Cybersecurity attacks have the potential to infiltrate medical devices and cripple health care, expert warns

March 20 2024

Credit: Pixabay/CC0 Public Domain

The cyberattack on Change Healthcare last month should serve as a wake-up call for the health care industry, which needs to focus on securing its infrastructure, says Kevin Fu, a Northeastern University professor of electrical and computer engineering and cybersecurity

adviser to the White House.

While the most recent attack impacted online billing and revenue systems, hackers have the potential to infiltrate medical devices that provide critical care.

In fact, they already have, Fu says.

He points to one example: In 2021, hackers broke into the infrastructure of software cancer provider Elekta. They found their way into the company's internal systems through the internet and took its software offline.

"They took down their private cloud and that effectively shut down all cancer radiation therapy machines for about six weeks globally," he says. "I think the industry has learned a lot from that because they were one of the first victims of ransomware affecting an actual medical device."

But the threat still remains, says Fu, a member of The President's Council of Advisors on Science and Technology Working Group.

Cloud technology is to blame, he says.

"I think that because many medical device manufacturers are beginning to integrate cloud services into their products, we can expect outages of entire medical device product lines, if they are not resilient to ransomware and other cyberthreats," says Fu, who recently published research on privacy and data concerns.

So what does that mean?

First, we need to be proactive rather than reactive, he says.

"We are still in the initial 'deer in headlights' shock stage," he says. "We know the right approach is to engineer not just secure systems, but resilient systems that can continue to operate essential services unimpeded even if ransomware gets into the cloud or even if all the firewalls are compromised."

Second, companies need to abandon what is called "perimeter-based" thinking. It's a term used in cybersecurity to describe protecting yourself against an intruder through the use of a virtual firewall or moat of sorts.

"A lot of companies today, I would say 99%, still think about firewalls, and if they are protected at the border," Fu says. "But guess what, there is no border. When you have perimeter-based thinking, you have very ungraceful failures. What you want to do is have a system that is resilient if pieces of software fail."

"The industry has to cleanse its colon of perimeter-based thinking and move toward cyber-physical resilience," he adds.

For guidance, Fu suggests health care providers turn to the Joint Security Plan filed by the Healthcare Sector Coordinating Council for cybersecurity suggestions.

"This group has over 400 contributing health care organizations of the leading medical device cybersecurity experts," he says.

Unfortunately for patients, there is not much they can do aside from continuing to follow the advice of their medical care providers.

"Americans should continue to trust the advice of their caregivers and clinicians. However, there is still a risk of outages that could cause much frustration when ransomware delays a procedure or interrupts the basic workflow," he says.

Change Healthcare is a great example of that, he explains. It is still dealing with the fallout of last month's cyberattack.

While the company has resumed providing online billing and revenue services for pharmacies, some of its essential services remain compromised, Fu says, including Medicare reimbursements.

He points to the creation of a new website outlining the impact and scale of the attack.

"As the outage continues they basically said, "There are too many outages, so we're no longer going to share this information [here]," so they created a brand new website," Fu says. "Also, the federal government has noticed the outage is so big, they've actually asked insurance companies to waive their requirements for reimbursements. It's unbelievable. It's so big. They're changing the rules just for Change Healthcare."

Given the scale and impact of the incident, the U.S. Department of Health and Human Services has also opened an investigation into Change Healthcare.

It might be weeks or even months before Change Healthcare's situation is fully resolved, highlighting the complexity and fragility of our health care systems, Fu says.

"Health care is just an amazingly complicated set of subsystems, and they're all interconnected," he says. "That's why it's taking so long. There's just so many systems and according to Change Healthcare's website, they process one out of three patients in the U.S. That's a lot of payments.

"What you're seeing as these outages move from weeks to months is just

unimaginable problems, like small clinics not being able to meet payroll, not able to pay rent."

More information: Yan Long et al, EM Eye: Characterizing Electromagnetic Side-channel Eavesdropping on Embedded Cameras (2024)

This story is republished courtesy of Northeastern Global News news.northeastern.edu.

Provided by Northeastern University