ces fraudes risquent de prospérer au même rythme que la facilité de collecter des renseignements publics sur l'entreprise ou ses collaborateurs (en ce comprises des informations relatives à la vie privée) dans la presse, sur Internet, au travers de réseaux sociaux (Facebook, LinkedIn), auprès du Registre du commerce et des sociétés. L'utilisation de plateformes de dématérialisation de numéros de téléphone (apparence de numéros locaux, mais appels depuis l'étranger), l'utilisation de cartes de paiement prépayées en espèces anonymes et non traçables, l'utilisation du mail « to fax » permettant l'envoi de fax à partir d'une boîte e-mail, facilitent là encore ce type de fraude.

Et pourtant, quelques heures de sensibilisation des équipes Conformité, Trésorerie, Comptabilité et Finances suffiraient à alerter les opérationnels sur les dernières formes de cybercriminalité, y compris au sein même des entreprises victimes d'une première tentative et que les fraudeurs n'hésitent manifestement pas à viser de nouveau. ■