NOU VEY
CYBERSÉCURITÉ SANTÉ RÉUNION

FICHE REFLEXE EN CAS DE CYBERATTAQUE -DIRECTIONS-

L'établissement est touché par une cyberattaque, celle-ci peut affecter l'ensemble des services et devenir une crise sanitaire.

Dans l'immédiat avertir votre référent sécurité des systèmes d'information et avec son appui :

1. **Déconnecter du réseau et d'internet** les machines touchées (ordinateurs et serveurs) et **conserver les preuves** (mails reçus, journaux des équipements).
   Ne pas éteindre les machines.
   En cas d'une demande de rançon, **ne rentrez pas en contact avec l'attaquant, ne le payez pas.**

2. **Identifier le périmètre de l'attaque (secteur, métiers et outils impactés)** puis les référencer dans un compte rendu qui sera initié puis complété dans le temps.

3. **Réunir une cellule de crise constituée à minima de** la direction, du responsable informatique, du référent sécurité, des responsables de chaque filière métier et du responsable de la communication afin de :

   - ✓ **Tracer les évènements, en chargeant un des membres de la cellule d'établir un registre** (dates/heures, actions et décisions prises, acteurs impliqués)
   - ✓ **Confirmer et ajuster l'identification du périmètre (cf. 2.)**
   - ✓ **Identifier les actions et conséquences** sur la structure et **compléter le compte-rendu**

4. **Contacter le PRIS** (Prestataire de Réponse aux Incidents de Sécurité) ou le CERT SANTE (cf. annuaire au verso)

5. **Informer tout le personnel** de la situation et du déclenchement des modes dégradés (secteurs concernés, modalités de travail et de fonctionnement)

6. **Préparer une communication externe transparente de la situation,** sans entrer dans les détails que vous pourrez diffuser le moment venu selon l'ampleur et l'impact de l'attaque (presse, page internet, réseaux sociaux…)

7. **S'il y a une violation de données à caractère personnel, prévenir la CNIL dans les 72h** (cf. annuaire au verso)

8. Dès que vous avez qualifié l'incident, **déposer une main courante / une plainte à la police ou la gendarmerie et alerter vos assurances si des dommages sont avérés.**

NOU VEY
CYBERSÉCURITÉ SANTÉ RÉUNION

QUI PREVENIR ? ANNUAIRE APRES L'INCIDENT ?

Qui prévenir ? Annuaire :

- ✓ **Déclarer l'incident à la CNIL,** si cela concerne une violation des données à caractère personnel dans les 72h
  Adresse du téléservice : https://notifications.cnil.fr/notifications/index

- ✓ **Déclarer l'incident sur le portail de signalement des événements sanitaires indésirables** en cas d'impact sur le traitement des soins :
  Adresse du téléservice : https://signalement.social-sante.gouv.fr/psig_ihm_utilisateurs/index.html#/accueil

- ✓ **Le PRIS** (Prestataire de Réponse aux Incidents de Sécurité) :
  - Téléphone : +262 (0) 6 93 93 37 35 (Mathias Laurent RSSI et DPO GCS TESIS)
    TEMPORAIREMENT CAR EN COURS DE RENOUVELLEMENT
  - Email : incidents.cybersec@tesis.re *

- ✓ **Le CERT SANTE** :
  - Téléphone au +33 (0)9 72 43 91 25 (en urgence, 24h/24 et 7j/7)
  - Email : cyberveille@esante.gouv.fr

- ✓ **Police ou la gendarmerie** :
  - Par téléphone au 17
  - Au commissariat le plus proche

Après l'incident :

- ✓ Lorsque le ou les incidents ayant entrainé la crise ont été traités, **communiquer sur la résolution de la crise** (presse, page internet, réseaux sociaux…).

- ✓ **Organiser un retour d'expérience post incident et capitaliser** sur les évènements en vue d'une amélioration de la réponse à incident de sécurité et des différents processus en place dans votre organisation.

Important :

Ne pas tomber dans la précipitation. Des décisions inappropriées pourraient être prises et nuiraient à la bonne résolution de la crise.

* le PRIS, l'ARS et le GRADeS seront informés via cette adresse.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

ars Agence Régionale de Santé La Réunion

TESIS E-SANTÉ