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

ACM Reference Format:
Isaac Boaz. 2024. Historic Cybersecurity Breaches Caused by a Lack of Physical Security. 1, 1 (January 2024), **??** pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

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

3 GOOGLE'S PLASMA GLOBE [**?**]

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.

XXXX-XXXX/2024/1-ART $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

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 [**?**], 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 [**?**] presents a potential example of a physical security breach. In the movie, the main characters