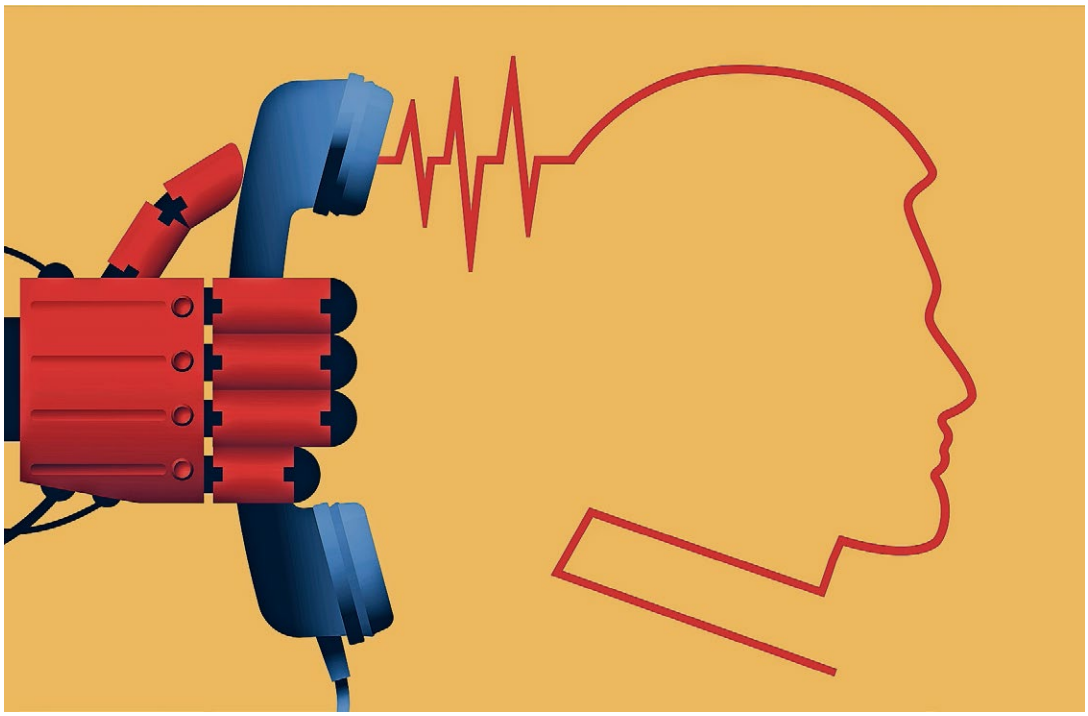
Les arnaques au CEO peuvent faire perdre des millions aux PME

TECHNOLOGIE De nouvelles attaques, dopées à l'IA, ciblent les petites entreprises, alertent les autorités. Une société schwytzoise vient ainsi de perdre plusieurs millions de francs

ANOUCH SEYDTAGHIA



(GETTY IMAGES)

Des e-mails suspects, des SMS douteux, des messages étranges reçus via WhatsApp ou encore des appels téléphoniques bizarres. Chaque jour, nous sommes assaillis de dizaines de tentatives d'arnaques. Des cyberattaques parfois sophistiquées, mais le plus souvent encore basiques et relativement facilement détectables par celles et ceux qui demeurent méfiants. Mais dans le monde des entreprises, la situation est tout autre: appâtés par des possibilités de gains substantiels, les hackers mettent en œuvre des moyens importants pour parvenir à leurs fins.

Les PME, notamment, sont depuis un moment ciblées par des arnaques dites au CEO, ou au président. Le principe est simple: de plusieurs manières, les pirates vont convaincre un employé haut placé dans l'entreprise d'effectuer un virement bancaire à l'étranger. Mais les technologies utilisées sont de plus en plus complexes, et compliquées à déjouer, comme vient d'alerter l'Office fédéral de la cybersécurité (OFSC). Les attaquants «ne se limitent plus à l'envoi de courriels frauduleux, mais recourent désormais de manière ciblée à la manipulation psychologique et à l'intelligence artificielle», avertissent les autorités.

Analyse sur LinkedIn

L'OFSC évoque ainsi une préparation minutieuse de la part des criminels, car ils analysent les réseaux sociaux professionnels comme LinkedIn, les sites internet des entreprises ainsi que le Registre du commerce afin d'identifier les hiérarchies, les responsabilités et les périodes d'absence. Selon les autorités, les pirates «savent précisément quelles personnes de la comptabilité disposent d'un accès aux comptes et quels membres de la direction sont habilités à donner des instructions.»

En général, les agresseurs ciblent un collaborateur du service financier de la PME, se faisant passer pour le directeur. Ils incitent la victime à effectuer un paiement urgent à effectuer en faveur d'un fournisseur étranger. L'OFSC note que les tentatives d'escroquerie ont désormais aussi lieu via WhatsApp ou par téléphone. «Une évolution particulièrement préoccupante est l'utilisation croissante de l'intelligence artificielle (IA). Les criminels s'en servent pour imiter le style rédactionnel du supérieur hiérarchique réel, y compris les formules de salutations ou les expressions habituelles. [...] Les appels audio ou les messages vocaux truqués (deepfake) sont de plus en plus utilisés. La voix du dirigeant ou d'un partenaire commercial est alors reproduite de manière très réaliste grâce à l'IA.»

Les pirates vont donc très loin. En plus, il est arrivé dernièrement que le premier contact passe par de prétendus avocats. «Les escrocs usurpent les noms de cabinets d'avocats existants et établis en Suisse afin d'instaurer un climat de confiance. Le faux supérieur hiérarchique demande alors à la victime si un avocat précis l'a déjà contactée au sujet d'une affaire confidentielle ou d'un mandat urgent. La mention d'un tiers vise à renforcer la crédibilité du scénario et à accroître la pression juridique.»

L'an dernier, le nombre de signalements de telles arnaques a nettement augmenté, passant de 719 en 2024 à 971, selon les statistiques de l'OFSC: et début 2026, une attaque a abouti dans le canton de Schwytz, causant des dégâts majeurs. Plusieurs millions de francs ont été perdus par une entreprise.

Cas majeur à Schwytz

La police cantonale schwytzoise a raconté que les escrocs ont contacté par téléphone le propriétaire de l'entreprise visée, se faisant passer de manière convaincante pour un partenaire commercial de longue date. «Ils ont utilisé une voix modifiée par intelligence artificielle. Grâce à cette supercherie, ils ont gagné la confiance du propriétaire. Sous prétexte d'une transaction commerciale internationale prétendument confidentielle, le propriétaire a été amené à effectuer plusieurs virements d'argent totalisant plusieurs millions de francs suisses», ont expliqué les autorités. Ces virements ont été effectués vers un compte bancaire en Asie, et les chances de récupérer cette somme semblent quasi nulles.

Rappelons qu'en 2024 la police cantonale valaisanne signalait qu'une entreprise du Valais central s'était vu dérober près de 300 000 francs, également via une arnaque au président. Des cas similaires avaient été signalés lors des deux années précédentes dans le canton.

Sur son site, l'OFSC livre plusieurs conseils, dont celui d'une vérification par un second canal: «Si vous recevez une demande de paiement par courriel, en particulier si elle est «urgente» ou «confidentielle», appelez directement l'émetteur. N'utilisez pas le numéro indiqué dans le courriel, mais celui que vous connaissez déjà.»