Ingénierie sociale: (nouvelle méthode d’attaque ciblant les entreprises)

23.01.2017

D'un coup d'oeil

Ces derniers jours, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de la Confédération a été informée de plusieurs cas dans lesquels des escrocs se font passer pour des employés d’une banque et appellent des entreprises. Ils annoncent alors qu’une prétendue mise à jour concernant l'e-banking devra être effectuée au cours d’un deuxième appel, qui aura lieu le lendemain. Ils requièrent la présence de plusieurs collaborateurs du service des finances lors de ce deuxième appel. L’objectif des escrocs est de s’assurer de la présence des personnes nécessaires afin de transmettre un paiement en signature collective.

Ces derniers jours de nombreuses entreprises ont reçu des appels lors desquels des escrocs tentent de se faire passer pour leur banque. Dans de nombreux cas, les criminels peuvent identifier la banque de l'entreprise grâce aux informations accessibles publiquement sur le site web de cette dernière. Cette information peut aussi être parfois obtenue par un appel téléphonique ou une demande d'information via courriel à l'entreprise.

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) de la Confédération a publié une newsletter sur cette question.

Pour prévenir ce type d’attaque, MELANI recommande les mesures suivantes:

- Il est important de sensibiliser les collaborateurs quant à l’existence de ce type d’attaques, tout particulièrement les collaborateurs dans des positions clés.
- Tous les processus relatifs à des virements devraient être clairement définis à l’interne et appliqués de manière rigoureuse par tous les employés, en toute situation. Les établissements financiers ne vous demanderont jamais de leur transmettre vos données d’accès que ce soit par écrit ou par oral.
- Aucune banque sérieuse ne vous demandera de collaborer à des tests liés à des mises à jour de sécurité. Les banques et leurs fournisseurs IT disposent d’environnements d’évaluation pour tester les mises à jour de sécurité avant de les mettre à disposition de leur clientèle.
- N’installez jamais de logiciels lorsque l’on vous le demande de manière téléphonique ou par courriel.
- N’autorisez jamais un accès à distance à votre système informatique.
- Réduisez l’information que vous publiez sur votre entreprise sur internet au minimum nécessaire. Évitez si possible de nommer vos collaborateurs ainsi que de donner des informations sur vos relations bancaires.
- Lors de prises de contact suspectes ou inhabituelles, évitez de divulguer des informations internes à l’entreprise.
- Il est fortement recommandé de vérifier à l'interne la légitimité d'une demande ou d'une prise de contact, lorsque celle-ci paraît douteuse ou inhabituelle.
- Si vous êtes victime d'une fraude, signalez-le à l’Office fédéral de la police (Fedpol) via le formulaire d’annonce et déposez plainte auprès de votre police cantonale.

Pour la sécurité informatique des PME, MELANI a publié un aide-mémoire spécifique.