Fraude au PDG (CEO fraud)

La fraude au PDG est une forme très perfide d'escroquerie qui cible les salariés chargés des paiements. Ces derniers reçoivent en effet de leur supérieur hiérarchique l'ordre de procéder sans délai à un virement sur un compte donné. Le problème est que le véritable expéditeur du message n'est pas le chef ou le PDG d'une entreprise, mais un escroc.

Principaux conseils à suivre pour les salariés :

- En cas d'une prise de contact inhabituelle ou douteuse, ne donnez aucune information et ne suivez aucune instruction, même si vous êtes sous pression.
- Demandez à votre supérieur de confirmer directement les ordres de virement à travers un autre canal de communication (de vive voix ou par téléphone).
- Méfiez-vous dès lors que vous remarquez une incorrection ou l'absence d'un élément de sécurité, comme la signature numérique d'un email (https://www.ebas.ch/fr/signature-de-courriel-outlook/) par exemple.

Principaux conseils à suivre pour les entreprises :

- Sensibilisez vos collaborateurs sur ce type d'escroquerie.
- Vérifiez les informations concernant votre entreprise auxquelles il est possible d'accéder en ligne et limitez-les le cas échéant.
- Définissez et mettez en place une procédure de validation des paiements prévoyant un double contrôle à travers un système de signature collective.
- Informez immédiatement la police de toute tentative d'escroquerie.
- Vérifiez que le personnel utilise bien des éléments de sécurité fiables, tels que les signatures numériques des courriels, lors des processus opérationnels critiques comme les procédures de paiement.

Le bon comportement à adopter de la part des salariés

Si un supérieur vous ordonne par courriel d'effectuer immédiatement un virement imprévu ou non programmé, vous devez faire preuve de la plus grande vigilance. Dans ce genre de situation inhabituelle, il est conseillé de vérifier la légitimité de l'ordre, en contrôlant par exemple les éléments de sécurité présents, tels que la présence ou non de la signature numérique. **Il convient dans tous les cas de solliciter directement votre supérieur hiérarchique (personnellement ou par téléphone) pour lui demander si le paiement en question doit effectivement être effectué ou non.**

Les précautions à prendre côté entreprise

Sensibilisation des salariés

Il existe un certain nombre de mesures techniques qui permettent de limiter - mais non de supprimer complètement - l'envoi de ce type d'emails frauduleux. Les arnaqueurs changent constamment d'adresse et dissimulent ainsi leur identité et leur origine. Il leur arrive aussi parfois de réussir à pirater le véritable compte de messagerie d'un supérieur pour l'utiliser à leurs fins.

La principale mesure à prendre pour se prémunir contre ce danger est donc de sensibiliser les collaborateurs des services les plus exposés à ce type d'attaque, comme par exemple le service comptabilité.

Informations disponibles en ligne
Pour concevoir une fraude au PDG, l'attaquant doit disposer d'un certain nombre de renseignements concernant l'entreprise et ses collaborateurs. Le site web de l'entreprise ou le registre du commerce révèlent déjà suffisamment d'informations utiles. Les escrocs s'intéressent également aux réseaux sociaux (ex. LinkedIn (https://www.ebas.ch/fr/parametres-linkedin/) ou Xing) qui contiennent des informations intéressantes sur les relations commerciales ou l'identité et la fonction des collaborateurs. Vérifiez donc quelles sont les informations concernant votre entreprise et vos collaborateurs accessibles en ligne et limitez-les le cas échéant.

Procédure de validation des paiements
L'arnaque se produit matériellement au moment du virement. En général, le destinataire est un compte bancaire étranger où l'argent ne fera que transiter avant d'être transféré sur un autre compte. Pour éviter que ce genre d'opérations frauduleuses ne se produise, il est recommandé de mettre en place une procédure de validation des paiements prévoyant plusieurs contrôles, l'idéal étant d'appliquer le principe du double contrôle avec la signature collective. On augmente ainsi les probabilités que l'arnaque soit découverte par au moins une des personnes chargées de valider l'ordre de paiement.

Signature numérique des emails
La fraude au PDG intervient au niveau de la procédure de paiement et l'escroc se fait passer pour l'expéditeur légitime de l'ordre de paiement.

La variante la plus simple consiste à falsifier l'adresse email de l'expéditeur. Dans ce cas, la signature numérique, qui ne peut être apposée que par le titulaire du compte de messagerie, apporte une bonne protection. Cette procédure est toutefois relativement lourde à mettre en place et suppose également que la signature soit correctement vérifiée par le destinataire du courriel.

La situation est plus problématique lorsque le compte de messagerie de l'expéditeur est piraté, suite par exemple à une attaque de phishing. Dans ce cas, la signature numérique du compte peut être également piratée et utilisée à l'insu du titulaire du compte. Une procédure stricte de validation des paiements et la sensibilisation de toutes les personnes susceptibles de se trouver confrontées à ce type de situation s'avèrent donc très utiles pour lutter contre ce type d'attaque.

La fraude au PDG ou fraude au Président (de l'anglais « CEO fraud », CEO signifiant Chief Executive Officer) consiste à se faire passer pour le PDG d'une entreprise et à ordonner aux collaborateurs autorisés à effectuer des opérations bancaires de procéder à des virements bancaires de sommes importantes.