Health Industry Cyber Security Practices:
Managing Threats and Protecting Patients (HICP)

Ransomware Attacks

What is a Ransomware Attack?

Ransomware is a type of malicious software (malware) designed to encrypt data stored on devices. Ransomware renders any data and the systems that rely on them unusable without a "key" known only to the malicious actor. The actors then demand ransom payments in exchange for the "key" required to perform decryption and regain access to the captured data.

Malicious actors have adjusted their ransomware tactics over time, and have become more destructive and impactful in nature and scope. They use tactics such as pressuring victims for payment by threatening to release stolen data if they refuse to pay, and publicly naming and shaming victims as secondary forms of extortion. The attackers may also destroy information such as deleting system backups, that makes restoration and recovery more difficult or infeasible for impacted organizations. Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. The economic and reputational impacts of ransomware incidents, from the initial disruption and recovery, at times, an extended period, have also proven challenging for many organizations both large and small.

Real-World Scenario:

A small town's family medical practice went from treating its patients, to being locked out of patient records, appointment schedules, and payment information after attackers encrypted the data. The attackers demanded $7,000 for the key to decrypt the files, or they would delete all of the data. The practice owners made the tough decision to not pay the ransom, as the key was not guaranteed and the attackers could just demand more money.

Impact

These attacks have serious monetary repercussions that can lead to permanent closures, especially for small healthcare organizations. In many instances, hackers delete the files, and owners are forced to close their practice. These threats are on the rise and becoming more advanced. In healthcare our business is caring for people. In many cases this care must be timely in the interest of the patient. Ransomware operators know this, which is one reason why healthcare is often targeted and considered a high value industry. Due to this, expect attacks to steadily spike in the tears to come.

How Can HICP Help?

The publication, Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP), aims to raise awareness, provide vetted cybersecurity practices, and move towards consistency in managing the current most pertinent cybersecurity threats to the sector. The material on this flyer is a section of the publication that examines cybersecurity threats and vulnerabilities that affect the healthcare industry.

Staying Resilient to Ransomware Attacks

Most ransomware attacks are sent in phishing campaign emails asking you to either open an attachment or click on an embedded link. Be sure you know how to identify these phishing e-mails! Stay alert when any email asks you to enter your credentials. As a proactive measure, check to see whether the computer and network to which you are connected have the proper intrusion prevention system or software in place. That means asking:

- Do I have a business-grade firewall?
- Do I have my firewall configured to only allow certain ports to be open?
- Is there training I should be aware of to understand my organization's security policies?

- Do I have an incident response plan? Do I have an emergency response plan?
- Do I have visibility to detect unusual behavior?

When To Ask About Ransomware Attacks

Provide user awareness and compliance training during the onboarding process or when purchasing a new laptop or desktop equipment. If you discover that your computer has been infected, immediately disconnect from the network and notify your IT security team. Do not power off or shut down the computer or server, in case a volatile Random Access Memory (RAM) memory image needs to be collected for forensics and incident response investigations.

How Can You Mitigate Ransomware Attacks?

Each individual threat discussed in the HICP publication provides threat specific mitigation practices. The table below lists the ransomware mitigations along with a quick reference key to help locate further information.

Ransomware Attacks Mitigation Practices to Consider
Ensure that users understand authorized patching procedures **(7.S.A)**
Patch software according to authorized procedures **(7.S.A)**
Acquire and use data loss prevention tools **(4.M.E, 4.L.A)**
Use strong/unique username and passwords with multi-factor authentication (MFA) **(1.S.A, 3.S.A, 3.M.C)**
Limit users who can log in from remote desktops **(3.S.A, 3.M.B)**
Limit the rate of allowed authentication attempts to thwart brute-force attacks **(3.M.C)**
Deploy anti-malware detection and remediation tools **(2.S.A, 2.M.A, 3.L.D)**
Separate critical or vulnerable systems from threats **(6.S.A, 6.M.B, 6.L.A)**
Maintain a complete and updated inventory of assets **(5.S.A, 5.M.A)**
Implement a proven and tested data backup and restoration test **(4.M.D)**
Implement a backup strategy and secure the backups, so they are not accessible on the network they are backing up **(4.M.D)**
Implement proven and tested incident response procedures **(8.S.A, 8.M.B)**
Establish cyber threat information sharing with other healthcare organizations **(8.S.B, 8.M.C)**
Develop a ransomware recovery playbook and test it regularly **(8.M.B)**
Once ransomware is detected, the covered entity or business associate must initiate its security incident and response and reporting procedures **(HHS Ransomware Fact Sheet)**

Key: 1-10 = Cybersecurity Practice | S = Small (Tech Vol 1) | M = Medium (Tech Vol 2) | L = Large (Tech Vol 2) | A-Z= Respective Sub-Practice

Example: "1.S.B Education": "1" refers to the cybersecurity Practice "Email Protection System" | "S" refers to Small size organization | "B" refers to the sub practice for small size organization within the Email Protection System – Cybersecurity Practice, which in this case is "Education"

To learn more about how you can protect your patients from cyber threats check out the Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients publication at hhs.405d.gov or email us at CISA405d@hhs.gov. Check out the available resources 405(d) has to offer by visiting our social media pages: @ask405d on Facebook, Twitter, LinkedIn and Instagram!