HEALTHCARE SECURITY & COMPLIANCE

SANS | GIAC CERTIFICATIONS

Ransomware + Healthcare: A Deadly Combination

Ransomware is not only becoming a more prevalent threat to all industries, but it also presents a triple-threat to healthcare:

- **Availability -** It threatens the availability of information and systems, directly impacting patient care.
- **Confidentiality -** It has evolved into "blackmail-ware," threatening patients' right to privacy.
- Ransomware infection is likely a **HIPAA-reportable event**.

Unless the covered entity or business associate can demonstrate that there is a "...low probability that the PHI has been compromised," based on the factors set forth in the Breach Notification Rule, a breach of PHI is presumed to have occurred (per hhs.gov).

Ransomware in the healthcare industry affects ability to care for patient and could even lead to death!

Maturity Model of Ransomware:

- 1986 First ransomware "attack." Ransom was paid through the mail!
- 2006 Internet ransomware started. Advanced encryption techniques and introduction of Bitcoin!
  - Scattershot techniques. High volume/low ransom
- 2021 Attackers know who they are attacking, and what data they are encrypting.
  - Customized ransoms. Negotiated payments.
  - Introduction of RaaS (Ransomware as a Service)
    - A more sophisticated business model.
    - Separate creators, distributors, customer service divisions.
    - Ransom is collected and split amongst multiple roles.
  - Introduction of blackmail-ware: The stealing of data before encryption.
  - Introduction of professional ransomware negotiators.

Vectors of Ransomware:

- Phishing emails with malicious attachments
- Phishing emails with malicious links
- Malvertising

2020 Healthcare Stats:

- 92 Ransomware attacks
- 600 organizations
- 18 million patient records
- $20.8B in ransom, downtime, recovery, etc.

What to do?

- Backup your data! Test your backups!
- Reduce user privileges
- User behavior monitoring
- User training and awareness
- Use Domain Blocklist and Allowlist

www.sans.org/blog/sans-healthcare-security-resources