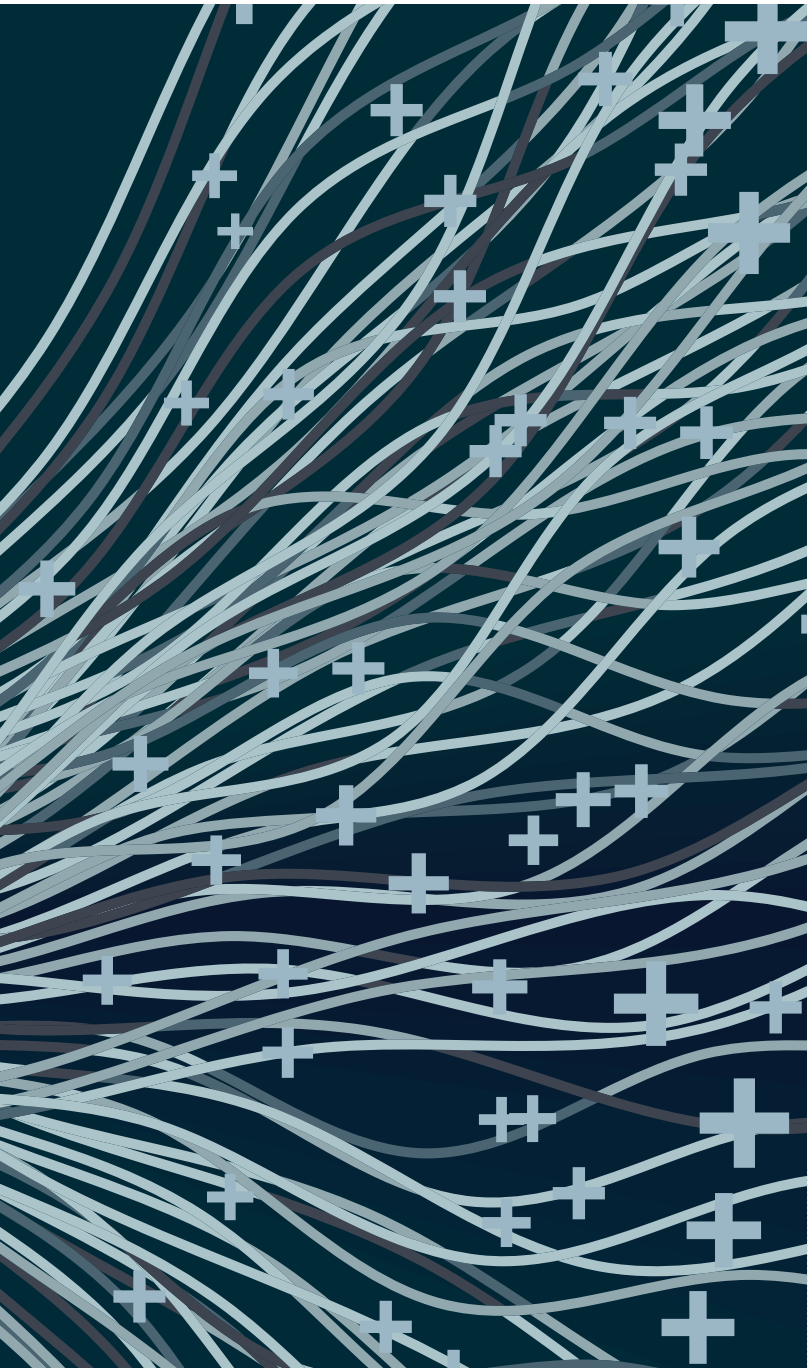

E-Guide

HEALTHCARE RANSOMWARE ATTACKS: THE CRITICAL ROLE OF BACKUP AND 5 STEPS FOR RESPONSE

TechTarget | SearchHealthIT

IN EARLY 2016 ALONE, healthcare organizations saw a 300% increase in daily ransomware attacks from 2015. Here, Harun Rashid, CIO of Children's Hospital of Pittsburgh, demonstrates 6 pointers for the prevention of a ransomware attack. And if those tips aren't enough, health IT expert Reda Chouffani then shares 5 steps for responding to ransomware attacks.

HEALTHCARE RANSOMWARE ATTACK: PREVENTION AND BACKUPS ARE CRITICAL

Kristen Lee, News writer

There are a lot of complicating factors when it comes to a healthcare ransomware attack. Like any cybersecurity threat or attack, health IT professionals want to do everything in their power to prevent one from happening. But equally as important is planning for what can be done after a healthcare organization has been hit by a ransomware attack.

Unfortunately, being hit by a ransomware attack is likely. In early 2016 alone, there were 4,000 daily attacks against healthcare organizations. That's a 300% increase from the 1,000 daily ransomware attacks reported in 2015, according to a U.S. government interagency report.

However, healthcare CIOs agree that if an organization is hit by a ransomware attack, the ransom should not be paid.

"You really should not be paying these people," said Harun Rashid, vice president of Global Health Services and CIO of Children's Hospital of Pittsburgh of University of Pittsburgh Medical Center (UPMC). "Because

once you start paying, you will only, probably, be more of a suspect for other ransomware because they know you are paying and you are giving into those things."

Not only that, but Rashid makes the point that, even if an organization pays the ransom, there's no guarantee that the attackers will return its data.

"You don't know where they're coming from," he said. "They could be in China, they could be who knows where, and you may never hear anything from them."

Ultimately, Rashid said, prevention and backups are key.

PREVENTING A HEALTHCARE RANSOMWARE ATTACK

For robust prevention against healthcare ransomware attacks, hospitals and health systems need to take a multipronged approach. Rashid offers up six pointers.

Detecting vulnerabilities. Rashid suggests investing in technologies to help detect any vulnerable backdoor Trojans like CryptoLocker, downloads, spam, executable files that are coming into the organization, in addition to filtering emails and identifying people gaining access to the organization that could steal passwords.

Emails. "Any email that comes into your organization that has an .exe file, you should be able to scan those and filter those to understand, 'Why do I have these executables?'" Rashid said. "Because once you open up the executable, you're ... basically allowing the ransomware to come in. So, figure out how to kill that before it comes [into your organization]."

Remote desktop. Tightly govern any staff accessing the healthcare organizations' network remotely, Rashid said, and make sure they are doing what they're supposed to be doing while connected. Rashid suggests taking a strict approach and really making sure only certain people are allowed access.

Mobile. "At UPMC, what we do is, anybody that uses a mobile device, we basically force them to create strong, authenticated passwords," Rashid said. "We basically put our firmware in those devices to protect them. So in the event they lose that device, we can remotely wipe any information in those devices."

Wi-Fi. Rashid advises healthcare organizations to segment their Wi-Fi and have Wi-Fi for guests to connect to and Wi-Fi for employees to connect to.

Software updates. "This is an area that organizations don't do very well," Rashid said. "Vendors are constantly putting up patches and updates for software; for malware, for vulnerabilities. They do a good job of it."

Rashid explained that, sometimes, organizations are not aggressive enough when it comes to updates and patches.

"It's very important that you stay on top of those patches and ... to upgrade your software because that will help you with minimizing attacks ... [by ensuring] that all your devices are up to speed and the penetrations will be, hopefully, minimized because of that," Rashid said.

RECOVERING FROM A HEALTHCARE RANSOMWARE ATTACK

Although healthcare organizations should do everything within their power to prevent healthcare ransomware attacks, sometimes, it's just not possible to stop them.

That's why healthcare organizations should also prepare for after they've been hit by a ransomware attack, so that they can avoid paying the ransom and still have access to their data, Rashid said. The key here is frequently and consistently backing up data.

"The biggest thing that will defeat ransomware is to have regular backups," Rashid said. "So if you do get attacked ... you may lose some of the documentation from earlier [in] the day or something, but at least you can restore your information from your backup."

FIVE STEPS FOR RESPONDING TO HOSPITAL RANSOMWARE ATTACKS

Reda Chouffani, Co-founder, Biz Technology Solutions

Ransomware incidents have become more frequent in 2016. So frequent that cyber criminals extorted $209 million from organizations in the first three months in 2016, according to an FBI report. These attacks are far more concerning in the healthcare arena because they can potentially interrupt patient care if clinicians are disrupted. Hospital ransomware attacks can also cause breaches of protected patient care data. While this form of malware has risen to the top of the security list of healthcare IT executives, the preventative steps involve the users more than just the systems.

When a hospital first detects a ransomware incident, it is usually the result of a staff member telling IT they are unable to open some or all of their documents. In some cases the user receives an odd notification on their desktop. If the files in question have been encrypted, and the user has permissions to other network and server resources, other files have likely been encrypted as

well and are no longer accessible. Once IT has confirmed that this is in fact a ransomware infection, there are several steps that should be taken.

LIMITING AND STOPPING THE RANSOMWARE FROM FURTHER DAMAGE

The first step is to identify the workstation or infected machine within the network. This is usually the PC that is being used by the staff member who reported the issue. Isolating that machine helps reduce any further file encryption. Another method is to use tools that allow IT to look for suspicious activity on file servers to prevent further data encryption.

UNDERSTANDING THE TYPE OF INFECTION

Cybercriminals release different variants of ransomware on a regular basis. Changing the tools that encrypt files allows them to become undetected by the antivirus and antimalware tools in the marketplace. As a result, most IT teams find it valuable to identify which version of ransomware they are dealing with to understand the extent of damage that can be expected.

INITIATING THE RECOVERY PLAN

At this stage almost all hospitals and large organizations are aware of the ransomware attack, and are generally aware of what must be done in order to recover from the incident. For those who are uncertain how to tackle a ransomware attack, the two options are to either pay the ransom in order to receive the encryption key -- and in which case there is no guarantee they will receive it -- or simply initiate the data recovery process and restore all the files that have been encrypted.

EVALUATING IF A DATA BREACH HAS TAKEN PLACE

As part of the CMS data breach rules, hospitals are required to report when patient information is stolen. Since different variations of ransomware impact data in different ways, and some are able to affect locked database files, hospital IT must evaluate what type of infection they have at hand. There have been reported cases of hospital ransomware attacks where the ransomware hijacks the information and sends it back to the cybercriminal, in which case it is then considered a patient data breach and needs to be treated as such.

COMMUNICATING INTERNALLY THE OVERALL RECOVERY PLAN

When it comes to restoring normal system functionality, IT leaders need to notify their affected users with a general ETA on when they expect access to data to be restored. But more importantly, IT should communicate what occurred and use it as an opportunity to train or retrain users on what can be done to avoid ransomware attacks in the future. Communicating with end users frequently and training them on what to look for is the best way to protect against these infections.

Rising hospital ransomware attacks show how crippling these incidents can be to the healthcare group. IT departments are implementing tools and software-based safeguards to mitigate risks of infections. But despite all the tools available today, there are still several occurrences of infections and many agree that training end users is and will continue to be a great investment of IT's time.

FREE RESOURCES FOR TECHNOLOGY PROFESSIONALS

TechTarget publishes targeted technology media that address your need for information and resources for researching products, developing strategy and making cost-effective purchase decisions. Our network of technology-specific Web sites gives you access to industry experts, independent content and analysis and the Web's largest library of vendor-provided white papers, webcasts, podcasts, videos, virtual trade shows, research reports and more —drawing on the rich R&D resources of technology providers to address market trends, challenges and solutions. Our live events and virtual seminars give you access to vendor neutral, expert commentary and advice on the issues and challenges you face daily. Our social community IT Knowledge Exchange allows you to share real world information in real time with peers and experts.

WHAT MAKES TECHTARGET UNIQUE?

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals and management. We leverage the immediacy of the Web, the networking and face-to-face opportunities of events and virtual events, and the ability to interact with peers—all to create compelling and actionable information for enterprise IT professionals across all industries and markets.