Ransomware: A Ticking Bomb for Public Safety

emsworld.com/node/212691

OPS

By Matthew R. Streger, Esq., MPA, NRP May 25, 2016

Print Version

On February 5, 2016, Hollywood Presbyterian Medical Center was virtually shut down after its computer systems were infected with a virus that encrypted the hospital's electronic medical records system. The hospital was rendered operational again only after paying a ransom of $17,000 in Bitcoin, a virtually untraceable internet currency.

A little more than one month later, Medstar Health was the target of a similar attack that disabled the integrated computer system across 10 hospitals in Maryland and Washington, D.C. Medstar eventually regained full operational capacity, reportedly by restoring functionality from backups and other internal processes.

Both of these events put patient care at risk by disabling critical information systems, and both clearly cost the hospital systems untold sums of money from business interruption and lost productivity.

From January to March 2016, the FBI reports a total of $209 million in ransom payments from cybercrime events, up from $25 million in 2015.

These types of incidents are becoming more common. Police departments in Massachusetts, Maine and Illinois recently fell victim, paying ransoms to re-enable their computer systems. The high-level encryption used by these attacks makes it virtually impossible to crack the systems and defeat the ransom directly.

It is only a matter of time before EMS agencies become victims of these attacks. EMS systems continue to have greater dependence on technology, with electronic medical records systems, computer-aided dispatch systems, other communications systems and standard computer networks accessed by a variety of devices from handheld phones and tablets to dedicated computers.

These systems are not always well-protected, updated and controlled, resulting in soft targets for hackers. In fact, the interconnected nature of the systems presents a cascading series of vulnerabilities, and may place larger systems that EMS technology connects to at secondary risk.

Protecting Your Agency

There are several best practices agencies can follow to help reduce risk and mitigate issues that might arise:

- **Back up your system:** Just like personal computing best practices, your critical computer infrastructure should be backed up. You should have multiple backups in multiple places, and these backups should include your operating system and software, as well as your data. Test your process for restoring from a backup to regain operational capability. This single factor, if properly employed, will reduce ransomware exposure to almost zero. The worst-case scenario, with a solid backup methodology, would be to restore your systems, patch your vulnerabilities and continue to operate. This type of backup best practice also protects your system from other disasters as well.
- **Protect your passwords:** The easiest way to compromise a computer system is simply by walking in through the front door, so if your devices or login credentials are not protected this is a critical vulnerability. Do not fall for the false security of requiring users to change passwords every 90 days, as it will result in users simply writing their credentials on a piece of paper next to the computer. That being said, requiring users to have complex passwords, disallowing common words and requiring the password to be different from those of other systems are good practices for security.
- **Get expert advice:** Systems should employ information systems specialists to ensure system reliability and validate those activities with an outside security audit. Patch common application vulnerabilities as soon as issues are identified and ensure older known issues are patched as well. Robust firewalls should control outbound communications, preventing some problems and providing early identification of others.
- **Train your personnel:** Training should include device and password security, as well as identifying phishing and spearphishing attacks. Phishing attacks involve e-mails that appear to be valid requests for information, or requests to reset a password or take a specific action that results in negative action or vulnerability, and spearphishing attacks are well-formed and directed to a specific individual. Users should have awareness of these types of attacks and what do to, and what not to do, if they receive such an e-mail. Awareness of these threats is the most effective protection.

BYOD Policies

Continue Reading
Bring your own device (BYOD) policies are more common in the workplace, but present a set of vulnerabilities that may not be worth the costsavings or convenience to personnel. Carrying two separate phones, for example, is annoying but that remains a small price to pay for ensuring that your employees' inadvertent actions do not compromise your system integrity. There are reports, for example, of malware that appear to be common games such as Candy Crush Saga that infect Android handsets so deeply that it may be necessary to replace the phone. The root-level access that these apps establish can grant access to a phone's entire file system, and potentially your computer system as a result. This may happen as a result of

an unsophisticated user who installs apps from outside the normal channels (Google Play, Apple App Store), or from a sophisticated user who “jailbreaks” an iPhone to remove security restrictions.

Matthew R. Streger, Esq., MPA, NRP, is a Partner at Keavney & Streger, LLC, in Princeton, NJ, and a senior consultant with Fitch and Associates. Matthew is a paramedic with over 30 years of healthcare experience, and is a member of the EMS World Editorial Advisory Board.