Team: Team 3

Inject Number: 46

Inject Duration: 20 Minutes

Inject Start Date/Time: Sat, 24 Mar 2018 14:11:26 -0500

From: CISO

To: Security Team

Subject: [S-227] Shareholder Breach Inquires

Relayed from: CEO, CPO and the Corporate Public Relations Officer

The Security Team has been asked to answer our shareholder and customer inquiry letters that are asking about possible matters and public rumors, that our network has been hacked and in essence being held ransom unless our executives disclose their personal financials. We need to implement our Incident Response Policy to handle any of these inquiries.
Please respond with a memo that your Team is ready to handle this.

Here is an example of one of the letters from an unnamed senator:
March 24, 2018
Ms. Jane Smith
Chief Executive Officer
Acme Company Inc.
701 First Avenue
Somewhere, CA 94089

Dear Ms. Smith:

We write following a possible troubling rumor that account information for more than 500 million Acme users is being held for ransom by hackers, compromising users' personal information across the Acme platform and on its sister sites, including Acme Mail, Flickr, Acme Finance, and Acme Fantasy Sports. The stolen data will include usernames, passwords, email addresses, telephone numbers, dates of birth, and security questions and answers. This is highly sensitive, personal information that hackers can use not only to access Acme customer accounts, but also potentially to gain access to any other account or service that users access with similar login or personal information,

including bank information and social media profiles.
We are even more disturbed that user information may have been compromised in 2018, and yet the company has not announced the breach at all to the public. That means millions of Americans' data may have been compromised and this is unacceptable. This breach is the latest in a series of data breaches that have impacted the privacy of millions of American consumers in recent years, but it is by far the largest. Consumers put their trust in companies when they share personal and sensitive information with them, and they expect all possible steps be taken to protect that information.
In light of these troubling rumors, if a breach of data has occurred and the ransom is paid, please answer the following questions to help Congress and the public better understand what went wrong and how Acme intends to safeguard data and protect its users, both now and in the future. We also request that Acme provide a briefing to our staff on the company's investigation into the breach, its interaction with appropriate law enforcement and national security authorities, and how it intends to protect affected users.

1.When and how did Acme first learn that its users' information may have been compromised? Please provide a timeline detailing the nature of the breach, when and how it was discovered, when Acme notified law enforcement or other government authorities about the breach, and when Acme notified its customers.
2.Press reports indicate the breach first occurred in 2018, but was not discovered until August of this year. If this is accurate, how could such a large intrusion of Acme's systems have gone undetected?
3.What Acme accounts, services, or sister sites have been affected?
4.How many total users are affected? How were these users notified?
5.What protection is Acme providing the 500 million Acme customers whose identities and personal information are now compromised?
6.What steps can consumers take to best protect the information that may have been compromised in the Acme breach?
7.What is Acme doing to prevent another breach in the future? Has Acme changed its security protocols, and in what manner?
8.Did anyone in the U.S. government warn Acme of a possible hacking attempt by state-sponsored hackers or other bad actors? When was this warning issued?

Thank you for your prompt attention to this critical matter.

Sincerely,
United States Senator _____

Press Contact David Carle: 202-123-3693

The security teams is tasked with drafting a response to this inquiry and to submit a professional well written response letter following your incident response plan and following your data classification polices, create a individual security or data breach notification letter and send it to the public relations officer ASAP.

Thank you.

CISO