ETUDE DE CAS / SANTÉ / FRANCE

# Comment un compte compromis a perturbé un hôpital

En mars 2025, le CHD Stell de Rueil-Malmaison a subi une attaque par rançongiciel. Un ancien compte administrateur a permis l'intrusion puis la propagation aux serveurs de l'établissement. [1]



**RUEIL-MALMAISON**

CHD STELL / MARS 2025

## CHRONOLOGIE DE L'ATTAQUE [1]

### 1 COMPROMISSION INITIALE

**4 puis 17 mars 2025**

Réactivé pour un audit, un compte administrateur de domaine au mot de passe faible ouvre l'accès via le VPN.

### 2 ABUS DE PRIVILÈGES

**22 mars 2025**

L'attaquant accède au contrôleur de domaine et y installe un service de persistance.

### 3 PROPAGATION ET CHIFFREMENT

**28 mars 2025**

L'attaquant gagne d'autres serveurs du réseau et chiffre les serveurs Windows.

### 4 CRISE ET REPRISE

**Dès le 31 mars 2025**

Le chiffrement est constaté. Les flux VPN sont coupés. L'Active Directory est reconstruit du 7 au 10 avril.

## MESURES DE PRÉVENTION [1, 3]

### Maîtriser le cycle de vie des comptes

- Revoir les comptes et leurs droits
- Utiliser des mots de passe robustes
- Activer l'authentification multifacteur

### Encadrer les accès à privilèges

- Appliquer le moindre privilège
- Tracer et superviser les sessions sensibles

### Freiner les déplacements latéraux

- Séparer les niveaux d'administration
- Surveiller les connexions inhabituelles

### Impact documenté [1]

- Certains soins indisponibles ou ralentis
- Gestion administrative des patients et des repas indisponible
- Accès au dossier patient difficile

## CE QUE NIS2 PRÉVOIT [2]

Pour les entités concernées dans l'UE, des mesures proportionnées au risque.
La gestion des accès à privilèges peut contribuer à ces objectifs.

### Exigences de l'article 21

- Politiques de contrôle d'accès
- Authentification multifacteur ou continue, selon les besoins
- Gestion des incidents
- Continuité, sauvegardes et reprise

SOURCES : [1] CERT Santé, RETEX CHD Stell (2025), p. 2-6 | [2] Directive (UE) 2022/2555, art. 21 [3] ANSSI, Sécurité des SI hybrides (10/08/2021) | Mise à jour éditoriale : 21/10/2026

Découvrez comment la gestion des accès à privilèges aide à renforcer votre conformité NIS2

wallix

L'alternative européenne de confiance pour la sécurité des identités et des accès

www.wallix.com