Wie Schwachstellen in der Zugriffskontrolle in einer nationalen Krise endeten

Der Cyberangriff auf den irischen Health Service Executive (HSE) im Jahr 2021 zeigte, wie schwache Access Governance aus einem begrenzten Sicherheitsvorfall eine nationale Krise machen kann.

1 Erster Zugriff

Die Angreifer verschafften sich über kompromittierte Zugangsdaten Zugriff auf die Umgebung.

Zentrale Schwachstellen

- Keine Transparenz über privilegierte Aktivitäten
- Unzureichende Überwachung von Sitzungen

2 Unbemerkte laterale Bewegung

Die Angreifer bewegten sich fast zwei Monate lang unbemerkt innerhalb des Netzwerks und breiteten sich zwischen verschiedenen Systemen aus.

Zentrale Schwachstellen

- Keine Echtzeitüberwachung
- Zu weitreichende Zugriffsrechte
- Unzureichende Eindämmung lateraler Bewegungen

3 Eskalation von Berechtigungen

Kompromittierte Konten entwickelten sich zu hoch privilegierten Zugängen.

Zentrale Schwachstellen

- Schwache Kontrollen für privilegierte Zugriffe
- Fehlende Umsetzung des Least-Privilege-Prinzips

4 Operative Auswirkungen

Gesundheitssysteme in ganz Irland waren massiv beeinträchtigt.

Auswirkungen

- Landesweite Störungen von Services
- Kritische Systeme nicht verfügbar
- Erhebliche operative und finanzielle Folgen

Was NIS2 jetzt verlangt

NIS2 verpflichtet Unternehmen dazu, privilegierte Aktivitäten kontinuierlich transparent zu überwachen und jederzeit Kontrolle nachweisen zu können.

Schwerpunkte von NIS2

- Echtzeitüberwachung von Sitzungen
- Kontrolle privilegierter Identitäten
- Nachvollziehbarkeit von Zugriffsaktivitäten
- Schnellere Reaktion auf Sicherheitsvorfälle

Erfahren Sie, wie Privileged Access Management Sie bei der Umsetzung von NIS2 unterstützt

wallix

Europas vertrauenswürdige Alternative für Identity- und Access-Security

www.wallix.com