1-The New York Times-LinkedIn

June 10, 2012

SAN FRANCISCO — LinkedIn is a data company that did not protect its data. *[Disappointment]*

Last week, hackers breached the site and stole more than six million of its customers' passwords, which had been only lightly encrypted. They were posted to a Russian hacker forum for all to see.

That LinkedIn was attacked did not surprise anyone. Companies' computer systems are attacked every day. Indeed, the CBS music site Lastfm.com and the dating site eHarmony confirmed last week that millions of user passwords were stolen.

What has surprised customers and security experts alike is that a company that collects and profits from vast amounts of data had taken a bare-bones approach to protecting it. *[Disappointment]* The breach highlights a disturbing truth about LinkedIn's computer security: there isn't much. *[Disappointment]* Companies with customer data continue to gamble on their own computer security, even as the breakins increase.

"If they had consulted with anyone that knows anything about password security, this would not have happened," said Paul Kocher *[Disappointment]*, president of Cryptography Research, a San Francisco computer security firm.

Part of the problem may be that there are few consequences for companies with a devil-may-care attitude toward data. There are no legal penalties. Customers rarely defect. And in LinkedIn's case, its stock price actually rose in the days after the breach. *[Hope]*

What especially concerns many people on this particular breach was that LinkedIn was not some green start-up or a company unfamiliar with data. After a highly successful initial public offering in May last year, it has piles

of cash. It recruits top talent. And it makes money. It also has 160 million members who share their business connections in the hopes of making a broader and more efficient network. And they want their data to be protected. *[Disappointment]*

"I expected better from LinkedIn," said Craig Robert Smith *[Disappointment]*, a professional musician and product manager at Buzzmedia. "But I can't delete my account because it's the place to be in terms of getting recruited and networking. *[Hope]*"

Image

LinkedIn's headquarters in Mountain View, Calif. The breakin has surprised some because data is the company's business.Credit…Paul Sakuma/Associated Press

It was not immediately clear how hackers were able to breach the system, how long they had been there, or if they are still poking around inside. LinkedIn does not have a chief security officer whose sole job it is to monitor for breaches. *[Disappointment]* The company says David Henke, its senior vice president for operations, oversees security in addition to other roles, but Mr. Henke declined to speak for this article. *[Deny]*

On a grading scale of A through F, experts say, LinkedIn, eHarmony and Lastfm.com would get, at best, a "D" for password security *[Disappointment]*. The most negligent thing a company can do with users' passwords is store them in plain text. That was the case with RockYou, a gaming site that lost 30 million user passwords in a 2009 breach. The most basic step they can take to protect passwords is camouflage them with basic encryption — what is known as "hashing" — in which they mash-up a password with a mathematical algorithm and store only the encoded, or "hashed," version.

But hackers are a determined bunch. They use automated tools that can test up to a million passwords a second. To crack hashed passwords, they exploit so-called dictionaries, extensive online databases of common passwords and their precalculated hash values. Some sites contain sublists of foreign passwords — in Finnish, say — or even religious-themed

passwords (“angel,” “Jesus” and “God” were among the top 15 LinkedIn passwords cracked). Other hackers use “rainbow tables,” which list hash values for nearly every alphanumeric character combination, up to a certain length. Some sites publish as many as 50 billion hash values.

To make hackers’ jobs more difficult, diligent companies will append a series of random digits to the end of each hashed value, a process known as “salting,” which requires only a few more lines of code and can be done at no cost.

Salting passwords, security experts say, is Security 101 — a basic step that LinkedIn, eHarmony and Lastfm.com all failed to take. *[Disappointment]* (An A+ security grade involves hashing passwords with complex cryptographic functions, salting them, hashing the result again and storing those credentials on separate, secure Web servers where hackers cannot easily break in.)

“This isn’t rocket science,” Mr. Kocher said.

In a blog post after the breach, Vicente Silveira, a director with LinkedIn, said the company had invalidated passwords for compromised accounts and said members would “benefit from the enhanced security we just recently put in place, which includes hashing and salting of our current password databases.” *[Rebuild]*

But Julie Inouye, a spokeswoman for LinkedIn, would not say when the company started hashing and salting its passwords, or why it did not enact these security measures in the first place. *[Deny]*

On its face, a compromised LinkedIn account — where people rarely store more than their résumé — would not appear to have broad consequences. But hackers know full well that people tend to use the same password across multiple sites and will test those passwords on Web mail, bank, corporate or brokerage firm accounts, where precious personal and financial data is free for the taking. *[Worry]*

Video

June 11, 2011 — Data companies and the bare-bones approach to online security.

In this case, hackers posted a list of 6.4 million hashed passwords online and asked others to help crack them. By Thursday, some 60 percent of passwords had already been decoded. Mr. Kocher estimates that some 95 percent will eventually get cracked.

What to Know About Ransomware Attacks

Card 1 of 5

What are ransomware attacks? This form of cybercrime involves hackers breaking into computer networks and locking digital information until the victim pays for its release. Recent high-profile attacks have cast a spotlight on this rapidly expanding criminal industry, which is based primarily in Russia .

Why are they becoming more common? Experts say ransomware is attractive to criminals because the attacks take place mostly anonymously online, minimizing the chances of getting caught. The Treasury Department has estimated that Americans have paid $1.6 billion in ransoms since 2011.

Is there any connection to the rise of cryptocurrencies? The criminal industry’s growth has been abetted by cryptocurrencies , like Bitcoin, which allow hackers to transact with victims anonymously, though experts see virtual currency exchanges as a weak point for ransomware gangs.

What is being done about these attacks? The U.S. military has taken offensive measures against ransomware groups, and the Biden administration has taken legal and economic action. Recent attacks have propelled ransomware to the top of President Biden’s national security agenda .

Why is the government getting involved? The attacks, which were mostly directed at individuals a few years ago, have dramatically escalated as hackers have begun targeting critical infrastructure in the U.S. , including a major gasoline pipeline and meat processing plants .

In its blog post, LinkedIn noted that the user names associated with those passwords had not been posted online, *[Rebuild]* but security experts say that is probably because whoever breached its systems simply kept those for themselves.

“You don’t give up the crown jewels so other people can match them up,” said Jeremiah Grossman, founder and chief technology officer of WhiteHat Security.

The motivation of the hackers is apparent. But what mystifies security experts is why breaches keep happening. Mr. Grossman estimates that the cost of setting up proper password, Web server and application security for a company like LinkedIn would be a one-time cost of “a couple hundred thousand dollars.” *[Disappointment]* The average breach costs a company $5.5 million , or $194 for each record breached, according to a Symantec-sponsored study by the Ponemon Institute, an organization that tracks data breaches.

Mr. Kocher thinks he sees one reason in two charts he consults. One shows the number of airplane fatalities per miles flown, which decreased to one-thousandth of what it was in 1945, with the advent of the Federal Aviation Administration in 1958 and stricter security and maintenance protocols. The other, which charts the number of new computer security threats, shows the opposite. There has been a 10,000-fold increase in the number of new threats since 2002, according to data from Symantec, the antivirus firm.

The problem, Mr. Kocher and others security experts say, is a lack of liability. Computer security is not regulated and even as loads of sensitive personal, corporate and financial data gets uploaded daily, companies continue to skimp on basic protections. If 5 percent of airplanes in the United States crashed tomorrow, there would be investigations, lawsuits, a cutback in air travel and airlines’ stock prices would most likely suffer. With social networks, Mr. Kocher says, “People don’t vote with their feet.”

LinkedIn would not say whether any members had dropped the service since the breach became public on Wednesday, *[Deny]*but even as hackers worked diligently to crack its passwords, the company’s stock rose 4 percent by the end of the week. *[Hope]*

“Every time a plane crashes, the F.A.A. investigates and publishes the data in aggregate,” Mr. Grossman said. “With breaches, there’s no such thing. There’s no government agency. We don’t know where the bodies are buried, or how they got there.”