Usage des mots de passe

Règles de bon usage d'un mot de passe

Suite à la publication, ces dernières semaines, de plusieurs millions de condensats de mots de passe exfiltrés de divers réseaux sociaux, le CERTA rappelle que des bonnes pratiques sont disponibles dans le document intitulé Recommmandations de sécurité relatives aux mots de passe (DAT-NT-001/ANSSI/SDE), sur le site Internet de l'ANSSI (section documentation). Elles comprennent notamment : * la nécessité de *différencier les mots de passe utilisés sur des systèmes d'information professionnels et des sites web publics* (messagerie, réseaux sociaux, vente en ligne) ; * le besoin d' *utiliser un mot de passe complexe*, voire non rejouable (one time password) ; * le besoin de *renouveler ces mots de passe avec une fréquence raisonnable* ; * *ne pas configurer les logiciels pour se souvenir des mots de passe sensibles*. Le document présente également des méthodes d'attaque sur mots de passe dictant ces recommandations. Enfin, il est rappelé aux autorités administratives que l'annexe B3 du référentiel général de sécurité (RGS) fixe l'ensemble des règles techniques à respecter en matière d'authentification.

Documentation : – Recommandations de sécurité relatives aux mots de passe : http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

Source : Bulletin CERTA du 8 juin 2012

Vigilance sur le vol de mot de passe (hameçonnage ou phishing)

On nous signale une tentative de phishing via le message malveillant ci-dessous.

L'émetteur se fait passer pour l'assistance CNRS et demande de cliquer sur un lien qui amène à un site qui cherche à voler le mot de passe de l'utilisateur.

Il ne faut en aucun cas répondre à ce message ou cliquer sur le lien contenu dans le message.

Merci de transmettre cette alerte à l'ensemble de vos utilisateurs en leur rappelant les règles élémentaires de sécurité concernant les messages provenant d'internet (règle N°5) : « 5- Attitude prudente vis à vis des messages reçus Nous sommes toujours tentés de savoir qui nous écrit, cependant de nombreux escrocs et pirates utilisent notre curiosité et notre crédulité pour tenter de voler nos données. Dans certains cas le message frauduleux demande le changement du mot de passe d'un compte et redirige l'utilisateur vers un site pirate qui va voler ce mot de passe (c'est le « phishing ») pour utiliser le compte de l'utilisateur à son insu et ainsi pénétrer dans sa messagerie, son compte bancaire, etc.»

<pre> ——————————————— message malveillant ——————————————————————————–

Début du message transféré :

Expéditeur: CNRS bma@stmarys-ca.edu Date: 25 août 2012 17:18:15 HAEC Destinataire: undisclosed-recipients:; Objet: avis Important

Conseils CNRS Web du centre-mail à tous les utilisateurs de compte de messagerie à s'il vous plaît répondre à ce courrier.

Nous sommes en train d'améliorer notre base de données et le centre compte e-mail. Nous sommes la suppression de comptes qui ne sont pas en cours d'utilisation pour créer plus de l'espace pour les nouveaux comptes. Pour éviter que votre compte ne doit pas être tronqué, nous vous conseillons de cliquer ou copier le lien ci-dessous et de bien vouloir remplir le l'information requise;

Cliquez ici: lien sur le site malveillant

Nous sommes sincèrement nos excuses pour ce désagrément. Cordialement, IT Service!
Administrateur Système ® Mettez à niveau votre compte?

———————————— fin du message malveillant ————————————————————————-
</pre>

Source : DSI - CNRS le 27 août 2012

Quelques exemples de phishing récents