Sony hack adds to security pressure on companies

December 19 2014, byJoe Mcdonald

SONY
SONY
ソニー株式会社
Sony Corporation
ソニーマーケティング株式会社
Sony Marketing (Japan) Inc.
ソニービジネスソリューション株式会社
Sony Business Solutions Corporation

In this Thursday, Dec. 18, 2014 file photo, people walk out from the headquarters of Sony Corp. in Tokyo. Faced with rising cybercrime like the attack on Sony Pictures Entertainment, companies worldwide are under pressure to tighten security but are hampered by cost and, for some, reluctance to believe they are in danger. The studio's parent, Sony Corp., launched an overhaul of its own security in 2011 after hackers broke into its PlayStation Network gaming system and stole data of 77 million users. (AP Photo/Eugene Hoshiko, File)

Faced with rising cybercrime like the attack on Sony Pictures

Entertainment, companies worldwide are under pressure to tighten security but are hampered by cost and, for some, reluctance to believe they are in danger.

The Sony attack, which U.S. officials blamed on North Korea, was unusual because it included threats of violence if the Hollywood studio released its movie "The Interview," a comedy that depicts the assassination of the North's leader. But it is just the highest-profile case in a growing flood of data breaches that have risen in sophistication over the past five years.

The growing skill of hackers has driven a shift in strategy for companies, which see they cannot be stopped and have switched to trying to limit losses, said Kwon Seok-chul, president of Cuvepia Inc., a security firm in Seoul. He said his company has received a growing number of requests from financial institutions and other businesses alarmed by reports of break-ins including last month's Sony attack.

"There is no way to block hacking," said Kwon. "They are consulting with us for new types of defense measures."

U.S. officials have told reporters they believe North Korea was connected to the Sony attack, though the evidence is only circumstantial. The threats of violence prompted Sony to cancel the release of "The Interview." The North Korean government earlier denied involvement but called the attack a "righteous deed."

Other governments also have been implicated in commercial hacking. In May, U.S. authorities charged five officers from the Chinese military's cyber warfare unit with hacking into American companies to steal trade secrets.

During last year's Christmas shopping season, U.S. department store chain Target Corp. disclosed it suffered a breach that exposed details of as many as 40 million credit and debit card accounts.

This month, a virus was discovered in Japan that steals credit card data from retail checkout systems. Police said more than 30 companies, government agencies and organizations have been targeted since 2009.

Too many companies, though, assume they are too small to be targeted, said Chester Wisniewski of Sophos, a London-based security firm.

"It is generally ignored," said Wisnewski. "When it does happen, most people you talk to say, I'm not Target, or, I'm not Sony."

Companies in developing countries face additional disadvantages.

In China, widespread use of unauthorized copies of software downloaded from websites run by pirates allows to insert malicious code to gain access to company networks, according to Wisniewski. In countries such as India, Thailand or Pakistan, even security-conscious companies may not be able to afford the most advanced software tools.

"Out of desperation, people get software wherever they can find it, but often that puts them in harm's way," said Wisniewski.

Chinese companies also face official pressure to stop using foreign information technology, which communist leaders see as a potential national security threat. In 2010, banks and other major companies were ordered to use domestic technology whenever possible in an apparent effort to support growth of China's fledgling security industry.

Beijing this year said it would review all imported security products for potential security flaws following revelations by former National Security Agency contractor Edward Snowden that U.S. technology companies cooperated with widespread government spying. In August, the Chinese government said it would no longer buy foreign anti-virus systems.

China is regarded as the biggest global source of computer hacking. Experts say that in addition to Chinese hackers, those from other countries can easily take control of a computer network in China and use it to launch an attack because many lack adequate security.

The Chinese government has rejected accusations it is involved in hacking, though it has given no indication it investigates complaints of attacks launched from its territory.

"China is a victim of hacking," a foreign ministry spokesman, Qin Gang, said Thursday. "We do not support cybercrimes anywhere on our soil."

Asked whether the government was investigating reports North Korean hackers launched the Sony attack from within China, the foreign ministry press office said Friday it had nothing to add to Qin's statement.

The studio's parent, Sony Corp., launched an overhaul of its own security in 2011 after hackers broke into its PlayStation Network gaming system and stole data of 77 million users.

The Japanese government has spent heavily on improving its information security systems and has formed teams to study possible threats to power supplies and other infrastructure.

But the country still tends to react instead of preventing attacks, according Ryusuke Masuoka, a security expert.

"Japan needs what we might term a 'forum for thinking the unthinkable,' not only to react, but also to anticipate threats," said Masuoka in a recent paper for the government-affiliated Center for International Public Policy Studies in Tokyo.

The uproar over Sony might help technicians persuade reluctant executives to spend more on security, said Wisniewski. He said many companies pay more attention to securing laptop computers and other portable technology, while failing to protect equipment in their offices.

"A lot of these guys already know it's a problem," he said. "Now you've got a poster child. You can take Sony to management and say: Here's what can happen if we don't act."

Citation: Sony hack adds to security pressure on companies (2014, December 19) retrieved 5 April 2024 from https://phys.org/news/2014-12-sony-hack-pressure-companies.html