Historic Cybersecurity Breaches Caused by a Lack of Physical Security

ISAAC BOAZ

Cybersecurity requires many layers and aspects of security to achieved. This article analyzes and reviews historical occurences where a lack of physical security lead to a lack of cybersecurity. In addition to introduction, an analysis and review of such occurences will be presented.

Additional Key Words and Phrases: Cybersecurity, Security, Software, Physical, Breaches

1 INTRODUCTION

In the world of software and programs, many people in the cybersecurity field focus on the security and practices used in their software and programs. However, one of the most well-known ideas for security is the idea that your security is only as strong as your weakest link. Just as electricity follows the path of least resistance, hackers and cybercriminals need only find a single weak point in your security to gain access to the rest of your system.

Physical security is a part of cybersecurity. The act of protecting and securing IT assets, data, and resources from physical attacks is a part of cybersecurity. This article will review and analyze historical occurences where a lack of physical security lead to a lack or even breach of cybersecurity.

2 BASIC PHYSICAL SECURITY

Regardless of what a device is doing, it is always important to understand the physical environment and security that the device is in. Even the best anti-virus software cannot be protected from a malicious actor uninstalling it. Physical access can mean a man in the middle attack, power outages, or even a keylogger being installed.

Some basic physical security practices include:

- Locking a device when not in use
- Restricting physical access to those that need it
- Locking the doors and windows of a building
- Scanning and limiting who can enter a building

Ultimately, physical security can be just as important and just as in-depth as cybersecurity.

3 GOOGLE'S PLASMA GLOBE [1]

One of the best ways to test your security is by doing it yourself. Google went about this by creating a "Red Team", a team of white-hat hackers that were tasked with trying to hack Google. Though this task certainly includes doing software-based attacks, one of the successful attacks was actually a physical attack.

Author's address: Isaac Boaz, isaac.k.boaz@gmail.com.

3.1 Attack

The Red Team designed a Plasma Globe that had a USB cable attached to it for power. Only five plasma globes were created with a malicious modification to them. The Red Team added an internal chip that would emulate a USB keyboard when plugged in to a computer. After approximately 5-10 minutes [3], the device would quickly type out a command to download a larger payload from the internet. In order to give the device to Google's employees, the Red Team disguised the device as an anniversary gift from Google (based off of LinkedIn).

While not everyone that received the device plugged it in, it only took one of Google's employees to plug it in for the attack be successful. The Red Team gained unauthorized access to the documentation on Google's Glass, which at the time was heavily in development.

3.2 Analysis

What ultimately allowed this attack to be successful was improper training, understanding, and awareness of physical security. Google's employees were not trained to be aware of the potential dangers of plugging in a USB device was given to them.

This attack also highlights the importance of physical security. If Google employees were not allowed to bring in unauthorized external devices, this attack would not have been successful.

3.3 Mitigation

Google learned from this breach and created a software that would listen to extremely fast keystrokes from USB devices and block them. This software was then installed on all of Google's computers.

While a software solution is a good start, it is not a complete solution. A theoretical slow USB device could still be used to bypass this software. A better solution would be to train employees to be aware of the dangers of plugging in unauthorized devices.

4 NOW YOU SEE ME 2

While not a real-life example, the movie Now You See Me 2 [2] presents a potential example of a physical security breach. In the movie, the main characters are able to breach a company's phone presentation by disguising as server maintenance, quickly convincing security that the original server maintainer was crazy, and installing a device that would allow them to control the presentation.

4.1 Attack

While very entertaining, the attack in the movie is not entirely realistic. Quick uniform changes and pretending that you belong was presented to seem entirely plausible. Regardless, the important parts of the attack were that the server room was easily accessible by all staff without only one layer of security. The single layer was a wired door that was left open by the original server maintainer.

Once the main character was in the server room disguised, he took a portable camera that could immediately print out a picture and pretended that it was "picture day" for the maintainer. The maintainer was not fooled by the lies, however, he was too confused and insisted that the character should not be there. Regardless, The main character printed out the picture and placed it on a badge for a mental facility.

Upon calling for security, the main character was able to convince the security that the maintainer was crazy and that he was the real maintainer. The main character was then able to install a device that would allow him to control the presentation.

4.2 Analysis

This attack was successful because of a lack of physical security. The server room was easily accessible by all staff and only had a single layer of security. The maintainer also left the door open, allowing the main character to easily enter the room. With no physical keycard, identification, or other security, the main character was able to easily enter the room.

4.3 Mitigation

Ideally, the server room would have had a physical keycard, identification, or other security that would have prevented the main character from entering the room. The maintainer should have also locked the door behind him, preventing the main character from entering the room. Lastly, ideally the security guards would have been trained to be aware of social engineering and to not be easily convinced by lies.

5 MISSION IMPOSSIBLE

A much more realistic example of a physical security breach is in the movie Mission Impossible. In the movie, Ethan Hunt (played by Tom Cruise) is tasked with stealing the NOC list from a CIA building. The NOC list is a list of all CIA agents that are currently undercover. The CIA building is heavily guarded and has many layers of security.

5.1 Attack

In the movie, we are shown the many physical layers of security that the CIA building has. The building has a security guard, a security camera, a keycard reader, and a physical key. Access to the NOC list is also restricted to only the physical computer that the NOC list is on. The server room employs many measures and monitors to prevent unauthorized access.

Specifically, the server room has pressure-sensitive floors, a temperature monitor, sound sensor, and lasers above the ventilation system. All of these measures are disabled while an authorized person is in the room, and re-enabled when they leave.

Ethan Hunt goes through the ventilation system, uses a mirror to reflect the lasers, and is slowly lowered to the floor by a wire. He then hacks into the computer and steals the NOC list.

5.2 Analysis

Here we can see that the CIA building has many layers of physical security. Despite all of these layers, Ethan Hunt was still able to breach the security. Unfortunately, the CIA building failed to account for plot armor, which is a classic mistake in the field of cybersecurity.

Realistically, the CIA building should have had a more secure ventilation system; we see that the team was able to get into the ventilation system (and the building itself) by disguising as firefighers. The CIA did not have proper protocols or procedures for fire alarms or drills, which allowed the team to easily enter the building.

Additionally, requiring an authorized person to be in the room to access the computer would be a good requirement.

REFERENCES

[1] Google. 2022. *EP003: Red Team | Hacking Google*. YouTube. Retrieved Jan 28, 2024 from https://youtu.be/TusQWn2TQxQ
[2] L. Leterrier. 2016. Now You See Me 2. https://www.imdb.com/title/tt3110958/
[3] Michal Zalewski. 2012. The Google plasma globe affair of 2012. *Coredumb.cx* plasma_globe (2012).