Ransomware Guidance For Health Centers

HEALTH INFORMATION TECHNOLOGY, EVALUATION, AND QUALITY CENTER

Overview

- Introduction to Ransomware
- Problem Statement
- Modes of transmission
- Potential Repercussions
- Prevention Methods
- Further Resources

Introduction

- Ransomware
  - Is a type of malware that takes control over a computer or computer system by encrypting all the data on the drive
  - The data is then held at ransom until a predetermined cost is paid.
  - Due to the use of cryptocurrencies (e.g., bitcoins) for payment it is difficult to track those demanding the ransom making it tough to prosecute

Problem

- A rapid increase in the computerization of health care organizations, many without the capacity to keep up to date with the extensive privacy and security measures required, has made them targets for cyber-criminals. In the last couple of years there have been numerous ransomware attacks that has held critical hospital data at ransom.
- Health Centers may be perceived as more vulnerable targets by cyber-criminals due to a potentially smaller IT staff and older set of IT infrastructure (e.g., operating systems without latest security updates).

Examples in the News

- Massive Locky ransomware attacks hit U.S. hospitals
  - http://www.healthcareitnews.com/news/massive-locky-ransomware-attacks-hit-us-hospitals
- Security report - Nearly 90 percent of ransomware attacks target healthcare
  - http://www.hiewatch.com/news/security-report-nearly-90-percent-ransomware-attacks-target-healthcare
- Virginia dermatologist hit by ransomware attack, records for 13,000 patients seized
  - http://www.hiewatch.com/news/virginia-dermatologist-hit-ransomware-attack-records-13000-patients-seized

Ransomware Transmission

- E-mails posing as legitimate business or tempting links
- Trojans acting as update requests
  - Anti-Virus programs patches and updates
  - Windows system updates
  - False “You’ve got a virus” notifications
- Gaining access by exploiting known network or security softwarae vulnerabilities

Turn the Lights on Ransomware

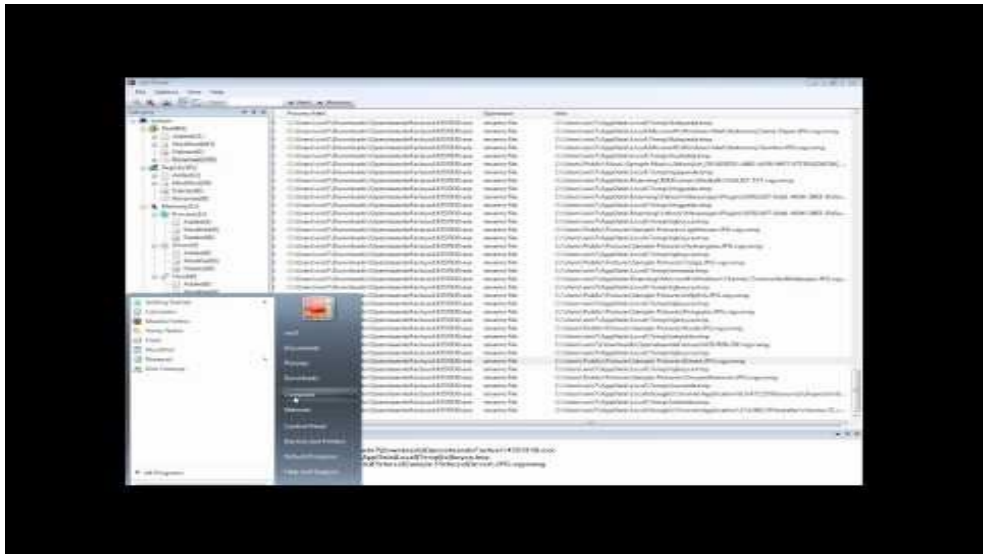
This YouTube video provides an exciting ransomware re-enactment that helps explain how a ransomware incident occurs, common mistakes and methods for mitigation. It also includes a link to a Ransomware Readiness Assessment by the security vendor TrendMicro.

- Ransomware Readiness Assessment: http://ransomware-assessment.trendmicro.com

Ransomware in Action

In this YouTube video security specialists show a live example of how ransomware moves through and encrypts a system's files.

- YouTube video link: https://www.youtube.com/watch?v=Sm5TbBKeFvU



Ransomware in the Cloud

- **Ransomware spreading via the cloud: Virlock another twist on cyber scourge**
  - **http://www.healthcareitnews.com/news/ransomware-spreading-cloud-virlock-another-twist-cyber-scourge**

Repercussions

- Financial
  - Ransoms through ransomware continue to grow in costs as ransomware methods become more sophisticated.
  - Outside of the ransom, the cost due to downtime, recovery, and security maintenance can be considerable
- Legal
  - Privacy and security negligence may constitute legal ramifications based on state and federal policies and regulations (e.g. HIPAA).
  - Personal lawsuits may be leveled if there is perceived harm
- Reputation
  - Ransomware events have become a hot topic and speak poorly of the victims regardless of the exact circumstances.
  - Patient's may be hesitant to initiate or reconsider care if they perceive that a provider is unsafe with their health data

Primary Prevention Methods

- Employee Security Training and Awareness
  - Educate staff on what ransomware is and common traps they might experience
    - Instill email and website suspicion. Help staff know what to look for and what to do if they find something suspicious
    - Teach staff to not click on any links or files un-related to work and inform them of the possible consequences of these types of actions
    - Test and educate: Send a false email with a traceable link

Primary Prevention Methods

- Backups
  - Confirm that backup routines are actively deployed
  - Confirm that backups can be effectively restored
- Anti-Virus programs
  - Scan both inbound and outbound emails regularly
  - Authenticate inbound emails
- Firewalls & Network Access Control
  - Block access to known malicious IP addresses. Many are well documented.
  - Provide concise configurations for access to files, directories and networks

Removal

- The following provides a preliminary list of videos with examples on how conduct specific types of ransomware removal: https://www.youtube.com/playlist?list=PL302CE7037FD86F7B

- Depending on your vendor, as a preventive measure, you should request direct advisement on the processes required for removal of commonly known ransomware

WannaCry Ransomware

- **Primary Systems Affected -** Microsoft Windows operating systems
- **Aliases -** A ransomware variant, known as WannaCry, WCry, or Wanna Decryptor, was discovered May 12, 2017
- **Method** - access gained to enterprise servers either through Remote Desktop Protocol (RDP) compromise or through the exploitation of a critical Windows SMB vulnerability. According to open sources, one possible infection vector is via phishing emails.
- **Prevention** - Microsoft released a security update for the MS17-010 vulnerability on March 14, 2017.
- **Further Information:** https://www.us-cert.gov/ncas/alerts/TA17-132A

Further Ransomware Resources

- U.S. Justice Department's Protecting Your Networks from Ransomware: https://www.justice.gov/criminal-ccips/file/872771/download
- ONC's Ransomware and HIPAA Fact Sheet: http://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- NSA's Information Assurance Department's Top 10 Information Assurance Mitigation Strategies: https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm
- A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks: https://aci.schattauer.de/contents/archive/manuscript/26013.html

THIS PROJECT IS SUPPORTED BY THE HEALTH RESOURCES AND SERVICES ADMINISTRATION (HRSA) OF THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) TRAINING AND TECHNICAL ASSISTANCE NATIONAL COOPERATIVE AGREEMENTS UNDER GRANT # U30CS29366 FOR $1,954,318. THIS INFORMATION OR CONTENT AND CONCLUSIONS ARE THOSE OF THE AUTHOR AND SHOULD NOT BE CONSTRUED AS THE OFFICIAL POSITION OR POLICY OF, NOR SHOULD ANY ENDORSEMENTS BE INFERRED BY HRSA, HHS OR THE U.S. GOVERNMENT.

HEALTH INFORMATION TECHNOLOGY,
HITEQ
EVALUATION, AND QUALITY CENTER