PROCESS EN CAS D'INCIDENT

Vous n'avez pas eu le temps de mettre en œuvre les règles décrites dans ce guide ou les attaquants ont réussi à les contourner. ***Ne cédez pas à la panique, et ayez les bons réflexes.***

• **En cas de comportement inhabituel de votre ordinateur**, vous pouvez soupçonner une intrusion (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation…)

• **Déconnectez la machine du réseau / désactivez le Wi-Fi**, pour stopper l'attaque. En revanche, maintenez là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque

• **Prévenez votre service informatique**, au téléphone ou de vive voix, car l'intrus peut être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque

• **Faites faire une copie physique du disque**

• **Faites rechercher les traces disponibles liées à la compromission**. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.)

• **Déposez une plainte** auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société, de la Brigade d'enquêtes sur les fraudes aux technologies de l'information (Paris et petite couronne), ou de la Direction générale de la sécurité intérieure.

• **Après l'incident : réinstallez complètement le système d'exploitation** à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information

A noter **:** En cas d'infection, le support informatique sera obligé de reformater le contenu de votre disque dur. Cette opération pourrait entraîner une perte irréversible de vos données dans le cas où vous n'auriez pas sauvegardé vos données.

Source ANSSI : www.ssi.gouv.fr/en-cas-dincident/

Réalisé par ATIXNET
2 bis avenue Foch 94160 Saint-Mandé - TEL. 01 84 23 00 60 – www.atixnet.fr