How to Protect Against Ransomware in Healthcare

Ransomware is the ultimate scourge on healthcare. It locks your systems and data until you pay up. In an industry where every second counts, ransomware exploits your reliance on digital data, making you a prime target for threat actors who know you can't afford downtime. Worse yet, ransomware can even have life-altering consequences for patients relying on your systems for care.

Common Attributes of Ransomware

Phishing

Most ransomware attacks begin with phishing emails, which trick recipients into downloading malware or divulging their credentials or other sensitive info.

Rapid Encryption

Once inside the system, ransomware can encrypt thousands of files within minutes, making them inaccessible to you before you know it.

Ransom Demands

Threat actors demand a ransom payment, often as cryptocurrency, in exchange for a "key" that decrypts your data.

Ransomware-as-a-Service (RaaS)

Nearly anyone can now purchase ransomware kits from sophisticated cybercriminal groups and launch their attacks against you, all without advanced technical skills.

Data Exfiltration

In addition to encrypting data, attackers may steal sensitive data, such as protected health information (PHI), and threaten to release it or sell it if the ransom isn't paid.

Consequences of Falling Victim to Ransomware

Operational Disruption

The inability to access your critical systems and data can halt medical services, jeopardizing patient care.

Financial Losses

The average cost of a healthcare data breach in 2023 was nearly $11M, including ransom payments, legal fees, and recovery costs.[1]

Increased Mortality Rates

Hospitals under ransomware attacks have reported up to a 35% increase in in-hospital mortality rates.[2]

Reputational Damage

Loss of trust from patients and partners can negatively affect your organization's reputation.

Incomplete Data Recovery

Even when ransoms are paid, less than 65% of data is typically restored, and only 2% of organizations fully recover all their data.[3]

[1] https://securityintelligence.com/articles/cost-of-a-data-breach-2023-healthcare-industry-impacts/
[2] https://www.npr.org/2023/10/20/1207367397/ransomware-attacks-against-hospitals-put-patients-lives-at-risk-researchers-say3
[3] https://www.hipaajournal.com/healthcare-cybersecurity/

Why You Might Be Vulnerable to Ransomware

Outdated Systems
Many healthcare facilities still use outdated software with known vulnerabilities.

Complex Networks
Large, interconnected networks increase your attack surface.

High-Stress Environment
The fast-paced nature of healthcare can lead to careless mistakes and lapses in cybersecurity judgment.

Valuable Data
Your organization stores vast amounts of sensitive data, making it a lucrative target for malicious actors. PHI can fetch up to $1000 a pop on the dark web.

Limited Budgets
Financial constraints may limit investment in advanced cybersecurity measures.

Frequent Data Sharing
Regular sharing of patient data with external entities increases the risk of exposure.

Insufficient Training
Lack of comprehensive cybersecurity training for staff makes it easier for attackers to exploit human error.

Solutions to Better Fight the Threat of Ransomware

- ☐ **Employ Multi-Factor Authentication (MFA)**
  Implement MFA to add an extra layer of security, ensuring that even if passwords are compromised, unauthorized access is still prevented.
- ☐ **Develop an Incident Response Plan**
  Maintain a robust plan to address and mitigate the impact of ransomware attacks.
- ☐ **Regularly Update Systems**
  Ensure all systems and software are updated with the latest security patches.
- ☐ **Adopt Endpoint Detection and Response (EDR)**
  A managed EDR fuses automated technologies with real cybersecurity experts, both working to monitor your endpoints and respond to threats in real time.
- ☐ **Deploy Security Awareness Training (SAT)**
  SAT educates your staff to recognize and respond to phishing emails and other social engineering tactics.
- ☐ **Encrypt Your Data**
  Encrypt sensitive data to protect it from unauthorized access.
- ☐ **Back Up Regularly**
  Back up all critical data to ensure you can recover it in the event of an attack.
- ☐ **Segment Networks**
  Divide your network into smaller segments to limit the spread of ransomware.

Ransomware is a severe threat to healthcare organizations, potentially endangering patient lives and causing substantial financial and reputational damage. By implementing comprehensive cybersecurity strategies and utilizing advanced tools like managed EDR, your healthcare organization can better protect itself against this scourge.

Want to dive deeper into ransomware in healthcare?

Check out our blog for more insights and strategies.

HUNTRESS