Lab - Cybersecurity Case Studies

Objectives

Research and analyze cyber security incidents

Background / Scenario

Governments, businesses, and individual users are increasingly the targets of cyberattacks and experts predict that these attacks are likely to increase in the future. Cybersecurity education is a top international priority as high-profile cyber-security related incidents raise the fear that attacks could threaten the global economy. The Center for Strategic and International Studies estimates that the cost of cybercrime to the global economy is more than $400 billion annually and in the United State alone as many as 3000 companies had their systems compromised in 2013. In this lab you will study four high profile cyberattacks and be prepared to discuss the who, what, why and how of each attack.

Required Resources

- PC or mobile device with Internet access

Step 1: Conduct search of high profile cyberattacks.

a. Using your favorite search engine conduct a search for each of the cyberattacks listed below. Your search will likely turn up multiple results ranging from news articles to technical articles.

   Home Depot Security Breach

   Target Credit Card Breach

   The Stuxnet Virus

   Sony Pictures Entertainment Hack

   Note: You can use the web browser in virtual machine installed in a previous lab to research the hack. By using the virtual machine, you may prevent malware from being installed on your computer.

b. Read the articles found from your search in step 1a and be prepared to discuss and share your research on the who, what, when, where, and why of each attack.

Step 2: Write an analysis of a cyberattack.

Select one of the high-profile cyberattacks from step 1a and write an analysis of the attack that includes answers to the questions below.

a. Who were the victims of the attacks?

1. Home Depot Security Breach: Victims of the attack are Home depot customers who were doing shopping at the time of the attack. Over 50 million customers had their credit card information and email addresses stolen.
2. Target Credit Card Breach: Victims of this attack are Target customers who used credit or debit cards at the retailer during the time the attack occurred. Over 40 million customers had their credit card information, names, addresses, and telephone numbers stolen.
3. The Stuxnet Virus: The primary victims of the Stuxnet virus were organizations that used industrial control systems, specifically those in the energy and critical infrastructure sectors. The virus was believed to have been specifically targeted at Iran's nuclear program.
4. Sony Pictures Entertainment Hack: The primary victim of this hack was Sony Pictures Entertainment, a subsidiary of Sony Corporation. The breach resulted in the release of sensitive company information, including employee and executive information, emails, and unreleased films.

b. When did the attack happen within the network?

1. Home Depot Security Breach: In 2014 and affected 56 million credit and debit card accounts.
2. Target Credit Card Breach: In 2013 and exposed 40 million credit and debit card accounts, as well as 70 million records containing customer names, addresses, phone numbers, and email addresses.
3. The Stuxnet Virus: In 2010 and was aimed at disrupting Iran's nuclear program by damaging centrifuges used in uranium enrichment.
4. Sony Pictures Entertainment Hack: In November 2014 and resulted in the release of confidential information, including emails, personnel files, and financial data.

c. What technologies and tools were used in the attack?

1. Home Depot Security Breach: The attackers used custom-built malware to steal payment card information from Home Depot's point-of-sale systems.

2. Target Credit Card Breach: The attackers used malware to steal payment card information from Target's point-of-sale systems.

3. The Stuxnet Virus: The Stuxnet virus is a complex piece of malware that was discovered in 2010 and was used to attack the Iranian nuclear program. The virus used a number of different techniques to spread and infect systems, including the use of vulnerabilities in industrial control systems and the use of removable drives.

4. Sony Pictures Entertainment Hack: The attackers used a combination of social engineering, malware, and access to the company's internal network to steal sensitive information, including confidential emails.

d. What systems were targeted?

1. Home Depot Security Breach: The systems targeted in the Home Depot security breach were the company's point-of-sale (POS) systems, which process credit and debit card transactions.
2. Target Credit Card Breach: The systems targeted in the Target breach were the company's payment card systems, including their point-of-sale registers.
3. The Stuxnet Virus: The Stuxnet virus was aimed at disrupting industrial control systems (ICS), specifically those used in Iran's nuclear program. The virus targeted programmable logic controllers (PLCs), which are used to control industrial processes.
4. Sony Pictures Entertainment Hack: The systems targeted in the Sony Pictures hack were the company's computer networks and servers, which contained confidential information such as

emails, personnel files, and financial data. and personal employee information. The attackers also used a wiper malware to destroy data on the company's systems

e. What was the motivation of the attackers in this case? What did they hope to achieve?

1. Home Depot Security Breach: The motivation of the attackers in the Home Depot security breach was financial gain. They likely sought to steal credit and debit card information, which they could then sell on the black market or use for fraudulent purchases.
2. Target Credit Card Breach: The motivation of the attackers in the Target breach was similar to the Home Depot breach, with the goal of stealing credit and debit card information for financial gain.
3. The Stuxnet Virus: The motivation behind the Stuxnet virus was geopolitical in nature. It is believed to have been created by the U.S. and Israel in an effort to disrupt Iran's nuclear program.
4. Sony Pictures Entertainment Hack: The motivation behind the Sony Pictures hack was a combination of political and financial.

f. What was the outcome of the attack? (stolen data, ransom, system damage, etc.)

1. Home Depot Security Breach: The outcome of the attack is stealing 56 million credit and debit card details and associated personal identification numbers.
2. Target Credit Card Breach: The outcome breach was the theft of 40 million credit and debit card numbers, as well as the exposure of 70 million customer records containing personal information.
3. The Stuxnet Virus: The outcome of significant physical damage to Iran's nuclear program. It is believed to have destroyed up to one-fifth of Iran's centrifuges, which are used in uranium enrichment.
4. Sony Pictures Entertainment Hack: The outcome of the attack is theft and release of confidential information, including emails, personnel files, and financial data.