Fiche réflexe cyberattaque

2024

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé Provence-Alpes Côte d'Azur

Cette fiche reflexe est un outil opérationnel indiquant les mesures à mettre en œuvre par un établissement victime d'une cyberattaque.

Destinataires :

Sont concernés par la présente fiche :

Pour action :

- Les établissements de santé et médico-sociaux de la région Provence-Alpes-Côte d'Azur (PACA).
- L'Agence régional de santé (ARS) PACA.

Pour information :

- Les structures d'exercices coordonnés.
- La cellule d'Appui à la Protection des Systèmes d'Information de la Région PACA (CAPSI)
- L'agence du numérique en santé (ANS)
- L'agence nationale de la sécurité des systèmes d'information (ANSI)

Phase 1 : Premières mesures à appliquer

Confiner/endiguer	Alerter et communiquer
1. Réunir une cellule de crise avec une composante informatique et métiers qui prendra les décisions de : a. Couper le système d'information d'internet pour stopper la propagation du cryptovirus. b. Couper les liens intersites (applicatifs partagés entre ES). c. Isoler les VLAN compromis. Importance de pouvoir compartimenter isoler les systèmes les plus sensibles. 2. Ne plus utiliser le matériel informatique avant de l'avoir nettoyé ou masterisé. 3. Vérifier qu'aucune propagation aux établissements partenaires n'a eu lieux.	En fonction de la gravité de l'attaque, il convient de mobiliser les acteurs suivants dont vous devez avoir les coordonnées mail et téléphone: ▪ Votre DSI. ▪ Prestataires, prestataires de réponse à incident. ▪ SOC (EDR). ▪ GHT. ▪ CAPSI, Taskforce régionale (centre de ressource cyber régional). ▪ ARS. ▪ ANS, ANSSI.

La chaine d'alerte :

L'ARS PACA peut être contactée à tout moment, 7j/7 et 24h/24, par mail à l'adresse :

ars-paca-alerte@ars.sante.fr ou par téléphone au 04 13 55 80 00.

L'astreinte technique du GRADES IES sud peut être contactée à tout moment, 7j/7 et 24h/24, par mail à l'adresse :

alertes-capsi@ies-sud.fr ou par téléphone au 06 45 54 00 23.

Tout incident de sécurité des systèmes d'information grave doit faire l'objet d'une déclaration sur le portail de signalement national des évènements sanitaires indésirables :

Portail de signalement des événements sanitaires indésirables (social-sante.gouv.fr).

Ce signalement sera pris en charge par le **CERT-SANTE de l'Agence du Numérique en Sante**, disponible 7j/7, 24h/24 qui accusera réception et vous assistera dans la résolution de l'incident, par mail à l'adresse :

cyberveille@sante.gouv.fr ou par téléphone au 09 72 43 91 25.

Si votre établissement est Opérateur d'Importance Vitale ou Opérateur de Service Essentiel, vous devez contacter **le CERT-FR** de l'Agence Nationale de Sécurité des Systèmes d'information, disponible 7j/7, 24h/24, par mail à l'adresse :

cert-fr.cossi@ssi.gouv.fr ou par téléphone au 01 71 75 84 68.

Si des données personnelles ont fait l'objet d'une violation (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite) vous devez le déclarer à la CNIL dans les 72h sur le lien suivant : Notifier une violation de données personnelles | CNIL ou https://notifications.cnil.fr/notifications/ ou par téléphone au 01 53 73 22 22

Il convient également de porter plainte via l' Outils de diagnostic - Assistance aux victimes de cybermalveillance ou au commissariat de police ou à la brigade de gendarmerie dont vous dépendez, ou par courrier au procureur de la République du tribunal judiciaire.

Communiquer :

Il convient, en cas d'attaque cyber, d'organiser la communication de l'établissement qui doit répondre aux principes suivants :

- **Faut-il communiquer sur l'attaque? A quel moment doit-on annoncer qu'il s'agit d'une cyberattaque ou d'un incident?**

  - Vous n'aurez pas forcément le choix, tout dépend des informations publiées dans les médias.
  - Suivre les conseils de l'ANSSI ou ANS.
  - Livrer un message transparent et rassurant.
  - En cas de diffusion des données, vous serez contraint de communiquer.
  - Etablir avec les partenaires le circuit de communication officie et partager les communiqués avec eux: ARS, préfecture.

- **Divulgation de données sur le darknet**

  - L'obligation d'informer les victimes.
    - Saisir votre DPO.
    - Demander conseil à la CNIL.
    - Faire valider par la CNIL votre plan d'information des victimes.

- **Demande de rançon, comment réagir? La consigne des autorités nationales est de ne pas y répondre favorablement.**

Phase 2: passer en mode de fonctionnement dégradé

Suite à une cyberattaque, ce mode de fonctionnement peut s'inscrire dans la durée (ex : les cyberattaques du CH d'Arles et du CH Sud francilien ont entraîné un fonctionnement en mode dégradé durant une année suivant la cyberattaque) et être consommateur de ressources humaines supplémentaires.

Activer les procédures de fonctionnement dégradé dans tous les services (mode papier). Il convient de faire preuve de vigilances sur la sécurisation des documents papiers

- Utiliser la sauvegarde hors ligne du Dossier patient informatisé (qui doit être mise en place en amont). Dans le cas d'un DPI en mode SaaS, se rapprocher de son éditeur.
- Prévoir une imprimante locale (non connectée au réseau).
- Déployer des modes de communication de secours:
    - Des téléphones portables.
    - Une messagerie de secours.
    - Une messagerie instantanée secteur public TCHAP : https://www.demarches-simplifiees.fr/commencer/utiliser-tchap
    - ou tout secteur azurezo https://ies-sud.fr/azurezo/
    - ou Signal Installer Signal – Assistance de Signal

- Déployer du matériel informatique de secours qui ne doit pas être connecté au réseau de l'établissement attaqué:
    - PC tampons de secours (ce stock de PC tampons devrait représenter 1 à 2% de votre parc informatique) et lié à votre plan de continuité d'activité (PCA).
    - Des clés 4G.
    - Des disques durs externes.
    - Des imprimantes locales.

Phase 3 : Anticiper et répondre à l'impact sur les activités de soins des établissements.

En fonction des établissements, les services et activités pouvant être impactés, en cas de cyberattaques, sont les suivants (liste non exhaustive) :

- Soins critiques
- Laboratoires médicales
- Stérilisation
- SAU
- Pharmacie
- Biologie médicale
- Imagerie médicale
- Service logistiques (repas, blanchisserie) ou administratifs (gestion des paies, admission des patients etc.).

A ce titre, il convient d'anticiper l'impact que pourrait avoir une cyberattaque sur ces services et de prévoir des solutions de repli en amont (exemple : partenariat avec des laboratoires privés, identification des établissements, des structures d'exercices coordonnées pouvant servir d'appui).

En outre, en cas de cyberattaque, il conviendra d'évaluer rapidement l'impact de la cyberattaque sur ces services et les besoins d'appui pouvant en découler. En lien avec L'ARS, une solidarité pourra, alors, être envisagée et demandée afin de permettre à l'établissement de fonctionner et d'assurer la continuité des soins en mode dégradé (Orienter les flux de régulation médicale du Samu vers d'autres établissements), sorties anticipée de patients vers leur domicile ou d'autres structures : EPHAD, CPTS etc.).

Le rôle de l'ARS :

Une procédure de réponse à une cyberattaque sur un établissement est déclenchée lorsque l'alerte est donnée par l'établissement.

L'ARS prend l'attache de l'établissement concerné (et l'établissement support de GHT le cas échéant) par la cyberattaque pour faire un point précis sur:

- L'impact de l'incident sur le volet informatique et sur l'organisation des soins et qualifier l'incident.
- Les démarches entreprises par l'établissement auprès des acteurs de la chaine d'alerte.
- Les mesures mise en œuvres.
- Les besoins en soutien sur le volet informatique et sur la prise en charge patient.

En fonction de la gravité de l'incident les acteurs sont invités à organiser une première réunion de coordination.

La coordination de la réponse s'organise autour de réunions régulières sur chacun des deux volets suivants :

- Systèmes d'information selon la criticité sous pilotage ANSSI ou ANS.
- Offre de soin sous pilotage ARS, coordination entre l'établissement santé ou médico-social touché et les acteurs venant en appui.

Phase 4 : Diagnostic et reconstruction en vue du retour à la normale

Phase de diagnostic et d'analyse dont la durée minimum est d'environ une semaine (CERT FR ou Sante et prestataire PRIS Prestataires de réponse aux incidents de sécurité).

Les investigations vont chercher à répondre au points suivants:

1. Quelle est l'étendue de l'attaque? Identification des éléments du système compromis.
2. Y-a-t-il eu exfiltration de données? Quantité et sensibilité des données exfiltrées.
3. Comment l'attaquant s'est introduit dans le système? Le vecteur d'attaque, la chaine de compromission.
4. Quelle est la date de compromission? Différente de la date à laquelle vous vous êtes aperçu de l'attaque.
5. Vous devrez fournir des éléments d'analyse: logs, autres traces.

En parallèle, une phase de reconstruction progressive est mise en œuvre (durée minimum : 2 semaines voire plusieurs mois). Elle vise à appliquer les actions suivantes :

1. Réinstallation/ nettoyage des pc (en fonction du volume de votre parc).
2. Actions de remédiation:
    1. Changement des mots de passe.
    2. Révision de la politique des mots de passe.
    3. Installation des correctifs.
    4. Déploiement d'outils complémentaires.

3. Restaurations des serveurs à une date antérieure à la compromission. Des éléments du système ne pourront peut-être pas être remis en service (exemple matériel trop obsolète).
4. Vous ne pourrez pas restaurer le système avant de connaitre la date de compromission (plusieurs jours).
5. Si vos systèmes sont obsolètes, la remise en service complète peut être prolongée de plusieurs mois.

Il est indispensable d'identifier les services essentiels qui vous permettront d'établir des priorités de redémarrage.

- Le redémarrage se fera par étapes : 2 premières heures, 2 premiers jours, 2 premières semaines. Il ne faut pas envisager une reprise globale du SI.
- Faire valider le plan de reprise par l'ARS.

Se préparer pour limiter l'impact d'une cyberattaque

1. **Faire des exercices** afin tester la résilience et la réactivité de l'établissement en cas d'attaque mais également de diffuser les bonnes pratiques aux agents (ne pas oublier de faire un RETEX).

2. **Effectuer des audits réguliers ADS (ORADAD) et surface d'exposition à internet (SILENE), suivi d'actions de remédiation.**
   Inscription au club SSI https://club.ssi.gouv.fr/inscription-sante/ ADS Secteur santé (ssi.gouv.fr).

3. **Renforcer le système d'authentification**
   1. Des utilisateurs surtout en télétravail (robustesse des mots de passe et changement réguliers).
   2. Des prestataires de service par une authentification forte (double facteur) ou n'ouvrir l'accès que pour la durée de l'intervention.

2. **Mettre à jour vos équipements pour corriger les vulnérabilités des alertes publiées par les CERT**
   1. alertes et avis du CERT_FR.
   2. alertes et avis CERT_EU.

3. **Déployer un EDR et le positionner en mode bloquant.**

4. **Mettre à jour vos modes de fonctionnement dégradés avec le prisme de la durée de l'indisponibilité d'au moins deux semaines.**

5. **Tester votre PCA PRA.**

6. **Rédiger et tester votre plan blanc numérique**