AEREN LPO
...providing more with much less

Cyber Incident Response

RANSOMWARE INCIDENT

Scenario

A sudden lockout of all laptops and systems triggered widespread ransomware alerts across multiple departments of a large healthcare provider. A ransom demand with a 78-hour deadline was identified, prompting immediate escalation and incident response measures. The organization swiftly notified the supervisory authority and initiated a comprehensive post-breach investigation to identify affected individuals and issue notifications in full compliance with regulatory requirements.

NEXT STEPS:

The provider rapidly preserves, processes, and analyzes potentially compromised electronically stored information (ESI) to assess the scope of the breach. The next phase focuses on identifying affected customers and sensitive data—including personally identifiable information (PII), protected health information (PHI). By leveraging the advanced analytics and review workflows of its Partner, the Provider generated an accurate and defensible notification list, ensuring that all regulatory reporting requirements and strict notification timelines were met.

AEREN'S ROLE:

Aeren partners with such organizations to deliver a fast, auditable, end-to-end response solution tailored to ransomware incidents within regulated environments.

Our comprehensive support includes:

- **Immediate native processing and indexing** of preserved ESI (emails, files, logs, and archives) to make data instantly searchable while maintaining data integrity.
- **Hybrid review model:** combining automated triage with targeted manual team review to confirm the presence of sensitive information and capture key data elements (names, SSNs, policy numbers, dates of birth, health data categories, etc.).
- **Deduplication and automated analysis** of junk and structured/unstructured files to significantly reduce review volume.
- **Preparation of a validated notification** list containing affected individuals, categories of compromised data, and an accompanying evidence trail for legal and regulatory review
- **Comprehensive reporting** to support organizations in meeting regulatory inquiries and internal governance requirements.