SECURITY FUNDAMENTALS

CHIJIOKE FRANKLIN EMEJURU

Project Description: Improving cybersecurity by addressing supply chain vulnerabilities and security roles.

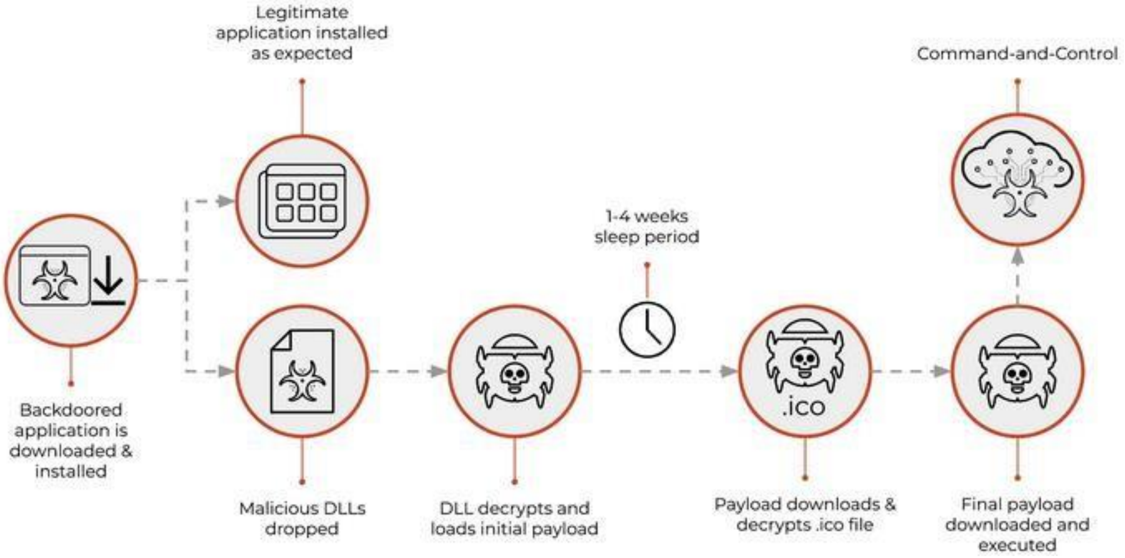
Project Summary:
This project focuses on enhancing cybersecurity in organizations by addressing the increasing complexity of cyber-attacks, particularly those targeting supply chains. It highlights real-world incidents such as the 3CX Supply Chain Attack and the MOVEit Supply Chain Attack, which demonstrate how attackers exploit vulnerabilities in interconnected systems and software to access sensitive data and compromise businesses. The project emphasizes the need for stronger security measures in the face of these evolving threats.

The project explores the CNSS Security Model (McCumber Cube), a framework that helps organizations secure their data across different stages: at rest, in motion, and in use. It outlines security controls such as Full Disk Encryption, SSL/TLS encryption, and redundant systems to protect data and ensure its confidentiality, integrity, and availability.

The project also outlines the importance of various cybersecurity roles within an organization, including the CISO, Data Protection Officer, and Network Security Engineer, each of whom plays a crucial part in developing and maintaining a strong security strategy. Ultimately, the goal of this project is to provide a comprehensive approach to securing supply chains and organizational systems from growing cyber threats.

According to Pandey et al. (2020) cyber-attacks on supply chains are becoming more complex and are rising continuously. One of their primary targets is the intricate web of connections that exists between businesses and the suppliers, distributors, and other service providers that they interact with. The attackers exploit vulnerabilities that arise as a result of the linked nature of technological supply chains that always span several businesses, systems, and geographical locations (Colicchia et al., 2019). Among the two recent supply chain attacks include 3CX Supply Chain and MOVEit Supply Chain Attacks.

3CX Supply Chain Attack


Legitimate application installed as expected
Command-and-Control
1-4 weeks sleep period
.ico
Backdoored application is downloaded & installed
Malicious DLLs dropped
DLL decrypts and loads initial payload
Payload downloads & decrypts .ico file
Final payload downloaded and executed

This was a supply chain attack conducted by 3CX in March 2023 targeted desktop applications for both Windows and macOS as per Refsnes (2023). This attack raised issues over the confidentiality and safety of the software's supply chain. The attack was launched by integrating a malicious library file which compromised the applications. This resulted in the downloading of an encrypted file that included information about command and control. Through this, the attackers were allowed to carry out harmful operations inside the surroundings of the victim. It is possible that the development environment of the organization has been infiltrated, as shown by the fact that malicious versions of the applications were signed with authentic 3CX certificates.

As a consequence of this, modified applications were distributed straight from the download servers administered by 3CX according to Madnick (2023). This underscores the vulnerability inherent in software supply chains, since even a compromise that seems to be relatively trivial may have far-reaching effects for consumers who depend on and trust the program. It is clear that threat actors are becoming more sophisticated and persistent in their efforts to target supply chains in order to enter businesses and obtain access to sensitive information.

This attack was recognized and characterized as a multi-stage operation that ultimately aimed to steal data from computers that were infected with malware. The attackers were able to access inside 3CX's network by using a built version of the Fast Reverse Proxy project, which is open to the public. This allowed them to compromise both the Windows and macOS development environments. Because of this, the attacker was capable of infecting the 3CX DesktopApp with code that included malware and was accessible for download on the 3CX desktop application website.

Upon examination, it was found that the first point of attack for 3CX's system was malicious malware downloaded from the Trading Technologies website. According to Refsnes a software package containing malware distributed through a previous software supply chain compromise that originated from a modified installer for X_TRADER, a software package from Trading Technologies (Refsnes, 2023). Mandiant found that a sophisticated loading mechanism resulted in the installation of VEILEDSIGNAL, a multiple levels modular backdoor, as well as its components.

MOVEit Supply Chain Attack

The "MOVEit supply chain attack", also known as CVE-2023-34362, was launched in June and targeted consumers of the MOVEit Transfer tool, which is owned by Progress Software, a firm based in the United States (US) (Madnick, 2021). Within the US, MOVEit has gained a lot of popularity due to its ability to move sensitive data in a safe manner. Heath et al. note that the attackers have successful compromised over 620 businesses, some of which include the BBC, British Airways, and Aer Lingus companies (Heath et al., 2020). Some of the staff members' addresses, identification numbers, as well as national insurance numbers were among the personally identifiable information data that was exposed.

Cl0p, an organization that produces ransomware, has been connected to the assault. In order to do major harm, the attackers made advantage of exposed web interfaces, often known as EWIs. It was discovered that the online-facing MOVEit application has been compromised by a web shell known as LEMURLOOT (Teale, 2023). Following that, this technique was utilized for stealing data from databases belonging to MOVEit Transfer.

EWIs have the potential to be a huge menace to security. If these interfaces are left widely available, possible attackers may be able to exploit them in order to obtain sensitive data or enter critical systems. They act as gateways to services that are either internal or secret. To reduce the impact of this danger, it is necessary to identify EWIs and to send out notifications at the appropriate time. This incident demonstrates how rapidly an attack on a supply chain can scale, as well as how tiny suppliers may have a significant influence on larger organizations like the BBC and British Airways.

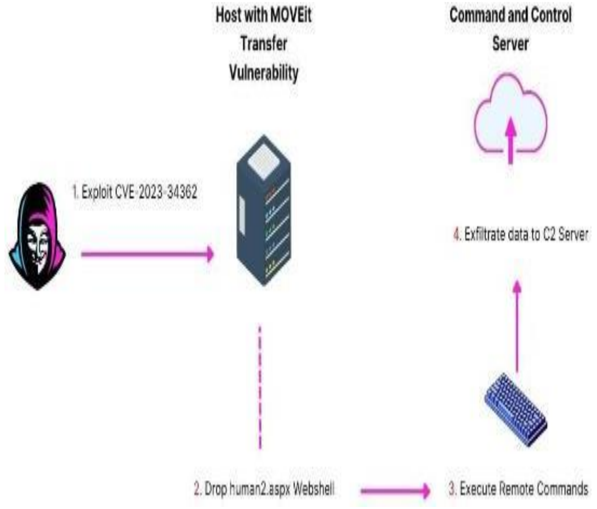

Host with MOVEit Transfer Vulnerability
Command and Control Server
1. Exploit CVE-2023-34362
4. Exfiltrate data to C2 Server
2. Drop human2.aspx Webshell
3. Execute Remote Commands

Figure 2: Addressing a MOVEit vulnerability

The CNSS Security Model, also known as the McCumber Cube, is a framework that helps organizations address various security challenges by examining the intersections of three dimensions: Data States (Data at Rest, Data in Motion, Data in Use), Information Security States (Confidentiality, Integrity, Availability), and Security Categories (People, Technology, Operations) (Whitman & Mattord, 2021). Here, four intersections within the CNSS model are provide and a discussion of one security control for each to enhance the cybersecurity posture the company discussed.

Intersection 1: Data at Rest, Storage, Technology Security Control: Full Disk Encryption (FDE) Explanation: It is recommended that the organization deploy Full Disk Encryption (FDE) on all storage devices, including servers and laptops, in order to achieve the goal of protecting the secrecy of data while it is stored (Chowdhuryy et al., 2023). With FDE, even if a device goes missing or is stolen, all information that is stored on it will continue to be encrypted and unavailable to anybody who does not have the appropriate credentials.

Intersection 2: Data in Motion, Integrity, Technology Security Control: Secure Sockets Layer (SSL) / Transport Layer Security (TLS) Explanation: Employing SSL/TLS protocols for data transfer is the best way to ensure that the data's integrity is preserved while it is in transit (Touil et al., 2021). The use of SSL/TLS guarantees that data is transferred over the network in a secure manner and identifies any unauthorized alterations, so guaranteeing that data integrity is maintained.

Intersection 3: Data in Use, Availability, Operations Security Control: Redundant Systems and Failover Mechanisms Explanation: The organization has to use multiple systems and failover techniques in order to guarantee the availability of data that is currently being utilized (Sharma & Prasad, 2023). This guarantees that in the event that one system crashes, another system will take over without any disruption, hence reducing the amount of time that the system is down and guaranteeing that vital resources are always accessible.

Intersection 4: Data at Rest, confidentiality, People Security Control: User Access Controls and Authentication Explanation: It is very necessary to implement stringent user access restrictions and powerful authentication procedures in order to guarantee the security of data that is stored in a state of rest. Access to sensitive information should be restricted to only authorized workers, and those individuals should be required to verify themselves using robust means such as multi-factor authentication.

To this end, the organization has the potential to greatly improve its cyber-security posture and better mitigate the risks and difficulties it confronts in today's developing security environment if it addresses these intersections according to the CNSS Security Model and implements the security controls that are suggested.

Various security roles are key in providing overall organization security.

Application Security Engineer

The process of creating applications is facilitated by application security engineers, who also ensure that the applications are safe. Additionally, it is their responsibility to exercise control over apps developed by third parties that have access to corporate data. They are responsible for the correct setup of technical security settings, the execution of application risk assessment, the creation of allow/blacklists for applications, and the execution of pen testing (Do et al., 2019). SaaS applications need to be evaluated by app security engineers in order to decide whether or not they should be prohibited.

CISO

One of the most important responsibilities of the Chief Information Security Officer (CISO), a position at the C-level, is to control the security strategy of the company (van et al., 2021). They are responsible for the planning and management of the execution of a DLP method and a security policy. In addition to this, they are responsible for managing access, as well as performing general compliance control, conducting risk assessment, investigating cyber occurrences, and planning preventive. Moreover, they are in charge of managing awareness training for cyber security.

Data Protection Officer

Under the General Data Protection Regulation (GDPR), businesses that routinely monitor and handle significant data collections are required to appoint a Data Protection Officer (Merrick & Ryan, 2019). A Data Protection Officer (DPO) is responsible for ensuring that the data protection of the company complies with the legislation and satisfies the requirements for security (Šidlauskas, 2021). The individuals in question are required to possess a comprehensive understanding of data protection and the legislation that regulate it.

Network Security Engineer

An engineer who specializes in network security works with business networks. Their protection from data breaches and other forms of cyberattacks is the primary objective of this security measure. Among their tasks are the right configuration of network security, the execution of penetration testing, and the development and implementation of systems for detecting possible cyber-attacks. In addition to this, they also ensure that the rules regarding network security are enforced. Another one of their responsibilities is to establish security tools and ensure that they are operating effectively.

IT Security Administrator

It is the responsibility of an IT security administrator to ensure the safety of the company's data. Access management, safeguarding data transfer, establishing and maintaining security tools, and regulating anomalous data behavior are some of the activities that fall within their purview (Del Giorgio Solfa, 2022). As an additional measure, they are ensuring that the settings of the environment are in accordance with the security regulations. In addition to this, they look for possible dangers and openings in the environment, generate reports on security incidents, and determine whether security automation technologies are available.

Security Analyst

For the purpose of preventing cyberattacks and insider threats, security analysts are required to conduct risk assessments and prepare risk assessments (Daubner et al., 2023). They do an analysis of the company information technology environment and determine the correct configurations for it. A DLP analysis and policy development, vulnerability discovery and repair, and aberrant data behavior detection are all tasks that they carry out. Additionally, it is their responsibility to ensure that the information of the organization is kept discreet, accessible, and safe.

Security Architect

A secure-by-design system is anything that is developed by a security architect. This is a senior-level position that needs extensive understanding in a variety of departments related to corporate security, particularly network and hardware security. It is the responsibility of the individual to do tasks such as assessing the security architecture, looking for security holes, arranging the transformation of the information technology infrastructure to meet the requirements for security, and ensuring that the integrity of the IT environment is maintained (Furnell, 2021). In addition to this, they should implement the processes for disaster recovery and the techniques for controlling internal threats, among other things.

References

Chowdhuryy, M. H. I., Jung, M., Yao, F., & Awad, A. (2023, February). D-Shield: Enabling Processor-side Encryption and Integrity Verification for Secure NVMe Drives. In *2023 IEEE International Symposium on High-Performance Computer Architecture (HPCA)* (pp. 908-921). IEEE.

Colicchia, C., Creazza, A., & Menachof, D. A. (2019). Managing cyber and information risks in supply chains: insights from an exploratory analysis. *Supply Chain Management: An International Journal*, *24*(2), 215-240.

Daubner, L., Macak, M., Matulevičius, R., Buhnova, B., Maksović, S., & Pitner, T. (2023). Addressing insider attacks via forensic-ready risk management. *Journal of Information Security and Applications*, *73*, 103433.

Del Giorgio Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM)*, *2*.

Do, Q., Martini, B., & Choo, K. K. R. (2019). The role of the adversary model in applied security research. *Computers & Security*, *81*, 156-181.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080.

Heath, E. A., Mitchell, J. E., & Sharkey, T. C. (2020). Models for restoration decision making for a supply chain network after a cyber attack. *The Journal of Defense Modeling and Simulation*, *17*(1), 5-19.

Madnick, S. E. (2023). The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase.

Merrick, R., & Ryan, S. (2019). Data privacy governance in the age of GDPR. *Risk Management*, *66*(3), 38-43.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Refsnes, M. W. (2023). *Exploring Trojanized Closed-Source Software Supply Chain Attacks Through Differential Malware Analysis* (Master's thesis, NTNU).

Sharma, P., & Prasad, R. (2023). Techniques for Implementing Fault Tolerance in Modern Software Systems to Enhance Availability, Durability, and Reliability. *Eigenpub Review of Science and Technology*, *7*(1), 239-251.

Šidlauskas, A. (2021). The role and significance of the data protection officer in the organization. *Socialiniai tyrimai*, *44*(1), 8-28.

Teale, C. (2023). The fallout from the MOVEit hack continues as more agencies announce breaches. *Route 50*, NA-NA.

Touil, H., Akkad, N. E., & Satori, K. (2021). Secure and guarantee QoS in a video sequence: a new approach based on TLS protocol to secure data and RTP to ensure real-time exchanges. *Int. J. Saf. Secur. Eng*, *11*(1), 59-68.

van Yperen Hagedoorn, J. M., Smit, R., Versteeg, P., & Ravesteyn, P. (2021). Soft Skills of The Chief Information Security Officer.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.