CASO REAL / SANIDAD / FRANCIA

Cómo una cuenta comprometida afectó a un hospital



RUEIL-MALMAISON

CHD STELL / MARZO 2025

En marzo de 2025, el CHD Stell de Rueil-Malmaison sufrió un ataque de ransomware. Una antigua cuenta de administrador permitió la intrusión y la posterior propagación a los servidores del hospital. [1]

CRONOLOGÍA DEL ATAQUE [1]

1 COMPROMISO INICIAL

4 y 17 de marzo de 2025

Reactivada para una auditoría, una cuenta de administrador del dominio con contraseña débil permitió el acceso VPN.

2 ABUSO DE PRIVILEGIOS

22 de marzo de 2025

El atacante accedió al controlador de dominio e instaló un servicio de persistencia.

3 PROPAGACIÓN Y CIFRADO

28 de marzo de 2025

El atacante se desplazó a otros servidores de la red y cifró servidores Windows.

4 CRISIS Y RECUPERACIÓN

Desde el 31 de marzo de 2025

Se detectó el cifrado y se bloqueó el tráfico VPN. Active Directory se reconstruyó del 7 al 10 de abril.

MEDIDAS PREVENTIVAS [1, 3]

Gestionar el ciclo de vida de las cuentas

- Revisar las cuentas y sus permisos
- Utilizar contraseñas robustas
- Activar la autenticación multifactor

Controlar los accesos privilegiados

- Aplicar el principio de mínimo privilegio
- Registrar y supervisar las sesiones sensibles

Limitar el movimiento lateral

- Separar los niveles de administración
- Supervisar las conexiones inusuales

Impacto documentado [1]

- Parte de la atención no disponible o retrasada
- Gestión administrativa de pacientes y de comidas no disponible
- Dificultades de acceso a historias clínicas

REQUISITOS DE NIS2 [2]

Las entidades sujetas a NIS2 en la UE deben adoptar medidas proporcionales al riesgo. La gestión de accesos privilegiados puede contribuir a estos objetivos.

Requisitos del artículo 21

- Políticas de control de acceso
- Autenticación multifactor o continua, cuando proceda
- Gestión de incidentes
- Continuidad, copias de seguridad y recuperación

FUENTES: [1] CERT Santé, CHD Stell (2025), págs. 2-6 | [2] Directiva (UE) 2022/2555, art. 21
[3] ANSSI, Administración segura de sistemas de información (versión 3) | Actualización editorial: 22/10/2026

Descubra cómo la gestión de accesos privilegiados ayuda a reforzar su cumplimiento de NIS2

wallix

La alternativa europea de confianza para proteger identidades y accesos

www.wallix.com