Connor Lauerman

11/22/2020

Analysis of the OPM Data Breach

With technology becoming increasingly more integrated into everyday life the need for cybersecurity is of utmost importance. A cyberattack is defined as "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information".[1] The fallout of such attacks can range from the loss of personal data to millions of dollars in recovery. With such a range in attack severity anyone who interacts with cyberspace is at risk.

One of the most severe types of attack is a state sponsored cyberattack which in some cases are considered acts of war.[2] While there have been many state sponsored attacks, this document will go into detail the Office of Personal Management or OPM attack of 2013 through 2015. This paper will go into detail the OPM breach, including the vulnerabilities and threats involved in the OPM attack. This paper will also present control objectives which would have mitigated the attack and reduce the impact. Additionally, this paper will explore the actions taken after the attack by OPM.

On June 4th,2015 OPM will announce to the public a breach to their system. This would be the start of the unraveling of a yearlong breach within OPM. By the end it will be revealed that 4.2 million personal files of current and former government employees, 21.5 million security background clearance investigation information including SF-86 forms, and 5.6 million fingerprints had been stolen.[3] In an unprecedented attack this would be in the top 5 largest data

breaches to be inflicted on the U.S. government.[4] While being such a large breach it all could have been avoided if the proper steps were taken to increase cybersecurity before the attack. Later the next year an even larger breach on the U.S. government will surface from a voting data base affecting 191 million U.S residents.[4] Attacks such as these bring into question the importance of cybersecurity for state actors and how the U.S. government prioritizes the information it keeps for its residence. Fortunately, by the end of the ordeal OPM will streamline its cyber security upgrade to prevent any further attacks and damage to the agency.

The OPM is an agency that creates products and services to enable HR strategy across different government agencies. One of the main functions of OPM is to conduct background information check on possible employees of the federal government.[13] Some of the information taken is employment history, financial history, mental health problems, drug abuse, gambling abuse, and home addresses of the employee along with the address of family members.[3] Other functions of OPM include training leaders of government agencies and handling retirement policies for federal employment.

Details of OPM breach

After Congressional hearings and testimony from employees of OPM it will be revealed that two separate but connected groups are able to gain foot holds on OPM network. The first group, which will be called X1, breaks into OPM networks. The second, called X2, will also break into the networks of OPM although several months later than X1. X2 will go unnoticed for months on OPM networks. In these months they will obtain 4.2 million personal files of federal employees. 21.5 million security background clearance investigation information, and 5.6 million fingerprints.[5] A complete breakdown of the breach goes as following[5,6]:

- In November 2013, the group X1 infiltrate OPM servers obtaining manuals OPM IT assets which give the intruders a framework of the OPM networks assisting in later attacks.
- The next month in December 2013 two contractors KeyPoint Government Solutions and USIS are breached. These contactors are involved with background investigations for national security workers.
- The following months OPM will come to realize that their networks were compromised. At this point OPM will not disclose to the public of this information. Instead, since the intruders were deemed not in a position to cause damage, OPM will allow them to remain on the systems to run counterintelligence on the hackers. In the meantime, OPM will develop a strategy called the "big bang" which would reset the system and purge X1 of access.
- Within these months the second group X2 will use credentials of KeyPoint employees to establish a foothold on OPM network. At this point X2 will install a remote access trojan under the name mcutil.dll to appear as a McAfee software. This trojan gave X2 a backdoor to OPM networks.[7] This breach was unnoticed by OPM.
- On May 27th, 2014 when X1 began installing keyloggers onto database administrators' workstations this will cause OPM to implement the "big bang" wiping X1 from the network. However, X2 will still have access through the backdoor trojan installed previously.
- At this point OPM believes it has removed any malicious traffic on its network. This allows X2 to go on unnoticed by OPM for close to a year. Early in this time

X2 will elevate the privilege of a non-admin account through attack vectors.[7] Additionally, X2 will gain credentials of many OPM employees login credentials including several admin credentials. X2 will then extract from OPM systems the background investigation information.

- This was not the end of X2 intrusion. As time continued X2 traversed OPM environment eventually gaining access to the Department of Interior Server. Once here X2 will extract the personal information of many federal employees.
- Near the end of the year long hack, X2 will extract the fingerprint data. This will be the last chunk of data stolen by X2.
- Shortly after a contractor from the company Cylance was applying cybersecurity updates. When one of their tools for finding malicious activity was activated the workings of X2 became clear. With the help of Cylance tools OPM is capable of expelling the hackers over a month time.[8]
- On June 4th, 2015 OPM will publicly announce that 4.2 million current and former employees were affected by the attack. It will not be for a month until the full scope of the attack is realized. This realization brings the total to 4.2 million personal files of federal employees. 21.5 million security background clearance investigation information, and 5.6 million fingerprints.

Now that the attack is described in full above the threats and vulnerabilities can be understood in this context. This paper will now go into an analysis of the threats and vulnerabilities.

Threats

Through the lack of cybersecurity in the OPM system, OPM was exposed to threats which resulted in the breach. A threat is defined as "event, action, actor, that searches for, identifies, and/or exploits vulnerabilities in a target environment or system which results in derogatory/harmful outcomes". The threats causing the breach were malicious actors successfully breaking into OPM's system. These malicious actors, also known as black hat

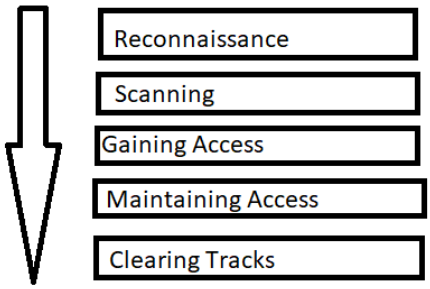

Figure 1[9]

hackers, executed steps from the phases of hacking(figure 1) to learn the environment, gain access and maintain access in the environment. In completing these phases X2 was able to steal a large amount of data.

The first threat is the reconnaissance from the hacker group X1 to breach the system initially and gain access to manuals and system architecture documents.[5] While the hacking phases may have been taken to initially gain access to OPM's it is known for sure the documents that X1 stole would help the hackers X2 in the reconnaissance and scanning phases for the second breach. With these documents the hackers learned the environment that would be targeted in the second breach by X2. Since the hackers attempted and succeeded to learn the system environment, this step was crucial for the hacker group X2 to succeed in stealing the data. However, the hacker group X2 still needed access to OPM's network.

To gain access the hackers breached a contractor KeyPoint Government Solutions. The hackers were able to get a hold of a compromised KeyPoint user credentials which allowed them

access to OPM's network.[10]. Since KeyPoint was a contractor they were given certain privileges on OPM's network. By leveraging the third-party cybersecurity weakness X2 was able to get access to OPM's network and since KeyPoint users were authorized they remained discreet within OPM's network.

Since malware is considered a separate threat it is worth mentioning that keyloggers began to be used by the group X1.[5] A keylogger is a type of spyware that monitors a user's activity. When installed maliciously it can be used to steal information from a user using an infected computer. The target of X1's keyloggers were admin computers in attempt to gain heightened privilege within OPM's network.[5]

Another form of malware used by the hackers was a remote access trojan.[7] A trojan is a type of malware that disguises itself as desirable code or software. In this instance, the trojan was disguised as a McAfee program. The trojan allowed the hackers X2 to maintain access within OPM's system after the "big bang" was executed. Additionally, the trojan allowed the hackers to exfiltrate the data by connecting to a domain of opm-security.org.[7] With the installation of the trojan the hackers were in an ideal spot since they were able to maintain access to the network while maintaining secrecy.

Vulnerabilities

The OPM had for a long time failed to prioritize cybersecurity in their agency and ignored requests from its inspector general to strengthen their security.[3] This led to a weak system that was very susceptible to attack. This paper will now go into detail each vulnerability that was exploited from the attack.

The first vulnerability was the leadership for OPM at the time of the attack. As stated previously, cybersecurity was not prioritized in OPM.[3] Moreover, the response to the first attack was a failure that led to theft of the personal information. After the first breach was discovered leadership at OPM should have taken it as a wake-up call and increased their security. However, with their response to eradicate the first breach with no upgrades security they left themselves vulnerable to more attacks. If the leadership had chosen to upgrade the system, then X2 would have been stopped and no personal information. This is especially saddening since the upgrades to the system would have been relatively easy which leads us to the next vulnerability.

OPM, against cybersecurity standards for government agency, had no two-factor authentication.[5] Two-factor authentication is a step to verify a user logging in by providing a second form of evidence that shows that are authorized on the network. This is usually done by sending an email or text to confirm the user with the login credential is indeed who they say they are. This was a major fail for OPM since with recommendation they did not add the two-factor authentication. In doing so, it allowed the hackers X2 to use compromised credentials from the contractors KeyPoint to gain access to OPM. This was such a failure by OPM since this step alone could have stopped the second breach and thus the data from being stolen.

Another vulnerability in OPM was the failure to keep inventory of their servers, databases, and networks.[3] Without inventory of these components there is no way for OPM to realize when something goes wrong. This led to poor knowledge of OPM's environment and allowed the hackers to traverse the network unnoticed. The keeping of inventory is standard for any enterprise and yet OPM failed to do so. This is not the only standard that OPM fails to accomplish.

OPM also failed to complete vulnerability scans on their network for several years.[11] Without this vulnerability scans there is no way for OPM to understand the possible risks within their system. This leads to a weak system that can be exploited and for hackers to go unnoticed on the network. In this specific hack the lack of vulnerability scans led to the hackers being able to increase their privileges to access unauthorized areas of the network.[7]

Control Objective

These vulnerabilities led to the breach of OPM and the theft of a large amount of data. This paper will now offer control objectives that would have mitigated or stopped the breach.

To cover the lack in leadership:

- Reduce lack of action in the case of a breach by the creation of protocol in the instances of a breach.
- Maintain the importance of cybersecurity and understand the risk involved om cybersecurity attacks.

For the weak network security:

- Validate users are who they say they are
- Reduce possibility of stolen credentials
- Understand all servers, systems, and networks in OPM
- Identify vulnerabilities in environment
- Limit communications from networks within OPM when not required
- Increase protection of OPM's network
- Have ability to scan network for malicious activity

- Only allow communication with domains on the internet that are known

For the malware:

- Understand all servers, systems, and networks in OPM
- Ensure that no malware has made its way into the environment
- Only allow systems to interact with known systems and code

OPM's Response

After the breach, OPM had underwent a complete rework of the IT infrastructure. Along with this rework, the addition of a new IT environment that included security controls.[3] One of these controls would be requiring two-factor authentication. With this upgrade OPM would cover the control objectives to validate users. With the reworks and addition of new environment OPM would complete the increase of protection in the environment. To further increase the protection of OPM systems OPM would begin modernizing its systems and networks. Additionally, cybersecurity tools were purchased giving OPM the ability to scan the environment for vulnerabilities and malware. Taking care of understanding all servers, systems, and networks OPM installed tools allowing them to see all devices connected to the network.[12] Since the hackers gained entrance through a third party credentials OPM has taken steps to avoid the use of third parties in background searches.[12] These changes substantially increased OPM's security from what it was. The other control objectives for the weak network security would not have action taken on them.

Changes to the leadership happened when the OPM director resigned and the CIO resigned. These changes in leadership would allow OPM to bring in new leadership that would take the cybersecurity risk more seriously. This can be seen since many of the

updates to the system were pushed by the new OPM director.[12] With these changes in leadership the culture of OPM has changed to focus more on the importance of cybersecurity, addressing the control objectives involved with leadership.

Summary

The OPM breach has been one of the top data breaches to hit U.S. government. With the lack of security and outdated system it was only a matter of time until a breach of this caliber hit OPM. If the correct steps were taken to identify vulnerabilities in OPM system a breach of this scale could have been avoided.

1. Editor, C. (n.d.). Cyber Attack - Glossary. Retrieved November 23, 2020, from https://csrc.nist.gov/glossary/term/Cyber_Attack

2. Corbeil, S. (2020, October 30). When should cyber attacks be considered acts of war? Retrieved November 23, 2020, from https://www.wearethemighty.com/mighty-culture/cyber-attacks-acts-of-war/
3. Meadows, M., Chaffetz, J., & Hurd, W. (2016, September 7). Committee on Oversight and Government Reform U.S. House of Representatives 114th Congress The OPM Data Breach: How the Government Jeopardized Our National Security for More than a Generation. Retrieved from https://web.archive.org/web/20180921190218/https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf
4. Lord, N. (2020, October 06). Top 10 Biggest Government Data Breaches of All Time in the U.S. Retrieved November 23, 2020, from https://digitalguardian.com/blog/top-10-biggest-us-government-data-breaches-all-time
5. Fruhlinger, J. (2020, February 12). The OPM hack explained: Bad security practices meet China's Captain America. Retrieved November 23, 2020, from https://www.csoonline.com/article/3318238/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html
6. Sternstein, A., & Moore, J. (2016, December 22). Timeline: What We Know About the OPM Breach (UPDATED). Retrieved November 23, 2020, from https://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/
7. Saade, C., Li, B., & Oh, S. (2017, April 20). OPM Data Breach. Retrieved from https://asamborski.github.io/cs558_s17_blog/2017/04/20/opm.html
8. Tucker, E. (2016, September 07). Missed opportunities detailed ahead of personnel agency hack. Retrieved November 23, 2020, from https://apnews.com/article/42ddc084ce184218bb3d83d706d71ea2
9. Greycampus. (n.d.). Retrieved November 23, 2020, from https://www.greycampus.com/opencampus/ethical-hacking/phases-of-hacking
10. Boyd, A. (2017, August 08). Contractor breach gave hackers keys to OPM data. Retrieved November 23, 2020, from https://www.federaltimes.com/smr/opm-data-breach/2015/06/23/contractor-breach-gave-hackers-keys-to-opm-data/
11. Pham, T. (2015, June 10). OPM Security Audit: No Two-Factor Authentication. Retrieved November 23, 2020, from https://duo.com/blog/opm-security-audit-no-two-factor-authentication
12. Naylor, B. (2016, June 06). One Year After OPM Data Breach, What Has The Government Learned? Retrieved November 23, 2020, from https://www.npr.org/sections/alltechconsidered/2016/06/06/480968999/one-year-after-opm-data-breach-what-has-the-government-learned
13. https://www.opm.gov/about-us/our-mission-role-history/what-we-do/#url=Human-Capital-Management-Leadership