AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

CH d'Armentières – Chiffrement des postes de travail et serveurs

Contexte d'intervention

CH Armentières

Centre Hospitalier d'Armentières

- Région : **Hauts-de-France**
- **Centre Hospitalier :**
  - En Direction commune avec le **CHU de Lille**, dessert un bassin de population de **200 000 habitants**
  - **200** personnels médicaux senior, et **1100** personnels non médicaux
  - **520** lits et places d'hospitalisation, plus de **40 000** passages aux Urgences en 2023

Origine(s) de la crise

- Intrusion sur le SI **au travers d'un compte VPN**
- **Prise de contrôle du domaine en tant qu'administrateur**
- Mise en œuvre de **mécanismes de persistance** sur le pare-feu

Impacts et Risques identifiés

Impacts

- **Chiffrement** des postes de travail et serveurs
- **Chiffrement** des sauvegardes

Risques

- **Exfiltration** de données

Chronologie des actions de l'attaquant

Décembre au 18/01

ACCES INITIAL ET RECONNAISSANCE

(ÉLÉVATION DES PRIVILÈGES)

19/01 au 23/01

PRISE DE CONTRÔLE ET DÉPLOIEMENT DES MÉCANISMES DE PERSISTANCE

27/01 au 09/02

PRÉPARATION DE L'ATTAQUE PRINCIPALE

(IMPACT SUR LES SAUVEGARDES, DÉPLOIEMENT DE LA CHARGE DE CHIFFREMENT)

Nuit du 10/02 au 11/02

EXÉCUTION DE L'ATTAQUE PRINCIPALE

(CHIFFREMENT DES POSTES)

*Evènements identifiés à postériori grâce à l'investigation

Chronologie détaillée de l'incident

Compromission et actions illégitimes

Actions de l'établissement

Décembre 2023 - 18 Janvier 2024

Accès initial

- Accès initial au Système d'information du CH Armentières
- Reconnaissance et Élévation de Privilèges

19 Janvier 2024

Prise de contrôle du Domaine

- Prise de contrôle du domaine (administrateur du domaine)

23 Janvier 2024 – 27 Janvier 2024

Déploiement d'outils

- Mise en œuvre de mécanismes de persistance sur le pare-feu
- Impacts sur la sauvegarde (arrêt des mécanismes de réplication et chiffrement)

9 Février - 11 février 2024

chiffrement

- Dépôt de l'executable de chiffrement
- Chiffrement des postes de travail et serveurs

11 février 2024

Première cellule de crise

- Déclenchement de la cellule de crise établissement au cours de la nuit
- Déclenchement du Plan Blanc

12 février 2024

Gestion dans la durée

- Mise en place de cellules de crise journalières
- Réouverture des urgences annoncée à J2 pour J3 – et tenue !

À partir du 12 février 2024

Relancer un Système d'information

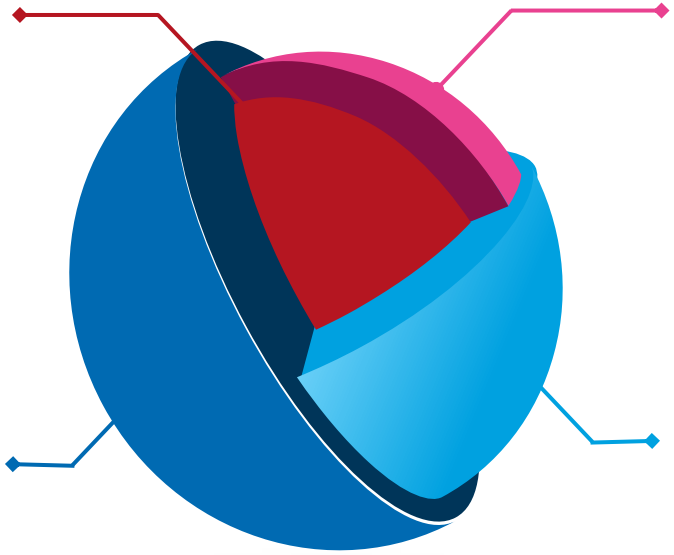
- Restauration des systèmes en fonction des priorisations des cellules de crise
- Pour une partie du SIH, reconstruction des systèmes

Accompagnement post- crise

ACTIONS MISES EN ŒUVRE PAR LE CENTRE HOSPITALIER D'ARMENTIÈRES LORS DE LA CRISE

1. Alerter les entités compétentes

Alerter IT locale, ARS, CERT Santé, ANSSI, Wavestone pour une intervention sur site (gestion de crise et appui technique)



2. Isolation du SI

Empêcher une propagation de l'attaque sur le reste du SI

3. Restauration et reconstruction des systèmes « en mieux »

Réalisées en fonction des priorisations des cellules de crise, en accord avec les métiers

4. Renforcement du PCRA

Renforcer le PCRA, à l'échelle de tout le GHT, suite à l'incident et aux leçons apprises

FÉVRIER 2024

ACTIONS MISES EN ŒUVRE EN SOUTIEN DE LA CRISE PAR LE CERT SANTÉ

/ Les principaux **axes mis en œuvre** sont :

- **Transmission de consignes** de remédiation
- **Relais des communications** aux RSSI et établissements
- **Co-pilotage des actions** d'investigation

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

Décembre 2023 :
Accès initial au système d'information du CH Armentières au travers d'un compte VPN

18 Janvier 2024 :
Reconnaissance et élévation de privilèges

19 Janvier 2024 :
Prise de contrôle du domaine en tant qu'administrateur

23 Janvier 2024 :
Mise en œuvre de mécanismes de persistance sur le pare-feu

27 Janvier 2024:
Impacts sauvegarde (arrêt des mécanismes de réplication et chiffrement)

9 Février :
Dépôt de la charge de chiffrement

11 février :
Chiffrement des postes de travail et serveurs

11 février :
Première cellule de crise établissement avant 6 heures
Déclenchement du Plan Blanc

Résultats et éléments clés

L'intrusion sur le SI s'est effectuée au travers d'un **compte VPN**. Une prise de contrôle du domaine au niveau administrateur a ensuite été réalisée, suivie par la **mise en œuvre de mécanismes de persistances**.

L'attaquant a pu **chiffrer les serveurs et les postes de travail** du SI du Centre Hospitalier d'Armentières

Points à retenir

1

L'importance du **PCRA et des exercices**

- Toutes les données importantes/sensibles doivent être identifiées et sécurisées
- Entrainement lors des exercices des 6 derniers mois et les RETEX associés
- Les contraintes d'un fonctionnement en mode dégradé sur une longue durée doivent être prise en compte

2

L'importance de la **collaboration et de la réactivité des acteurs** pour la **résolution d'incident** de sécurité

- Implication du CHU de Lille, SAMU, ARS, EFS, ANSSI et du CERT Santé
- Travail conjoint sur les mesures de remédiation suite à l'identification des faiblesses du SI

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé