CODE TRIAGE:
Protecting Vulnerable Healthcare Data from Security Attacks

Christopher Porter, Chief Intelligence Strategist at FireEye and the former Cyberthreat Intelligence Briefer at the White House, understands the challenges associated with protecting sensitive data. His empathy currently lies with healthcare organizations because they are facing "unenviable difficulty when it comes to securing their information technology and systems."

Frustrations for cybersecurity in healthcare

Vulnerability runs high. Because healthcare organizations provide life and death services in time-sensitive environments, healthcare IT security personnel are always under extreme pressure to keep systems running, making it possible for cybercriminals to confidently mount denial-of-service or ransomware attacks.

The need to share information beckons. Most healthcare data is sensitive and needs to be protected, yet healthcare organizations are simultaneously under pressure to share this information across the continuum of care from doctors' offices to hospitals, to insurance companies to suppliers, and to the patients themselves. "Other industries that have sensitive data don't really have those kinds of burdens," Porter said. "They can rely more on security by obscurity or by isolating sensitive data so that it's not internet connected, but that doesn't apply to modern healthcare."

Software updates can be complicated. After a vulnerability is detected, IT personnel cannot simply apply a patch update to software, especially when working with medical devices. For example, the control software

Produced in partnership with
HIMSS Media

"Financial information has a much shorter lifespan and value than clinical information. Blood type and lab results will never change. If you are held ransom for a credit card number, you can simply call and get a new number. But if you are a C-level executive who's been diagnosed with a new form of cancer, that type of information could have a significant impact on stock performance or the valuation of a global enterprise."

Dave Baumgartner | CTO of the Americas | FireEye

used to run an MRI machine is regulated by the Food and Drug Administration (FDA). When an update is required, the device update must be submitted to the FDA for review and testing, which is "good for patient safety but makes the IT security team's job much more difficult," Porter said.

Also, according to Dave Baumgartner, CTO of the Americas at FireEye, "there might be contractual limitations that prevent healthcare organization IT personnel from interacting with or making changes to some of these life-saving devices for fear of potentially breaking warranty."

The data collected carries significant value. Healthcare organizations typically maintain data repositories that contain not only financial information but personal and clinical data as well.

"Financial information has a much shorter lifespan and value than clinical information," Baumgartner noted. "Blood type and lab results will never change. If you are held ransom for a credit card number, you can simply call and get a new number. But if you are a C-level executive who's been diagnosed with a new form of cancer, that type of information could have a significant impact on stock performance or the valuation of a global enterprise."

Patient safety often takes precedence over data security. "The implementation of a data security control is often seen by clinicians as something that could impede patient safety, not something that can help avert disaster," said John DeLozier, Mandiant Technical Director at FireEye. For example, IT security controls such as a screen saver timeout or two-factor authentication could be seen by clinicians as impediments to quickly getting patient care information.

The real threat

With all these challenges, it's not surprising that significant security incidents are a nearly universal experience for U.S. healthcare organizations, according to the 2019 HIMSS Cybersecurity Survey. The study, analyzing responses from 166 U.S.-based health information security professionals, found that 56% of threat actors involved in security incidents can be characterized as bad actors (cybercriminals and others with malicious intent). Respondents most commonly cited email as a point of compromise (59%). The report points out that "online scam artists using phishing emails are known to masquerade as a senior leader (such as CEO or CFO) within the email recipient's organization and request sensitive information (such as credentials) or even the transfer of funds to an account accessible to the scammer."[1]

Through executive impersonation, cybercriminals attempt to "create a bit of angst" among employees by asking them to do something they would normally not do if they had more time to think about it, according to Baumgartner.

"Over 92% of cyberattacks actually start with email as the point of entry.[2] These email attacks work because they apply pressure and prey on the basic human instincts of wanting to ensure that you're doing what is asked of you as quickly as possible," Baumgartner said. "Humans are still the weakest security

"....email phishing exploits have been increasing in healthcare due to the ease of attack and the threat actor only having to be right once and our security teams needing to be right 100 percent of the time. The value of a phishing attack on healthcare is very high."

Darrell Keeling | Vice President of Information Security | Parkview Health

links. We tend to want to help, and we have this naïveté that security attacks 'can't happen to me.' But it does happen over and over at scale simply because humans can be duped."

Executive impersonation attacks typically play out in one of two ways. Bad actors will either send a well-crafted, targeted phishing email to a single individual for a specific purpose, or they will send a phishing campaign to thousands of recipients. "It's almost guaranteed that someone will click on that link," Baumgartner said. In fact, one out of every seven phishing emails is opened by hospital employees, according to a study published on JAMA Network Open.[3]

Cyberattackers often trick staff members with techniques such as typosquatting to produce emails that appear to be authentic. "Instead of sending an email from Joe.Johnson@world.com, it's Joe with a zero instead of the letter 'O,'" Baumgartner said. "When you look at certain font types, the human eye doesn't notice the difference. It's very easy to impersonate an executive in an email that asks you to perform a legitimate task in an accelerated manner."

Darrell Keeling, Vice President of Information Security at Parkview Health, a Fort Wayne, Indiana-based health system, noted that such "email phishing exploits have been increasing in healthcare due to the ease of attack and the threat actor only having to be right once and our security teams needing to be right 100 percent of the time. The value of a phishing attack on healthcare is very high." Indeed, the number of healthcare systems that have been compromised in the last few years proves that bad actors see healthcare as a rich target.

A strong defense

To protect against attacks, healthcare organizations need to mount both technical and educational defenses. Because organizations are likely to receive a significant number of suspect emails, technology needs to be the first line of defense.

"Without the use of technology, it is literally impossible to protect your organization," DeLozier said. "It goes back to the odds of success. How many security decisions are you asking your staff members to identify? So, while user education is important, technology simplifies the task because it reduces the number of attacks and the number of decisions that end users must make. Your staff members are not looking at dozens or hundreds of emails and having to decide if they are suspicious. Your chance of failure is greatly reduced."

Parkview Health has built a foundation for such data protection by relying on FireEye Managed Defense, a managed detection and response (MDR) service that combines cybersecurity expertise, FireEye email threat protection, and two-factor authentication technologies. These technologies go beyond signature and reputation-based updates, which only offer protection after another organization is attacked and infected by malware. FireEye email threat protection, however, can verify identity, look for attempts to compromise or impersonate key personnel, and examine links for malicious content not only when the emails are received but also days later when the content on those links might have changed to deliver a malicious payload.

"We have a wealth of knowledge about what the most dangerous hackers are actually doing on the systems. Not just the software they're using, but also their behavior on the system."

Christopher Porter | Chief Intelligence Strategist | FireEye

To develop this capability, FireEye collects and analyzes both machine-based and human intelligence, Baumgartner said. "We have about 20 million sensors across the globe that are continuously collecting information about attack patterns," he noted. "Our human analysts are also looking at underground dark web sources and open source forums, and collecting information about techniques and strategies and motivations. FireEye Mandiant consultants respond to breaches in the public domain every day and gain firsthand knowledge about the things that cause our clients harm."

All this intelligence gathering enables FireEye to amass insight into cybercriminals' behavior, Porter said. "We have a wealth of knowledge about what the most dangerous hackers are actually doing on the systems. Not just the software they're using, but also their behavior on the system — how they hide, how they avoid detection and how they use various tools." he pointed out.

In the final analysis, with proper training, organizations can use this intelligence to identify potentially malicious phishing attempts before users ever encounter suspect emails — thereby making it possible to significantly reduce the number of times that staff members click on malicious sites and, most importantly, stop sensitive data from being compromised.

REFERENCES:

1. 2019 HIMSS Cybersecurity Survey, https://www.himss.org/2019-himss-cybersecurity-survey.
2. Verizon, 2018 Data Breach Investigations Report, 11th edition, http://www.documentwereld.nl/files/2018/Verizon-DBIR_2018-Main_report.pdf.
3. Gordon, William J. et.al, Assessment of Employee Susceptibility to Phishing Attacks at US Health Care Institutions, JAMA Network Open, https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2727270.