Vigi@net

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'ÉDUCATION NATIONALE,
DE L'ENSEIGNEMENT SUPÉRIEUR ET
ET DE LA RECHERCHE

Vigilance pour internet et les systèmes d'information

La lettre SSI du Haut Fonctionnaire de Défense et de sécurité **Août 2015**

Responsable de la Publication :
Frédéric Guin

Comité de rédaction :
Frédéric Morinière
Josiane Guilhot-Mahler
Benoît Moreau

Contacts :
hfds@education.gouv.fr
hfds@recherche.gouv.fr

Retrouvez vigi@net sur le portail du ministère :
https://www.pleiade.education.fr
(nécessite une authentification)

Pour recevoir Vigi@net régulièrement :
Abonnement

Pour ne plus recevoir Vigi@net :
Désabonnement

Une recrudescence de courriels véhiculant des logiciels malveillants a été constatée depuis plusieurs semaines. Ce bulletin de rentrée est l'occasion de rappeler l'importance de se montrer extrêmement prudent avec les messageries électroniques, particulièrement avec les messages « inattendus ». Il reviendra sur trois catégories de bonnes pratiques informatiques avant de parcourir l'actualité récente.

De bonnes pratiques individuelles en sécurité informatique

Cet article rappelle trois niveaux de vigilance sans rentrer dans le détail des mesures disponibles notamment sur le site de l'ANSSI (guide) qui peuvent être décrits par une analogie avec la sécurité routière.

Chaque conducteur doit veiller à : avoir une voiture entretenue et sûre, être prudent au volant, et dans certains cas, comme pour les ambulanciers, adopter une conduite vigilante tenant compte de l'état des passagers.

Il en va de même pour la cyber sécurité, chacun doit veiller à : avoir un ordinateur entretenu et à jour, avoir un comportement raisonnable et dans certains contextes sensibles, être encore plus vigilant.

1. Entretenir régulièrement son ordinateur et le protéger à chaque instant :

Utiliser un système à jour, activer le verrouillage automatique et n'utiliser le compte administrateur qu'au besoin.

Sécuriser physiquement les ordinateurs et ne pas les laisser sans surveillance, notamment dans les transports.

2. Avoir un cyber comportement raisonnable et conscient :

Utiliser des mots de passe robustes, variés et ne pas les partager, même avec les administrateurs.

Ne pas réagir trop vite aux messages, se méfier des offres trop alléchantes et n'ouvrir que les pièces jointes semblant légitimes. Utiliser une messagerie adaptée aux échanges (professionnelle ou personnelle) et ne jamais faire suivre les canulars.

Naviguer sur Internet avec prudence, éviter les sites peu connus ou douteux. Contrôler la diffusion d'informations, car tout ce qui apparait sur Internet y perdure longtemps.

Effectuer des sauvegardes régulières sur les réseaux locaux et sur des supports amovibles, et vérifier la restauration des informations. Signaler les incidents et les dysfonctionnements

3. Adapter sa vigilance lors de la manipulation d'informations sensibles (données personnelles, identifiants bancaires, documents confidentiels …) :

Maitriser et chiffrer ses données sensibles, par exemple avec un outil tel que Zed! (qualifié par l'ANSSI), localement et pour les échanges par mail ou sur supports amovibles.

Utiliser avec prudence les copieurs partagés. Effacer les fichiers sensibles à l'aide d'outils qualifiés par l'ANSSI.

Cette rentrée est l'occasion de s'interroger sur ces trois points et en cas de doute sur les réponses , de contacter le service compétent.

L'importance stratégique de la maitrise des communications

L'enjeu stratégique de la maitrise des communications a été démontré à de multiples reprises, notamment lors de l 'épisode historique de « la machine Enigma ». Elle reste une priorité pour tous les états qui essayent de la mettre en place en tenant compte des droits individuels.

La loi relative au renseignement a été promulguée au Journal officiel après la déclaration de conformité prononcée par le Conseil constitutionnel. Cette loi porte notamment sur les dispositif d'analyse automatique des données que devront installer les fournisseurs d'accès à internet (FAI) afin de surveiller le trafic et de détecter des comportements suspects. (www.legifrance.gouv.fr 24/07/2015)

L'existence du programme ECHELON mis en place par les « Five Eyes *» est confirmée. Le programme d'espionnage des communications par satellite était supposé depuis près de trente ans. Son existence a été confirmée par le journaliste Duncan CAMPBELL après l'étude des documents publiés par Edward SNOWDEN. (The Register du 3/08/2015) * alliance des services de renseignement de l'Australie, du Canada, de la Nouvelle-Zélande, du Royaume-Uni et des États-Unis.

La problématique de la confiance dans les tiers

La question du niveau de confiance accordée à un tiers reste compliquée et ne doit pas être éludée, que cela concerne des informations personnelles, des contrats ou des responsabilités opérationnelles.

La liste des inscrits à un site de rencontres extraconjugales a été publiée par des hackers. Le site *Ashley Madison* qui mettait en avant la confidentialité des services offerts s'est fait pirater. Les données personnelles des inscrits ont été divulguées, parmi lesquelles des adresses, des numéros de téléphone ou des préférences sexuelles. La CNIL avait publié en juillet des recommandations pour la fréquentation des sites de rencontre après avoir constaté d'importantes fragilités dans la gestion des données personnelles. Elle préconisait notamment l'utilisation de pseudonymes et la désactivation de la géolocalisation. (lemonde.fr 19/08/2015 , CNIL 28/07/2015) *Plus généralement, il ne faut en aucun cas utiliser une adresse professionnelle pour se connecter à des services personnels.*

Une société de piratage piratée : la société *Hacking Team* qui offrait des services et des outils de piratage a été elle même victime d'une intrusion informatique. L'attaquant a ensuite révélé la liste des clients et les détails des outils vendus qui semblaient d'ailleurs contenir une porte dérobée. Cette société avait par ailleurs connaissance de plusieurs vulnérabilités non corrigées qui ont été réutilisées après leur publication par d'autres groupuscules. (arstechnica.com 14/07/2015) *Il convient de toujours s'assurer de la fiabilité des partenaires, même s'il s'agit d'une société « experte en SSI ». Pour cela l'ANSSI propose un guide.*

La sécurité des technologies récentes

Ce n'est pas parce que « c'est» récent que c'est mieux sécurisé.

Une voiture piratée en conditions réelles : deux chercheurs ont pu prendre le contrôle à distance d'une Jeep Cherokee après s'être introduits dans l'ordinateur de bord qui pilote toutes les fonctions du véhicule et qui est relié en permanence à Internet par une connexion cellulaire. (www.wired.com 21/07/2015) *Comme tout ordinateur, celui de bord doit être mis à jour. (cf. Point 1 du premier article)*

Les téléphones Android sont piratables à distance à l'aide d'un MMS spécialement conçu. Un correctif existe mais il devra être adapté par chaque constructeur et de nombreux terminaux n'étant plus maintenus, ils ne recevront pas de correctifs. (lemonde.fr 29/07/2015, ANSSI 28/07/2015) *En cas de doute, l'ANSSI recommande la désactivation des MMS.*

Un nouveau type d'attaque cible les espaces de stockage en nuage. Un code malveillant installé sur les postes des victimes reconfigure les fonctionnalités de synchronisation automatique pour envoyer les documents vers un autre espace de stockage sous maitrise de l'attaquant. Or de plus en plus d'utilisateurs souhaitent accéder à leurs documents les plus importants (professionnels ou personnels) en tout temps et en tout lieux, et ont tendance à les enregistrer dans ce type de service qui devient naturellement une cible privilégiée pour les attaquants. (www.darkreading.com 05/08/2015). *Il faut être particulièrement vigilant avec les informations sensibles et vérifier qu'elles sont sauvegardées au bon endroit et dans la bonne version. (cf. Point 3 du premier article)*

Windows 10 disponible depuis peu est « gourmand » en données personnelles. Il enregistre par défaut des données d'identification telles que la localisation ou l'historique de navigation et, en fonction de la configuration, peut également transmettre les contacts, les centres d'intérêt ou la vitesse de frappe. (www.wired.com 05/08/2015). *Il est recommandé de n'activer que les fonctionnalités nécessaires.*