

Cómo los fallos en la gestión de accesos acabaron en una crisis nacional

El ciberataque sufrido en 2021 por el Health Service Executive (HSE) de Irlanda demostró cómo una gestión deficiente de los accesos puede transformar una intrusión limitada en una crisis nacional.



1 ACCESO INICIAL
Los atacantes accedieron al entorno utilizando credenciales comprometidas.

Principales fallos de acceso

- › Falta de visibilidad sobre la actividad privilegiada
- › Supervisión insuficiente de las sesiones

2 MOVIMIENTO LATERAL SIN DETECCIÓN
Los atacantes permanecieron dentro de la red durante casi dos meses, desplazándose entre sistemas sin ser detectados.

Principales fallos de acceso

- › Ausencia de monitorización en tiempo real
- › Exceso de privilegios de acceso
- › Escasa contención del movimiento lateral

3 ESCALADA DE PRIVILEGIOS
Las cuentas comprometidas evolucionaron hasta obtener accesos privilegiados de alto nivel.

Principales fallos de acceso

- › Controles débiles sobre accesos privilegiados
- › Falta de aplicación del principio de mínimo privilegio

4 IMPACTO OPERATIVO
Los sistemas sanitarios en toda Irlanda sufrieron graves interrupciones.

Impacto

- Servicios afectados en todo el país
- Sistemas críticos fuera de servicio
- Importante impacto operativo y financiero



LO QUE EXIGE LA NIS2

La NIS2 exige que mantengas una visibilidad continua sobre la actividad privilegiada y puedas demostrar control en cualquier momento.

Áreas clave de la directiva

- › Supervisión en tiempo real de las sesiones
- › Control de identidades privilegiadas
- › Trazabilidad de la actividad de acceso
- › Respuesta más rápida ante incidentes

Descubre cómo la gestión de accesos privilegiados te ayuda a **reforzar el cumplimiento de NIS2**

wallix

La alternativa europea de confianza para la seguridad de identidades y accesos

www.wallix.com