Agence Nationale de la Sécurité des Systèmes d'Information

Fiche des bonnes pratiques en cybersécurité

Date de création : 13/01/2015

1. Que faire pour se prémunir des cyberattaques ?

a. Utiliser des mots de passe robustes

Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.

Pour cela :

- Choisir des mots de passe de 12 caractères minimum
- Utiliser des caractères de type différent (majuscules, minuscules, chiffres, caractères spéciaux)
- Ne pas utiliser de mot de passe ayant un lien avec soi (noms, dates de naissance,…)
- 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
- 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
- Renforcer les éléments permettant de recouvrir les mots de passe d'un compte en ligne (question secrète, adresse de secours). Dans la plupart des cas, une adresse de messagerie ou un numéro de téléphone est nécessaire pour recouvrir un compte : il convient de renforcer l'accès à ces éléments

b. Ajouter ou modifier du contenu 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 (DSI) et dédié à cette activité. Elle ne doit en aucun cas s'effectuer à distance depuis le domicile, une tablette 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).

c. 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 la DSI.

d. 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 central dans les cyberattaques (courriels frauduleux, pièces jointes piégées, etc.).
Lors de la réception de ce type de courriels, prendre les précautions suivantes :

- Vérifier la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail
- Ne pas ouvrir les pièces jointes provenant de destinataires inconnus
- Si des liens figurent dans un courriel, passer la souris dessus avant de cliquer. L'adresse complète du site s'affichera dans la barre d'état du navigateur située en bas à gauche de la fenêtre (à condition de l'avoir préalablement activée)
- Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles

2. 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 les responsables informatiques (DSI, FSSI). S'ils ne sont pas joignables, prendre contact avec le Centre Opérationnel de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Point de contact H24 (7j/7, 24h/24) :
Messageries Internet : cossi@ssi.gouv.fr
Téléphone : +33 (0)1 71 75 84 68
Télécopie : +33 (0)1 84 82 40 70