Conseils et pratiques pour pallier aux attaques du type « aux faux ordre de virement » ou « au président »

01 Prendre des mesures d'ordre technique

Du point de vue technologique, une solution à plusieurs niveaux peut contribuer à réduire considérablement le risque que l'email de ce type d'attaque arrive à destination. L'ensemble des contenus et métadonnées des messages doivent faire l'objet d'une authentification.

02 Vérifier l'adresse "Répondre à

Bien que chaque logiciel client de messagerie soit différent et qu'il ne soit pas toujours facile de visualiser le champ "Répondre à", il suffit de cliquer sur Répondre et de vérifier l'adresse qui s'affiche alors. S'agit-il d'une adresse interne authentique, extérieure à l'entreprise ou bien inhabituelle ?

03 Vérifier le nom de domaine

Les attaques emploient de plus en plus le "typosquatting", c'est-à-dire un nom de domaine orthographiquement proche de celui de l'entreprise afin de leurrer les destinataires assez prudents pour vérifier l'adresse "Répondre à". Toute opération sensible (telle qu'un virement) mérite d'y regarder à deux fois pour s'assurer que le nom de domaine est le bon.

04 Respecter et renforcer les procédures

Mettre en place des dispositifs de contrôle appropriés pour les types de transactions ciblées par ce type d'attaque, notamment des vérifications internes au sein des services financiers et achats, afin d'authentifier les demandes légitimes. Il peut s'agir par exemple d'exiger l'autorisation en personne ou par téléphone d'un autre responsable au sein de l'entreprise.

05 Prendre garde à l'utilisation de comptes personnels

Dans certains cas, les attaques peuvent également sembler provenir d'un compte e-mail personnel de sorte que l'adresse "Répondre à" paraisse moins suspecte. Par exemple, une adresse telle que [nom_du_pdg]_personnel@gmail.com échappera souvent aux filtres antispam et aura l'air plus authentique. L'utilisation de comptes personnels doit non seulement être proscrite par les règles de sécurité mais aussi constituer un signal d'alerte pour les destinataires.