HIT INFRASTRUCTURE
xtelligent HEALTHCARE MEDIA
(https://hitinfrastructure.com/)

Topic

FEATURES

How Network Segregation, Segmentation Can Stop Ransomware Attacks

Ransomware attacks against healthcare organizations have been on the rise in recent years, with sometimes devastating results. Here's how network segregation and segmentation can help.

Source: Getty Images

(https://www.facebook.com/share.php?u=https%3A%2F%2Fhitinfrastructure.com%2Ffeatures%2Fhow-network-segregation-and-segmentation-can-stop-ransomware-attacks&title=How%20Network%20Segregation%2C%20Segmentation%20Ca (https://twitter.com/intent/tweet?text=How%20Network%20Segregation%2C%20Segmentation%20Can%20Sto network-segregation-and-segmentation-can-stop-ransomware-attacks) (https://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fhitinfrastructure.com%2Ffeatures%2Fhow-

network-segregation-and-segmentation-can-stop-ransomware-attacks&title=How%20Network%20Segregation%2C%20Segmentation%20Ca

February 08, 2019 - Ransomware attacks against healthcare organizations have been on the rise in recent years, with sometimes devastating results.*

From EHR downtime to compromised patient data, these cyberattacks can significantly disrupt the operations of healthcare organizations large and small.

Deploying countermeasures, such as network segregation and network segmentation, can help to mitigate the risks from these common attacks.

Network segregation is the separation of critical networks from the Internet and other internal, less sensitive networks.

Network segmentation, which involves splitting the larger network into smaller network segments, can be accomplished through firewalls, virtual local area networks, and other separation techniques.

Both strategies have the potential to prevent ransomware attacks which encrypt files on the network, block access to those files, and then direct the victim to a webpage with instructions on how to pay a ransom in bitcoin to unlock the files.

How can healthcare organizations develop and deploy network segmentation or segregation techniques to protect their infrastructure against ransomware?

**Portions of this article have been updated for clarity.*

***Network Segregation Is Best Way to Thwart Ransomware Attacks* (https://hitinfrastructure.com/news/network-segregation-is-best-way-to-thwart-ransomware-attacks)**

Defending Against Healthcare Ransomware Attacks (https://healthitsecurity.com/features/defending-against-healthcare-ransomware-attacks)

Source: Thinkstock

THE RISKS AND IMPACT OF RANSOMWARE

Healthcare organizations have been struggling to weather some of the biggest ransomware attacks to date.

In 2017, WannaCry **took down (https://healthitsecurity.com/news/hhs-urges-caution-in-wake-of-wannacry-ransomware-attack)** the UK's National Health Service and targeted medical devices, which caused widespread problems for healthcare organizations globally.

The following year, SamSam **went after (https://healthitsecurity.com/news/samsam-ransomware-attackers-target-healthcare-providers)** healthcare and government organizations, infecting a number of hospitals and prompting a warning from HHS about the dangers of the ransomware strain. Ryuk ransomware made its appearance in mid-2018, prompting HHS to issue an **advisory (https://assets.documentcloud.org/documents/4829428/TLPWhite-20180830-Ryuk-Hermes-Ransomware.pdf)**. Ryuk is still evolving and has recently added to its **arsenal of malware weapons (https://healthitsecurity.com/news/notorious-ryuk-ransomware-adds-trojans-to-cyberattack-method)**.

In fact, 27 percent of healthcare employees surveyed by Kaspersky Lab's **Cyber Pulse report (https://hitinfrastructure.com/news/network-segregation-is-best-way-to-thwart-ransomware-attacks)** said their organization had been hit by ransomware in 2018.

Ransomware can have devastating effects on healthcare organizations. It can result in downtime for critical systems and an inability to access patient records, which can endanger patients. It can also result in theft of PHI, reputational damage to the organization, and potential fines and lawsuits.

For example, a **2016 ransomware attack (https://www.theguardian.com/us-news/2016/feb/16/los-angeles-hospital-cyberattack-ransomware-data-computers)** against Hollywood Presbyterian Medical Center disrupted operations at its emergency room and forced doctors and nurses to use fax machines to communicate and record patient information on paper charts.

In 2018, Cass Regional Medical Center in Harrisonville, Missouri, **had to divert (https://healthitsecurity.com/news/cass-diverts-patients-shuts-down-ehr-due-to-ransomware-attack)** trauma and stroke patients to other hospitals and shut down its EHR system as the result of a ransomware attack.

Security firm Sophos **surveyed (https://news.sophos.com/en-us/2018/02/01/understanding-ransomware-and-the-impact-of-repeated-attacks/)** 2,700 IT managers and found that the median total cost of a ransomware attack was $133,000. Five percent of respondents said that the attack costs them between $1.3 million to $6.6 million.

In addition, ransomware attacks can be difficult to defend against. Attackers use social engineering techniques, such as **spearphishing (https://healthitsecurity.com/features/perils-of-healthcare-phishing-and-what-you-can-do-about-it)**, to trick employees into clicking on links in emails or visiting malicious websites.

Spearphishing targets a specific individual or department within the organization and uses information about the company, gathered from social media and/or from a previous breach of the company, to trick victims into downloading the ransomware.

Once the ransomware infects one machine, it can spread quickly by self-replicating throughout the network. Ransomware scans for file shares or computers on which it has access privileges and uses these to spread from one computer to many others.

One of the most effective ways for healthcare organizations to combat the ransomware threat is to deploy network segregation and segmentation.

Dangers of Legacy Solutions to Health IT Infrastructure Systems **(https://hitinfrastructure.com/news/dangers-of-legacy-solutions-to-health-it-infrastructure-systems)**

HHS Warns Health IT Infrastructure Could Put Patient Data At Risk **(https://hitinfrastructure.com/news/hhs-warns-health-it-infrastructure-could-put-patient-data-at-risk)**

Source: Thinkstock

SETTING UP AN AIR-GAPPED NETWORK

Network segregation is the separation of critical networks from the broader Internet and other less sensitive networks.

“When you have a potential risk to life or physical harm to people when a system goes offline, we recommend putting those assets on a separate network. There's much less of a chance of a ransomware incident affecting those systems,” Kaspersky Lab Senior Security Researcher Brian Bartholomew told *HITInfrastructure.com*.

Air-gapping — complete separation of a network from the internet and unsecured internal networks — is an effective way to stop ransomware, but it can be expensive. Bartholomew explained that organizations undertaking air-gapping would need to reproduce everything on a separate network: hardware, switches, routers, etc.

“The whole point is that there's no physical cable that connects the two networks, so you have to basically rebuild another network to house those critical systems,” he said.

Network segregation could raise usability issues within the organization, he added. “Users would get used to it, but it will be a pain to use multiple systems that aren't connected at first. It could cause some initial headaches,” Bartholomew observed.

Improving Medical Device Security Beyond Patching, Traditional Tools **(https://healthitsecurity.com/news/improving-medical-device-security-beyond-patching-traditional-tools)**

Network Management Makes Top 10 Cybersecurity Best Practices List **(https://hitinfrastructure.com/news/network-management-makes-top-10-cybersecurity-best-practices-list)**

(https://hitinfrastructure.com/images/site/features/_large/ThinkstockPhotos-101765995.jpg)

Source: Thinkstock

SPLITTING THE NETWORK INTO SEGMENTS

Another network-based solution to ransomware is network segmentation, which involves splitting the larger network into smaller network segments. This can be done using firewalls, virtual local area networks (VLANs), and other separation techniques.

Networks can be segmented by function, such as separating finance from human resources, or by data type, such as splitting PHI from non-regulated data.

Segmentation lays the groundwork for controls that protect against lateral movement on the network by ransomware or hackers, preventing an infection or compromise from spreading across the network.

“A lot of organizations basically have a strong perimeter on the outside and relatively few controls inside. The idea of segmentation is that finance does not necessarily need to talk to operations. Marketing does not necessarily need to talk to engineering or have access to engineering resources,” explained BlackRidge CTO John Hayes.

“In the case of a hospital, not only do you have IT systems, but you also have medical devices that are tied into the networks that provide various functions, whether they're a CAT scanner, X-ray machine, or blood pressure or heart rate monitor. All of these things are networked,” Hayes told *HITInfrastructure.com*.

Network segmentation places internal boundaries in the network. “This is especially important because of how ransomware operates. Ransomware gets a foothold in an organization and then goes around and actively scans and leapfrogs its way into other things,” Hayes said.

“You stop ransomware from spreading by blocking communications. If I have a completely open internal network, it can spread anywhere. But it can't spread with network segmentation. You're really containing it and limiting it to the local enclave that it infected.”

Chris Convey, vice president of IT risk management and CISO at Sharp Healthcare in San Diego, is a beneficiary of the network segmentation implementation taking place at Sharp's facilities because of the security advantages it can provide. Sharp operates four acute-care hospitals, three specialty hospitals, three affiliated medical groups, and a health plan.

“Network segmentation helps protect against self-propagating viruses and malware, including ransomware. If you logically segment your network and an end user double clicks on a bad link, the impact will be contained to that network segment, so it doesn't cross contaminate other areas of the network,” Convey said.

“If you can more tightly segment your network, then at least you're controlling the blast radius of the ransomware. The hard part is that you don't want to segment so narrowly that it becomes a maintenance nightmare. So, it's a balance of how tightly you want to segment,” he said.

Using software-defined policy management, an organization is “able to apply policies and push them out across network devices without having to access them individually,” he said.

"That dramatically reduces the amount of overhead associated with network segmentation and managing access control lists."

Convey cautioned that if an organization has older network equipment, it needs to check to see if the hardware is compatible with its network segmentation solution strategy.

"We're upgrading equipment to make it compatible so that we can then apply this type of segmentation strategy, but it's a process. It's a lot of work and likely requires network downtime," he said.

"One of the main issues is the overhead of maintaining these types of segmentation strategies and balancing how tightly you lock them down. If you're not able to maintain them appropriately, then the users are not going to be able to access something, or a system is not going to work or function properly," he noted.

Healthcare Orgs, Device Makers Debate Cybersecurity Vulnerabilities **(https://healthitsecurity.com/news/healthcare-orgs-device-makers-debate-cybersecurity-vulnerabilities)**

Best Practices to Secure Healthcare IoT, Connected Devices **(https://healthitsecurity.com/news/best-practices-to-secure-healthcare-iot-connected-devices)**

Source: Thinkstock

THE 10-STEP PLAN FOR NETWORK SEGMENTATION

While implementing network segmentation might be beneficial for security, it can be a complex process. Organizations may need to replace hardware and software, hire additional IT staff, and retrain users.

To implement network segmentation, KPMG's CIO advisory practice **recommends (https://advisory.kpmg.us/content/dam/advisory/en/advisory-institute/pdfs/2017/network-segmentation-imperative.pdf)** that organizations follow a 10-component framework:

1) Develop a plan of action that set out the goals and defines the segmentation

2) Draw up a network architecture that shows the number of segments and the number and type of control points between segments

3) Set up an IT asset management program that defines the requirements for segmentation and network authorization levels based on user, device, and location

4) Use network access controls, firewalls, and intrusion prevention systems as part of the network segmentation implementation

5) Leverage advanced user analytics to develop a baseline profile for each user — who they are, what devices they use, where they connect from, and how they authenticate —and monitor user behavior based on that profile

6) Employ network policy management tools to analyze network traffic and compare it to control rules

7) Implement micro-segmentation for data centers by dividing data centers into even small zones than the network segments

8) Institute a data classification program that defines micro-segments and different levels of data center authorization based on user, device, and location

9) Set up a dedicated program management office and architecture management office to keep the network segmentation project on track

10) Establish an organizational change management function to ensure end users are informed and engaged and to develop strategies, plans, and tactics to ensure stakeholder buy-in.

In addition to network segmentation and segregation, organizations should take other steps to mitigate the risks from ransomware.

Organizations should back up networks and data to ensure speedy recovery if a ransomware attack succeeds.

“If you don't have good backups, then you are rebuilding everything from scratch or you could suffer a massive real loss of data,” observed Hayes.

In addition, **employees should be trained (https://healthitsecurity.com/news/prevent-healthcare-phishing-with-employee-security-training)** on ways to recognize spearphishing emails and ransomware attacks. “If your users are aware of what ransomware does, what it looks like, and how it acts, you can train them to recognize ransomware ahead of time and mitigate the risk,” Bartholomew said.

Organizations need to ensure they conduct regular vulnerability patching, deploy antivirus software, and follow cybersecurity hygiene best practices. “It's about patching and vulnerability management, training your workforce, using good email filters to keep some of the bad stuff from getting in, as well as having good antivirus that's constantly updating,” Convey stressed.

Ransomware will continue to pose a significant threat to healthcare organizations into the near future, but there are steps organizations can take to stop ransomware from infecting their systems and lessen the damage if an attack initially succeeds.

Network segregation and segmentation are two measures healthcare organizations should consider to mitigate the risks from ransomware. They might be complex and costly, but they will save organizations from the costs, system and reputation damage, and patient risk that a successful ransomware attack will cause.

5 Critical Healthcare Data Security Implementations for Providers **(https://healthitsecurity.com/news/5-critical-healthcare-data-security-implementations-for-providers)**

Achieving Healthcare Compliance, Security in Provider Settings **(https://healthitsecurity.com/news/achieving-healthcare-compliance-security-in-provider-settings)**

(https://www.facebook.com/share.php?u=https%3A%2F%2Fhitinfrastructure.com%2Ffeatures%2Fnetwork-segregation-and-segmentation-can-stop-ransomware-attacks&title=How%20Network%20Segregation%2C%20Se
(https://twitter.com/intent/tweet?text=How%20Network%20Segregation%2C%20Segmentati
network-segregation-and-segmentation-can-stop-ransomware-attacks)
(https://www.linkedin.com/shareArticle?mini=true&url=https%3A%2F%2Fhitinfrastructure.com%2
network-segregation-and-segmentation-can-stop-ransomware-attacks&title=How%20Network%20Segregation%2C%20Se

Submit

Related Resources

Security Awareness Training Strategies for Account Takeover Protection (https://hitinfrastructure.com/resources/white-papers/security-awareness-training-strategies-for-account-takeover-protection)

Cybersecurity For Healthcare - Enabling the Latest Advances in Patient Care While Protecting Against Cyber Attacks (https://hitinfrastructure.com/resources/white-papers/cybersecurity-for-healthcare-enabling-the-latest-advances-in-patient-care-while-protecting-against-cyber-attacks)

Executive Summary: The Cybersecurity Remedy: How Healthcare Security Professionals Can Reduce Risk (https://hitinfrastructure.com/resources/white-papers/executive-summary-the-cybersecurity-remedy-how-healthcare-security-professionals-can-reduce-risk)

Infographic: Looking for the ideal security partner for healthcare? (https://hitinfrastructure.com/resources/white-papers/infographic-looking-for-the-ideal-security-partner-for-healthcare)

Webcast: [Panel] The Cybersecurity Remedy: How Healthcare Security Professionals can Reduce Risk (https://hitinfrastructure.com/resources/webcasts/panel-the-cybersecurity-remedy-how-healthcare-security-professionals-can-reduce-risk)

Recent Features

Rapid Threat Evolution Spurs Crucial Healthcare Cybersecurity Needs (https://healthitsecurity.com/features/rapid-threat-evolution-spurs-crucial-healthcare-cybersecurity-needs)

Best Practices When Outsourcing Revenue Cycle Management (https://revcycleintelligence.com/features/best-practices-when-outsourcing-revenue-cycle-management)

Key Considerations for Permanently Integrating Telehealth Coverage (https://healthpayerintelligence.com/features/key-considerations-for-permanently-integrating-telehealth-coverage)

Using AI, Data Analytics to Enhance Person-Centered Care for Seniors (https://healthitanalytics.com/features/using-ai-data-analytics-to-enhance-person-centered-care-for-seniors)

Factoring in Caregivers Adds Value to a Telehealth Program (https://mhealthintelligence.com/features/factoring-in-caregivers-adds-value-to-a-telehealth-program)

Popular Topics

Cloud Computing (https://hitinfrastructure.com/tag/cloud-computing)

Interoperability (https://hitinfrastructure.com/tag/interoperability)

Analytics Infrastructure (https://hitinfrastructure.com/tag/analytics-infrastructure)

Network Security (https://hitinfrastructure.com/tag/network-security)

Artificial Intelligence (https://hitinfrastructure.com/tag/artificial-intelligence)

Internet of Things (https://hitinfrastructure.com/tag/internet-of-things)

Data Storage (https://hitinfrastructure.com/tag/data-storage)

Virtualization (https://hitinfrastructure.com/tag/virtualization)

Wireless Networking (https://hitinfrastructure.com/tag/wireless-networking)

Cybersecurity (https://hitinfrastructure.com/tag/cybersecurity)

Most Read Stories

Top 10 Cloud Data Storage Companies (https://hitinfrastructure.com/news/top-10-cloud-data-storage-companies)

IBM Launches Blockchain-Powered Digital Health Pass for COVID-19 (https://hitinfrastructure.com/news/ibm-launches-blockchain-powered-digital-health-pass-for-covid-19)

Microsoft Azure Forms Collaboration to Enhance AI in Healthcare (https://hitinfrastructure.com/news/microsoft-azure-forms-collaboration-to-enhance-ai-in-healthcare)

Healthcare Leaders Find AI a Top Digital Health Priority for 2021 (https://hitinfrastructure.com/news/healthcare-leaders-find-ai-a-top-digital-health-priority-for-2021)

Fred Donovan

Senior Editor
fdonovan@xtelligentmedia.com
(mailto:fdonovan@xtelligentmedia.com)

Newsletter Signup