FALLSTUDIE / GESUNDHEITSWESEN / FRANKREICH

Wie ein kompromittiertes Konto ein Krankenhaus beeinträchtigte

Im März 2025 wurde das CHD Stell in Rueil-Malmaison Opfer eines Ransomware-Angriffs. Ein altes Administratorkonto ermöglichte den ersten Zugriff und die anschließende Ausbreitung auf die Krankenhausserver. [1]



RUEIL-MALMAISON

CHD STELL / MÄRZ 2025

ANGRIFFSVERLAUF [1]

1 ERSTE KOMPROMITTIERUNG

4. und 17. März 2025

Für ein Audit reaktiviert, bot ein Domänenadmin-Konto mit schwachem Passwort Zugriff über das VPN.

2 MISSBRAUCH VON RECHTEN

22. März 2025

Der Angreifer griff auf den Domänencontroller zu und richtete einen Dienst zur Persistenz ein.

3 AUSBREITUNG UND VERSCHLÜSSELUNG

28. März 2025

Der Angreifer erreichte weitere Server im Netzwerk und verschlüsselte Windows-Server.

4 KRISE UND WIEDERHERSTELLUNG

Ab 31. März 2025

Verschlüsselung entdeckt, VPN-Verkehr blockiert. Active Directory vom 7. bis 10. April neu aufgebaut.

SCHUTZMASSNAHMEN [1, 3]

Lebenszyklus von Konten steuern

- Konten und Berechtigungen prüfen
- Starke Passwörter verwenden
- Mehrfaktor-Authentifizierung aktivieren

Privilegierte Zugriffe kontrollieren

- Prinzip der minimalen Rechte anwenden
- Sensible Sitzungen protokollieren und überwachen

Lateralbewegungen begrenzen

- Administrative Berechtigungsebenen trennen
- Ungewöhnliche Verbindungen überwachen

Dokumentierte Folgen [1]

- Einzelne Behandlungen nicht oder später verfügbar
- Patienten- und Verpflegungsverwaltung nicht verfügbar
- Zugriff auf Patientenakten erschwert

NIS2-ANFORDERUNGEN [2]

Erfasste Einrichtungen in der EU müssen risikogerechte Maßnahmen treffen. Die Verwaltung privilegierter Zugriffe kann diese Ziele unterstützen.

Anforderungen nach Artikel 21

- Regeln zur Zugriffskontrolle
- Mehrfaktor- oder kontinuierliche Authentifizierung nach Bedarf
- Bewältigung von Sicherheitsvorfällen
- Kontinuität, Backups und Wiederherstellung

QUELLEN: [1] CERT Santé, CHD Stell (2025), S. 2–6 | [2] Richtlinie (EU) 2022/2555, Art. 21 [3] ANSSI, Sichere Administration von IT-Systemen (Version 3) | Stand: 22.10.2026

Erfahren Sie, wie die Verwaltung privilegierter Zugriffe Ihre NIS2-Compliance unterstützen kann

wallix

Die vertrauenswürdige europäische Alternative für Identitäts- und Zugriffssicherheit

www.wallix.com