**5-1 Case Study: Triple A and Defense in Depth**

Shaun D. Rester

Department of Technology, Southern New Hampshire University

CS-405-T4238: Secure Coding 23EW4

Professor. Aaron Demory

April 02,2023

While delving into Defense-in-Depth as it pertains to major security breaches, it is unambiguously clear that these instances could have benefited or perhaps been outright avoided by utilizing these approaches, Today I wish to speak more in depth on my finding regarding the Microsoft Exchange Server Data Breach which happened in 2021. The reason being, is because Microsoft is one of the largest tech and software companies around the globe, so any breaches regardless of scale or magnitude always tend to be newsworthy and deeply researched. Microsoft’s breach affected roughly 10,000 to 250,000 individual victims world-wide and in particular targeted small businesses and even government entities. Link: <https://cyberlaw.ccdcoe.org/wiki/Microsoft_Exchange_Server_data_breach_(2021)> . The first known breach was observed January 3rd of 2021.

For the shear scale of the attack one would assume a massive collaboration of attackers, in this case just over ten advanced persistent threat(APT) groups were working in cohesion to perform these attacks. They accomplished this by utilizing multiple methods during these attacks, four zero-day exploits by using vulnerabilities within Microsoft Exchange which gave them initial access to the servers. After gaining access they used the web shell backdoor method to prolong the access to the compromised servers, one of which even had the ability to execute commands such as upload, delete, and view files. The reason they targeted Microsoft was because of the vast reach they have around the globe be it private accounts, small to large businesses, even government agencies. Or in other words, the risk was well worth the potential reward.

As far as immediate threats go, the introduction of a new ransomware family called DearCry was one of the most preeminent. DearCry hijacked the servers making them unusable and then requested payment for the recovery of files. Potential threats, like these, could presumably go on forever if the vulnerability was not attended to immediately. Not only could loss of servers increase exponentially from the current attack, but with the breach becoming more well known other entities could start attacking the system, for their own malicious purposes. Such as gaining access to sensitive information to either ransom, or blackmail a company or individual for no other reason but to cause harm. The other potential issues are on the company itself, if they did not handle the vulnerability swiftly, their trust would be called into question which would certainly result in the loss of customers and potential lawsuits that would result in ever cascading financial losses.

Establishing proper tests and diagnostics of systems well in advance of the implementation date should be the initial step, when you are dealing with such large amounts of sensitive information one should never trust that the system is secure enough, always look to make it better. Utilization of the DiD method and establishing multiple layers of security around their servers would make it more difficult for attackers to gain access. Customer and server side could establish a continuous diagnostics system to help scan for potential ransomware frequently. CISA organization also suggests making sure that all systems are patched and up to date at all time to avoid risks, doing inventory frequently to verify sensitive information is protected, and adding security layers.

Authentication handles verification of users with a credential or other form of validation, gaining access through a vulnerability or faulty code makes that a bit more difficult to accomplish but it could have helped mitigate the web shell attacks that followed. Authorization goes hand in hand with authentication it is the verification of users by allowing permissions. Accounting can be broken down into the following, cost management, or keeping up with the day to day costs which could help focus on lost assets and money to be allocated towards security, and the actual accounting of the system, software, and assets. Defense in Depth is a security measure that utilizes multiple layers of security for each piece of information or software. This is an extremely pragmatic method for all aspects of software engineering by adding multiple redundant layers and adding fail safes in the event of a vulnerability to any specified layer.

**References**

The Cybersecurity and Infrastructure Security Agency. (n.d.) *How Can I Protect Against Ransomware.* Retrieved from https://www.cisa.gov/stopransomware/how-can-i-protect-against-ransomware

The Cybersecurity and Infrastructure Security Agency. (2021) *Mitigate Microsoft Exchange Server Vulnerabilities.* Retrieved from https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-062a

International cyber law: interactive toolkit contributors. (2021, August 12). “*Microsoft Exchange Server Data Breach” : International cyber law: interactive toolkit.* Retrieved from https://cyberlaw.ccdcoe.org/wiki/Microsoft\_Exchange\_Server\_data\_breach\_(2021)