AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé

Retour d'Expérience

Incident du Centre Hospitalier de Cahors

Contexte d'intervention

Centre Hospitalier de CAHORS

/ Région : **Occitanie**

/ Département : **Lot**

/ **Principal établissement de santé du département**

- **1 des 5** grands centres hospitaliers du Lot pour 171 000 habitants
- **365 lits** disponibles avec plus, de **1000 agents permanents** (en 2022)
- Environ **171 médecins** (en 2019)
- **1400 postes utilisateurs**
- 4 contrôleurs de domaine
- 50 serveurs

Origine(s) de la crise

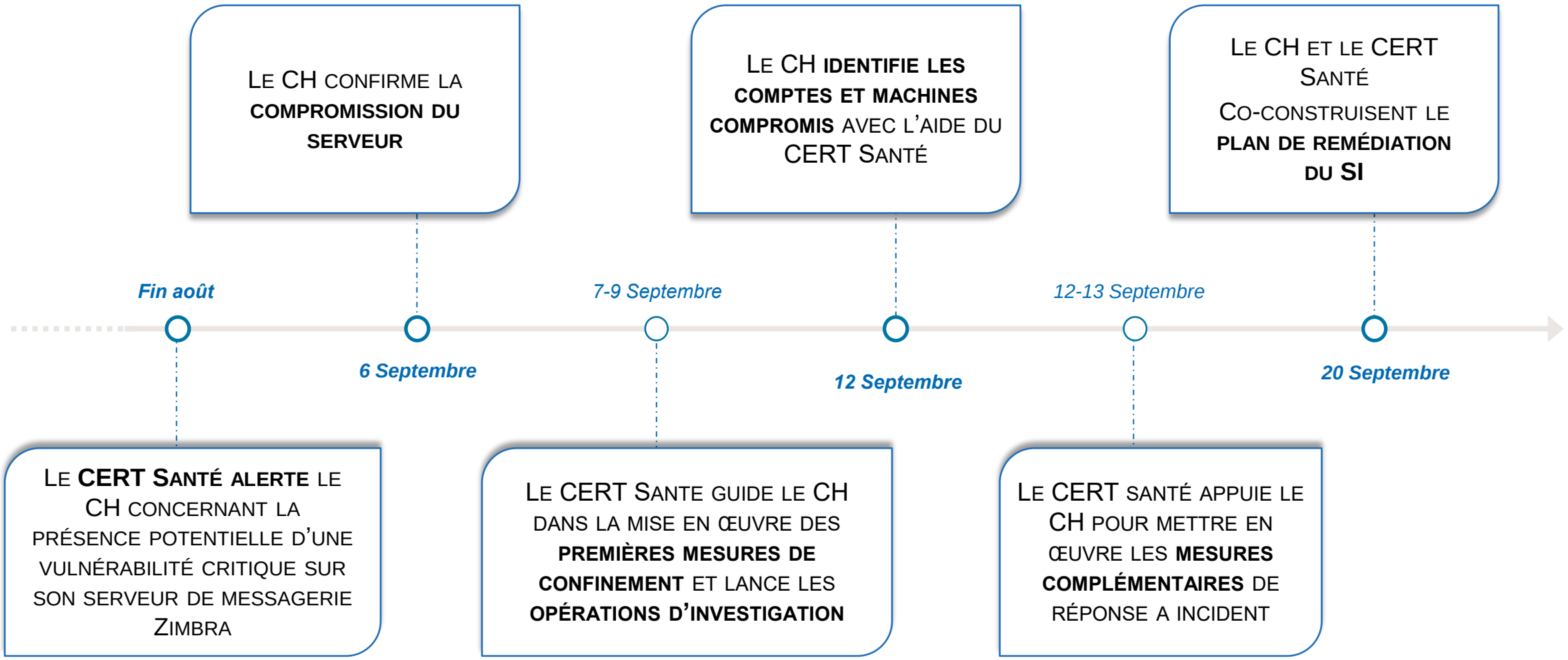
- **Alerte du 23.08.2022 du CERT Santé**
- Système concerné : Serveur de Messagerie
  - **Zimbra Collaboration versions 8.8.15** ne disposant pas du correctif de sécurité « Patch 33 »
  - **Zimbra Collaboration versions 9.0.0** ne disposant pas du correctif de sécurité « Patch 26 »
- **Exploitation** d'une **vulnérabilité critique** (CVE-2022-37042) permettant une exécution de code arbitraire

Risques identifiés*

- **Prise de contrôle à distance** des équipements
- **Chiffrement des données et des systèmes** par le biais d'un rançongiciel provoquant l'**indisponibilité des ressources**
- **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



Chronologie détaillée de la crise

Actions du CENTRE HOSPITALIER

Accompagnement du CERT Santé

31 AOÛT 2022
PRISE EN CHARGE DE L'ALERTE PAR LE CH

- **DÉPLOIEMENT DU CORRECTIF** SUR LE SERVEUR DE MESSAGERIE PAR LE PRESTATAIRE

6 SEPTEMBRE 2022
MISE EN PLACE DES MOYENS NÉCESSAIRES ET CONFIRMATION DE LA COMPROMISSION DU SERVEUR DE MESSAGERIE

- PREMIÈRE MESURE DE SURETÉ : **DÉCONNEXION DU SERVEUR**
- **DÉCLARATION DE L'INCIDENT** COMME **RÉSOLU** SUR LE PORTAIL DÉDIÉ ET AUCUNE DEMANDE D'ACCOMPAGNEMENT AUPRÈS DU CERT SANTÉ

7 SEPTEMBRE 2022
IDENTIFICATION D'ACTIONS MALVEILLANTES RÉALISÉES SUITE À LA COMPROMISSION

- INVESTIGATIONS DU CH : L'ATTAQUANT RÉALISAIT DES **ACTIONS DE MINAGE DE CRYPTOMONNAIE**
  - AUCUNE MODIFICATION DES CODES SECRET OU DE RÉINSTALLATION DU SERVEUR N'A ÉTÉ EFFECTUÉ

9 SEPTEMBRE 2022
SUITE DES INVESTIGATIONS SUR L'ÉTENDU DE LA COMPROMISSION

- CONFIRMATION PAR LE CENTRE HOSPITALIER QUE LE **SERVEUR ZIMBRA UTILISAIT UNE AUTHENTIFICATION AD** POUR LES CLIENTS, CELLE-CI EST AUSSI **UTILISÉE PAR LE VPN DE LA STRUCTURE**

12 & 13 SEPTEMBRE 2022
COLLABORATION AVEC LE CERT SANTÉ DANS LA RÉPONSE À INCIDENT

- **MISE EN PLACE DE NOUVELLES MESURES DE CONFINEMENT** PRÉCONISÉES PAR LE **CERT SANTÉ :**
  - ISOLATION DU SI ET FIN DE LA SESSION ILLÉGITIME
  - DÉCONNEXION DU SERVEUR DE SAUVEGARDE PHYSIQUE
  - DÉSACTIVATION DES ACCÈS EXTERNES À LA MESSAGERIE AINSI QU'AU VPN ET COMPTES ADMINISTRATEURS COMPROMIS
  - BLOCAGE DES PIÈCES JOINTES EN ENTRÉE
  - CHANGEMENT DES MOTS DE PASSE EXPOSÉS SUR INTERNET
- **CO-CONSTRUCTION** AVEC LE CERT SANTÉ D'UN **PLAN D'ACTIONS POUR MENER LA SUITE DES INVESTIGATIONS** (VÉRIFICATION D'ABSENCE DE CHIFFREMENT DES ÉQUIPEMENT, ANALYSE DES FLUX ET DES INTERCONNEXIONS, COLLECTE DES LOGS ET VÉRIFICATION DE LA LÉGITIMÉ DES COMPTES)

14 & 15 SEPTEMBRE 2022
FILTRAGE ET RÉOUVERTURE PROGRESSIVE DES FLUX ET INTERCONNEXIONS VITAUX

- **DÉPÔT DE PLAINTE** ET **DÉCLARATION D'INCIDENT** AUPRÈS DE LA **CNIL**
- **COMMUNICATION EN INTERNE** AUPRÈS DES UTILISATEURS

23 AOÛT
LANCEMENT D'ALERTE PAR CYBERVEILLE SUR L'EXPLOITATION DE FAILLES ZIMBRA

- **NOTIFICATION À 26 ÉTABLISSEMENTS** POTENTIELLEMENT VULNÉRABLES

31 AOÛT 2022
DEMANDE D'INVESTIGATION DU CERT SANTÉ

- **DEMANDE** DE **VÉRIFICATION D'ABSENCE DE COMPROMISSIONS** SUR LE SERVEUR

9 SEPTEMBRE 2022
SUSPICION DU CERT SANTÉ SUR L'ÉLARGISSEMENT DU PÉRIMÈTRE IMPACTÉ

- **CONSEIL DU CERT SANTÉ** DE POURSUIVRE LES INVESTIGATIONS ET **ORGANISATION D'UNE RÉUNION ENTRE EXPERTS**

12 SEPTEMBRE 2022
COLLABORATION POUR DÉTECTER LA COMPROMISSION AVANCÉE DU CH

- IDENTIFICATION DE LA **COMPROMISSION D'UN COMPTE ADMINISTRATEUR** DE DOMAINE SUITE À L'APPUI TECHNIQUE POUR LA COLLECTE ET L'ANALYSE DES LOGS
- **INTERVENTION EXCEPTIONNELLE EN HNO** POUR APPUYER LE CH

20 SEPTEMBRE 2022
"SORTIE DE CRISE"

- PRÉPARATION D'UN **PLAN DE REMÉDIATION** SUITE À L'IDENTIFICATION D'AXES PRIORITAIRES
- COMMUNICATION INTERNE AUPRÈS DES UTILISATEURS DU CH DE **PROSCRIRE L'USAGE DES CLEFS 4G / SMARTPHONE**

Accompagnement post- crise

13 au 16 SEPTEMBRE 2022

Définition d'un plan de remédiation et Accompagnement du CERT Santé

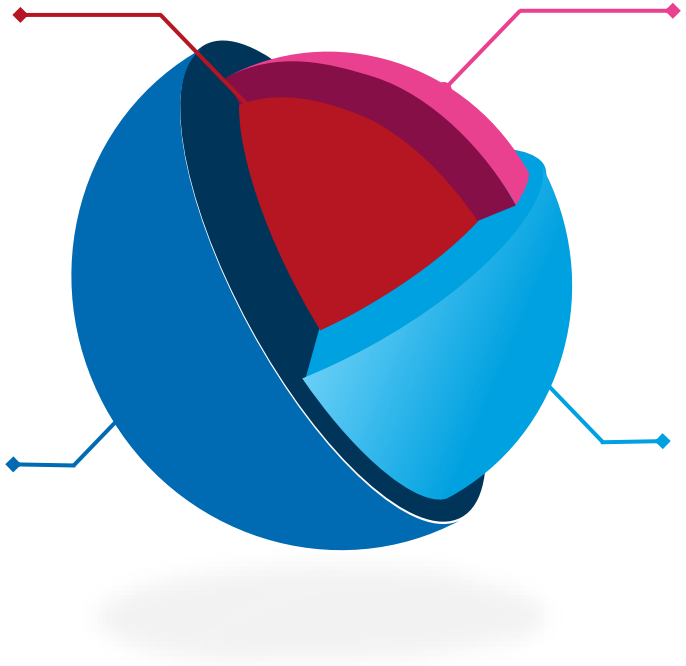
/ Les principaux **axes mises en œuvre** sont :

- **Segmentation réseau** du système d'information
- **Limitation** de **l'obsolescence** du parc informatique (plus particulièrement sur les machines/équipements critiques)
- **Durcissement** des machines/équipements
- **Changement** 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



2. Services métiers et la messagerie

Contrôler les périmètres métiers et reprendre peu à peu un usage standard

3. Autres services / serveurs

Rouvrir les services, serveurs moins prioritaires

4. Postes de travail

Remettre en service les postes de travail pour tous les collaborateurs

Bilan de l'accompagnement durant la crise

Rappel de la chronologie des évènements

23 - 31 août 2022 :
Lancement de l'alerte par Cyberveille. Retour et prise en compte de l'alerte par le CH de Cahors

31 août 2022 :
Demande du CERT Santé d'investiguer sur une éventuelle compromission

6-7 septembre 2022 :
Investissement des équipes du CH de Cahors et confirmation de la compromission du serveur de messagerie et déconnexion des serveurs concernés

9 septembre 2022 :
Suspicion du CERT Santé sur l'élargissement du périmètre impacté

12-13 septembre 2022 :
Confirmation de l'extension du périmètre et collaboration avec le CERT Santé dans la réponse à incident et la mise en place de mesures de confinement après un appui technique sur la collecte et l'analyse des logs

20 septembre 2022 :
Sortie de crise et préparation du plan de remédiation

Résultats et éléments clés

L'alerte du CERT Santé et l'investissement du Centre Hospitalier de Cahors ont permis d'**éviter une compromission majeure du système d'information** de l'établissement

Les **données** des dossiers patients **n'ont pas été impactées par l'attaque car elles étaient hébergés chez** un "prestataire certifié hébergeur de données de santé« (HDS)

Des **impacts identifiés** sur les **services administratifs en raison de la déconnexion des serveurs de messagerie**

Points à retenir

1. La remontée et la prise en compte de l'alerte, la collaboration du Centre Hospitalier de Cahors et du CERT Santé et l'investissement des deux équipes ont permis de circonscrire rapidement l'incident.
   - Alerte issue de Cyberveille
2. **Une mise à disposition d'experts en cybersécurité pour les établissements** afin de les accompagner et les aider face à ces situations complexes
   - Accompagnement au déploiement des capacités et moyens nécessaires afin de réaliser des investigations plus poussées
3. Importance de la **collaboration** pour la **résolution d'incident** de sécurité
   - Travail conjoint sur les mesures de remédiation suite à l'identification des faiblesses intrinsèques au SI et réalisation d'investigation afin de confirmer les hypothèses de la compromission

AGENCE DU NUMÉRIQUE EN SANTÉ

CERT Santé