AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

Annexe 2 – Fiche réflexe en cas d'incident de sécurité informatique

Statut : validé | Classification : publique | Version : V2.0 – 17/11/2021

Mémento de sécurité informatique pour les professionnels de santé en exercice libéral

Annexe 2 - Fiche réflexe en cas d'incident de sécurité informatique

Des incidents de nature malveillante peuvent survenir sur les équipements informatiques : poste et/ou serveur bloqué par un « cryptovirus » qui affiche une demande de rançon, présence d'un programme inconnu qui se lance au démarrage ou à l'utilisation de l'équipement, communications anormales vers Internet détectées par le pare-feu…
Si un incident de sécurité informatique est constaté ou suspecté sur un équipement, il est recommandé d'appliquer en premier lieu les mesures suivantes :

1 ⚠ **Déconnecter** d'abord **du réseau** la machine sur laquelle l'incident est suspecté (déconnexion du câble réseau ou désactivation du wifi). S'il s'agit d'une intrusion, l'attaquant connecté à distance perdra alors l'accès à la machine compromise. D'autre part, si la machine fait partie d'un réseau et si elle a été infectée par un logiciel malveillant, celui-ci ne sera pas en mesure de se propager à d'autres machines du réseau.

⚠ **Maintenir** en revanche **la machine sous tension**, ne pas l'arrêter ni la redémarrer et ne plus interagir avec la machine afin de conserver l'information utile pour l'analyse de l'attaque potentielle.

2 **Prévenir l'équipe informatique** ou le fournisseur de service informatique en charge du suivi de la machine et leur demander de l'assistance pour le diagnostic. S'il n'existe ni équipe technique ni contrat avec un fournisseur de service informatique, il est recommandé de faire appel à un professionnel de l'informatique.

3 **Décrire l'incident de sécurité** sur le site cybermalveillance.gouv.fr et suivre les conseils proposés. Un outil de diagnostic et d'assistance en ligne est disponible à cet emplacement :

https://www.cybermalveillance.gouv.fr/diagnostic/accueil

Cas spécifiques :

- **Si l'incident constitue une violation de données à caractère personnel**[1], susceptible d'engendrer un risque pour les droits et libertés des personnes concernées par les données, une notification auprès de l'autorité compétente ainsi que, dans certains cas, une information des personnes concernées, doivent être réalisées dans les délais impartis. Des informations sont disponibles sur le site internet de la CNIL à ce sujet :

  www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles

- **Si l'incident s'avère être la conséquence d'une malveillance**, il est important de le déclarer auprès des services de police ou de gendarmerie, d'autant plus en cas de vol de matériel informatique ayant hébergé des données de santé à caractère personnel ou d'accès illicite à des données de santé.
  Le site cybermalveillance.gouv.fr déjà mentionné plus haut indique les contacts utiles dans ce cadre :

  https://www.cybermalveillance.gouv.fr/diagnostic/accueil

- **La réception de spam** (ou courriers indésirables) peut être déclarée sur le site internet suivant :

  www.signal-spam.fr

- Il est conseillé de conserver un exemplaire imprimé de cette fiche à un endroit dont vous vous souviendrez facilement, au cas où votre poste de travail ne serait pas accessible du fait de l'incident subit.

[1] Violation de données à caractère personnel : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données (article 4.12 du Règlement Général sur la Protection des Données n°2016/679 du 27 avril 2016).