Sony emails show a studio ripe for hacking

December 18 2014, byTed Bridis

In this Oct. 13, 2004 file photo, Sony Pictures Entertainment Chairman and Chief Executive Michael Lynton is seen in Beverly Hills, Calif. In the weeks before hackers broke into Sony Pictures Entertainment, the studio suffered significant technology outages blamed on employees keeping too many old emails and hackers targeted executives to trick them into revealing their online credentials. The company's chief executive regularly was reminded in unsecure emails from his executive assistant of his own secret passwords for his and his family's mail, banking, travel and shopping accounts, according to a review of more than 32,000 stolen corporate emails circulating on the Internet. (AP

Photo/Danny Moloshok, File)

In the weeks before hackers broke into Sony Pictures Entertainment, the studio suffered significant technology outages it blamed on software flaws and incompetent technical staffers who weren't paying attention, even as hackers targeted executives to trick them into revealing their online credentials.

Its chief executive was regularly reminded in unsecure emails of his own secret passwords for his and his family's mail, banking, travel and shopping accounts, according to a review of more than 32,000 stolen corporate emails circulating on the Internet.

Scrutiny of Sony's stolen computer data hasn't yet revealed exactly how hackers managed to slip inside to steal such an enormous cache, when it happened, who was behind the theft or their motives.

But late Wednesday, a U.S. official told The Associated Press that federal investigators have now connected the Sony hack to North Korea. The official was not authorized to discuss an ongoing criminal case openly, and spoke on condition of anonymity.

Confirmation of the North Korean link came just after Sony cancelled plans for the Dec. 25 release of "The Interview," which had been one of the hackers' public demands due to its depiction of the fictional assassination of North Korean leader Kim Jong-un.

The stolen files expose lax Internet security practices inside Sony such as pasting passwords into emails, using easy-to-guess passwords and failing to encrypt especially sensitive materials such as confidential salary and revenue figures, strategic plans and medical information about some employees. Experts say such haphazard practices are common across corporate America.

"Most people who say they're not doing that are lying," said Jon Callas, co-founder and chief technology officer for Silent Circle Inc., a global encrypted-communications service.

The emails show CEO Michael Lynton routinely received copies of his passwords in unsecure emails for his and his family's mail, banking, travel and shopping accounts, from his executive assistant, David Diamond. Other emails included photocopies of U.S. passports and driver's licenses and attachments with banking statements. The stolen files made clear that Diamond was deeply trusted to remember passwords for Lynton and his family and provide them whenever needed.

"I still need the password to your Amazon account," Diamond wrote to Lynton in August.

Sony spokeswoman Jean Guerin did not respond to a phone message left with an assistant in her office and email from The Associated Press on Wednesday.

In an October email, the company's chief financial officer, David C. Hendler, complained to Lynton that Sony Pictures had experienced months of "significant and repeated outages due to a lack of hardware capacity, running out of disk space, software patches that impacted the stability of the environment, poor system monitoring and an unskilled support team." Hendler also blamed a company rule that required employees to keep too many old emails.

"Sloppy, really sloppy," said Kevin Mitnick, a former hacker who served five years in federal prison and now runs Mitnick Security Consulting

LLC. But Mitnick was quick to acknowledge that other top chief executives are "probably doing it, too." Companies can use password-management software, which can store dozens or hundreds of encrypted passwords to various accounts behind one protected password.

"It's pretty ordinary for CEOs and executive assistants to share confidential information by email," he said. "They feel that their email is secure and they have nothing to worry about."

The fact that Lynton regularly received emails with his passwords was particularly a problem for Sony because hackers who steal corporate data often will immediately search for the word "password" or a variation of the word across thousands of messages.

"If I'm trying to get credentials, that's the first search I'm going to run," said Mitnick, who is hired by companies to test their internal security.

The October email inside Sony, among tens of thousands of messages stolen in the crime, described specific software and hardware upgrades and plans to hire an outside consulting firm to improve the company's network, plus new rules to limit the amount of old emails that would be stored on servers. Lynton received it roughly three weeks before employees reported signs that hackers were rummaging inside Sony's computer network.

Citation: Sony emails show a studio ripe for hacking (2014, December 18) retrieved 27 April 2024 from https://phys.org/news/2014-12-sony-emails-studio-ripe-hacking.html