How worried should we be about the rise in hospital ransomware attacks?

February 2 2022, by Zach Champion

Kevin Fu. Credit: University of Michigan

American hospitals witnessed an onslaught of security breaches throughout 2021, with more than 40 million patient records compromised in incidents reported to the federal government. Some attacks even threatened healthcare delivery, knocking communications systems offline for weeks or causing an outage in radiation therapy.

Kevin Fu, associate professor at the University of Michigan and Acting Director, Medical Device Cybersecurity at the US FDA Center for Devices and Radiological Health, met with us and discussed the alarming trend and what measures are possible to address it.

Tell us about the scope of this issue

2021 was a fairly substantial year for ransomware attacks on healthcare delivery. It's very disruptive, and it cuts to the heart of weak points in security—the human element sneaking its way in.

In April at the FDA we saw the first instance where ransomware went further than disrupting electronic health records, which to date was a fairly common and inconvenient issue. This attack affected the safety and efficacy of radiation therapy for cancer radiation oncology.

This attack targeted a manufacturer, invading a private cloud they used for the dosimetry of radiation oncology with ransomware and causing a significant outage for hospitals using their technology. What's interesting is that it wasn't the ransomware itself, but the remediation process, that caused the outage. The manufacturer followed their IT security playbook by taking their cloud offline when it was infected.

Unfortunately, that meant the cloud was unavailable for a particular product line of radiation oncology, and so hospitals using the product were not able to deliver the radiation therapy.

When we think about hospital ransomware, we tend to think about the building itself and the devices that are confined to those walls, but really it sounds like the failure points at risk extend well out into the supply chain

Yes, and I think a real challenge is a change in thinking. There are IT systems—email, classroom lectures, things like this—and they have their own set of risks. But on the other hand you have operational technology, what we call OT, including things like medical devices, autonomous vehicles, or satellite assets in space. They have a different set of requirements and tend to be focused on safety first.

So, whereas you might tolerate taking the email system down for an enterprise because of a security incident, that's not really something on the table for a kinetic system where people's lives depend on it.

Why now? Is there any particular reason this is a rising problem?

I would suggest multiple factors. These problems have been baked into computing since the beginning, and this type of attack very well could have been executed in the 1960s.

But I think the reason why it's happening in 2022 is that we've reached an inflection point where the degree of connectivity between devices and services in all sectors has exploded. We are now dependent on distributed computing. Five or ten years ago we might have employed cloud computing for convenience, or perhaps for backup or secondary storage. But now it's moving into the critical path, it's part of the essential components of a medical device. And if it goes down, the medical device loses its core therapeutic functionality.

It's a tough era. There's nothing intrinsically wrong with cloud computing, but you have to control for the risks according to your threat model. And my observation is that the threat model for a medical device is very different from corporate email.

Are there any primary weaknesses that are low hanging fruit to tackle?

The low hanging fruit in terms of ease of repair would be what's become known as threat modeling. This is something we actually teach in computer security courses. It involves playing the role of the adversary, trying to think about how the system could resist not just today's threats, but future threats.

This is something that I think can be very helpful because, even with a legacy device, manufacturers can better understand what's at risk. They start by acknowledging that the device is susceptible to modern malware because it was designed 20 years ago.

Do patient record attacks more often target isolated hospitals, or do they target shared servers?

I am not yet aware of a cloud provider being targeted specifically because it serves a multitude of medical device manufacturers. I would not be surprised if this happens accidentally at some point.

We certainly hope that the cloud service providers that serve the healthcare industry are paying attention to some of the standards development to ensure that hospitals' devices remain safe and effective, even if they do use the cloud.

This is possible to achieve from an engineering perspective but requires conscious, deliberate steps if you want reasonable assurance. You don't want to have security by luck, you want to have security by design.

What's the message for stakeholders and the public?

This is not a run for the hills kind of event, it's more of a slow boil.

The public can have some degree of satisfaction that the different regulatory agencies across different countries are actually working together ahead of time on these issues. They're working on helping to keep hospitals informed about the security risks of each device, so that they can deploy them in a safe manner.

There are a lot of things going on in the background, both technical and in policy, that are going to improve devices.

The FDA is working strategically on standards development to design out a lot of security risks, but a challenge is that there's quite a bit of legacy software out in the marketplace—much of it decades old. Trying to keep those devices secure is incredibly challenging once the horse is out of the gate.

To that end there are also a lot of temporary measures underway to address the outdated, legacy devices. It's challenging, but not impossible, to keep these devices safe and effective until a more ideal device, with security built in from the get-go, becomes available.

Provided by University of Michigan

Citation: How worried should we be about the rise in hospital ransomware attacks? (2022, February 2) retrieved 4 May 2024 from https://techxplore.com/news/2022-02-hospital-ransomware.html