Why hack the FDA?

Aaron Boyd, Federal TImes *11:29 a.m. EST February 16, 2016*

(Photo: Michael J. Ermarth/FDA)

A review of cybersecurity incident reports from the Food and Drug Administration show the agency is fighting off many of the same kinds of intrusions—attempted and successful—as the majority of bureaus within the Department of Health and Human Services. But hackers aren't rooting around for personal health information.

Check back with Federal Times Monday, Feb. 22, for a comprehensive breakdown of cybersecurity incidents reported from all HHS components, the potential impact to national security and what the agency is doing to prevent a major breach.

The FDA reported 1,036 security incidents between January 2013 and June 2015, according to data Federal Times obtained through a Freedom of Information request. Some 50 percent of those incidents were attributed to unauthorized access, while 21 percent were scans, probes or attempted access and 19 percent were malicious code discovered on FDA systems.

FEDERAL TIMES

Civilian IT spending surpasses projections by $4.5B

(http://www.federaltimes.com/story/government/it/2015/03/20/civilian-it-spend-over-projections/25100425/)

These threat vectors track closely to what is happening at most HHS components but the likely reasons behind the hacks are unique to FDA.

"There has been a huge amount of hacking in the pharmaceutical world," said Al Berman, a health care security expert and president of DRI International. "One of the reasons this is being done is for stock manipulation. If you can find out where somebody is in the testing phase for a drug … if you can figure out where they are in that cycle or how well it's going, I think that's tremendous information, with different reasons than every other hack you've seen."

FDA networks suffered a breach in 2013 of 14,000 records maintained by the Center for Biologics Evaluation and Research, mostly containing user account details. At the time, officials said no data or log ins had been altered but bad actors could use just such an approach to compromise a system and get an economic edge.

FEDERAL TIMES

HHS calls in all players for health IT strategic plan

(http://www.federaltimes.com/story/government/interview/program-view/2015/11/12/hhs-calls-all-players-health-roadmap/75655506/)

"It's a huge advantage," Berman said. "If you can hack the pharmaceutical [databases] and find out what their information on clinical testing is and get a preview of what the FDA is about to do, it's a huge, huge financial advantage."

Information security officials at HHS components are "very aware of the sensitivity of the data they protect," and are actively working to keep that data safe, said Leo Scanlon, acting CISO for all HHS.

The department uses the threat data contained within the FOI to build a profile of how components like FDA are being attacked and respond in kind.

"Once we know how we're going to get attacked, we apply that to our unique situation," Scanlon said. "HHS does that in a very fascinating and aggressive way."

Find out exactly how the department is fending off attackers and what is at stake if they fail in our upcoming report on Feb. 22.

Read or Share this story: http://fedtimes.ly/1XvuAxP