LILY HAY NEWMAN SECURITY 03.02.17 10:30 AM

MEDICAL DEVICES ARE THE NEXT SECURITY NIGHTMARE

THIERRY DOSOGNE/GETTY IMAGES

HACKED MEDICAL DEVICES make for scary headlines. Dick Cheney ordered changes to his pacemaker to better protect it from hackers. Johnson & Johnson warned customers about a security bug in one of its insulin pumps last fall. And St. Jude has spent months dealing with the fallout of vulnerabilities in some of the company's defibrillators, pacemakers, and other medical electronics. You'd think by now medical device companies would have learned something about security reform. Experts warn they haven't.

As hackers increasingly take advantage of historically lax security on embedded devices, defending medical instruments has taken on new urgency on two fronts. There's a need to protect patients, so that attackers can't hack an insulin pump to administer a fatal dose. And vulnerable medical devices also connect to a huge array of sensors and monitors, making them potential entry points to larger hospital networks. That in turn could mean the theft of sensitive medical records, or a devastating ransomware attack that holds vital systems hostage until administrators pay up.

"The entire extortion landscape has changed," says Ed Cabrera, chief cybersecurity officer at the threat research firm Trend Micro. "You do get into this life or death situation potentially."

The Internet of Health Care

Implanted medical device hacks are so memorable because they're so personal. You wouldn't want something inside your body or on your skin to

be remote-controlled by a criminal. Unfortunately, many types of these devices are broadly vulnerable to attack. For example, in a December investigation of new generation implantable cardiac defibrillators, British and Belgian researchers found security flaws in the proprietary communication protocols of 10 ICDs currently on the market.

Medical devices with these features—like wireless connectivity, remote monitoring, and near-field communication tech—allow health professionals to adjust and fine tune implanted devices without invasive procedures. That's a very good thing. But those conveniences also create potential points of exposure. And the proprietary code on these devices means it takes painstakingly reverse-engineering the software (like the researchers did for implantable cardiac defibrillators) for anyone outside a manufacturer to even assess the security of a device, much less discover flaws.

Given the prevalence of connected medical devices, there's a lot of exposure to go around. While implanted devices draw the most attention, the broader universe of medical care gadgets creates major exposure and potential danger in the healthcare industry. US hospitals currently average 10 to 15 connected devices per bed, according to recent research from IoT security firm Zingbox. A large hospital system, like Jackson Memorial in Miami, can have more than 5,000 beds.

"We tend to think healthcare is very conservative, healthcare is very slow because of regulations and liabilities, but because of the huge benefits they're seeing by using IoT devices hospitals are deploying more and more of them," says May Wang, chief technology officer at Zingbox. "For the past three years the healthcare sector has been hacked even more than the financial sector. And more and more hacking incidents are targeting medical devices."

That's partly because there are so many easy targets. More than 36,000 healthcare-related devices in the US alone are easily discoverable on Shodan, a sort of search engine for connected devices, according to a recent Trend

Micro survey. Not all are necessarily vulnerable to attack, but since they are publicly exposed attackers are more likely to target them. The research also showed that a non-trivial portion of exposed healthcare systems still use outdated operating systems, which can make them vulnerable. For example, in the survey more than 3 percent of exposed devices still used Windows XP, the retired Microsoft operating system that no longer receives security updates. “The challenge is identifying all of your vulnerable infrastructure and developing a plan for how to secure it,” Cabrera says.

MedJack Be Nimble

Unlike desktop computers and servers that run anti-virus software and other “endpoint” security checks, the diversity of IoT devices and initial lack of concern about their role in network security often makes them trivial to compromise. In one currently used exploit, known as MedJack, attackers inject malware into medical devices to then fan out across a network. The medical data discovered in these types of attacks can be used for tax fraud or identity theft, and can even be used to track active drug prescriptions, enabling hackers to order medication online to then sell on the dark web.

These attacks also constantly evolve. MedJack, for instance, has adopted new, more sophisticated approaches in recent months, according to network visibility and security firm TrapX. The company used emulation technology to plant fake medical devices on hospital networks, impersonating devices like CT scanners. As hackers probed and compromised these phony targets, TrapX observed that the MedJack attackers were intentionally using old malware to target their assaults at medical devices running outdated operating systems, like Windows XP and Windows Server 2003. By attacking legacy tech, hackers can avoid detection more easily, since other parts of a network running current operating systems won’t flag the activity. Those newer services are already patched against the older malware, and automatically classify it as a minor threat.

“Every time we’ve gone into a healthcare facility to demonstrate our product we unfortunately find that they’re also a victim of this MedJack attack,” says TrapX vice president of marketing Anthony James. “Most of these facilities have no clue, because no one is monitoring their healthcare devices for the presence of an attacker. No one is thinking about a CT scanner or an MRI machine and seeing a launchpad for a broader attack.”

Once hackers have a foothold, they can exploit their position for a number of different types of network assaults. An increasingly popular choice is to mount a ransomware attack against a large hospital so hackers can get a quick and generous payout in one go. Many of these attacks, like the one on Rainbow Children’s Clinic in Texas last summer, take the traditional route of encrypting digital records and holding them hostage. But a new wave of ransomware attacks take a different approach, disrupting access to digital systems and then demanding ransom in exchange for releasing the services so they can operate normally. In the infamous Hollywood Presbyterian Medical Center ransomware attack last year, computers were offline for a week, and a ransomware attack on a German hospital around the same time disabled email and pushed hospital employees back to using paper and fax machines. The effectiveness of holding hospital data or systems for ransom lies in the urgency to regain control. Hospitals face losing not just money, but critical resources for keeping patients alive.

Make It Work

As with other IoT devices, there are two components to fixing the device security nightmare. First, medical devices like clocks and monitoring machines that have been on the market for years need defenses, like security scanning, and an easy mechanism for downloading patches and updates. Looking forward, though, there also need to be incentives for future generations of devices to include more robust security protections from the start. Many manufacturers either ignore security in the early planning stages, or rely on third-party components that may themselves be

vulnerable.

Fortunately, there's already been some progress. The Food and Drug Administration began more seriously evaluating device cybersecurity as a criteria for product approval in roughly 2013, and has updated it since. The FDA largely based its guidance on the National Institute of Standards and Technology's 2014 Framework For Improving Critical Infrastructure Cybersecurity. NIST is currently working on revisions, and also released a separate landmark document that details a fundamental approach to developing secure and trustworthy digital systems. It's not enforceable, but it's a start.

"If people choose to adopt the guidance you can have a dramatic effect on the trustworthiness of any system from a small smartphone to a medical device to industrial control systems, even power plants," says Ron Ross, one of the NIST authors. "It absolutely can help ensure that medical devices are more trustworthy, because the guidance in the document can help eliminate vulnerabilities and things that can be exploited either accidentally or on purpose by hostile threat actors."

That's a big *if*.

"What the FDA offers to the medical device technology community is basically nothing more than a tap on the shoulder reminder," says James Scott, a senior fellow at the non-partisan Institute for Critical Infrastructure Technology. "It's really up to the industry to actually do something."

The FDA does have some actionable authority though. The agency has delayed and even blocked medical devices from coming to market if they don't meet the agency's cybersecurity standards, says Suzanne Schwartz, the associate director for science and strategic partnerships at the FDA's Center for Devices and Radiological Health. And she adds that the FDA has seen improvement in the foundational cybersecurity protections that are baked in to new products coming under review. Since a device can take years to develop, and the FDA has only really been focused on cybersecurity concerns

in the past few years, the agency isn't surprised that it's taking some time to see results.

"It's not that security is optional," Schwartz says. "Should a manufacturer choose an alternate approach [to implementing security] they're able to do so, but the idea of security being an optional consideration, that's not the case."

Even with these measures in place, though, it's clear that securing existing devices and putting the work into protecting new ones is a gradual process. In the meantime, the healthcare industry as a whole remain exposed—as do its patients.