Courriels malveillants: liste de contrôle destinée aux parlementaires

Les institutions politiques et les parlementaires sont aujourd'hui des cibles privilégiées d'attaques informatiques. Les cas récents ayant par exemple touché le Comité national démocrate américain ou le Bundestag allemand témoignent de cette tendance. Bien souvent, les attaquants obtiennent l'accès à des systèmes grâce à des courriels malveillants, enjoignant la cible à transmettre des informations sensibles, suivre un lien ou ouvrir une pièce jointe contenant un maliciel (virus). Il est possible de se prémunir dans une large mesure contre ce type d'attaque en suivant quelques règles simples.

1. Apprendre à reconnaître le phishing et les autres courriels malveillants

Dans un premier cas de figure, les pirates utilisent une méthode appelée phishing pour pousser l'utilisateur à communiquer des données confidentielles (p. ex. les données d'accès à son compte e-mail ou d'autres services en ligne). Un courriel peut par exemple lui annoncer que ses informations ne sont plus sûres ou plus actuelles et qu'elles doivent être modifiées ou confirmées en suivant un lien. Ce dernier ne mène cependant pas à la page du fournisseur e-mail ou du réseau social, mais à une page Internet identique créée par le pirate, sur laquelle les données d'accès seront saisies.

Une deuxième méthode utilisée est l'envoi d'un courriel contenant un lien ou une pièce jointe ayant comme finalité d'installer un maliciel sur la machine de l'utilisateur. Les attaquants ont recours à de nombreux subterfuges pour tromper l'utilisateur et lui faire croire que le courriel est légitime. L'adresse expéditeur est falsifiée et un scénario plausible est présenté, pour inciter la cible à suivre un lien ou ouvrir une pièce jointe.

2. Comprendre les risques

Si l'utilisateur lui a communiqué ses données d'accès suite à une attaque de phishing, le pirate peut accéder à l'intégralité du compte. Il peut en télécharger les données, mais aussi envoyer des courriels piégés aux contacts de la victime en se cachant derrière l'identité de cette dernière. Si l'attaquant a réussi à installer un maliciel, il aura potentiellement un accès encore plus large et pourra utiliser la machine de l'utilisateur à distance, accéder à tous ses comptes et consulter toutes ses données.

3. Se protéger contre les courriels malveillants

Il convient d'adopter une attitude de saine méfiance avec les courriels en général. Il vaut mieux ne pas donner suite à un courriel, à moins d'être absolument certain que son contenu et son expéditeur sont légitimes. Si le doute persiste, il est parfois possible de procéder à des éclaircissements à travers un autre canal (p. ex. par téléphone). Plus spécifiquement MELANI conseille de :

- Se méfier des courriels inattendus, surtout s'ils demandent de suivre un lien ou d'ouvrir un document.
- Ne jamais ouvrir les pièces jointes ou les liens figurant dans un courriel suspect et ne pas divulguer d'informations sensibles (p. ex. mot de passe).
- Activer l'authentification multi-facteurs pour vos comptes en ligne.
- Utiliser un mot de passe différent pour chaque compte.

4. Limiter les dommages

D'une manière générale:

- Les communications concernant l'activité professionnelle ne devraient pas avoir lieu sur des comptes e-mail privés.
- Les communications sensibles devraient être protégées par chiffrement (« cryptées »).

Si vous pensez avoir été victime d'un courriel malveillant, il est recommandé de :

- Modifier le mot de passe des services en ligne auxquels le pirate pourrait avoir accédé.
- Réinstaller le système d'exploitation et changer tous les mots de passe en cas de suspicion d'infection.

De nombreuses autres informations figurent sur le site Internet de MELANI: www.melani.admin.ch.

Annoncer tout message suspect à la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), à l'adresse reply@melani.admin.ch.

MELANI