PHYS.ORG

Keeping hackers out of hospitals

January 7 2015, by Joe Carlson, Star Tribune (Minneapolis)

The humble infusion pump: It stands sentinel in the hospital room, injecting patients with measured doses of drugs and writing information to their electronic medical records.

But what if hackers and identity thieves could hijack a pump on a hospital's information network and use it to eavesdrop on sensitive data like patient identity and billing data for the entire hospital?

It is not a far-fetched scenario. Though it hasn't happened yet, the hacking of wireless infusion pumps is considered a critical cybersecurity vulnerability in hospitals - so much so that federal authorities are focusing on the pumps as part of a wide-ranging effort to develop guidelines to prevent cyberattacks against medical devices.

Pumps with Wi-Fi were selected to kick off the new effort because their individual vulnerabilities are magnified by their sheer numbers inside hospitals and clinics.

"Infusion pumps are ubiquitous. At Allina, we have over 3,000 infusion pumps across the system," said Linda Zdon, director of information security and compliance at the 12-hospital Twin Cities health system. "Almost every hospital patient at some point has an infusion pump. So it certainly strikes at an area that has a broad application for most patients, and therefore has a significant impact on health systems."

Allina is one of several Twin Cities health care players that has been working with the National Institute of Standards and Technology since the spring to develop a type of technical analysis known as a "use case" for wireless pumps. The companies' goal is to speed along the development of new standards to harden medical devices against cyberattacks and computer viruses.

Devicemakers say they're already hard at work improving security, but hospitals complain that the companies have been moving too slowly on a vulnerability that puts hospitals' information systems at risk.

In a Nov. 21 letter to the Food and Drug Administration, the American Hospital Association urged the federal government to "hold device manufacturers accountable for cybersecurity." The Homeland Security Department, meanwhile, is reportedly investigating suspected cybersecurity flaws in one model of infusion pump.

Patients tend to fear a malicious person would try to steal data or even scramble the dosing instructions for an individual pump. While those risks are real, security experts say they're far less likely than a hack to gain access to a hospital's wider network traffic. For one thing, attacking an individual through their pump would draw attention and close off what could be a potentially lucrative entry point to many patients' data.

Minnesota companies like Allina, Fairview Health Services and HealthPartners are playing a central role in the development of the new federal guidelines through early collaboration with researchers. The NIST project was unveiled in December in a presentation before the University of Minnesota's Technological Leadership Institute. NIST hopes to publish this first set of recommendations as soon as next fall, and then move on to security vulnerabilities in implantable medical devices and large equipment like magnetic-resonance imaging scanners.

Cyber-vulnerabilities are a top-of-mind concern in health care these days. In July, the 200-hospital Community Health Systems revealed in securities filings that a group from China hacked its files and stole information including names, addresses, birth dates and Social Security numbers for about 4.5 million patients. Company officials haven't said how the hackers got into the system.

Recent headlines have been dominated by the international intrigue surrounding the massive hack at Sony Pictures Entertainment, but several people at the NIST meeting in Minneapolis compared hospitals' infusion pump vulnerability to what happened at Target Corp. Last year hackers accessed personal data on more than 70 million customers after breaching the retailer's computer system through a digital side-door created for a heating, ventilating and air-conditioning contractor. The retailer's sales immediately slumped and its CEO resigned a few months after the company revealed the breach.

"The infusion pump is to the hospital what the HVAC system was to Target. That is, it becomes the vector to get in," said Ken Hoyme, a computer-security scientist at Minneapolis' Adventium Labs.

The risk, as described in a Dec. 18 draft of the NIST infusion-pump study, is that a hacker could write malware to compromise a pump, and then use the pump's network access to plant malicious computer code in the hospital's central systems. Hoyme said specialized code could be written that would cause the network to send sensitive information outside the hospital to an anonymous network of other infected computers, where it could be sold to identity thieves or used to generate negative publicity about the target.

Although it's a common fear that talking openly about cybersecurity vulnerabilities will give hackers ideas, experts note that attackers would still need an extraordinary amount of skill and access to a device to pull off an attack.

Gavin O'Brien, one of the lead authors of the NIST report, said public discussion will cause consumers of health-information technology to become better-informed and start demanding more security features.

"Educating enterprises on how to improve their security will benefit the industry," O'Brien said in an email. "To ignore these issues or just talk about them in small circles may not be enough to push the market into building the security into the products."

The FDA - working independently from the NIST study - has been concerned with infusion pumps since it launched a 2010 review of software defects and related issues in response to 56,000 reports of adverse events.

Separately, the FDA last fall convened its first-ever cybersecurity conference for medical devices, including infusion-pump makers. That work is ongoing. Following the FDA meeting, Reuters reported that Homeland Security officials have opened investigations into suspected cybersecurity flaws in medical devices, including an infusion pump sold by Chicago-based supplier Hospira.

Hospira, which is listed as the lone devicemaker company working with NIST on the infusion pump guidelines, declined to comment for this story. CareFusion, a major infusion-pump devicemaker based in San Diego, listed several specific steps it takes to secure its devices, including working with third-party experts to test and validate product security and using strong data encryption.

It remains to be seen whether the news about hacks at Sony and Target or the NIST will spur more rapid action by devicemakers. But it if doesn't, the companies won't be able to say they weren't warned.

After the Sony hack, Homeland Security Secretary Jeh Johnson issued a statement saying, "This event underscores the importance of good cybersecurity practices to rapidly detect cyber intrusions and promote resilience throughout all of our networks. Every CEO should take this opportunity to assess their company's cybersecurity."

Citation: Keeping hackers out of hospitals (2015, January 7) retrieved 25 April 2024 from https://phys.org/news/2015-01-hackers-hospitals.html