Healthcare IT News

Hospital security risks worry execs

February 19, 2009 | Eric Wicklund, Managing Editor

BOSTON – Every seven seconds, someone tries to hack into the Beth Israel Deaconess Medical Center.

It's not an unusual threat, nor is the Boston-based hospital alone in dealing with cyber attacks. Hospitals and healthcare providers are under constant pressure to maintain the security of their online information, with varying degrees of success.

"The faster we innovate, the faster the attackers innovate," says John Halamka, chief information officer of the Massachusetts-based CareGroup Health System and an expert on healthcare IT. In fact, he said, when his hospital launched its new Web site and URL last year, it was attacked within 30 seconds, and more than 600 attacks were recorded on the first day alone.

To deal with these threats, Beth Israel Deaconess and its three partner hospitals - Beth Israel Deaconess Hospital in Needham, Mass., New England Baptist Hospital in Boston and Mount Auburn Hospital in Cambridge - turned to Third Brigade to set up a security network at the server level.

"We're blocking it at a much higher level" than at the application level, he said. "Things have gotten so sophisticated that we need this level of protection."

Steven Porter, director of IT at Arizona-based Touchstone Behavioral Health, agrees. Porter is using Symantec's End-Point Protection software to ensure the security of laptops sent out into the field - be it a client's house, a school, a park or a fast-food restaurant.

The key to any security software, he said, is separating the legitimate users and uses from those looking to steal data or wreak havoc.

"Because we're dealing with children, and with the dark side of human behavior, there are times when our therapists are dealing with Web sites that we would normally block," he said. Symantec "is a lot less intrusive, but allows us to be aggressive in monitoring and dealing with malware."

"I have 3,000 doctors who actually need legitimate access," added Halamka. "You don't want to tie them up during a medical emergency."

State and federal agencies are coming down harder on healthcare providers who fail to properly protect their data. In California, for instance, two new laws took effect this January that require providers to maintain the confidentiality of patient medical information. The penalty for a security breach can range from $25,000 to $250,000 per reported event. More importantly, patients can

recover damages without proving actual loss or harm - a provision that's expected to lead to an increase in lawsuits.

In New Orleans, the Ochsner Health System called upon Carlsbad, Calif.-based Breach Security to identify Web application defects and secure its Web sites from attack. Breach Security's WebDefend software is now in use at the systems seven hospitals and its more than 35 health centers, which employ more than 11,000 people.

"The challenge is that hospitals and healthcare providers aren't IT experts," said Sanjay Mehta, Breach Security's senior vice president, whose company focuses on application security.

"The keys to the kingdom lie in the application," he said, estimating that 70 percent to 80 percent of all successful attacks are application-layer intrusions. "The idea is to capture all of the information at hand, identify the data and classify it."

"Defense in depth is still the best approach," he said.

Halamka, Porter and Mehta all point out that today's threats to hospital security are more elaborate, with hackers gaining access to newer, better tools just as quickly as hospital security experts devise new safeguards. Mehta laments that hospitals and healthcare providers are loath to admit security breaches, often preventing others from learning from their mistakes. On the flip side, he said, "hackers love to brag."

Mehta foresees a day when providers and vendors are more proactive than reactive to security threats.

"In the future, I'd like to see us move away from application security and move toward application integrity," he said.

Axis Technology is approaching the problem from a different angle. The Boston-based provider of enterprise data solutions recently launched DMsuite, a data masking platform that allows hospitals to profile, provision and mask sensitive healthcare information, replacing it where needed with usable, fictitious data.

"Insider threats of data theft are at a record high, especially in the financial services and healthcare sectors," said Mike Logan, the company's president. "Additionally, new privacy standards are emerging on both state and federal levels, making it even more important than ever that businesses are protected. Noncompliance means more than just harsh penalties and fines; it can lead to a negative reputation and loss of customers."

Halamka, who estimated he spends more than $1 million a year protecting patient records, would like to see funding in the new federal stimulus package spent on security for clinicians. He envisions a trusted state-level "healthcare SWAT team," or perhaps a public-private cooperative.

And while many people cringe when news reports surface of a data security breach at a hospital, he finds cause for optimism.

"At least that proves the security systems do work," he said. "Eventually."