Team Members: Tia W., Al-Khem Wilson, Jadyn Anderson, Steven Geter, Amari Boyd

Sony Pictures Hack Report

The Sony Pictures Hack shows the need for basic cyber hygiene at all levels of a company's workforce, and how sociology and psychology are closely connected to cybercrime.

What was the breach?

The breach was officially discovered by Sony on Monday, November 24th, 2014, a year after the initial breach occurred. It was started by a North Korean hacker group called the "Guardians of Peace", also known as the "Lazarus Group". The breach consisted of personal employee information, executive salaries, emails, and at the time, unreleased films and content.

What was impacted?

Attackers gained unrestricted access to the entirety of Sony's network. Malware infected and erased data across nearly half of the 6,800 personal computers, and more than half of the 1,555 servers in the Sony studio network. Sony lost access to all of their online resources and was forced to use offline machines and paper checks. Public image was in shambles, and Sony had a challenging task in having to recover that data while already being pressed financially. Sensitive information was leaked across the next few weeks, and Sony spent the next two months trying to fix and repair all of the damage.

Theatres refused screenings for the movie, leading Sony to cancel the premiere of the film almost entirely. The film was then limited to digital download with a limited theatrical release the following day. Other movies were leaked before release as well, which cost Sony even more in damages.

How did it happen and why?

The company used outdated information security practices and reportedly their employees had poor digital hygiene. Sony failed to implement basic security measures such as two-factor authentication, which was paired with weak, easy-to-guess passwords that often contained personal information. The emails were stored encrypted on their servers for more than 7 years, and employees were targeted via spear-phishing emails with fake Apple ID verification links. The hackers used modified tools like worms and wipers to get into the system without being detected by antivirus software that only could detect previous malware. Motives were mostly unclear, but later demanded that Sony stop the release of "The Interview," a comedy film involving a plot to assassinate North Korea's leader.

How does the CIA triad come into play?

Attackers used a malware called the "Wiper" erasing data from the company's servers and destroying original data. This affected integrity because it corrupted Sony's information systems and decreased the trustworthiness or their accuracy. The hack also caused the leak of public data, where confidentiality was affected, which was private only to Sony Pictures before. This also caused Sony's servers to go down, which affected the availability of their online services like PlayStation Network for about 2 months.