Exclusive: Lax security at Nasdaq helped hackers

Andrea Shalal-Esa and Jim Finkle, Reuters

A federal investigation into last year's cyber attack on Nasdaq OMX Group found surprisingly lax security practices that made the exchange operator an easy target for hackers, people with knowledge of the probe said. The sources did not want to be identified because the matter is classified.

The ongoing probe by the Federal Bureau of Investigation is focused on Nasdaq's Directors Desk collaboration software for corporate boards, where the breach occurred. The Web-based software is used by directors to share confidential information and to collaborate on projects.

The investigators found that Nasdaq's basic computer architecture was sound, which kept its trading systems safe from the hackers, according to four people who were briefed on the FBI probe or had knowledge of Nasdaq's efforts to improve its security with the help of external consultants.

The sources, however, said the investigators were surprised to find some computers with out-of-date software, misconfigured firewalls and uninstalled security patches that could have fixed known "bugs" that hackers could exploit. Versions of Microsoft Corp's Windows 2003 Server operating system, for example, had not been properly updated.

While Nasdaq is not the first company to allow software updates to lapse inadvertently, investigators were surprised that the exchange operator was not more vigilant about what the industry calls "cyber hygiene" given its importance to financial systems.

"This was easy pickings," said one person familiar with Nasdaq's security practices. "You would have thought they would be like a cyber Fort Knox, but that wasn't the case at all."

Nasdaq defended its security practices and said no data was compromised by the cyber attack, which was detected in October 2010.

Carl-Magnus Hallberg, senior vice president of information technology services for Nasdaq OMX, told Reuters it was unfair to conclude that security practices were lax simply because the Directors Desk program was breached. He said it would have been virtually impossible to defend against the hackers who used malware that had not been disclosed.

"This was a sophisticated attack," Hallberg said. He declined to comment further on the specifics of the investigation, saying his company does not publicly discuss details of its security practices.

BROADER CONCERNS

The Nasdaq attack has sparked concerns about the severity of the threat facing the financial industry and the need for enhanced security at many companies.

Computer security is uneven across industry and many companies, even in the defense sector, are unaware of malware lurking in their networks, cyber experts say.

Sources said the malware found in Nasdaq's network was complex and insidious, but tougher security measures and more vigilance could have helped the company detect the intrusion more quickly.

While declining to comment on that claim, Nasdaq said it invests heavily in network security and has about 1,000 people working on information technology issues worldwide.

Officials at the FBI and the National Security Agency, which is also involved in the investigation, declined comment.

It was not clear how long the malicious software was present on Nasdaq's network before it was found.

Hallberg said Nasdaq detected the breach, took action to mitigate it and notified federal authorities, who are still investigating. Nasdaq also shared the electronic signatures it identified from the attack with other companies to help them avert similar attacks, Hallberg said.

Nasdaq has about 10 companies advising it on security issues, including a major U.S. defense contractor, he added.

Nasdaq disclosed in February the cyber attack on Directors Desk, a service the company sells to corporate boards. Nasdaq bought the privately held Washington-based company in 2007.

Hallberg said Nasdaq was working closely with other companies and government agencies around the world to increase data-sharing on security threats.

He said the company's security systems were heavily regulated in every country where it operates, and especially in the United States, where the Securities and Exchange Commission conducts four audits per year. Any concerns identified through such audits were dealt with immediately, he said.

(Additional reporting by Jonathan Spicer and Basil Katz in New York. Editing by Tiffany Wu)

Source URL (retrieved on *03/12/2014 - 9:56am*):
http://www.ecnmag.com/news/2011/11/exclusive-lax-security-nasdaq-helped-hackers