Cyberthreats, ransomware, malware: Is your healthcare organization prepared?

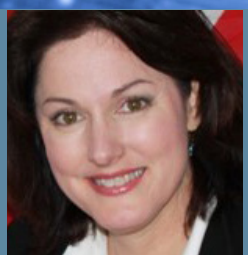
Of all the cybercrime armies currently battling with businesses, none conjures concern, even fear, among healthcare executives like those behind ransomware. In recent years, healthcare organizations have made headlines after being hit by malicious hacks that lock down infected machines and systems until payment has been procured, usually using cryptocurrency like bitcoin.

Consider just a few recent examples where the malware crippled operations. At Titus Medical Center in Texas, a ransomware attack prevented providers from accessing electronic health records (EHR). Presbyterian Medical Center near Los Angeles paid $17,000 to have critical computing systems unlocked. And at Emory Healthcare, Georgia's largest healthcare system an attack removed a database of 200,000 patient records from the Emory Brain Health Center.

Reports of hacking associated with ransomware rose sharply, from 24 cases in 2015 to 137 the following year, according to a HIMSS Analytics report. And ransomware is just one type of attack targeting healthcare systems, said Judith Baker, an experienced healthcare executive and healthcare policy professor and consultant based in Columbia, Mo.

Sponsored by: Juniper Networks

Produced by: HIMSS Media



"New healthcare payment models and alignments are creating cyber ecosystems with constantly changing needs and challenges."

Judith Baker | Healthcare Executive | Healthcare Policy Professor | Consultant

"New healthcare payment models and alignments are creating cyber ecosystems with constantly changing needs and challenges," she said. "These alignments challenge governance and management to create and maintain a responsive security culture."

The need for a stronger security posture is undergoing more consideration at the executive level as IT infrastructures are expanded to keep up with patient and provider demands. The same technologies that can be a competitive advantage can also make these organizations more susceptible to cyberattacks. This is forcing healthcare leaders to develop new strategies and enforce best practices around:

- Extended networks (including public and private Wi-Fi)
- Mobile health (including devices and applications to improve workflows and patient care)
- Internet of Things (the proliferation of "smart" devices that extract and deliver data via the Internet)
- Cloud-based technologies and services (which greatly expand application, computation and storage possibilities)

The need may be growing, but the dollars are not following. The healthcare sector continues to lag others in cybersecurity spending, according to ADI Research, which predicts $10 billion in global healthcare spending on cybersecurity by 2020. "I know that sounds like a lot of money, but it is just under 10 percent of total cybersecurity spends," Baker pointed out.

That low investment rate also comes at a time when medical data is becoming the darling among identity thieves and criminal syndicates. "Healthcare data is more sought-after now than credit card data because medical records can't be reissued easily, like a credit card can," she explained. "Healthcare data now fetches more on the black market."

The Changing Threat Landscape

Of course, ransomware isn't the only threat. Malware developers are constantly refining code used to create advanced persistent threats (APTs) that continually morph and maneuver around conventional security controls to avoid detection and eradication. One reason for the rise in target precision and sophistication is an uptick in malware sourcing: a growing number of nation-states are behind a number of APTs.

Along with state-sponsored malware development comes an elevated means to introduce it to vulnerable systems. Phishing scams remain a primary means to invade a computer or network. The technique requires a user to click malicious links packaged in targeted and legitimate-looking emails, texts or social media posts.

No one wants to be hacked, but the stakes are higher in heavily regulated industries, including healthcare. There are hefty fines when a network is compromised, with disruption in daily operations and reputational damage coming at huge costs.

"In the security world, having the ability to consume threat intelligence from multiple sources and use that intelligence in an actionable manner is very important."

Bopaiah Puliyanda | Senior Product Manager for Security | Juniper Networks

"Clearly, there's a lot of manual work if you must shut your systems down," said experienced IT healthcare executive Thomas Smith, who is based in St. Louis, Mo. "Someone still needs to run to the lab or to the pharmacy and so on. But there are also secondary issues, such as the kind of confidence the public has in your organization and what kind of trust issues you may have with your physicians who are already concerned about the computing systems you run."

Those trust issues can greatly impact public perception, clinician recruitment and retention, and performance levels that influence reimbursement rates. Therefore, more healthcare organizations, including everyone from board directors and chief executives to IT security and network operations teams, are leveraging the latest technologies to prevent attacks.

THE JUNIPER SOLUTION

Software-Defined Secure Networks

One reason ransomware and similar cyberthreats have managed to outmaneuver organizations is because long-established security tools like signature-based antivirus software and intrusion protection systems cannot compete with constantly evolving malware code designed to evade detection. System and network administrators also can't manually compete with the proliferation of "zero-day" attacks that exploit vulnerabilities in software, firmware and hardware residing within networks. A new approach is needed.

As such, technology providers are developing new frameworks and advanced response tools to help healthcare customers better combat cyberthreats, including APTs and ransomware. One example is Juniper Networks' unified security platform called the Software Defined Security Network (SDSN).

The SDSN framework includes three key elements:

- Advanced detection technologies
- Adaptive policy engines that communicate beyond firewalls to switches and routers, and using natural language if needed, not just IP addresses or ports
- Expands the enforcement device ecosystem beyond firewalls, to include switches and routers

In 2016, to support that vision of a stronger cyber defense across a larger network footprint, Juniper Networks unveiled its cloud-based Sky Advanced Threat Prevention, which combines cutting-edge technologies to detect and deter would-be cyberthreats, including APTs and zero-day attacks.

The subscription service incorporates four technologies:

- Analytics used in a defense-in-depth approach, sandboxing and deception techniques (to lure but block malware for analyses like a honeypot)
- Machine learning that processes a growing body of data to accurately deliver “verdicts” that lead to actionable intelligence
- Cloud velocity to ensure rapid development and deployment of security components because there are no physical constraints like on-premise appliances
- Share threat intelligence through an open platform, API-rich ecosystem to consume threat information in real time

Juniper’s Sky ATP extracts content from web browsing and email traffic to analyze in the cloud. Those analyses are combined with other threat intelligence to render maliciousness scores of 1 to 10, which it calls a verdict. This greatly reduces the risk of malware infections while also limiting false positives.

“In the security world, having the ability to consume threat intelligence from multiple sources and use that intelligence in an actionable manner is very important,” said Bopaiah Puliyanda, senior product manager for security at Juniper Networks.

This provides healthcare organizations broader and focused visibility to flag threats before they can penetrate the network. This also includes ransomware variants such as Locky, which uses Visual Basic macros to download malicious code and encrypt disks, and Petya/Mischa that not only encrypts files but installs itself to the Master Boot Record.

“Some of our healthcare customers have multiple copies of their data for additional protection against these kinds of attacks,” Puliyanda said. “I’m not saying that the backups can’t be compromised, but that’s one way to do it.”

Regardless of an organization’s approach to risk management, everyone’s strategy should incorporate current technologies designed to fight emerging threats. That includes ransomware that can lock up access to vital records and other advanced persistent threats on the horizon. Leveraging tools designed to combat cyberattacks will help healthcare organizations keep out malware while building a stronger barrier against future intruders.