Hacking Gains New Heights with Threat to Big Pharma

3/7/2016 by Brenda Fulmer | Searcy Denney Scarola Barnhart & Shipley

SEARCY DENNEY
SEARCY DENNEY SCAROLA BARNHART & SHIPLEY

Cyber attacks have broken free from their initial molds of carting off with consumer credit card numbers or stealing someone's identity. The act of digitally digging into cyberspace has hit the U.S. Department of Health & Human Services and some of its 11 government agencies.

Are crackers targeting Big Pharma servers for their trade secrets?

Instead of hackers hounding out personal information for financial gain, they are looking to uncover data from pharmaceutical companies researching and developing devices and drugs.

The Food and Drug Administration (FDA) has been among the most targeted agency because of its role as both the starting point for bringing new products to market and the ending point for eventual approval or denial. Committee meetings, public hearings, test trials and other protocols along the way generate a long paper trail, and the bad

guys see an opportunity to profit from it.

How? Why? Al Berman, a healthcare-security expert, has an answer for the uptick in hacking attempts on Big Pharma.

"One of the reasons this is being done is for stock manipulation," Berman said in a Federal Times article titled "Why hack the FDA?" "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."

Federal Times issued a Freedom of Information request for cybersecurity breaches and found that 1,036 incidents had been reported between 2013 and 2015. Of those, half were illegitimate, unauthorized access into FDA computers. Another 21 percent were classified as probes or scans – similar to phishing – and 19 percent were malware intrusions.

Further, in excess of 14,000 records maintained by an FDA sub-agency, the Center for Biologics Evaluation and Research, were compromised in 2013.

Berman said the goal probably was to gain an economic edge.

"It's a huge advantage," he 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."

The Center for Biologics Evaluation and Research, or CBER, handles

products governed under the Federal Food, Drug and Cosmetic Act and the Public Health Service Act. Such sensitive data should be more vigorously protected.

Leo Scanlon, the HHS information security officer, said the department is aware of the illicit trend and in the process of analyzing ways to beef up its online defense system.

RELATED POSTS

'Tis the Season for Data Breaches, Identity Theft

LATEST POSTS

Tobacco Companies Resist Truthful Disclosures

$11 Million Verdict Against Gynecare Prolift Pelvic Floor Repair System Under Appeal

Hacking Gains New Heights with Threat to Big Pharma

Power Morcellator Cases Transferred to Kansas

See more »

WRITTEN BY:

Searcy Denney Scarola Barnhart & Shipley + Follow

Brenda Fulmer + Follow

PUBLISHED IN:

Cyber Attacks + Follow

Cybersecurity + Follow

Data Breach + Follow

Data Protection + Follow

FDA + Follow

Hackers + Follow

Pharmaceutical Industry + Follow

Popular + Follow

Research and Development + Follow

Business Organization + Follow

Intellectual Property + Follow

Science, Computers & Technology + Follow

Searcy Denney Scarola Barnhart & Shipley on: