Comment un accès compromis à mené à une crise nationale

La cyberattaque menée en 2021 contre le Health Service Executive (HSE) irlandais a montré comment une gouvernance insuffisante des accès peut transformer une simple intrusion en crise nationale.

1 COMPROMISSION INITIALE

Les pirates ont pénétré l'environnement à l'aide d'identifiants compromis.

Principales failles d'accès

- Absence de visibilité sur les activités à privilèges
- Supervision insuffisante des sessions

2 DÉPLACEMENTS LATÉRAUX NON DÉTECTÉS

Les attaquants sont restés présents dans le réseau pendant près de deux mois, en se déplaçant entre les systèmes sans être détectés.

Principales failles d'accès

- Absence de supervision en temps réel
- Droits d'accès trop étendus
- Manque de maîtrise des déplacements latéraux

3 ESCALADE DES PRIVILÈGES

Les comptes compromis ont permis d'obtenir des accès à privilèges élevés.

Principales failles d'accès

- Contrôles insuffisants des accès à privilèges
- Absence d'application du principe du moindre privilège

4 IMPACT OPÉRATIONNEL

Les systèmes de santé à travers toute l'Irlande ont été fortement perturbés.

Impact

- Services perturbés à l'échelle nationale
- Systèmes critiques indisponibles
- Impact opérationnel et financier majeur

CE QUE NIS2 EXIGE

NIS2 impose désormais aux organisations de maintenir une visibilité continue sur les accès à privilèges et de pouvoir justifier leur niveau de contrôle en à tout moment.

Axes clés de la Directive

- Supervision des sessions en temps réel
- Contrôle des identités et des privilèges
- Traçabilité des sessions des accès
- Réactivité renforcée face aux incidents

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