EMC's anti-hacking division hacked

March 18 2011

Art Coviello, Executive Chairman of RSA, speaks at a conference in 2007. US computer security titan RSA said Thursday that hackers broke into its computers and swiped data that could be used to breach defenses of some systems guarded with its technology.

The world's biggest maker of data storage computers on Thursday said that its security division has been hacked, and that the intruders compromised a widely used technology for preventing computer break-ins.

The breach is an embarrassment for EMC Corp., also a premier security vendor, and potentially threatens highly sensitive computer systems.

The incident is a rare public acknowledgement by a security company that its internal anti-hacking technologies have been hacked. It is especially troubling because the technology sold by EMC's security division, RSA, plays an important role in making sure unauthorized

people aren't allowed to log into heavily guarded networks.

The scope of the attack wasn't immediately known, but the potential fallout could be widespread. RSA's customers include the military, governments, various banks and medical facilities and health insurance outfits. EMC, which is based Hopkinton, Mass., itself is an RSA customer.

EMC said in a filing with the Securities and Exchange Commission that RSA was the victim of what is known as an "advanced persistent threat," industry jargon for a sophisticated computer attack. The term is often associated with corporate espionage, nation-state attacks, or high-level cybercriminal gangs.

EMC didn't offer clues about the suspected origin of the attack. It said it recently discovered an "extremely sophisticated" attack in progress against its networks and discovered that the infiltrators had made off with confidential data on RSA's SecurID products. The technology underpins the ubiquitous RSA-branded keychain "dongles" and other products that blanket important computer networks with an additional layer of protection.

The products make it harder for someone to break into a computer even if a password is stolen, for example. The RSA device, working in concert with back-end software, generates an additional password that only the holder of the device would know. But if a criminal can figure out how those additional passwords are generated, the system is at risk.

RSA is one of the best-known names for this type of "two-factor authentication" technology.

RSA declined to comment on what type, or how much, information was stolen.

Richard Stiennon, a security analyst with the IT-Harvest firm, said there would be "tremendous repercussions" if the criminals were able to silently tap into critical systems using the stolen information.

"You'd never have a sign that you've been breached," he said.

In its SEC filing, RSA said that it is "confident that the information extracted does not enable a successful direct attack on any of our RSA SecurID customers." However, it warned that "this information could potentially be used to reduce the effectiveness of a current two-factor authentication implementation as part of a broader attack."

"We have no evidence that customer security related to other RSA products has been similarly impacted," said the company's executive chairman, Art Coviello. "We are also confident that no other EMC products were impacted by this attack. It is important to note that we do not believe that either customer or employee personally identifiable information was compromised as a result of this incident."

The company said it is providing "immediate remediation steps" for customers. It didn't specify what those are. It outlined some generic security tips that offer clues about how its customers might be targeted with the information stolen from RSA, such as closely monitoring the use of social networking websites by people with access to critical networks and the need to educate employees on the danger of clicking on links or attachments in suspicious e-mails.

EMC said it doesn't expect the breach to have a meaningful impact on its financial results.

Its shares slipped 8 cents to $25.58 in extended trading Thursday. They ended the regular session up 25 cents at $25.56.