Sécurité numérique en santé

TOUS CYBER VIGILANTS EN PAYS DE LA LOIRE

MÉMO

DÉPÔT DE PLAINTE SUITE A UN INCIDENT SI D'ORIGINE MALVEILLANTE

Rédigé en partenariat avec : Gendarmerie nationale

RÉPUBLIQUE FRANÇAISE

ars Agence Régionale de Santé Pays de la Loire

e-santé Pays de la Loire

Pays de la Loire

Sécurité numérique en santé

MÉMO – Dépôt de plainte suite à un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

POURQUOI DÉPOSER PLAINTE ?

- ✓ Être reconnu en tant que victime et ainsi faire valoir vos droits via l'ouverture d'une enquête pénale ;
- ✓ Être accompagné dans une situation complexe par des professionnels habilités et aguerris (expertise cyber, …)
- ✓ Permettre le cas échéant, selon vos contrats d'assurance*, le déclenchement du processus de prise en charge de tout ou d'une partie des coûts financiers résultant de l'incident, à condition que la plainte soit déposée dans les 72h comme stipulé dans la Loi du 24/01/23 d'Orientation et de Programmation du ministère de l'Intérieur (LOPMI) ;
- ✓ Bénéficier des résultats de l'enquête (identité de l'auteur des faits, indemnisation, récupération des données (le cas échéant), déchiffrement, …) ;
- ✓ Participer à la lutte contre la cybercriminalité en fournissant aux forces de l'ordre des informations précieuses permettant d'en apprendre davantage sur les méthodes des cybercriminels et permettre de leur arrestation potentielle.
- ✓ Limiter le risque d'engagement de votre responsabilité en cas d'utilisation non souhaitée de votre système d'information pour mener des attaques à l'encontre de tiers (partenaires, fournisseurs, usagers, …).

À noter qu'en aucun cas, un dépôt de plainte ne se substitue à la **déclaration sur le portail de signalement des évènements sanitaires indésirables** (https://signalement.social-sante.gouv.fr/#/accueil), qui est **OBLIGATOIRE pour tous les établissements de santé** (sanitaires et médico-sociaux) et une **déclaration à la CNIL** (dans les 72H) en cas de violation de données à caractère personnel.

COMMENT DÉPOSER PLAINTE ?

1. Etape 1 :

La structure victime d'un acte malveillant sur son système d'information réalise une analyse de la situation afin de caractériser les faits autant que possible (*Cf. § Questions / informations pour l'analyse de la situation*).

2. Etape 2 :

À la suite de cette première analyse, le représentant légal de la structure peut aller déposer plainte :

- Soit, en **se déplaçant physiquement dans un commissariat de police ou une brigade de gendarmerie** ;
- Soit, sur le **site internet** : https://www.pre-plainte-en-ligne.gouv.fr/ ;
- Soit, **en transmettant un courrier papier au procureur de la République** de la ville de l'établissement.

*Le dépôt de plainte doit intervenir **avant la réinstallation des appareils touchés**, de manière à conserver et collecter les preuves techniques de l'incident afin de les fournir aux enquêteurs. Cf. Fiche mémo – « Collecte des traces suite à une cyberattaque ».*

ABSENCE REPRÉSENTANT LÉGAL

Dans le cas où le représentant légal de la structure ne peut se déplacer lui-même pour effectuer le dépôt de plainte, il lui est possible d'envoyer une autre personne de la structure ayant en sa possession :

- Une **copie de la pièce d'identité du représentant légal**,
- Un **avis de situation SIRENE,**
- Un **mandat daté et signé** par le représentant légal de la structure.

*ZOOM ASSURANCE « CYBER »

Les contrats d'assurance « cyber » sont constitués d'un ensemble de garanties ciblant principalement en tant que causes, les actes malveillants, et certaines erreurs, ayant pour conséquence des compromissions de données et des perturbations d'activité.

En réponse à l'émergence de risques récents, elles apportent donc une couverture de frais de gestion et dommages immatériels, aux Tiers ou aux Assurés, venant ainsi compléter respectivement les offres assurantielles en « Responsabilité Civile » et « Dommages aux Biens » qui ciblent historiquement d'autres types de sinistres.

A noter que leur contractualisation demande en prérequis la mise en œuvre d'un niveau minimal de sécurité informatique.

Gendarmerie nationale
RÉPUBLIQUE FRANÇAISE
ars Agence Régionale de Santé Pays de la Loire
e-santé Pays de la Loire
Pays de la Loire

Sécurité numérique en santé

MÉMO – Dépôt de plainte suite à un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

PRÉPARER MON DÉPÔT DE PLAINTE

Afin de préparer au mieux votre dépôt de plainte et faciliter les investigations des forces de l'ordre, il est recommandé de :

- **Préserver toutes les traces** (données, état de la mémoire, journaux (logs), prendre des photos ou faire des captures d'écran, …, de tout ce qui est visible). Ces traces peuvent constituer des preuves à valeur juridique en cas de procédures ultérieures. *Cf. Fiche mémo – « Collecte des traces suite à une cyberattaque ».*
- **Ecrire toutes les actions entreprises** par **ordre chronologique** pour relater le plus précisément possible la situation en cours et son évolution (mise en œuvre d'une main courante par exemple).
- Apporter lors du dépôt de plainte ou mettre à disposition des enquêteurs **tout élément pouvant s'avérer utile pour les investigations** (clé USB, fichiers, photos, disques durs, documents initiés, etc.).

A noter : si le dépôt de plainte a lieu dans le temps de l'attaque, ces actions pourront être réalisées **avec l'appui** des forces de l'ordre.

La brigade numérique de la Gendarmerie nationale peut vous apporter une assistance en ligne 24h/24 dans vos démarches : https://www.gendarmerie.interieur.gouv.fr/contact/discuter-avec-un-gendarme?service=piratage

QUESTIONS / INFORMATIONS POUR L'ANALYSE DE LA SITUATION

Pour vous aider, vous trouverez ci-dessous une liste non exhaustive d'informations utiles à recueillir et à transmettre aux forces de l'ordre pour leurs investigations.

- 1/ Concernant le type d'appareil compromis :
  - Quel type d'équipement a été compromis ? S'agissait-il d'un ordinateur de bureau, d'un ordinateur portable, d'une tablette ou d'un smartphone, d'un serveur virtuel ou physique ?
  - Sous quel système d'exploitation fonctionnait l'équipement impacté et de quelle version s'agissait-il ?
  - S'agissait-il d'un équipement professionnel ou privé ?
  - Votre système contenait-il des données personnelles ou sensibles (ex : données de santé) ?
  - Etiez-vous protégé par un antivirus et, si oui, lequel ?
- 2/ En cas d'infection par un virus :
  - Combien de personnes ont utilisé l'équipement en question ?
  - Un professionnel de la structure a-t-il reçu un courriel contenant une pièce jointe dont l'ouverture est susceptible d'être à l'origine de la compromission de l'ordinateur / SI ? Si oui, l'adresse expéditrice a-t-elle été relevée ? En quelle langue était rédigée le message ? Le courriel reçu a-t-il été conservé ?
  - Un fichier a-t-il été téléchargé ? Et, si oui, lequel (nom, extension et si possible source) ? Disposez-vous d'une copie du fichier ?
  - Un site Internet a-t-il été visité en particulier ? Si oui, de quel site s'agissait-il ?
  - A quelle heure a été reçu le mail, ou à quelle heure a été téléchargé le fichier ?
  - La messagerie est-elle toujours accessible à partir d'un client messagerie (Outlook, Thunderbird..) ou via Webmail (navigateur Web) ?
  - Y avait-il un numéro de téléphone mentionné ? Une éventuelle adresse IP / URL a-t-elle pu être notée ?
  - En cas de courriel reçu, s'agissait-il d'un message en relation avec des activités professionnelles ou des centres d'intérêts personnels ?

Sécurité numérique en santé

MÉMO – Dépôt de plainte suite à un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

QUESTIONS / INFORMATIONS POUR L'ANALYSE DE LA SITUATION

- 3/ Concernant la fenêtre apparaissant sur l'écran (le cas échéant) :
  - S'agissait-il d'une page reprenant les logos d'un site gouvernemental ou officiel et, si oui, de quel pays et de quelle administration s'agissait-il ?
  - Quel était le nom du < groupe d'attaquant > et/ou du < virus/rançongiciel > apparaissant à l'écran ?
  - Sur la page apparaissant à l'écran, quelle était la raison expliquant le blocage de votre ordinateur (captation illicite d'image pédopornographique, téléchargement illicite de contenu, etc.) ?
  - Quelle était la langue utilisée sur cette page apparaissant à l'écran ? Y avait-il des fautes d'orthographe ou de conjugaison ? La langue utilisée pouvait-elle être considérée comme la langue maternelle de son rédacteur ?
  - Y avait-il des instructions spéciales spécifiées ?
  - Avez-vous conservé une copie d'écran de la page affichée par le < rançongiciel > (à joindre) ?
- 4/ Concernant les échanges avec l'attaquant :
  - Etes-vous entré en contact avec la personne ? Si oui, avez-vous conservé les traces des dits dialogues et par quel moyen aviez-vous dialogué avec cette personne ?
  - Dans quelle langue avez-vous dialogué avec cette personne ? Semblait-il s'agir de sa langue maternelle ?
- 5/ Impacts de l'incident :
  - Quels périmètres (site(s), service(s), unité(s), …) de votre structure ont été touchés par l'incident ? Le fonctionnement de ces derniers était-il partiellement atteint ou totalement ?
  - Des sites distants ou annexes (partageant une partie de votre SI ou plus) ont-ils été touchés également par cet incident ? Si oui, à quelle hauteur ?
  - Êtes-vous parvenu à récupérer l'ensemble de vos fichiers ? Avez-vous dû utiliser pour cela un outil de déchiffrement et, si oui, lequel ? Quelle en a été l'efficacité ?
  - Avez-vous pu identifier s'il y a eu une exfiltration de données ? Si oui, lesquelles ? Avez-vous fait le signalement auprès de la CNIL dans le délai réglementaire des 72 heures post-incident ?

RAPPEL DU CODE PÉNAL

- *Article 434-23* : **l'hameçonnage** est punissable par une peine de 5 ans de prison et 75 000€ d'amende.
- *Article 323-3* : **l'atteinte à un système de traitement automatisé des données** est condamnable par 2 ans de prison et 30 000€ d'amende.
- *Article 226-18* : la **collecte frauduleuse de données à caractère personnel** est sanctionnable par 1 an de prison et 300 000€ d'amende.

Gendarmerie nationale
RÉPUBLIQUE FRANÇAISE
ars Agence Régionale de Santé Pays de la Loire
e-santé Pays de la Loire
Pays de la Loire

Sécurité numérique en santé

MÉMO – Dépôt de plainte suite à un incident SI d'origine malveillante

[Octobre 2023]

Tout incident majeur d'origine malveillante impactant significativement le système d'information doit faire l'objet d'un dépôt de plainte.

EN SYNTHÈSE