BIZaffairs

How Did Medical Device Security Become a Problem?

Posted in Information Technology by Chris Wiltz on February 4, 2014

If you've watched the news around medical device security and cybersecurity, you probably know that malicious hackers could kill you through your insulin pump. FDA was prompted last summer to urge device makers to take cybersecurity more seriously as part of their development process. Medical device security is on more and more people's minds. But when did the trouble start? And is industry already too far behind the curve?

"Traditionally, in the IT world, the most important thing is confidentiality – that secrets remain secrets," says Mike Ahmadi, global director of medical security at Codenomicon, a security testing solutions provider. "The next thing is integrity – data that's there is always there. The third, and least important, has always been availability."

Think about your typical business setting. If a system goes down it's a less critical issue than data being lost or stolen. Just ask Target – no one cares if the cash registers don't work, but people certainly care if millions of credit card numbers are stolen.

In a healthcare environment the priorities are different. "The most paramount thing in healthcare is availability," Ahmadi says. "Confidentially and privacy issues are important but way less important than the [device] not working."

It's this emphasis on availability that has led many device makers to deprioritize device security overall and led many IT professionals to ask the wrong questions about it. "When we're looking at this new way of looking at medical device security, confidentiality is just really not as much of a consideration anymore," Ahmadi says. "I want to make sure you don't access [a device] and stop it from doing what it's supposed to do."

Mike Ahmadi will be speaking on" **Security Concerns of Network Connected Medical Devices**" at MDM West. Feb. 13, 2014.

Since the medical device industry has less experience in this arena than telecom or networking companies for example, many medical devices have security vulnerabilities that are actually quite common and easily preventable. "In some cases it's really, really bad. We can wipe out an entire hospital worth of patient monitors at once," Ahmadi says. "The problem in healthcare is that these organizations have never addressed security to any degree, in many cases because they've never had to." If FDA didn't raise the concern, there wasn't a reason for device makers to address it.

Cybersecurity attacks that would be easily shrugged off by a telecom company are actually hugely problematic for medical devices and hospitals. "Codenomicon did a firmware analysis on an infusion pump and found 35 known vulnerabilities. In many cases some of them have been known for a decade," Ahmadi says. The company in question had simply never bothered to update its device's old software. "Why is that? Because of the way the process is put together in FDA. If you don't update your library it's easier to get a 510(k) submission."

The first recorded incidence of a medical device hack came in 2008 when Kevin Fu, now a University of Michigan professor who teaches the first-ever course on medical device security, hacked an implantable cardiac device to deliver potentially fatal electric shocks. At the time, the device industry looked at Fu's hack as a curiosity. FDA was not concerned with the issue and manufacturers had bigger fish to fry on their road to regulatory approval.

In 2010, Jay Radcliffe, a cybersecurity expert, drew the attention of GAO when he demonstrated that an Animas insulin pump could be remotely hacked to deliver a fatal dose of insulin. GAO released a report in 2012 calling for FDA to develop a plan for improving its review and oversight of medical device security and vulnerabilities.

"GAO said FDA had to do something. But they didn't tell them what to do," Ahmadi says. He points out that, before the GAO investigation, all of the interest was in privacy – protecting patient data and other sensitive information. No one really thought about malicious misuse when it came to medical devices."When you look at the way FDA approaches things like safety, they look at everything from a functionality perspective. [FDA] would say, this [device] is intended to function this way and intended to be used this way; is there a safety or security issue that can arise out of intended use?"

Following recent moves by FDA, such as its release of new guidance intended to assist staff with identifying issues related to RF security in medical devices, Codenomicon is currently working with the agency to build a cybersecurity lab that will focus on enabling and empowering FDA investigators to have a better understanding of medical device security. FDA wants its investigators to be able to vet information that is delivered to them regarding vulnerability and security issues and determine whether or not a device's software passes testing.

Device makers and FDA are going to have to come to some sort of cohesion if the industry plans on getting in front of cybersecurity before it becomes a major problem. Device companies will have to take initiative. They can't wait on a regulatory body with limited resources to force them to do something. And FDA will have continue its efforts to educate and guide the industry about these issues. Of course, device makers will always focus on the most important issues – those that keep a device from going to market, but, as Ahmadi says, security professionals would like manufacturers to put security among those key issues. "The goal is not to shame manufacturers, the goal is to make safer devices. We want to see the industry building things that are secure by design."

-Chris Wiltz, Associate Editor, MD+DI
Christopher.Wiltz@ubm.com