How to Stop Ransomware Targeting Healthcare Data

Ransomware – A Clear and Present Danger

Ransomware is a serious problem in healthcare industry, and we've all seen lately the impact of ransomware attacks on the healthcare industry around the world.

How to Stop and Counter a Ransomware Threat?

Step 1:

Define an Action Plan

- Healthcare organizations must create and refine a plan of action in case their systems gets compromised.
- This plan should include ensuring disaster recovery and business continuity plans are up to date and that the team understands the various threats and their effects on the organization.

Step 2:

Educate and Help Prevent Attacks

- Keep in mind that PREVENTION is the preferred method of stopping the risks associated with ransomware attacks.
- By educating users on how systems are infected and how to safely browse the Internet, an IT department can help users avoid taking unnecessary risks

Step 3:

Keep All Systems Secure

- To remain compliant with HIPAA regulations and/or ISO 27799 standard requirements, all systems that may contain protected health information (PHI) are required to stay patched and up to date.
- To protect against a ransomware threat, a similar approach must be taken so that all systems are secured against any potential vulnerabilities.

Step 4:

Monitor Network Traffic and File Access

- One of the common behaviors of ransomware is it attempts to connect to infected websites using the onion routing (Tor) browser. This is done through the infected machines to get the encryption details to and from the cybercriminals.
- One method of scanning for data breaches and hackers activities is monitoring network traffic and unusual behavior within the systems. Detecting these outbound connections can pinpoint the location of an infection.

Step 5:

Backup all Data at all Times

- Having adequate backups in place is now a common occurrence within enterprises. While there might be few gaps within smaller healthcare groups where backups may not be as comprehensive, most backups will often offer some relief after a serious infection.
- If some or all of a system's files get encrypted, restoring the files from a backup is the only recovery option.

Step 6:

Allocate Access to Data

- When most users map to network resources, they are likely able to access more folders than they need on a regular basis.
- As a best practice, IT must only assign permissions to network resources that are required for the users. This will make it so that if a user gets ransomware on their machine, the extent of the damage will be limited.

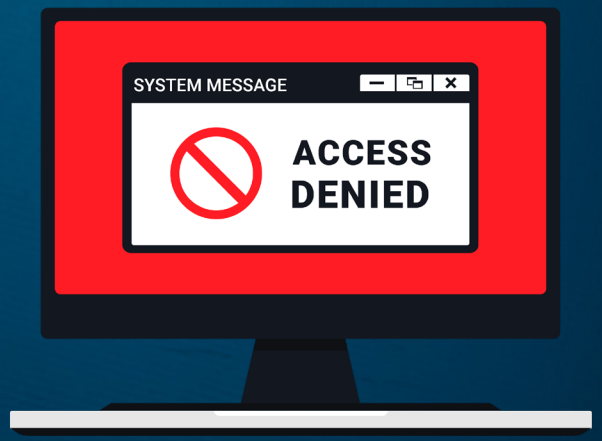
Step 7:

Get to Know Ransomware

- IT departments must understand the different strains of Cryptolocker and other infection types used by ransomware.
- This knowledge will allow them to know where to apply some of the protections and safeguards that they should enforce.

Step 8:

Adopt Additional Protection



- In some of the more recent attacks, ransomware went undetected by many antivirus tools. Infections have come through Word documents with macros, harmful
- websites and now flash-based online content.
- IT departments must apply safeguards to block suspicious emails and deploy additional filters that block potential harmful sites that could result in an attack.

Step 9:

Adopt Creative Security Methods

- Many of the recent ransomware attacks were found to be communicating with IP addresses linked to the deep Web. If these IP's are blocked, the encryption can be stopped.
- Blocking Tor traffic is another worthy endeavor, since that is a commonly used method of communication by these viruses.

Step 10:

Reduce Direct Access

- Some hospitals have moved some of their internal data to cloud-based services.
- File-sharing systems such as SharePoint and OneDrive for Business offer additional protection to users.
- The way files are accessed in SharePoint have prevented make them inaccessible to most of the ransomware thus far.

Conclusion

- Ransomware has already caused significant damage to organizations, especially in the healthcare industry.
- Healthcare organizations should take some of the preceding actions to avoid ransomware attacks and the resulting consequences, rather than standing by and hoping it doesn't happen to them.

GET IN TOUCH.

E-Guides for Information and Cyber Security

CONTACT US

www.issa.org.il

PHONE & FAX

Direct Line: +972-5150340

Fax: +972-5150341

MAIL

Info@issa.org.il