CLINIQUE Pasteur

Référence :
MO/POL/QUA/CRI/52 v1

Mode opératoire :

Mobiliser la fiche réflexe : Incident de sécurité du système d'information

Relié à la procédure : PR/POL/QUA/CRI/05 « Mettre en œuvre le plan de Gestion des Situations Sanitaires Exceptionnelles »

Service émetteur :	**Date de la Première émission :**	**Nombre de pages :**
DAC	**21/10/2021**	**14**

Référence externe :
Guide d'aide à la préparation et à la gestion des tensions hospitalière et des situations sanitaires exceptionnelles (ex-plan blanc) – 2019
Agir contre un maliciel – agence du numérique en santé – Septembre 2020

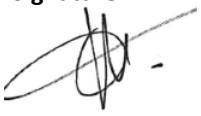
Destinataire(s) (service, périmètre) :
- **CODIR**
- **CME**
- **Encadrement**
- **Cellule de crise**
- **Service Informatique**
- **DAC**

Historique des modifications :
- **Annule et remplace la V0 du 21.10.2021**

Version	Date	rédacteur
V0	21/10/2021	DI SANTO Denis

Modifications :

Date	Page	A la place de	Lire
09.12.2021	**1**		**Mise à jour de la procédure de déclaration d'incident**

Rédacteur(s) ou Modificateur (DLG)	**Vérificateur (Département AC)**	**Approbateur**	**Visa**
Nom : DI SANTO **Prénom :** Denis **Fonction** : Responsable de la Sécurité du Système d'Information **Date** : 08/12/2021 **Signature** : 	**Nom** : CHATELIN **Prénom :** Sophie **Fonction :** Responsable du Département d'Amélioration Continue **Date :** 08/12/2021 **Signature :** 	**Nom :** PON **Prénom :** Dominique **Fonction :** Directeur D'Etablissement **/**	**Nom :** PON **Prénom :** Dominique **Fonction :** Directeur D'Etablissement **Date :** 08/12/2021 **Signature** : 

CLINIQUE Pasteur

Référence :
MO/POL/QUA/CRI/52 v1

MOBILISER LA FICHE REFLEXE

INCIDENT DE SECURITE DU SYSTEME D'INFORMATION

I. Réunir la cellule de crise

Prévenir le responsable de la sécurité des systèmes informatique (RSSI) ou à défaut le responsable informatique (RSI) qui va réunir la cellule de crise du système d'information et cyberdéfense. Toutes les actions seront prises sur ordre de cette cellule de crise.

La cellule de crise comprend à minima:

- Le directeur
- Le directeur des soins infirmiers
- La communication
- Le RSSI
- Le RSI/DSI

Le département d'amélioration continue.

II. Confinement

- **Isoler la machine du réseau** sans l'éteindre. Cela peut permettre notamment de retrouver des clés de chiffrement. Soit en débranchant le câble réseau si la machine est physique, soit en déconnectant la carte réseau dans le cas d'une machine virtuelle et effectuer un snapshot complet de la machine (avec RAM).

- **Bloquer l'accès des utilisateurs compromis si besoin.**

En cas d'un grand nombre de machines infectées :

- **Déconnecter les sauvegardes** et vérifier leur intégrité avant leur restauration
- Déconnecter les accès Internet.
- **Déconnecter les serveurs critiques potentiellement responsables d'une propagation interne** du maliciel/rançongiciel (Serveurs de fichiers, WSUS et faire **un snapshot complet** (RAM et disque))

III. Investigation et identification

- **Récupérer les logs périphériques** en lien avec la machine (Antivirus central, DNS, Firewall, Proxy, Smtp (sortant et courriel entrant vers l'utilisateur), ACL réseau, netflow, IDS ...)
- **En cas d'hameçonnage, rechercher si d'autres utilisateurs ont reçu le courriel** et l'ont ouvert.

- **Rechercher les canaux de communications utilisés par l'attaquant**, afin de couper les connexions existantes et d'identifier d'autres ressources compromises.

- **Identifier le début de la compromission**, afin de pouvoir restaurer le parc avec des sauvegardes intègres.
- **Identifier la famille du maliciel** pour connaître les méthodes et l'objectif de l'attaque (rançon, vol de données, crypto-minage...). Cela permet d'adapter la remédiation (communication, changement d'identifiants internes et externes, déclaration CNIL, ...). Identifier ces informations avec https://attack.mitre.org/software/ et rechercher l'existence d'un outil de déchiffrement sur https ://nomoreransom.org/.
- **Identifier les éléments exfiltrés ou la quantité d'informations transmises** vers l'attaquant afin d'avoir une idée de l'ampleur des fuites.
- **Identifier l'ensemble des utilisateurs** qui se sont connectés à la machine et leur demander de changer leur mot de passe (si l'accès de l'attaquant était à privilège, il a pu accéder au cache).
- **Rechercher les méthodes de propagation potentielles du maliciel** et vérifier qu'elles n'ont pas été activées.
- **Réitérer ces actions** d'investigation sur les nouvelles machines identifiées comme compromises

IV. Signaler un incident aux autorités

La déclaration des incidents graves de sécurité des systèmes d'information, sans préjudice des autres déclarations obligatoires, est effectuée sans délai par le directeur de la Clinique Pasteur ou la personne déléguée à cet effet, auprès du directeur général de l'agence régionale de santé Occitanie. L'agence régionale de santé est responsable de la qualification des incidents signalés.

Les incidents devant être déclarés sont :

- Les incidents ayant des conséquences potentielles ou avérées sur la sécurité des soins ;
- Les incidents ayant des conséquences sur la confidentialité ou l'intégrité des données de santé
- Les incidents portant atteinte au fonctionnement normal de l'établissement, de l'organisme ou du service.

La déclaration de l'incident s'effectue via le lien suivant : https://signalement.social-sante.gouv.fr).

En fonction de l'incident, une plainte est également déposée auprès des services de police ou de gendarmerie.

1. Critère de sécurité

Indisponibilité

Une indisponibilité des systèmes peut entrainer une inaccessibilité aux informations nécessaires au processus métier ou une interruption d'activité.

Perte d'intégrité

Un défaut d'intégrité entraine une perte ou une modification de l'information traitée ou produite par le système qui trompe l'utilisateur et nuit au processus métier.

Perte de confidentialité

Des personnes non autorisées ont pu avoir accès à des informations confidentielles.

2. **Critères pour signaler un incident de sécurité informatique ou lié aux nouvelles technologies**

   Doit être signalé :

   a. Toute action ou suspicion d'action malveillante causant une indisponibilité partielle ou totale de systèmes informatiques, une altération ou une perte de données
   b. Une indisponibilité partielle ou totale de systèmes informatiques impactant les systèmes participant à la prise en charge d'un patient et/ou les systèmes contribuant au fonctionnement de la structure ;
   c. Un impact direct sur la prise en charge d'un patient ;
   d. Un impact sur l'intégrité ou la confidentialité des données de santé à caractère personnel ;
   e. Un impact réglementaire (par ex. impact sur les données personnelles d'employés de la structure) ;
   f. Une perte de confidentialité de données techniques sensibles (mots de passe, clés cryptographiques, documents d'architecture et de configuration, etc…) ;

3. **Fiches pratiques en fin de document**
   a. Hameçonnage
   b. Maliciel
   c. Déni de service
   d. Réagir à un acte de cybermalveillance
   e. Fuite de données
   f. Intrusion Web
   g. Panne électrique
   h. Vol d'équipement

V. Remédiation / Restauration

- **Corriger les failles à l'origine de l'infection** : mise à jour (par ex: CVE sur VPN, adobe/flash/java/navigateur, ...), revoir la politique d'accès extérieur (politique de mot de passe, fermer RDP, anti brute force, limiter les plages IP, double authentification, segmenter son réseau, arrivée en DMZ spécifique...), amélioration des protections (durcissement général, AppLocker, antivirus, filtrage messagerie et/ou proxy, segmentation réseau, firewall local, ...).
- **Restaurer un système intègre** : changement d'identifiant interne et externe (vol d'identifiant), communication (vol données sensibles), récupération et réinstallation des sauvegardes avant la compromission, reconstruire l'AD (attention très complexe si on ne veut pas repartir de zéro), suppression des fichiers infectés sur le partage réseau/DFS.
- **Bloquer toute possibilité de reprise de l'infection** : suppression des fichiers infectés du DFS, mise à jour des postes, firewall local, mise en place de filtrage (ACLs) inter VLAN, GPO pour ne permettre les connexions vers un poste en interne que depuis un utilisateur spécifique, ...

VI. Retour à la normale

- **Remettre en service le réseau interne en premier** puis **l'accès vers Internet en ayant bien validé préalablement la mise en œuvre des mesures de remédiation présentés ci-dessus**

- **Surveiller pendant quelques jours** le réseau interne et les connexions vers Internet pour détecter d'éventuels comportements anormaux ou des connexions suspectes (pas d'UA, connexion directe sur IP, port suspect, ...).
- **Surveiller les marqueurs de l'attaque bloqués** pour vérifier qu'il n'y a plus de machine qui cherche à les utiliser
- **Remettre l'accès des services exposés sur internet** et surveiller qu'il n'y a aucune connexion suspecte réussie (GEOIP, horaire de connexion, useragent spécifique [mac, linux, navigateur qui n'est pas utilisé sur le SI, ...])
- **Investir sur la prévention avec le retour d'expérience** afin de limiter une potentielle nouvelle compromission.

Agir contre une attaque par hameçonnage

*Fiche à l'attention des **responsables de la sécurité des systèmes d'information (RSSI)***

Objectifs de l'attaque

Récupérer des informations sensibles pour accéder à des comptes (messagerie, administration, etc…) et qui serviront à des fins illégales (spam, intrusion, fraude, etc…)

La technique de **l'hameçonnage** (phishing) consiste à usurper l'identité d'un tiers légitime dans le but d'obtenir des informations sensibles. Elle est basée sur l'utilisation de la messagerie électronique, de SMS et des portails Web. Une fiche de sensibilisation est disponible sur le portail **cybermalveillance.gouv.fr.**

Mesures de détection

- **Surveiller l'espace de quarantaine de la messagerie** qui peut permettre d'identifier des campagnes de pourriels en cours
- **Mettre en place un module sur le client de messagerie** permettant de remonter les courriels suspects au responsable sécurité (avec l'entête et tous les éléments nécessaires)
- **Surveiller les logs du proxy** (blocage urlhaus, téléchargements suspects, url complexe accédée sans aucun referer…)
- **Surveiller les connexions d'adresse IP étrangères** et les tentatives de force brute sur le webmail (analyser les logs permettant d'identifier l'utilisateur ciblé pour vérifier avec lui s'il n'a pas été victime d'un phishing)
- **Surveiller quotidiennement les flux anormaux** de réception et d'envoi de courriels, par exemple le « top 20 » des courriels les plus diffusés en réception et en émission, les stats de supervision de la congestion de la file d'attente et les stats DMARC (usurpation du nom de domaine)
- **Vérifier si l'IP du service d'émission de courriels (smtp sortant)** n'est pas black-listée en utilisant le protocole DNS (Black Listing) (DNSBL.net par exemple)

Mesures de réaction

Comptes de messagerie

- **Désactivation des comptes compromis** puis changement des mots de passe
- **Désactivation temporaire du webmail** si tous les comptes compromis ne sont pas identifiés
- **Vérifier qu'aucune redirection** (ou script de redirection) n'a été paramétré

Au niveau de la réception (MX)

- **Filtrer les éléments** (atypiques ou uniques) susceptibles de pouvoir être bloqués (corp: uri, ip / entetes: useragent, from, ip émettrice, header spécifique)
- Analyser le contenu des courriels **et mettre en place des règles de scoring** basée sur des mots clés

Au niveau de l'émission (SMTP)

- **Bloquer l'émission de messages vers l'attaquant** (from & reply to)

Au niveau Proxy

- **Bloquer les tentatives d'accès HOST/IP** (la résolution IP de l'host) identifiée comme malveillante (action réalisée sur les flux http & https)
- **Bloquer les URLs contenant des éléments atypiques** (chemin, argument, nom de la page...) (action possible que sur les flux non chiffrés => http)

Organisation

- **Informer les utilisateurs** d'une campagne en cours

Alerter des tiers

Phishtank & signal spam (URL) **/ @abuse du domaine émetteur des courriels**

Si l'attaque provient d'une adresse légitime, **informer l'organisation concernée ou l'hébergeur du domaine**

Agir contre un maliciel

*Fiche à l'attention des **Responsables de la Sécurité des Systèmes d'Information (RSSI)***

1 Confinement

- **Isoler la machine du réseau** sans l'éteindre. Cela peut permettre notamment de retrouver des clés de chiffrement. Si ce n'est pas possible, isoler la machine d'Internet et des autres machines du réseau, en particulier des serveurs de fichiers.
- **Bloquer l'accès de la machine et les utilisateurs compromis** à l'ensemble des services exposés sur internet (RDP, Webmail, VPN, ...)

En cas d'un grand nombre de machines infectées :

- **Déconnecter les sauvegardes** et vérifier leur intégrité avant leur restauration
- Configurer le partage des fichiers **en lecture seule**
- **Fermer les services exposés sur Internet** en connexion direct avec votre réseau : RDP, WEBMAIL, VPN, SSH, ... **Et les possibilités de sortie** : pas de résolution DNS externe directe depuis un serveur/poste, pas de sortie internet directe, obligation de passer par un proxy en mode liste blanche (seulement vers des URL maitrisées, interdire tous les tunnels/RAT). Configurer les serveurs de fichiers (NAS/DFS) en lecture seule.
- **Déconnecter les serveurs critiques potentiellement responsables d'une propagation interne** du maliciel/rançongiciel (Pour l'environnement Windows : AD -> GPO / WSUS -> update / DFS -> file) et **faire un snapshot** pour les serveurs virtuels (RAM et disque)
- **Bloquer les communications** malveillantes identifiées sur vos différents équipements (firewall, proxy, smtp, dns, ...) lors de l'investigation, en surveillant celles qui sont initiées par de nouvelles machines (suspicion de compromission)
- **Configurer vos équipements (firewall, proxy, smtp, dns, ...) pour bloquer** les moyens de l'attaquant (URL, domaine, IP, adresse courriel...)

2 Investigation/Identification

- **Utiliser un outil forensique pour extraire des artefacts** (ORC[ANSSI], FastIR[CERT SEKOIA], Sysinternals, ...) d'un snapshot d'une machine virtuelle. Pour Windows, il faut récupérer les artefacts (autorun, mft, usn, registres, events, RAM ou process+handles, prefetch, taches planifiées, liste des utilisateurs, ...).
- **L'utilisation de ces outils nécessite des droits élevés** (privilégier l'utilisation du compte admin local). Si l'attaquant a des privilèges, il pourrait récupérer les identifiants lors de connexions. **Il est donc indispensable de ne pas reconnecter la machine à Internet pendant et après cette opération**.
- **Récupérer les logs périphériques** en lien avec la machine (Antivirus central, DNS, Firewall, Proxy, Smtp (sortant et courriel entrant vers l'utilisateur), ACL réseau, netflow, IDS ...)
- **Analyser les artefacts** pour :
  a) **Identifier l'origine de l'infection** (patient zéro ou rebond), afin que l'attaquant ne puisse plus compromettre le système avec le même scénario d'attaque.
  b) **Identifier le niveau de privilège de la compromission** (utilisateur ou admin/système), afin d'adapter l'analyse des artefacts. Parfois l'origine n'est pas sur le poste identifié et peut provenir d'un accès à distance VPN, RDP, SSH, RAT par rebond.
- **Vérifier** que les services d'accès à distance sont à jour de patchs et qu'aucun compte n'a été compromis.
- **En cas d'hameçonnage, rechercher si d'autres utilisateurs ont reçu le courriel** et l'ont ouvert.

- **Déclarer l'incident** auprès des autorités compétentes (Ministère de la Santé, ANSSI, CNIL) et **déposer plainte** auprès des services de police ou de gendarmerie (voir la fiche « Réagir à un acte de cybermalveillance »)
- **En cas de crise, informer les utilisateurs** et leur communiquer la conduite à tenir
- Faire une **sensibilisation** à cette menace avec le kit mis à disposition par **cybermalveillance.gouv.fr**

Agir contre un maliciel

2 Identification (suite)

- **Rechercher les canaux de communications utilisés par l'attaquant**, afin de couper les connexions existantes et d'identifier d'autres ressources compromises.
- **Identifier le début de la compromission**, afin de pouvoir restaurer le parc avec des sauvegardes intègres
- **Identifier la famille du maliciel** pour connaître les méthodes et l'objectif de l'attaque (rançon, vol de données, crypto-minage...). Cela permet d'adapter la remédiation (communication, changement d'identifiants internes et externes, déclaration CNIL, ...). Identifier ces informations avec https://attack.mitre.org/software/ et rechercher l'existence d'un outil de déchiffrement sur https ://nomoreransom.org/.
- **Identifier les éléments exfiltrés ou la quantité d'informations transmises** vers l'attaquant afin d'avoir une idée de l'ampleur des fuites
- **Identifier l'ensemble des utilisateurs** qui se sont connectés à la machine et leur demander de changer leur mot de passe (si l'accès de l'attaquant était à privilège, il a pu accéder au cache).
- **Rechercher les méthodes de propagation potentielles du maliciel** et vérifier qu'elles n'ont pas été activées
- **Réitérer ces actions** d'investigation sur les nouvelles machines identifiées comme compromises

3 Remédiation/Restauration

- **Corriger les failles à l'origine de l'infection** : mise à jour (par ex: CVE sur VPN, adobe/flash/java/navigateur, ...), revoir la politique d'accès extérieur (politique de mot de passe, fermer RDP, anti brute force, limiter les plages IP, double authentification, segmenter son réseau, arrivée en DMZ spécifique...), amélioration des protections (durcissement général, AppLocker, antivirus, filtrage messagerie et/ou proxy, segmentation réseau, firewall local, ...).
- **Restaurer un système intègre** : changement d'identifiant interne et externe (vol d'identifiant), communication (vol données sensibles), récupération et réinstallation des sauvegardes avant la compromission, reconstruire l'AD (attention très complexe si on ne veut pas repartir de zéro), suppression des fichiers infectés sur le partage réseau/DFS.
- **Bloquer toute possibilité de communication de l'attaquant** : mise en place d'un proxy, interdire les tunnels non standards via le proxy (RAT, ssh, ...), interdire la communication sur les ports non standards, interdire les tunnels DNS, ...
- **Bloquer toute possibilité de reprise de l'infection** : suppression des fichiers infectés du DFS, mise à jour des postes, firewall local, mise en place de filtrage (ACLs) inter VLAN, GPO pour ne permettre les connexions vers un poste en interne que depuis un utilisateur spécifique, ...
- **Installer** "sysmon" pour windows et "auditd" pour linux afin de pouvoir mieux identifier des éléments suspects lors du retour à la normale

4 Retour à la normale

- **Renforcer la protection du système contre l'exécution de programmes potentiellement malveillants** (ex: DFS -> FSRM, Applocker, ...)
- **Remettre en service le réseau interne en premier** puis **l'accès vers Internet en ayant bien validé préalablement la mise en œuvre des mesures de remédiation présentés ci-dessus**
- **Surveiller pendant quelques jours** le réseau interne et les connexions vers Internet pour détecter d'éventuels comportements anormaux ou des connexions suspectes (pas d'UA, connexion directe sur IP, port suspect, ...). Si c'est le cas, utiliser les informations de sysmon ou auditd afin d'identifier l'origine et la légitimité de la connexion.
- **Surveiller les marqueurs de l'attaque bloqués** pour vérifier qu'il n'y a plus de machine qui cherche à les utiliser
- **Remettre l'accès des services exposés sur internet** et surveiller qu'il n'y a aucune connexion suspecte réussie (GEOIP, horaire de connexion, useragent spécifique [mac, linux, navigateur qui n'est pas utilisé sur le SI, ...])
- **Investir sur la prévention avec le retour d'expérience** afin de limiter une potentielle nouvelle compromission.

Agir contre une attaque par déni de service

Les objectifs de l'attaque

Rendre indisponible un service en ligne pour porter directement atteinte à l'image de son propriétaire et à la confiance que peuvent avoir les utilisateurs.

Une attaque par déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service.

Mesures de réaction

Identifier la ou les origines de l'attaque ainsi que la méthode utilisée. Il faut s'assurer qu'il s'agit réellement d'un DOS ou d'un DDOS :

- **Identifier** où se situe le crash ou la saturation de la machine (ou des machines)
- **Identifier** la cible de l'attaquant
- **Déconnecter** le service si besoin durant les recherches

Si l'attaque vise les **couches applicatives** (basée sur l'exploitation d'une vulnérabilité / erreur de configuration) :

- **Appliquer les derniers correctifs** de l'équipement / système / application
- **Durcir la configuration** de l'équipement / système et/ou utiliser des applications spécifiques contre les attaques DOS
- **Surveiller** l'équipement / l'application (utilisation de Nagios, etc.). Attention au déchiffrement du trafic SSL.
- **Auditer** l'application / équipement visé(e) et réaliser régulièrement des scans

Si l'attaque consiste **à saturer le réseau** :

- **Utiliser un équipement de type pare-feu ou répartiteur de charge**. Attention même si ces équipements permettent d'améliorer la résistance à une attaque par déni de service, ils ne sont en général pas suffisants.
- **Utiliser un équipement de protection spécifique aux attaques DOS**. En plus de posséder des capacités de traitement adaptées, ces équipements possèdent des fonctionnalités de filtrage spécifique Anti-DOS.
- **Solliciter l'opérateur de transit ou le fournisseur d'accès à Internet** afin de filtrer le trafic en amont
- **Recourir à des services** de Content Delivery Network (CDN)
- Etudier si l'équipement / application visé peut être hébergé(e) dans le « cloud »
- **Planifier régulièrement** des tests de charge

LIENS UTILES ANSSI

Comprendre et anticiper les attaques DDOS
Dénis de service - Prévention et réaction

Réagir à un acte de cybermalveillance

Mesures de prévention

- **Sensibiliser le personnel à la menace de cybersécurité** (hameçonnage, demande de rançon, fichiers suspects, etc…)
- **Définir et faire connaitre la procédure** d'alerte à l'ensemble des personnels
- **Définir une organisation de crise** en capacité de réagir rapidement en cas d'incident et capable de mettre en œuvre les mesures d'urgence
- En cas de perte de disponibilité des données, **disposer d'un plan de reprise et de continuité du SI**, même sommaire, tenu régulièrement à jour et décrivant comment restaurer les données essentielles
- **Vérifier les engagements contractuels avec vos prestataires** concernant la gestion d'un incident de cybersécurité et la reprise d'activité
- **Etudier le recours à une assurance spécifique** couvrant les pertes potentielles liées à un incident de cybersécurité
- **Améliorer les pratiques** en capitalisant sur les incidents rencontrés

Mesures d'urgence

- **Ne pas payer de rançon** ni prendre contact avec un tiers suggéré
- **Déconnecter les machines du réseau** (ne pas les éteindre)
- **Alerter votre responsable et votre support informatique** (ou contacter votre prestataire). Rechercher un prestataire local au travers du portail https://www.cybermalveillance.gouv.fr/.
- **Déclarer l'incident sur le portail des signalements** https://signalement.social-sante.gouv.fr pour disposer d'un appui du ministère. Au-delà de 18h ou lors d'un jour non ouvré et au regard de la criticité de l'incident, en cas de besoin d'une assistance dans les plus brefs délais, informer le FSSI des Ministères sociaux (ssi[@]sg.social.gouv.fr) en parallèle du signalement sur le portail.

Dépôt de plainte

La plainte déposée a pour but de **protéger l'établissement** dans le cas où les infrastructures corrompues aient été utilisées à mener des attaques sur des tiers. Elle permet également parfois de confondre les auteurs. Elle consiste à **décrire l'attaque**, sa réussite ou son échec, les éventuels dommages qui peuvent en résulter ainsi que toutes les autres conséquences (perte de temps pour vérification de l'intégrité des données, pertes d'argent, perte de crédibilité auprès des patients, etc..). Il est donc important de **conserver toutes les traces utiles à l'enquête** (logs, copies écran, …).

Il est recommandé de déposer une plainte pour **atteinte à un traitement automatisé de données** (appellation juridique du piratage) prévu et dont la punition relève des articles 323-1 et suivants du code pénal. Cette plainte peut être recueillie par :

- Le **Service Régional de Police Judiciaire**. Le commissariat de police ou la gendarmerie le plus proche disposent de leurs coordonnées. Une fois en contact avec la S.R.P.J. il faut demander à parler à un « Investigateur en cybercriminalité » autrement dit un I.C.C qui pourra enregistrer la plainte ;
- L'**Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication** par téléphone (01 49 27 49 27) ou par courrier électronique oclctic@interieur.gouv.fr qui orientera la demande (voir coordonnées complètes au lien suivant O.C.L.C.T.I.C.).

Notification à la CNIL

Lorsque l'incident implique des **données à caractère personnel présentant un risque pour les droits et libertés des personnes**, il faut notifier les informations demandées à la CNIL au lien suivant https://notifications.cnil.fr/notifications/index. La notification à l'autorité de contrôle doit être faite **dans les 72 heures à compter de la découverte de l'incident** : la nature de la violation et les catégories et le nombre approximatif de personnes concernées par la violation ; les coordonnées du délégué à la protection des données ou toute autre personne responsable ; les conséquences probables et les mesures de remédiations prises ou envisagées. **En cas de risque élevé pour les personnes physiques**, la notification aux personnes concernées par la violation **doit se faire dans les meilleurs délais**.

Prévenir une fuite de données

Une fuite de données est la divulgation non autorisée de données d'une organisation à des tiers, de manière intentionnelle ou fortuite. Les fuites de données ou exfiltration de données sont généralement la conséquence de la compromission d'un système suite à une intrusion. L'objectif de l'attaquant est de nuire à l'image de l'organisation ou d'obtenir une rançon en contrepartie de la non divulgation des données.
Elles peuvent également se produire à cause de la perte ou le vol de périphériques tels que les clés USB ou les ordinateurs portables.

Mesures de prévention

Organisationnelles

Classifier les données pour mettre en œuvre le niveau de protection requis compte tenu de leur sensibilité

Implémenter une politique de sécurité pour tous les supports de données

Evaluer et sécuriser l'exposition sur internet (Fiche réflexe « Sécuriser son exposition sur internet »)

Diffuser les contacts à alerter en cas d'incident et **définir un plan d'action** en cas de fuite de données
La réponse sera adaptée aux enjeux de la fuite (origine, données concernées, criticité...).

Opérationnelles

Réduire les droits d'accès selon le principe de moindre privilège par une solution de gestion des habilitations (Identity Access Management)

Déployer un système de gestion de correctifs de sécurité (patch management)

Mettre en place des **politiques de mots de passe forts**

Mettre en place **l'authentification multi-facteurs**

Effectuer régulièrement des **scans de vulnérabilités et des tests d'intrusion**

Implémenter des politiques de protection contre les logiciels malveillants et les menaces internes

Mettre en place une veille/surveillance afin de détecter d'éventuelles fuites d'informations (interne ou externalisée)

Chiffrer le contenu des ordinateurs portables afin de limiter l'impact d'un vol potentiel

Sensibilisation

Promouvoir l'utilisation du chiffrement des données sensibles lors de leur stockage et de leur transmission

Encourager et faciliter le signalement d'activités suspectes auprès du responsable de sécurité

Prévoir des séances de sensibilisation (moodle, eformation, travaux pratiques, etc.) adaptées aux profils des utilisateurs

De mauvaises pratiques (mot de passe sous forme de post-it, stockage dans le navigateur, stockage dans un fichier texte, etc.) peuvent compromettre la sécurité des mots de passe des utilisateurs.

Mesures de réaction

Identifier les sources et le périmètre de la fuite. Conduire une investigation afin d'identifier la source de la fuite (compromission du système d'information, malveillance interne, accident ou erreur humaine, etc...)

Identifier les données qui sont ou peuvent être concernées par la fuite en analysant les journaux d'accès des systèmes potentiellement compromis (serveur web ou frontaux, outils d'administration, applications accessibles à distance, Active Directory, etc...)
En l'absence d'une expertise en interne, faire appel à un prestataire pour une analyse post-incident

Notifier la direction générale en vue d'évaluer les différents impacts sur les personnes et les conséquences juridiques et financières (prévoir le déclenchement d'une cellule de crise selon la gravité de l'incident). Se soumettre aux contraintes légales (RGPD – voir la fiche réflexe « Réagir à un acte de cyber-malveillance »)

Prévenir une fuite de données

Mesures visant à se protéger des attaques par utilisation des identifiants volés

Certains services, comme Dropbox, LinkedIn ou encore Adobe, ont fait l'objet de piratage et de violation massive de données à caractère personnel ces dernières années.
Les pirates ont réussi à accéder aux bases de données utilisateurs et les ont rendues publiques. Ces bases contiennent généralement les adresses email et les condensats de mots de passe. Selon les algorithmes de hachage utilisés et la complexité des mots de passe, il est possible de retrouver les mots de passe en clair.
Ces bases ayant été rendues publiques, il est possible d'y accéder et d'en obtenir une copie. Une personne malveillante pourrait donc récupérer ces identifiants afin de tenter des connexions sur d'autres services. Ces cyberattaques sont communément appelées les attaques par « credential stuffing » (réutilisation d'identifiants volés).

Voici une **liste des bonnes pratiques** pour se protéger de ce type d'attaque :

S'abonner à un service permettant d'être notifié en cas de fuite de données

Certains sites tels que ***have i been pwned?***, regroupent les bases de données fuitées. En renseignant une adresse email, il est possible de savoir si un mot de passe associé à cette adresse a fuité et le site sur lequel il permet de se connecter. Il faut donc immédiatement changer le mot de passe sur le site correspondant. En fournissant une preuve de la responsabilité de la gestion d'un domaine, il est aussi possible d'avoir directement toutes les adresses emails du domaine concernées par des fuites https://haveibeenpwned.com/DomainSearch.

Utiliser des mots de passe robustes et uniques

L'ANSSI recommande d'utiliser des mots de passe de 12 caractères avec au moins 4 familles différentes de caractère (majuscules, minuscules, chiffres, caractères spéciaux). L'utilisation de mots de passe uniques permet d'éviter que le vol d'un mot de passe donne accès à plusieurs comptes. Utiliser des mots de passe unique étant complexe, il est recommandé d'utiliser des gestionnaires de mots de passe.

Utiliser des gestionnaires de mots de passe

Ces logiciels, tels que KeePass, permettent de générer des mots de passe robustes et de les stocker localement chiffrés et protégés par un mot de passe maître. Cela facilite l'utilisation de mots de passe uniques et de limiter ainsi l'impact en cas d'éventuelle fuite de données.

Changer de mots de passe régulièrement

L'ANSSI recommande de changer tous les 90 jours pour les systèmes contenant des données sensibles. Cette action doit impérativement être effectuée à la suite de la compromission d'un système.

Activer l'authentification à double facteur

Cette option disponible dans la plupart des services les plus connus (Google, Facebook, LinkedIn, etc.) permet d'ajouter un contrôle supplémentaire lors d'une authentification sur un nouvel appareil. En plus d'un mot de passe, le service requiert l'utilisation d'un code aléatoire à usage unique (OTP) transmis à l'utilisateur (par e-mail ou par SMS en général).

Agir contre une intrusion web

Les objectifs de l'attaque

En général, il s'agit de maintenir un accès à distance à des fins malveillantes (utilisation du serveur comme vecteur d'attaque, hacktivisme, vol de données...).

Une intrusion web désigne un accès non autorisé à un serveur web. L'attaquant a potentiellement acquis des privilèges d'administrateur et est libre d'y effectuer les actions qu'il souhaite (modification des données, installation d'une porte dérobée, rebond vers d'autres machines, etc.).

Mesures de prévention et d'investigation

Réduire au maximum les droits liés aux environnements d'exécution des applications

Réaliser **une veille sécurité** et **mettre à jour régulièrement** le système et les applications (voir la fiche « Patch management »)

Réaliser des **sauvegardes régulières** et exporter les journaux vers un dépôt central **pour assurer leur intégrité**

Mettre en place une **politique de mots de passe forte**

Réaliser **des audits de sécurité** et **des scans de vulnérabilité** réguliers

Quelques pistes pour rechercher l'origine de la compromission :

Acquérir les données du système pour investiguer (copie de la mémoire vive et du système et calculer l'empreinte de l'image ; s'il s'agit d'une machine virtuelle, réaliser un snapshot)

Analyser les accès dans les journaux d'événements et **analyser les journaux d'événements** de l'ensemble des composants du système ou de tout serveur ou accès d'administration exposé sur Internet. Attention, si l'attaquant a pu obtenir un accès privilégié, celui-ci a pu effacer l'ensemble de ses traces.

Mesures de réaction

Déconnecter le serveur d'Internet et vérifier qu'il n'y a aucune connexion malveillante en cours (netstat)

Rechercher les failles exploitées (logiciel, configuration, etc…) et **le niveau de privilège acquis par l'attaquant** pour réaliser ses actions

Identifier le moyen d'accès de l'attaquant (webshell, au travers d'un proxy/serveur smtp/serveur dns]) et **rechercher les possibilités de rebond** en analysant les accès aux serveurs sur le même segment réseau

Restaurer le système/service et les données à partir de sauvegardes intègres **en ayant vérifié l'absence de compromission potentielle** (Webshell, backdoor, etc…), **en corrigeant les failles** et **en respectant les bonnes pratiques** (mises à jour de sécurité, moindre privilège, etc…)

Changer tous les mots de passe des accès présents sur le serveur. Sinon l'attaquant peut réutiliser les accès précédemment obtenus.

Surveiller le service durant les jours qui suivent sa remise en production (pare-feu applicatif & IDS & journaux d'évènements)

Déposer plainte auprès des services de police ou de gendarmerie. (Voir la fiche « Réagir à un acte de cybermalveillance »)

Réagir en cas de panne électrique

Mesurer le niveau de criticité

Le niveau de criticité de la panne électrique dépend des services impactés (problème au niveau d'un seul serveur, de plusieurs, dans une même salle, réparti), de la durée d'interruption de l'activité, de la nature des données impactées et de la durée d'indisponibilité de ces données par rapport à la Durée Maximale d'Interruption Admissible (DMIA).

Il est essentiel **d'identifier l'origine de la panne**, en recherchant en interne (disjoncteur, réseau électrique interne, etc), en externe (réseau du bâtiment, etc), auprès du fournisseur et/ou distributeur d'électricité. Il peut également s'agir d'une action malveillante (débranchement, etc) ou d'une intervention accidentelle sur l'alimentation.

Mesures de prévention

Renforcer la résilience de l'alimentation électrique :
S'équiper d'un groupe électrogène ou d'une seconde alimentation ondulée, indépendante, et mettre en place une alarme en cas de coupure sur l'alimentation principale
Tester régulièrement le dispositif en cas de coupure électrique (à raison d'au moins une fois par an)
Vérifier la conformité des installations et le bon dimensionnement des réseaux et équipements

En cas d'altération des systèmes et de la perte de données liées à une panne électrique, mettre en place une **sauvegarde des environnements et des données** afin de pouvoir restaurer le système

Disposer d'une **organisation de gestion de crise et d'un plan de continuité informatique** définissant les actions prioritaires en cas de panne électrique

Définir une procédure d'arrêt et une procédure de relance (en s'appuyant sur les procédures définies dans les dossiers d'exploitation)

Mesures de réaction

Vérifier le retour à la normale des services électriques
Vérifier que les cartes d'alimentation des machines sont toujours opérationnelles
Démarrer les services dans l'ordre défini dans la procédure de relance

Contrôler le retour à la normale des services / applications

Contrôler les éventuels problèmes d'intégrité (en cas de perte de données, fichiers corrompus …). Si les systèmes sont altérés ou les données perdues, **restaurer les sauvegardes.**

En cas d'impacts critiques sur la prise en charge ou sur le fonctionnement de la structure (en particulier indisponibilité prolongée des SI), **activer la cellule de crise** et évaluer la nécessité de communiquer auprès des professionnels, des patients, de l'ARS et des directions du ministère.

Agir contre le vol ou la perte d'un équipement

Objectifs de l'attaque

Récupérer des informations sensibles/confidentielles à des fins malveillantes. Il peut toutefois s'agir d'un vol opportuniste ne ciblant pas précisément le contenu de l'équipement (ordinateur portable, smartphone, tablette ou clé USB).

Le vol d'un équipement (ordinateur, tablette, clé USB, portable…) est souvent réalisé à l'occasion du déplacement d'un personnel mais peut être aussi effectué à l'intérieur des locaux de la structure de santé.

Mesures de prévention

Noter le numéro de série de l'équipement permettant son identification.

Sauvegarder régulièrement les documents sur un support externe (disque dur externe, USB…), ce qui facilite la reprise d'activité et évitera la perte de données.

Activer le verrouillage automatique et mettre en œuvre l'effacement à distance des données de l'équipement. L'utilisation d'une solution de MDM est recommandée. Cette solution doit au minimum disposer des fonctionnalités suivantes : verrouillage à distance de l'équipement (blocage des accès non autorisés à l'appareil sans avoir à supprimer les données) / effacement de l'intégralité des données enregistrées sur un appareil ou uniquement les informations sensibles / localisation des smartphones et des tablettes (GPS, 3G/4G ou WiFi).

Sécuriser les mots de passe avec l'utilisation de mots de passe non rejouables (One Time Password) et de gestionnaires de mots de passe tel que l'outil gratuit KeePass.

Faire l'inventaire des données sensibles et chiffrer le contenu (avec un mécanisme de chiffrement conseillé par l'ANSSI) en utilisant de préférence une solution permettant de chiffrer totalement le disque ou en partie*****.

Sensibiliser les utilisateurs à l'égard des données et des équipements mis à leur disposition et les former à la protection des fichiers qu'ils contiennent (lieu public, fermeture des sessions ...).

Mesures de réaction

Prévenir le service informatique de votre structure

Changer tous les mots de passe, en particulier ceux concernant la messagerie électronique, les comptes de connexion à distance (VPN, etc.) et les sites web (idéalement, il faut aussi changer les questions de vérification des comptes).

Déclarer la perte ou déposer plainte en cas de vol et garder une copie de la déclaration (mentionnant la date, l'heure et le lieu du vol).

En cas de vol de données sensibles, alerter les services concernés afin que des dispositions soient prises notamment en cas de déclaration à la **CNIL.**

Si l'équipement volé donne accès à des espaces de travail communs, ou permet de s'y connecter à distance, s'assurer que les utilisateurs du système en sont informés.

Si l'équipement peut être géré à distance par une solution de MDM (Mobile Device Management), supprimer les données à distance et bloquer l'accès à l'équipement.

* *Solutions qualifiées par l'ANSSI: Cryhod, STORMSHIELD Data Security, ZoneCentral*
Autres solutions: BitLocker2 (Microsoft), VeraCrypt