Sony Pictures Breach (2014): A Security Analysis

Divya Aradhya

Saint Leo University

Author's Note

Saint Leo University

Contact: divya.aradhya@saintleo.edu

May 13, 2017

Table of Contents

Abstract

On November 24, 2014, Sony Pictures was victim to a massive data breach which crippled the company's operations and was billed as one of the most sophisticated cyberattacks. This paper summarizes the details of the breach, the causes that lead to the attack, and explores possible measures which can prevent similar attacks in the future.

Issue

Around 7 a.m. Pacific time on Monday, Nov. 24 Sony Pictures employees logging on its network were welcomed with the "sound of gunfire, scrolling threats, and the menacing image of a fiery skeleton looming over the tiny zombie-looking heads of the studio's top two executives."

In no time, the malware spread across the network planning over multiple continents and wiped out half of Sony's global network. It completely erased everything stored on 3,262 of the company's 6,797 personal computers and 837 of its 1,555 servers, nuked the startup software, and efficiently rendered the affected machines brain-dead.[1]

The worst was yet to be discovered. Before destroying the company's data, the hackers had silently stolen it and over the next three weeks they proceeded to release nine batches of confidential files onto public file-sharing sites. Unfinished movie scripts, mortifying emails, salary lists, 47,000 Social Security numbers, and four unreleased Sony films were splashed across the Internet causing Sony to face a lot of embarrassment, complete loss of operations, and severe financial losses.

Causes

In December 2014, the Federal Bureau of Investigation (FBI) reported that it had evidence that North Korea was behind the attack. The group of hackers, who called themselves "Guardians of Peace" (GOP) launched the attack on Sony Pictures, as Sony had been plan its release of "The Interview," a satire targeting that country's dictator.[2]

The attack was a highly-skilled one, intensely and specifically targeted at Sony pictures, who didn't see it coming. Members of GOP, in various anonymous interviews with journalists, reported that Sony "doesn't do physical security" and that employees had let them into the premises with just a bit of social engineering. The hackers had then walked into offices which

were “unlocked”, accessed systems, and finally even stole a password from “someone in IT” [3]. They then implanted the malware which proceeded to steal other passwords and grant them access to confidential media files, databases containing employee PII data, emails, and financial documents.[3]

Prevention

Preventing a breach and a cyberattack requires both human and technical defenses.

A change in mindset regarding security needs to be ingrained into each and every employee top-down. Comprehensive security policies and strict enforcements which take to account physical security (locks and access cards), address password habits (changing of passwords, writing down passwords, sharing of passwords), train personnel on the perils of social engineering (physically, through the phone, and via phishing emails and texts) are necessary, and indeed critical for an organizations security health.

Technology should also be in place to detect, prevent, and log unusual activity (accessing confidential databases, copying files, modifying data, attempting to delete information) even if the source has been authenticated and has access permissions.

Conclusion

The Sony Pictures breach was a wakeup call to companies all over the globe to be constantly vigilant, to invest in protecting their digital data, and to understanding that the cost of carelessness can prove near fatal. Sony Pictures paid a very high price, though, to teach the corporate world essential cybersecurity lessons.

References

1. Elkind, P. (2015, June 25). Sony Pictures: Inside the Hack of the Century. Retrieved from http://fortune.com/sony-hack-part-1/
2. Barrett, D. (2014, December 19). FBI Says North Korea Behind Sony Hack. Retrieved from https://www.wsj.com/articles/fbi-says-north-korea-behind-sony-hack-1419008924
3. Bort, J. (2014, December 19). How The Hackers Broke Into Sony And Why It Could Happen To Any Company. Retrieved from http://www.businessinsider.com/how-the-hackers-broke-into-sony-2014-12