Fiche des bonnes pratiques en cybersécurité

L'agence nationale de sécurité des systèmes d'information (ANSSI) communique le message suivant : « L'actualité récente a entraîné un accroissement significatif du nombre d'attaques informatiques visant des sites internet français. La très grande majorité de ces attaques sont des défigurations de sites Internet, d'effacement ou des dénis de service. L'ANSSI rappelle qu'il est possible de se prémunir de ces types d'attaques en appliquant les bonnes pratiques indiquées ci-dessous. De plus l'application des recommandations du guide d'hygiène informatique de la note sur la sécurisation des sites web (accessibles sur le site www.ssi.gouv.fr) est fortement recommandée.

Que faire pour se prémunir d'une cyberattaque ?

Utiliser des mots de passe robustes

C'est-à-dire choisir des mots de passe de 12 caractères minimum mais sans lien avec votre nom, votre date de naissance, etc.... Le même mot de passe ne doit pas être utilisé pour des accès différents.
En règle générale, ne pas configurer les logiciels pour qu'ils retiennent les mots de passe et éviter de stocker ses mots de passe dans un fichier ou lieu proche de l'ordinateur si celui-ci est accessible par d'autres personnes.

Ajouter ou modifier sur les sites Internet et les réseaux sociaux

Toute mise à jour de contenu doit être effectuée exclusivement depuis un poste informatique maîtrisé par votre service informatique et dédié à cette activité. Elle ne doit en aucun cas s'effectuer à distance depuis le domicile ou un smartphone.
Les connexions doivent être réalisées uniquement à partir d'un réseau maîtrisé et de confiance. Il est important de ne pas utiliser de réseau WI-FI ouvert ou non maîtrisé afin d'éviter tout risque d'interception.
Il est important de vérifier que le site visité est légitime et possède une connexion sécurisée (HTTPS).

Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, etc...

La plupart des attaques utilisent les failles d'un ordinateur. En général, les attaquants recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous les logiciels afin de corriger ces failles. Pour effectuer ce type de démarche, prendre contact avec le responsable de votre système informatique.

Réaliser une surveillance du compte ou des publications.

Il convient de vérifier régulièrement les éléments publiés et prévoir une sauvegarde. En cas de suppression, il est possible de restaurer rapidement l'état préalable à l'attaque après avoir pris les mesures de réaction nécessaires.

Attention, les courriels et leurs pièces jointes jouent souvent un rôle dans les cyberattaques (courriels frauduleux, pièces jointes piégées, etc...)

Que faire en cas de cyberattaque ?

Il est recommandé de préserver les traces liées à l'activité du compte, notamment si un dépôt de plainte est envisagé.
Prendre immédiatement contact avec vos responsables informatiques. S'ils ne sont pas joignables ou si vous n'en n'avez pas, prendre contact avec le Centre Opérationnel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Point de contact (7/7, 24h/24)
Messageries Internet : cossi@ssi.gouv.fr
Téléphone : 01.71.75.84.68
Télécopie : 01.84.82.40.70

Indépendamment des recommandations données ci-dessus, il vous est conseillé de consulter :

Le guide de sécurisation des sites web :
http://www.ssi.gouv.fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-des-applications-web/recommandations-pour-la-securisation-des-sites-web.html

Et en cas d'attaque, il convient de se reporter à la note d'information sur les défigurations de sites web

http://www.cert.ssi.gouv.fr/site/CERTA-2012-INF-002/index.html

Ernest CANDELA