Detailed Analyses on Various Cyber Security Breaches

M. Fitzhugh

redeyesyami@yahoo.com

Columbia Basin College

CSIA 440 – 3014 Cyber Test and Penetration

Spring 2020

Case Studies on Various Cyber Security Breaches

Introduction

The purpose of this project is to write case studies on various cyber security breaches: Insider Threat; Advanced Persistent Threat; Ransomware; Cyberespionage; and Cyberstalking. Each case study will include a brief summary of the breach, a definition of each type of attack, an explanation of what went wrong, an explanation of how the attack could have been prevented, and measures to be instituted to guard against future attacks. The project will be concluded with a summary of key learning points in the management of cyber security within enterprises. These analyses will demonstrate knowledge of cyber security threats and the ways to prevent them.

Insider Threat

An Insider Threat is "users with legitimate access to company assets who use that access, whether maliciously or unintentionally, to cause harm to the business" (Goldstein, 2019). According to Goldstein, Insider Threats can not only be committed by current employees, but by former employees, contractors, or even partners who have had access to the organizations system or data. Insider Threats can be incredibly damaging to an organization due to the consequences of data breaches. According to Ekran Systems, data breaches could mean the loss of trade secrets and customers private data. The consequences of the loss of these data include "the loss of customer trust, financial losses, ruined business reputation, regulatory fines, and falling share prices" (Ekran System, 2020). Insider Threats represent 60 percent of data breaches (Goldstein, 2019), and have an average annual cost of $11.45 million (Sussman, 2020).

An example of an Insider Threat is of Anthony Levandowski and Waymo (Google's self-driving car project). Levandowski was a lead engineer who left Waymo in 2016 to start his own company Otto, to develop self-driving trucks that ended up being acquired by Uber a few months in (Ekran System,

2020). A month before leaving Waymo, Levandowski copied nearly 14,000 files from one of Google's servers that was used to house intellectual property, which Ekran System repots included trade secrets such as source code and simulations. Levandowski was able to steal this data because of his privileged access. According to Ekran Systems, Waymo's security team was not monitoring users with privileged access and failed to detect the theft until an investigation was done. This data breach could have been prevented if Waymo had policies in place for Privileged User Monitoring, Principle of Least Privilege and Server Room Security. If Waymo's security team was monitoring its privileged users, they would have detected the data breach sooner, and if they used the principle of least privilege, Levandowski would not have been able to access marketing information and possibly some of the confidential PDFs. Most importantly, if Waymo's servers were located in a designated room that could be locked and access limited, Levandowski would not have been able to plug his laptop into the server to steal the data. If Waymo institutes Privileged User Monitoring, Principle of Least Privilege and server room security, its security team will be able to detect and prevent data breaches.

Advanced Persistent Threat

Kaspersky defines Advanced Persistent Threats (APT) as "continuous, clandestine, and sophisticated hacking techniques to gain access to a system and remain inside for a prolonged period of time, with potentially destructive consequences." APT targets are "with the ultimate goal of stealing information over a long period of time" and "are increasingly using smaller companies that make up the supply-chain of their ultimate target as a way of gaining access to large organizations" (Kaspersky, 2018). APTs are incredibly dangerous because even after they are discovered and dealt with, there may still be backdoors left open by the attacker, and antivirus and firewalls are not always able to prevent APTs from occurring (Kaspersky, 2018).

An example of an APT is the Target breach of 2013. Attackers were able to gain access to one of Target's networks to steal 40 million customer debit and credit card information from over 1,800 stores nationwide (Krebs on Security, 2015). The attackers were able to steal logon credentials to Target's virtual private network (VPN) from Fazio Mechanical, a small heating and air firm that worked with Target, via malware from an email (Krebs on Security, 2015). This attack could have been prevented through User Awareness Training and Restricted RDP Access. Target could have required all employees from companies they partnered with, that would have access to their VPNs, to go through User Awareness Training; and by extension, Fazio Mechanical could have implemented a policy for User Awareness Training. User Awareness Training provides employees with knowledge of information such as phishing emails, and how to detect and avoid malicious links in emails. Had this training been implemented, it is highly possible that Fazio Mechanical would never have been infected by the malware that led to the Target breach. Another way this attack could have been prevented would be from Restricted RDP Access. Target could have restricted remote access to only the IP addresses they allowed, which would have prevented the attackers from being able to access the VPN remotely.

Ransomware

Malwarebytes defines ransomware as "a type of malware that prevents users form accessing their system or personal files and demands ransom payment in order to regain access." Ransomware began in the 1980s, demanding payment sent via snail mail, while payments demanded today are ordered to be sent via cryptocurrency or credit card (Malwarebytes).

An example of ransomware is that of WannaCry in 2017. WannaCry ransomware was used on computers using outdated Microsoft Windows operating systems (OS), holding user files hostage, and demanding a ransom paid of $300 worth of Bitcoin (Kaspersky, 2019). Shadow Brokers, the cyber criminals behind WannaCry, were able to take advantage of a vulnerability in the Microsoft Windows

OS. While a security patch was released two months prior to the WannaCry attack, many users and organizations did not update their OS allowing them to fall victim to WannaCry (Kaspersky, 2019). Kaspersky claims almost 230,000 computers were affected by the WannaCry attack (2019). This attack could have been prevented if organizations had a System Update Policy that maintained a regular schedule for updating the OS. Regular windows users could have also easily prevented this attack by configuring their computer to use Automatic Updates.

Cyberespionage

Cyberespionage is defined as "a form of cyber attack that steals classified, sensitive data or intellectual property to gain an advantage over a competitive company or government entity" (Carbon Black, Inc.). Many cyberespionage attackers use APTs to gain and keep access to their targeted network or system (Carbon Black, Inc.).

One example of cyberespionage is that of Operation Aurora in 2010. Back in the beginning of 2010, Google announced, "that it had been the target of a 'highly sophisticated' and coordinated hack attack against its corporate network. The hackers had stolen intellectual property and sough access to the Gmail accounts of human rights activists" (Zetter, 2010). Zetter cites Alperovitch, who claims "attackers used nearly a dozen pieces of malware and several levels of encryption to burrow deeply into the bowels of company networks and obscure their activity" (2010). Zetter goes on further to state that "the initial attack occurred when company employees visited a malicious website . . . Once the user visited the malicious site, their Internet Explorer browser was exploited to download an array of malware to their computer automatically and transparently" (2010). Like with APTs, this attack could have been avoided by User Awareness Training. Instructing employees on how to spot suspicious links in emails will reduce the number of links visited and reduce the chances of the user contracting malware from the suspicious website.

Cyberstalking

Cyberstalking can be defined as “stalking or harassment that takes place via online channels such as social media, forums or email. It is typically planned and sustained over a period of time” (Tripwire Guest Authors, 2019).

An example of cyberstalking is that of Kassandra Cruz, who cyberstalked a woman she found on a pornography website (FBI.gov, 2017). According to FBI.gov, Cruz created fake social media accounts of a U.S. Marine and friending the pornography actress, who she was able to track down online (2017). When the actress grew suspicious of the Marine, she blocked those accounts, which sent Cruz into a rage, who began to harass and threat the actress and the actress’ friends and family (FBI.gov, 2017). Before the FBI ended the stalking, from early 2016 through April, the actress received over 900 calls and texts to her cellphone, with nearly the same amount of calls made to her home and work phones (FBI.gov, 2017). The actress was able to fall victim to these massive amounts of calls and texts because she put her phone numbers on her profiles for all her friends, some of whom she did not know. There are a few ways in which a person can avoid a cyberstalking attack. The first way is to keep private information off the internet, including your address and phone number. To further expand on this, whatever information you do put online, make sure it is not posted with public access; keeping posts private will make sure only your friends can see what you post. Another way is to not accept friend requests from people you do not know.

Key Learning Points

There are many cyber security attacks aimed at obtaining private data. While there are many ways in which an attack can obtain that data, there are many ways in which users and organizations can protect themselves. One of the most important points I found was organizations implementing User Awareness Training. Many attacks can be prevented simply by training employees how to not fall victim

to phishing emails and suspicious links. Another key point I learned was how important it is to have proper password policies, especially with a password expiration policy. These policies force users to update their passwords. In doing so, it ends any unauthorized access that was obtain through the prior password, meaning an end to APTs and insider threats. The last key point I learned was how important it is to be aware of the various cyber security attacks and how to prevent them. While many attacks can be prevented by the same measures, there are many attacks that require different or additional measures to prevent those attacks from occurring.

Conclusion

In this project, I gave a detailed analysis on five different cyber security attacks. Included in these analyses were a description of the attack, a summary of the chosen case study and what went wrong, an explanation of how the attack could have been prevented, as well as any measures that should be implemented to avoid future attacks. I ended the project with a summary of my key learning points in cyber security management. Cyber security threats are ever growing in this day and age. Being educated on the different types of attacks, as well as on how to prevent and mitigate them is important, and this paper demonstrates just that.

References

Carbon Black, Inc. (n.d.). What is Cyber Espionage?: Cyber Espionage Definition. Retrieved June 03, 2020, from https://www.carbonblack.com/resources/definitions/what-is-cyber-espionage/

Ekran System. (2020, April 10). 5 Real-life Cases When Employee's Caused Data Breaches. Retrieved May 21, 2020, from https://www.ekransystem.com/en/blog/real-life-examples-insider-threat-caused-breaches

FBI.gov. (2017, January 03). Woman Sentenced for Cyberstalking. Retrieved June 03, 2020, from https://www.fbi.gov/news/stories/woman-sentenced-for-cyberstalking

Goldstein, J. (2019, November 12). What Are Insider Threats and How Can You Mitigate Them? Retrieved May 21, 2020, from https://securityintelligence.com/posts/what-are-insider-threats-and-how-can-you-mitigate-them/

Kaspersky. (2018, April 24). What Is an Advanced Persistent Threat (APT)? Retrieved May 21, 2020, from https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats

Kaspersky. (2019, November 06). What is WannaCry ransomware? Retrieved June 03, 2020, from https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

Krebs on Security. (2015, September 21). Inside Target Corp., Days After 2013 Breach. Retrieved May 21, 2020, from https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/

Malwarebytes. (n.d.). Ransomware - What Is It & How To Remove It. Retrieved June 03, 2020, from https://www.malwarebytes.com/ransomware/

Sussman, B. (2020, February 5). Ponemon: Insider Threat Costs Hit New Record. Retrieved May 21, 2020, from https://www.secureworldexpo.com/industry-news/ponemon-insider-threat-costs-hit-new-record

Tripwire Guest Authors. (2019, January 24). What Cyberstalking Is and How to Prevent It. Retrieved June 03, 2020, from https://www.tripwire.com/state-of-security/security-awareness/what-cyberstalking-prevent/

Zetter, K. (2010, January 14). Google Hack Attack Was Ultra Sophisticated, New Details Show. Retrieved June 03, 2020, from https://www.wired.com/2010/01/operation-aurora/

M. Fitzhugh

CSIA 440 – 3014 Cyber Testing and Penetration

Spring 2020

Project Deliverable 2: Retrospective

A. What worked well for you?

What worked well for me was that I was able to find many examples of the various cyber attacks to choose from and learn about.

B. What did NOT work well for you?

What did not work well for me was I was not able to write this paper in a way that would include visuals. Without delving deep into the mechanics of malware, there was no way for me to provide visuals for support.

C. What actions could you take to improve your work for the next project?

Actions to improve work on the next project that involves analysis of cyber security attacks would be to provide multiple examples of attacks. Take cyberstalking for instant, there are cases of people portraying themselves while stalking, and cases of people portraying a fake persona. Having multiple examples could help provide more insight into how attacks occur and why certain measures work to prevent them.

D. What did you learn most about yourself from this project?

What I learned most about myself is how shocked I was at finding out how many cyber security attacks were caused by employees falling for phishing scams. Even before I entered the Cyber Security program,

I was aware of fake emails and to not click on links from senders I did not trust. It is almost baffling that not everyone is aware of that in this day and age.