Health-care industry - the next cybercrime target?

By Perry Hutton

9 Mar 2015

Health-care systems, from electronic health records to medical devices, are more vulnerable than many of us realise - and the stakes are too high to ignore.

© weerapat1003 - Fotolia.com

Today, the black market for patient data is up to 20 times more valuable than that for credit card data often stolen in retail breaches. Health-care data is detailed, rich, and full of information that cybercriminals can use for identity theft and fraud.

More importantly, it takes far longer for patients to know that their information has been compromised - it can take up to a year or more for someone to realise that his patient data has been compromised. When a credit card is stolen, algorithms in the financial industry pick up unusual activity very quickly and systems often automatically provide protection. These same protections simply don't yet exist in health care.

Even within the health-care industry, few people realise just how vulnerable many of the health-care systems are to cyberattack:

- **Traditional cyberattacks**: These are the types of attacks that happen to all institutions. Malware, phishing schemes, Trojans, ransomware - they're all out there, but the health-care industry is particularly vulnerable because it lacks the built-in protections and underlying security mindset of other industries.

These types of malicious software, whether deployed through targeted attacks, compromised websites, spam, infected mobile devices, or otherwise, not only expose sensitive data but create distracting and expensive IT headaches.

These attacks aren't terribly new, but their sophistication is and the ability to expose patient data is of real concern. Cybercriminals have developed entire malware platforms that can be customised to attack health-care organisations;

- **Connected medical devices**: Today, everything from heart monitors to infusion pumps can be networked, automatically interfacing with electronic health record systems and providing real-time alerts to health-care providers. From the perspectives of patient care and operational efficiency, this is a good thing. From a security perspective, it's a potential nightmare.

Most of these devices, as well as MRI machines, CT scanners and countless other diagnostic machines were never designed with security in mind. Many diagnostic systems use off-the-shelf operating systems like Microsoft Windows, while other devices use purpose-built software designed to collect data - not keep it safe. Too many of these devices are eminently hackable and, once compromised, can provide hackers with unfettered access to the clinical data systems within which they interface.

And it isn't just patient data that's vulnerable through connected devices. Cyberterrorists could potentially manipulate machines to harm patients intentionally or shut down critical systems in hospitals. As early as 2011, one researcher demonstrated how an insulin pump could be hacked to deliver a lethal dose of insulin;

- **Personal and home health devices**: Device proliferation isn't just occurring in hospitals. An increasing numbers of home health devices, mobile apps, wearables, and more are collecting and transmitting personal health information. Not only do these devices and apps potentially expose patient data (or at least fail to protect it adequately), but they also often interface directly with electronic health record and clinical data systems.

When everything from a home glucose monitor to an iPhone app can become part of the attack surface, it should become clear just how badly exposed health-care institutions are. As with clinical devices, most of these new patient care modalities are designed for convenience and innovative functionality rather than security.

Health-care security should not be addressed when medical records are breached. The time is now. The health-care industry as a whole needs to be proactive and begin deploying systems with security baked in, protected at both the network and application levels. The stakes are simply too high to wait.

ABOUT PERRY HUTTON

Perry Hutton, regional director of Fortinet for Africa, comes from an accounting background and has spent the last 22 years in IT, the last 10 of which have been in IT security specifically. Contact him at phutton@fortinet.com.

- Security threats of the smart city - 7 Apr 2016
- Security rules for first time cloud users - 15 Feb 2016
- 6 ½ considerations for securing the home office - 23 Jun 2015
- Health-care industry - the next cybercrime target? - 9 Mar 2015
- Securing the new era of big data - 22 Jan 2015

View my profile and articles...