How access failures turned a ransomware intrusion into a national crisis

The 2021 cyberattack on Ireland's Health Service Executive (HSE) showed how weak access governance can turn a limited intrusion into a national crisis.

1 INITIAL COMPROMISE

Attackers entered the environment using compromised credentials.

Key access failures

- No visibility over privileged activity
- Weak session monitoring

2 UNDETECTED LATERAL MOVEMENT

Attackers remained inside the network for nearly two months, moving across systems without detection.

Key access failures

- No real-time monitoring
- Excessive access rights
- Poor containment of lateral movement

3 PRIVILEGE ESCALATION

Compromised accounts evolved into high-level privileged access.

Key access failures

- Weak privileged access controls
- Lack of least-privilege enforcement

4 OPERATIONAL DISRUPTION

Healthcare systems across Ireland were severely disrupted.

Impact

- Services disrupted nationwide
- Critical systems unavailable
- Significant operational and financial impact

WHAT NIS2 NOW EXPECTS

NIS2 now requires organisations to maintain continuous visibility over privileged activity and demonstrate control at any moment.

NIS2 focus areas

- Real-time session monitoring
- Privileged identity control
- Auditability of access activity
- Faster incident response

See how privileged access management helps support NIS2 compliance

wallix

Europe's trusted alternative for Identity and Access Security

www.wallix.com