Microsoft Exchange Server Hack

Microsoft Exchange Server is a platform developed by Microsoft that provides email, calendar, contact, scheduling, and collaboration features. It is typically used by businesses and runs on the Windows Server operating system. The platform is designed to allow users to access its messaging features from various devices, including desktops, mobile devices, and web-based systems (Bryan, n.d.). This platform is used by a large number of businesses and organizations for their communication needs. There have been instances of cyber-attacks targeting Microsoft Exchange servers in recent years, leading to substantial data breaches and other security incidents. However, in 2021 the vulnerabilities discovered in the Microsoft Exchange Server were exploited by threat actors to gain unauthorized access to many organizations' users email accounts and other sensitive information.

Why and how did the incident occurred?

The Microsoft Exchange Server hack in 2021 was suspected to be a nation-state hack, which refers to attacks conducted by hackers who receive financial and other support from governmental bodies to carry out their attacks. These groups have access to significant resources, which enables them to gain unauthorized access to targeted systems and accomplish their objectives. This attack resulted in the breach of several information accounting to several small to mid-sized companies, local government offices across the organizations in countries not limited just to United States, but also in Germany, United Kingdom, Netherlands, and Russia (Pitney, Spencer, Molly, & Suman, 2022). The Microsoft Exchange Server hack was not solely focused on stealing emails or intellectual property; rather, it had a larger objective. The nation involved in this attack collected the data with the ambition to lead the world in technology through artificial intelligence (Temple-Raston, 2021).

Attackers took advantage of multiple zero-day vulnerabilities found within the system. These vulnerabilities enabled them to bypass authentication controls, giving them access to crucial systems and data. This put sensitive information, such as email communications, customer data, and financial records, at risk of compromise. The first of the zero-day vulnerabilities were Server-Side Request Forgery (CVE-2021-26855) and other three were Deserialization (CVE-2021-26857), First File Write (CVE-2021-26858) and Second File Write vulnerability (CVE-2021-27065) respectively (Pitney, Spencer, Molly, & Suman, 2022). CVE is a glossary that categorizes vulnerabilities and assesses the level of threat posed by a vulnerability using the Common Vulnerability Scoring System (CVSS). The impact of all these vulnerabilities found in the Microsoft Exchange Server have a high severity except for Server-Side Request Forgery which has the highest impact if exploited and is assigned by the National Institute of Standards and Technology (NIST) as having critical severity (National Vulnerability Database, n.d.).

Server-Side Request Forgery (SSRF) allows an attacker to induce the server-side application to make requests to an unintended location. Insecure deserialization is another vulnerability that arises when an application uses untrusted data to execute code, inflict a denial-of-service attack, bypass authentication, or further abuse the logic behind an application. First File write and Second File Write vulnerability allows the attackers to arbitrarily write random files within the server and to create a web shell within the servers they exploit (Port Swigger, n.d.). The attackers leveraged the first and second vulnerabilities to gain entry to the system and disrupt its operations. They used the last two vulnerabilities to create web shells within the servers. By following these steps, the hackers managed to extract sensitive information such as emails, company data, passwords, and usernames from the targeted companies. Once the hack became public, the attackers proceeded to encrypt data and install ransomware and malware onto the systems. This enabled them to steal a significant amount of information.

How to avoid?

While zero-day attacks are inherently challenging to defend against, there are several measures organizations can take to prepare for and reduce the impact of these threats. Some of the practices that can help mitigate the impact of zero-day attacks include:

Use Windows Defender Exploit Guard

Microsoft introduced Windows Defender Exploit Guard in 2010, which has features to protect against zero-day attacks. Some capabilities of this software include Attack Surface Reduction, Network Protection, and Controlled Folder Access. These features protect against malware infection by blocking threats based on Office files, scripts, and emails. They also block all outbound connections before they are used and prevent malware from connecting with a command control server. Additionally, they monitor changes made by applications to files in protected folders (cynet, n.d.)

Implement Patch Management

Although patch management cannot fully prevent zero-day attacks, it can still be effective in reducing the amount of time that systems are exposed to vulnerabilities. In the event of a significant vulnerability, software vendors may issue patches within a short time frame, as was the case with Microsoft and their security updates for the Exchange Server attack. Despite this, only around half of all Exchange servers on the internet applied the patches immediately (Carlson, 2021). It is crucial to apply patches promptly to minimize potential harm in any future attacks.

Monitoring for Threats

By monitoring systems for abnormal behavior or suspicious activity, organizations can detect potential attacks early, enabling a quicker response and reducing the overall impact of the attack. This can be achieved through the use of intrusion detection systems and threat intelligence, which can identify both known and unknown threats within an organization's environment (Rapid7, n.d.).

Countermeasures

Install patches and regular updates.

It is recommended that organizations consistently update their software and apply available security patches promptly. These updates serve to address security vulnerabilities and provide added security features to the product.

Incident Response Plan

Having an incident response plan in place can help organizations respond quickly and effectively to a cyber-attack. The plan should include procedures for identifying and containing the attack, communicating with stakeholders, and restoring systems and data. Although NIST provides standards for incident response, the development, implementation, and evolution of these standards can vary between organizations. Methodologies and frameworks are important in incident response, as they can help streamline response efforts and establish a solid foundation for the organization's response activities. By creating a well-defined incident response framework, communicating it effectively, and making the response activities transparent, organizations can reduce obstacles and challenges for their responders (Phillips, 2021).

Regular Security Audits

Regular security audits can help identify vulnerabilities in an organization's systems and processes before they can be exploited by attackers. Audits should include vulnerability assessments, penetration testing, and security awareness training for employees (Stouffer, 2015).

Information Security Policies for future incidents

To prevent future incidents like the Microsoft Exchange Server hack, organizations should implement robust information security policies that are tailored to their specific needs and risk profile. Some key policies that should be considered include:

Access Control Policy

The Access Control Policy is a vital requirement that outlines how access is controlled and who is authorized to access information in various situations. This policy should involve robust authentication measures, like two-factor or biometric authentication, alongside routine reviews of user access rights to confirm their necessity and relevance. Risk-based authentication, contextual authentication or context-based authentication uses risk signals and telemetry data to evaluate the risks linked with an identity and assists in identifying the appropriate level of authentication required (Glover, 2021).

Security Awareness and Training Policy

In order to reduce the possibility of human errors and ensure that all employees are knowledgeable about the most recent security threats and best practices, organizations need to establish a policy for security awareness and training that offers regular training and education on topics related to information security. James Bore highlights in "97 things every information security professional should know" that in the field of information security, people, processes, and technology are the three most crucial assets, with people being the most significant. Any organization should be able to associate directly either to empowering people to achieve their aims or disempowering their threat people.

Vulnerability Management Policy

Dealing with software vulnerabilities necessitates having a vulnerability management plan that entails timely identification and patching. The goal of this process is to minimize the vulnerability window and the associated risk that comes with leaving exploitable vulnerabilities on IT assets. Prompt patching is crucial in reducing this risk. Failure to do so means that hackers are more likely to discover and exploit any software vulnerabilities they encounter (David Kim, 2023). Having vulnerability scanners and conducting periodic scans is not the only way to address vulnerabilities. Effective asset and configuration management serves as the foundation of a strong vulnerability management program. Security experts should delve further to understand all the configurations, frameworks, software patches, and the remediation process for issues that are identified (Bjarnason, 2021).

Data Backup and Recovery Policy

A backup and recovery policy is a written plan that outlines the procedures for data backup, disaster recovery, and backup access privileges. By having such a policy in place, an organization can prevent costly errors when it comes to their important data. To minimize the effects of a system failure or data breach, it is important for organizations to have a data backup and recovery policy that ensures that critical data is backed up regularly and can be swiftly restored in the event of a security breach (G, 2021).

Implementing these policies can help to create a strong foundation that minimizes the risk of future incidents like Microsoft Exchange Server hack. Furthermore, organizations should adopt a comprehensive and long-term approach to cybersecurity by considering it as an essential part of their overall business strategy. They need to align their security efforts with their broader objectives and take a proactive and strategic approach to protect themselves from the increasing threats of cyber-attacks and data breaches. As the Microsoft Exchange hack targeted small and midsized companies, even smaller organizations must enforce robust cybersecurity practices. In today's digitally dependent world, the repercussions of a security breach can be significant and widespread, making it imperative for organizations to prioritize cybersecurity.

References

Bjarnason, S. (2021). Vulnerability Management. In *97 things every information security professional should know* (p. 254). California: O'reilly Media.

Bryan, N. O. (n.d.). *Microsoft Exchange Server*. Retrieved from TechTarget: techtarget.com/searchwindowsserver/definition/Microsoft-Exchange-Server

Carlson, B. (2021, May 6). *The Microsoft Exchange Server hack: A timeline*. Retrieved from CSO: https://www.csoonline.com/article/3616699/the-microsoft-exchange-server-hack-a-timeline.html

cynet. (n.d.). *Zero-Day Attack Prevention: 4 Ways to Prepare*. Retrieved from cynet: https://www.cynet.com/zero-day-attacks/zero-day-attack-prevention/

David Kim, M. G. (2023). *Fundamentals of Information Systems Security.* Burlungton, MA 01803: Jones & Bartlett Learning.

G, M. (2021, August 13). *Backup and recovery policy - Protect Your Data with a Documented Plan*. Retrieved from ITSM DOCS: https://www.itsm-docs.com/blogs/security-management/backup-and-recovery-policy#:~:text=A%20backup%20and%20recovery%20policy%20is%20a%20document%20that%20specifies,comes%20to%20your%20business%20data.

Glover, U. (2021). The Access Control Policy is a vital requirement that outlines how access is controlled and who is authorized to access information in various situations. This policy should involve robust authentication measures, like two-factor or biometric authenticati. In O. Media, *97 things every information security professional should know* (p. 394). California: O'reilly Media.

National Vulnerability Database. (n.d.). Retrieved from NIST: https://nvd.nist.gov/vuln/detail/CVE-2021-26855

Phillips, Q. (2021). Incident Management. In O. M. Inc, *97 things every information security professional should know* (p. 344). Sebastopol, California: O'Reilly Media.

Pitney, A. M., Spencer, P., Molly, F., & Suman, B. (2022). *A Systematic Review of 2021 Microsoft Exchange Data Breach Exploiting Multiple Vulnerabilities.* IEEE.

Port Swigger. (n.d.). Retrieved from Port Swigger: https://portswigger.net/

Rapid7. (n.d.). *Threat Detection* . Retrieved from rapid7: https://www.rapid7.com/fundamentals/threat-detection/

Stouffer, K. (2015, May). *Guide to Industrial Control.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Temple-Raston, D. (2021, August 26). *China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying*. Retrieved from npr: https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying