Incident Response Team

Report №2

The Sony Pictures Hack

November 24, 2014

27.09.2025

Almaty

Table of Contents

Introduction

Sony Pictures Entertainment remains one of the major and most beloved mass media entertainment conglomerates of the world. *Skyfall, Spider-Man, Little Women, Ghost Rider, Gran Turismo* – the studio knows how to attend to anyone's needs.

In November 2014, Sony Pictures Entertainment experienced a cyber attack that would become a groundbreaking moment in cybersecurity realm. It was related to the planned release of the controversial film *The Interview* tied to North Korea, which intelligence reports later attributed to a nation-state attacker.

Foreign hacker group – *"Guardians of Peace"* – compromised SPE's network via an advanced form of malware:

- Several terabytes of SPE's sensitive data and intellectual data were stolen.
- Original copies were wiped out from all company technology.
- A warning was made – if Sony fails to meet their demands, all stolen data shall be released.

The hack not only led to the leaking of unreleased films and confidential data, it also highlighted the serious implications of inadequate cybersecurity measures for such big organizations, corporations and governments alike.

Noth Korea was blamed for the attack, but no official statements were made.

The Algorithm of The Attack

Behind the scenes (early - mid 2014)

- **Target:** Sony's corporate network, specifically its internet-facing servers.
- The threat actors, known as the "Guardians of Peace" (GOP), are believed to have first gained access by deploying malware on Sony's systems via a "spear-phishing" campaign.
- This likely involved tricking employees with privileged access into installing malicious software, giving the attackers a foothold. They also potentially exploited unpatched vulnerabilities in Sony's public-facing servers. Initial breach was stealthy and designed to avoid detection, allowing the attackers to establish a persistent presence within the network.

Movement Escalation (months up to November 2014)

- Once inside, the attackers performed extensive **internal reconnaissance**. They mapped the network to locate its most sensitive digital assets.
- Their primary targets were not just file servers, but also the Active Directory controllers - the "keys to the kingdom" that manage user accounts and permissions across a corporate network. By compromising these, they could effectively impersonate any user, including system administrator
- Using these stolen administrative credentials, the attackers moved freely throughout the network.

Detonation (November 24, 2014)

- After completing their data theft, the attackers initiated their final assault. Instead of deploying ransomware to encrypt files for money, they deployed a destructive Wiper malware.
- This malware was designed not for extortion, but for pure sabotage. It overwrote the hard drives and master boot records of thousands of computers and servers, rendering them permanently inoperable.
- Simultaneously, workstations across Sony Pictures were hijacked, displaying a red skeleton image and a message from the "*Guardians of Peace*" threatening to release the stolen data.

Impact (November 2, 2020)

- The attack caused catastrophic operational damage. Sony's entire IT infrastructure was crippled; employees could not access email, phones, or their workstations. The company was forced to return to using pen and paper for basic operations.
- The hack was ultimately blamed on the North Korean government, motivated by Sony's upcoming film *The Interview*, a comedy depicting the assassination of Kim Jong-un. This elevated the incident from a corporate data breach to an act of state-sponsored cyberterrorism with global geopolitical ramifications.

The Damage Made

Victims

The victims of this ransomware attack were the organization and its employees. Slow and deliberate release of the stolen data led to immense public embarrassment, legal liabilities, and security risks for employees.

Sony Pictures situations prior the attack:

The situation of Sony Pictures Entertainment prior the attack was already unstable. In 2011 alone not only the infamous 'War on Hackers' was declared, Sony's various divisions saw their networks breached more than 20 times.

Besides the toll on the company's public image, this scandal generated boycotts of Sony products, class-action lawsuits and lawsuits by states attorneys general, as well as charges by the U.S. Federal Trade Commission.

Post-attack:

The breach had significant immediate and long-term consequences for Sony Pictures. Beyond the immediate financial loss, the incident impacted Sony's reputation, shook its shareholder confidence, and raised questions about cybersecurity preparedness in the entertainment industry.

Consequences

- Reputational damage
- Great operational disruption
- Private information of employees as well as intellectual property was leaked
- Estimated damage of $15 million in the immediate aftermath

Vendors' Recommendations

The core lesson is that modern defense requires a "Assume Breach" mentality: make initial access harder, detect lateral movement faster. What does it mean for corporations like Sony? Defense must focus on limiting initial access, strictly controlling internal privileges, and aggressively hunting for threats – attacker's "dwell time" should be shrank from months to minutes

Microsoft – microsoft.com

Preventive recommendation: implement Microsoft's "Secure Privileged Access" framework. This involves strictly segmenting administrative accounts from standard user accounts and enforcing Multi-Factor Authentication (MFA) for *all* privileged access, especially to Active Directory. Additionally, deploy Microsoft Defender for Identity, which uses Active Directory signals to detect and alert on malicious reconnaissance and lateral movement techniques used to compromise identity systems.

Palo Alto Networks & CrowdStrike – paloaltonetworks.com & crowdstrike.com

Preventive recommendations:

- Adopt a *Zero-Trust Architecture*. This means moving away from the old "model where anyone inside the network is trusted and instead verifying every request as if it originated from an untrusted network.
- Use *Next-Generation Firewalls* (NGFWs) for micro-segmentation to create internal barriers that limit lateral movement.
- Complement this *with Endpoint Detection and Response* (EDR) tools on every workstation and server to record process activity and provide deep visibility for threat hunting, catching attackers during their internal reconnaissance phase.

Sony's Solution

Following the attack, Sony Pictures undertook a massive transformation of its security posture. This included a complete rebuild of its IT infrastructure with a foundational focus on *identity and access management* (IAM), strictly enforcing the principle of least privilege. They invested heavily in *Security Information and Event Management (*SIEM) technology to aggregate and analyze logs from across the network for anomalous activity.

The company also established a dedicated, well-funded internal security team and mandated cybersecurity training for all employees, with a special emphasis on identifying carefully hidden phishing attempts.

My Recommendations

My role: tech employee, pentester.

The Sony attack is a masterclass in what we fear most: a patient, silent takeover. From my perspective, Sony's breach wasn't about a single technical flaw, but a systemic failure in defending the "crown jewels": their identity and access management system. If I were tasked with hardening a company against such an attack, my focus would be on making the attacker's life unbearably difficult once they get past the front door.

Preventive measures

My goal would be to shatter the old notion of a trusted "internal network." I'd push for a *Zero-Trust architecture* built on two pillars. First, strict *segmentation*. I'd advise carving the network into isolated zones, so if I compromise a marketing workstation, I hit a wall before I can even see the Active Directory servers. Second, and most critically*, privileged access management* (PAM). I'd demand that administrative credentials are treated like nuclear codes - used only from dedicated, hardened machines, with multi-factor authentication that can't be bypassed. The Sony attackers won because they stole the keys to the kingdom; my job is to put those keys in a vault, not leave them under a mat.

Minimizing negative consequences

If an attacker does get in, the clock starts. My focus shifts to detection and response. I would insist on deploying *Endpoint Detection and Response* (EDR) tools on every critical server and workstation. These tools are my eyes and ears, recording activity so I can hunt for the subtle signs of reconnaissance - like when an attacker starts mapping the network or searching for sensitive files. The goal is to cut their dwell time from months to days or hours. Finally, I'd advocate for regular Purple Team exercises, where my Red Team works directly with the Blue Defense Team to test these detection capabilities. It's not about if they get in; it's about how quickly we can kick them out before they can pull off a Sony-scale heist.

Appendix

1. “Cyber Case Study: Sony Pictures Entertainment Hack”, Cyber Liability Insurance, https://coverlink.com/case-study/sony-pictures-entertainment-hack/
2. “Update on Sony Investigation”, FBI Press Releases, https://www.fbi.gov/news/press-releases/update-on-sony-investigation
3. “The Sony Pictures Breach: A Deep Dive into a Landmark Cyber Attack”, Framework Security, https://frameworksecurity.com/post/the-sony-pictures-breach-a-deep-dive-into-a-landmark-cyber-attack
4. “The Hacking of Sony Pictures: A Columbia University Case Study”, Columbia University School of International and Public Affairs, https://www.sipa.columbia.edu/sites/default/files/2022-11/Sony%20-%20Written%20Case.pdf
5. “Sony Pictures Entertainment Attack”, Cyberlaw, https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014)