Hack of US regulator a blow to confidence in financial system

September 21 2017

The hack disclosed at the US Securities and Exchange Commission deals a fresh blow to confidence in the security of the financial system weeks after news of a potentially catastrophic breach at a major US credit bureau.

The stock market regulator said late Wednesday a software vulnerability allowed hackers to gain "nonpublic" information that could have enabled them to make profits with inside information.

SEC chairman Jay Clayton said the leaked information from 2016 "may have provided the basis for illicit gain through trading," while noting that the vulnerability had been patched and that an investigation was underway.

The revelation comes two weeks after Equifax, one of three major credit bureaus which maintain financial and personal data on consumers, announced that attackers had hacked accounts of some 143 million Americans, in what could be the worst-ever breach because of the sensitivity of the information.

Johannes Ullrich, dean of research at the SANS Internet Storm Center, said that while the two events are likely quite different, both could undermine confidence in online financial systems.

"A lot of our financial systems particularly online systems are based on trust, and if that trust is violated people could opt out of these systems,"

Ullrich said.

But Ullrich noted that even if people stop using online networks, that may not protect them against hackers.

"Even if you don't set up online banking the criminal may set it up for you," he said.

"If you don't want to use your credit card online and give your number over the phone, that person is entering the same information in the system."

Ullrich said the SEC breach underscores weak cybersecurity in government networks, after the federal Office of Personnel Management breach disclosed in 2015 affecting tens of millions of employees and contractors.

He said government networks "are really behind the curve in designing the right values and the right protection" of data.

Ironically, the SEC now must point a finger at itself for delaying the disclosure which it requires from publicly traded companies.

"The breach itself appears to be fairly minor, but it erodes trust in government organizations where companies are required by law to report confidential or insider information," said Tatu Ylonen, a computer researcher and founder of SSH Communications Security.

Ylonen said federal cybersecurity guidelines are "in pretty good shape" but that "a problem is that agencies are implementing these measures in different stages, and some agencies haven't made it a priority."

Critical infrastructure at risk

James Scott, a researcher at the Institute for Critical Infrastructure Technology, said the latest incident highlight the vulnerability of financial networks despite a threat-sharing system which aims to prevent attacks.

"All of our critical infrastructure systems are not doing a sufficient job of protecting their treasure troves of data," Scott said.

"We are lacking confidence in our election systems, we are lacking confidence in the health system in protecting patient records and now the financial sector."

Until recently, Scott said the health sector appeared the most vulnerable "but the financial sector is evolving in 2017 as a major problem."

Scott said the SEC hackers could be from any number of elements including "cyber mercenaries" or nation-states.

"Russia is notorious for gaining access to this type of information but they are not known for acting on it," he said.

A more likely source, according to Scott, would be an extremist group seeking to raise cash quickly or a state such as North Korea which is "pressed for cash."

The SEC attack is especially embarrassing because it comes following the July release of a congressional audit which said the agency had failed to implement security recommendations made two years earlier.

The SEC "had not fully implemented 11 recommendations" on protecting data and encrypting sensitive information, said the report by the Government Accountability Office.

Dan Guido, co-founder of the security firm Trail of Bits, said the SEC incident is not surprising given the current state of affairs in cybersecurity.

"It reflects the status quo of our digital security," Guido said. "It's not substantially different than the ones that came before it. We will continue to tolerate these repeated breaches until it's clear that people's lives are stake."

Citation: Hack of US regulator a blow to confidence in financial system (2017, September 21) retrieved 27 April 2024 from https://phys.org/news/2017-09-hack-confidence-financial.html