UTSA

The University of Texas at San Antonio™

IS 3423-005 Network Security

Network Security Report – Microsoft Digital Defense Report

Student:

Dillen Dela Cruz, odv464

Prepared Network Security
02/27/2024
Professor: Natalie Sjelin

Introduction:

In the ever-evolving landscape of cybersecurity, a continuous battle persists between cybercriminals and the collaboration between both public and private sectors. While cyber threats continue to advance in sophistication, a unified front is emerging to disrupt criminal technologies, hold perpetrators accountable, and provide support to victims of cybercrime.

In the course of this report analysis, my focus will be on recognizing common network security threats faced by corporations and individuals, with a specific emphasis on Microsoft. My examination of the security situation will prioritize identifying the types of information and systems that require protection, ensuring they align with the organization's mission or essential services. I will also investigate recent attacks, using reports on breaches or vulnerabilities to pinpoint the most frequent threats in the chosen sector. Ultimately understanding these tactics employed by cybercriminals is important in comprehending their potential impact on the organization. Moreover, I will discuss some ways to enhance security by integrating insights from cryptography and network security, devising strategies aimed at mitigating potential threats.

The Sector: Microsoft operates in the technology sector, specifically in the software and hardware industry. It is a global technology company that develops, licenses, manufactures, supports, and sells computer software, consumer electronics, and personal computers (Microsoft). Microsoft is known for its widely used software products such as the Windows operating system, Microsoft Office suite, and various other productivity and business solutions. Additionally, the company engages in cloud computing services through its Azure platform.

Organizational Assets:

1. Protection of Credentials and Session Data (Microsoft 27): Protecting against AiTM phishing attacks is essential for protecting credentials, session cookies, and personal data. Strong systems and security measures are required, especially when dealing with Microsoft cloud identities.
2. Protection of User Credentials and Sensitive Data(Microsoft 34): Strengthening security measures to protect user credentials and sensitive data, particularly in the education sector, is crucial. Defending against password-based attacks helps maintain confidentiality and defends against potential breaches.
3. Protection of Financial Transaction Details: Defending against BEC activities is critical for protecting financial transaction details and preventing compromise of email accounts. Systems should be in place to counter internal phishing, impersonations, and mass spam mailing, ensuring the integrity of cloud-based infrastructures (Microsoft 32).
4. Embedded Software Security (Supply Chain Risks) (Microsoft 83): Embedded software introduces significant risks to the supply chain, with vulnerabilities potentially arising at any stage of a device's lifecycle, spanning from design to distribution. A major concern lies in the incorporation of third-party components into the software and hardware deployed in Operational Technology (OT) and industrial control system (ICS) networks. These components may operate discreetly, remaining invisible to organizations, and thereby pose a serious threat to networks.
5. DDoS Attacks on Healthcare (Healthcare Sector as a Target): Healthcare sector has become a target for Distributed Denial of Service (DDoS) attacks, evident by a growth in

incidents starting in January 2023 (Microsoft 39). The consequences of such attacks are great, as healthcare organizations must safeguard a great number of critical information and systems.

Types of Attacks:

1. Successful Identity Attacks (Microsoft 34) :

Attacks targeting identity security have displayed through traditional brute-force attempts, sophisticated password spraying across multiple countries and IP addresses, and adversary-in-the-middle (AiTM) attacks. Password attacks are attributed to low security posture of many organizations. A significant contributing factor is the lack of Multi-Factor Authentication (MFA) adoption in these organizations, leaving users exposed to risks such as phishing, credential stuffing, and brute force attacks.

Impact on Confidentiality: Could lead to unauthorized access, compromising sensitive information. This threatens the confidentiality of data stored or processed by the organization.

Impact on Integrity: Successful identity attacks may allow threat actors to manipulate or alter data, affecting the integrity of the information stored in the organization's systems.

Impact on Authentication: Compromised identities could be exploited to bypass authentication measures, leading to unauthorized access to critical systems and resources.

Impact on Availability: If unauthorized access leads to disruptions, it can impact the availability of services, affecting normal business operations.

2. Ransomware Encounters (Microsoft 17):

The term "ransomware encounters" in this report refers to instances of ransomware activity or attempted attacks that were detected, prevented, or alerted throughout various stages of a ransomware attack. The report highlights a notable large-scale ransomware campaign observed during the year. Attackers employed techniques like adding a secret or certificate to an application, allowing them to connect to Azure Active Directory and perform operations such as accessing confidential data and emails, as well as exfiltrating information.

Impact on Confidentiality: Ransomware attacks often involve encryption of sensitive data, leading to potential data breaches and compromising confidentiality.

Impact on Integrity: Destruction activities, such as the deletion of user resources, can result in permanent loss or alteration of data, impacting data integrity.

Impact on Authentication: Privilege escalation by attackers may compromise authentication mechanisms, allowing unauthorized access to privileged accounts.

Impact on Availability: The encryption and destruction activities conducted by ransomware can significantly disrupt the availability of critical systems and data.

3. Targeted Phishing Attempts (Microsoft 27):

Aims to compromise devices or users, encompasses both malware phishing with the intent to compromise devices and adversary-in-the-middle (AiTM) phishing with the goal of stealing identities. These attacks employ defense evasion techniques such as phishing from compromised vendors and the misuse of legitimate services.

Impact on Confidentiality: Successful phishing attempts, whether through malware or adversary-in-the-middle techniques, can result in the compromise of confidential information stored on compromised devices or stolen identities.

Impact on Integrity: Phishing attacks can lead to manipulation of information or the introduction of malicious content, affecting the integrity of data.
Impact on Authentication: Compromised credentials through phishing may lead to unauthorized access, undermining authentication measures.
Impact on Availability: Depending on the nature of the phishing attack, availability may be impacted through compromised devices or compromised user accounts.

4. Business Email Compromise (BEC) (Microsoft 32):

Involve various methods, including email conversation hijacking and mass spamming with malicious applications, aimed at perpetrating financial fraud. Attackers also deploy phishing emails with harmful links and attachments, often using the victim's email address to target other users within the same organization. BEC scams typically occur when threat actors compromise legitimate business email accounts through social engineering or computer intrusion techniques, enabling unauthorized funds transfers to accounts under their control.

Impact on Confidentiality: BEC attacks can result in the unauthorized access and exposure of confidential financial information or sensitive business communications.
Impact on Integrity: Email conversation hijacking, and mass spamming can manipulate or deceive users, affecting the integrity of communication channels.
Impact on Authentication: Compromised email accounts can be misused for further attacks, undermining authentication mechanisms.
Impact on Availability: Mass spamming and malicious applications may overwhelm email systems, affecting the availability of communication channels.

2-3 recommendations:

1. Implement Strong Cryptographic Measures: Employ end-to-end encryption for sensitive communications and data storage. This ensures that even if unauthorized access occurs, the intercepted information remains indecipherable without the proper encryption keys. Utilize strong cryptographic algorithms and regularly update them to stay ahead of emerging threats. Cryptographic protocols should align with industry best practices to maintain the confidentiality and integrity of data.
2. Enhance Network Security: Implement a comprehensive network security strategy, including firewalls, intrusion detection and prevention systems, and secure configurations, to safeguard against unauthorized access and lateral movement within the network. Regularly conduct penetration testing and vulnerability assessments to identify and address potential weaknesses in the network infrastructure. This proactive approach helps mitigate the risk of successful attacks by identifying and resolving vulnerabilities before they can be exploited.
3. Deploy Network Segmentation: Employ network segmentation to isolate critical systems and sensitive data from the broader network. This containment strategy limits the potential impact of successful attacks, preventing lateral movement and reducing the risk of widespread compromise. Implement access controls and authentication mechanisms within segmented networks to ensure that only authorized personnel have access to specific resources. This helps prevent unauthorized access and restricts the ability of attackers to move laterally within the network

Works Cited

Microsoft. “Business Description.” Microsoft, https://www.microsoft.com/investor/reports/ar12/financial-review/business-description/index.html. Accessed 27 February 2024.

Microsoft. “Overcoming today's escalating cyberthreats.” Microsoft, https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/documents/WIN24Pro-Research-Report.pdf. Accessed 27 February 2024.

Reiff, Nathan. “Investing in Microsoft Stock (MSFT).” Investopedia, https://www.investopedia.com/microsoft-stock-msft-5078359. Accessed 27 February 2024.