AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Handi Val de Seine – Compromission du SI suite à l'exploitation d'une vulnérabilité VPN critique

Contexte d'intervention

Handi Val de Seine

- Département : **Yvelines (Seine-Aval)**
- Handi Val de Seine, **une structure unique :**
  - Répartis sur **35 communes**
  - **20 établissements et services**
  - **+ 500 postes utilisateurs**
  - **55** machines virtuelles
  - **8** serveurs physiques

Origine(s) de la crise

- L'attaquant s'est potentiellement **connecté à distance** au travers d'un **accès VPN porté par un routeur ZYXEL**
- Le **rançongiciel « BABUK » a été identifié** suite aux investigations

Risques identifiés*

- **Prise de contrôle à distance** des équipements
- **Compromission d'identifiants de plusieurs comptes à privilèges**
- **Perte irréversible des données et des ressources** (données, comptabilité, etc.)
- **Fuite / vol de données sensibles** des patients et/ou des collaborateurs

** Enumération des risques identifiés en cas de succès de l'attaque.*

Chronologie des événements de la crise

Détection de l'incident

23 février

24 février

Signalement au CERT Santé et début de la prise en charge

Lancement des actions de confinement
Isolation totale du SI

25-26 février

2-6 mars

Reprise d'activité supervisée

Fin de la période de crise
Poursuite du plan de remédiation/durcissement

14-15 mars

*Evènements identifiés à postériori grâce à l'investigation

Chronologie détaillée de la crise

Actions de l'établissement Handi Val de Seine

Accompagnement du CERT Santé

23 février 2023

Détection de l'incident

- Découverte du rançongiciel
- débranchement de la baie réseau (demande du RSI)
- Lancement des investigations en interne

24 février 2023

Signalement de l'incident

- Ouverture de la cellule de crise
- Déclaration de l'incident (CERT Santé, CNIL..)
- Dépôt de plainte

24 février 2023

Début de prise en charge par le CERT Santé

- Réception du signalement et prise de contact avec l'établissement
- Partage du plan d'action contenant les premières recommandations de confinement
- Début des investigations

25-26 février 2023

Lancement des actions de confinement

- Isolation totale du SI
- Reprise des serveurs compromis

27 février 2023

Recentrage du plan de gestion de crise

- Poursuite des actions de remédiation

2 mars 2023

Recommandations du cert sante

- Identification des flux vitaux pour l'établissement
- Réouverture des flux au cas par cas
- Sauvegardes locales pour assurer la continuité de service des usagers du SI (proposé par le RSI de l'établissement)

2-6 mars 2023

Reprise d'activité supervisée

- Choix de redémarrage des serveurs sous supervision (EDR)
- Analyse des besoins métiers liés au SI

14-15 mars 2023

Fin de la période de crise

- Réouverture des flux en discussions avec le département des Yvelines
- Poursuite de la mise en œuvre du plan de remédiation/durcissement

Accompagnement post- crise

MAI-JUIN 2023

MISE EN PLACE DU PLAN D'ACCOMPAGNEMENT LONG TERME

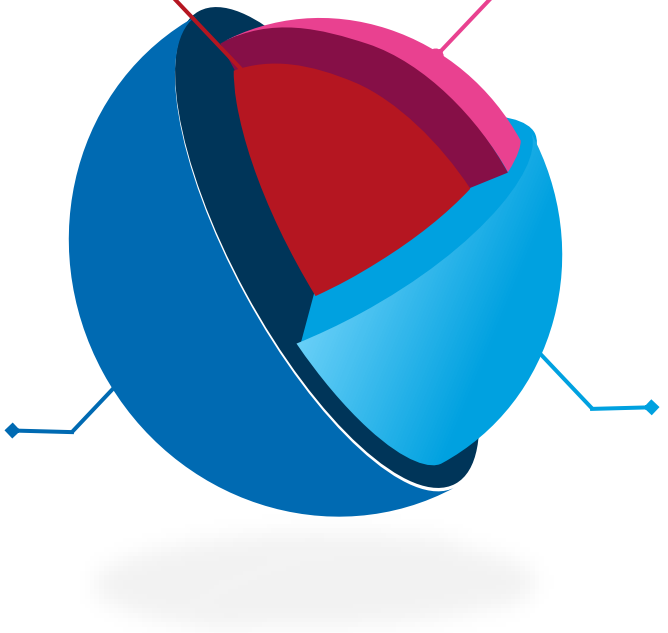
/ Les principaux **axes mis en œuvre** sont :

- Renforcement du **Plan de Reprise d'Activités (PRA)**
- **Limitation de l'obsolescence** du parc informatique (plus particulièrement sur les machines/équipements critiques)
- **Durcissement** des machines/équipements
- **Amélioration** des **pratiques** d'administration du système d'information
- Maintien dans le temps du **niveau de sécurité**

Les étapes du déploiement du plan de remédiation

1. Socle du SI (firewall, etc.)
S'assurer que le cœur du système d'information est sécurisé et à jour

2. Services métiers
Contrôler les périmètres métiers et reprendre peu à peu un usage standard



4. Renforcement du PRA
Renforcer le PRA suite à l'incident et aux leçons apprises.

3. Réouverture des flux réseaux
Réouvrir les flux réseaux moins prioritaires

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

23 Février 2023 :
Début de la crise grâce à l'alerte remontée par la secrétaire de HVS. Coupure réseau + machines

24 Février 2023 :
Signalement de l'incident et déploiement de la cellule de crise. Début de prise en charge par le CERT Santé

25-26 Février 2023 :
Mise en place d'un confinement SI adapté à l'architecture système. Collecte des artefacts liés à l'attaque.

27 Février 2023 :
Reprise des actions réalisées pendant le week-end. Recentrage du plan de gestion de crise

2-6 Mars 2023 :
Reprise d'activité supervisée

15 Mars 2023 :
Fin de période de crise, continuité du plan de remédiation par les équipes de la DSI. (Remédiation interne)

Mai-Juin 2023 :
Mise en place du plan d'accompagnement long terme. Durcissement système

Résultats et éléments clés

L'attaquant **a exploité une vulnérabilité critique et non corrigée sur un accès VPN** pour se connecter avec des privilèges au système d'information interne.

Des **impacts ont été identifiés** sur les **services administratifs en raison de la perte de certaines bases de données.**

Points à retenir

1. Lors d'une crise, la **communication entre les acteurs externes et internes à l'établissement** est une des clés de la réussite.

2. **Identifier** quelles sont les **données vitales** pour le fonctionnement de l'établissement de santé.

3. Identifier les **équipements informatiques essentiels et les plus critiques** pour le système d'Information. Créer un **plan de maintien en conditions opérationnelles** cohérent avec les priorités précédemment établies.