the Availability Digest

www.availabilitydigest.com
@availabilitydig

Hospitals Under Ransomware Attacks

July 2016

Hackers have found that hospitals are a soft target for ransomware cyberattacks. Their security is not strong, and their data is absolutely essential for patient well-being. The hospitals are therefore very willing to pay modest amounts of ransom to regain access to compromised patient information.

The attacks are typically carried out via phishing techniques. An employee is sent a seemingly harmless email. However, when an attachment to the email is opened or a referenced website is visited, malware is copied into the employee's computer. From there it can travel to every computer on the network. The malware encrypts whatever data it finds, and then sends a message to the organization asking for a ransom in order to be given the decryption key.

The ransomware also can be injected into a computer via a USB thumb drive or a diskette left lying around. It is likely that some employee will insert it into his computer, thus infecting the computer and all others on the same network.

A description of some major ransomware attacks on hospitals follows:

Beth Israel Deaconess

Beth Israel Deaconess takes a cautious approach to computer security. It does not attach any of its medical devices or the computers storing medical records to its network or to the Internet.

However, its medical-records computer needed an operating-system update. The manufacturer sent a technician to do the job. He connected the computer to the Internet and started the download of the update. He then went to lunch.

When he returned, long after the update had downloaded, the computer was so loaded with malware that it was no longer functional. In addition, someone in China had copied about 2,000 patient X-rays. It turns out that Chinese citizens cannot get a visa to travel outside of the country if they have an infectious lung disease. A clean lung X-ray is a valuable commodity.

MedStar Health Inc.

MedStar Health Inc. is a hospital chain that operates ten hospitals in the Maryland and Washington, D.C. areas. It has a staff of 30,000 with 6,000 affiliated physicians.

A hacker's attack on MedStar forced their patient records offline. Staff were unable to check email or even look up phone numbers. Patients couldn't book appointments.

The MedStar staff took down all of their systems as a precaution to prevent patient data from being corrupted and turned to using their paper backup systems.

Boston Children's Hospital

Boston Children's Hospital was struggling with a controversial case involving a teenage girl. She had been taken into state custody after her parents continued to push for treatments considered by doctors to be unnecessary, claiming that her ailment was largely psychological.

The hactivist group Anonymous viewed this as an infringement of the girl's rights. They decided to punish the hospital by launching a DDoS (Distributed Denial of Service) attack against the hospital. Unfortunately, they attacked the hospital's subnet rather than its URL, taking down Harvard University and all of its hospitals.

Hollywood Hospital

Hollywood Presbyterian Medical Center uses computer systems for patient-care documentation and for sharing lab work, X-rays, and CT scans. Their systems were attacked on February 5, 2016; and malware encrypted many of these files. Hospital staff could not access the medical records for many of their patients.

The hospital systems were down for two weeks until they agreed to pay a ransom of 40 bit coins (about $17,000). This was after an initial demand for $3 million in bitcoins.

In exchange for the ransom money, the hackers gave the hospital the decryption keys to unlock its files.

Another pair of Southern California hospitals was hit with similar ransomware attacks less than a week later.

Massachusetts General Hospital

Hackers created a phony website that accurately mimicked Mass General's payroll portal. They then sent emails to Mass General's affiliated physicians instructing them to go to the fake website and authorize a bonus payment.

When doctors did this, the hackers stole the doctors' credentials and used them to change the doctor's direct-deposit information in the actual payment system. The hackers used the doctors' money to buy Amazon gift cards.

Alvarado Hospital Medical Center

Alvarado Hospital Medical Center is located in San Diego, California, U.S.A. It is owned by Prime Healthcare Services, which owns 41 other hospitals across 14 states.

Prime Healthcare detected malicious software infections in March 18, 2016, in its Alvarado systems and in the systems of two other hospitals, Chino Valley Medical Center and Desert Valley Hospital. The company was able to recover their systems without paying any ransom.

Beth Israel Deaconess

A nurse at Beth Israel Deaconess decided to treat herself to a game and downloaded Angry Birds onto her Android mobile phone. Unfortunately, she downloaded it from a Bulgarian website. Accompanying the game was malware that installed itself on her phone.

It recorded her email credentials when she logged on to her email. The malware then sent a million spam messages from Harvard.edu. This spam mass caused Verizon to block Harvard as a spammer.

What Defenses Can Hospitals Deploy?

There are several steps that hospitals can take to protect themselves from attacks such as those described above.

- Make copies of all data. The system administrator can then simply wipe out the infected data and replace it with the non-corrupted copy.

- A further step is to back up every computer system with another computer that is not connected to the same network. If a system becomes corrupted, simply replace it with the non-corrupted system. If all hospitals did this, the motivation for hackers to conduct this type of attack would be removed

- Craft a plan. Assign systems to tiers, and protect the most critical systems.

- Test the plan. The best security plan is worthless unless you test it before you have to rely on it.

- Work with qualified cybersecurity vendors. The hospital should expand the capabilities of its internal security experts with external teams of experts.

- Employ multi-layered protection. Protect every access point to the hospital's computer systems, including email, web gateways, USB thumb drives, and insider threats.

- Educate the hospital's staff. Staff members should be familiar with all sorts of risks such as phishing emails, unapproved websites, and USB flash drives not obtained from trusted sources.

Acknowledgements

Information for this article was taken from the following sources:

Hollywood Hospital Pays Off Hackers To Restore Computer System, *Fortune*; February 18, 2016.
5 Major Hospital Hacks: Horror Stories from the Cybersecurity Foundation, *IEEE Spectrum*; March 16, 2016.
MedStar paralyzed as hackers take aim at another US hospital, *WTOP*; March 29, 2016.
Hackers Have Crippled Another Major Hospital Chain With a Cyberattack, *Fortune*; March 29, 2016.
Alvarado hospital fighting cyber attack, *San Diego Union-Tribune*; April 4, 2016.
Tips for protecting hospitals from ransomware as cyberattacks surge, *Healthcare IT News*; April 6, 2016.