GROUP 1

CASE STUDY :

COLONIAL PIPELINE RANSOMWARE ATTACK IN USA (2021)

Presented by :

De Vero, Eunice Jayce F.
Macaraeg, Adrian Jules C.
Simon, Rommel M.
Maninang, Ken G.
Salunga, Joyce Kenn L.

BSIT 3A

INTRODUCTION

The 2021 Colonial Pipeline ransomware attack exposed weaknesses in critical infrastructure cybersecurity, disrupting fuel supply and showing how cyberattacks can impact operations and public services. This study examines its causes, effects, and lessons for improving cybersecurity and resilience.

STATEMENT OF THE PROBLEM

1. Poor Authentication and Access Control
2. Unsegmented Network Infrastructures
3. Lack of Backups and Recovery Plan
4. Delayed Detection and Response
5. Public and Economy Impacts

OBJECTIVES OF THE STUDY

GENERAL OBJECTIVE

The General Objective of this study is to discuss the ransomware attack on Colonial Pipeline and to understand its effects on cybersecurity in important operations

SPECIFIC OBJECTIVES

Analyzing the causes and weaknesses

To investigate impact on operations and economy

To examine response actions

To recommend cybersecurity improvements

DISCUSSION / ANALYSIS

1. Methods of the Attack

2. System Gaps

A. Weak Authentication Security
B. Connected Networks
C. Lacked of Monitoring
D. No Backup Plans

3. Impacts on the Operations and the Public

4. Effects on the Policy and Organization

The incident shows that even major companies are vulnerable to cyber threats. Implementing network segmentation, strong passwords, multifactor authentication, employee training, system monitoring, and backup plans can help prevent attacks and reduce their impact.

PROPOSED SOLUTION / RECOMMENDATION

Strengthen the Access Controls and Authentication

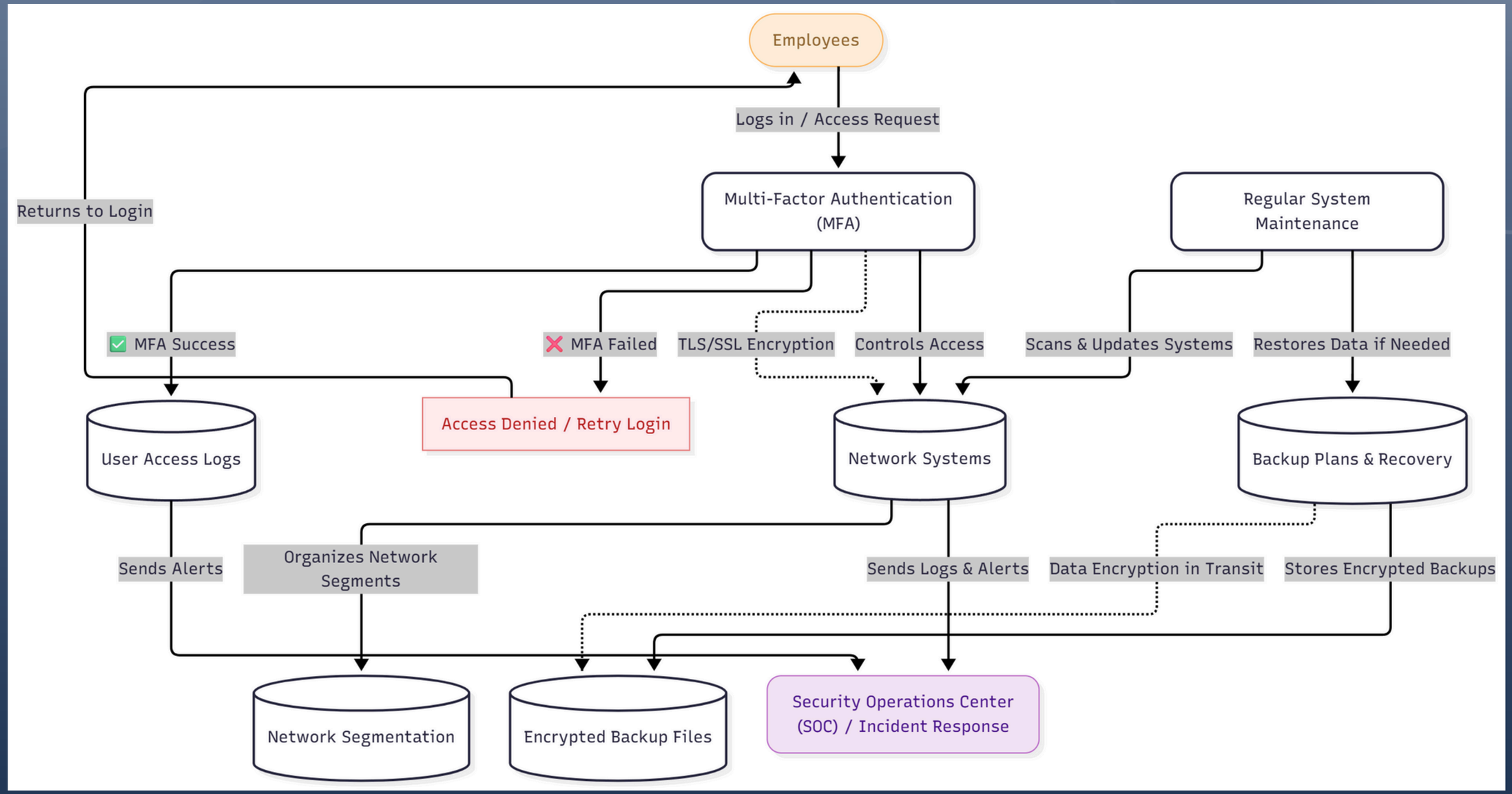
Network Segmentation

Regular System Maintenance

Backup Plans and Recovery

Employees Cybersecurity Training

THREAT ANALYSIS MODEL



CONCLUSION

The Colonial Pipeline attack revealed how weak authentication and poor network security can disrupt essential services, leading to widespread fuel shortages, panic buying, and economic impact. It emphasized the need for stronger cybersecurity practices, such as multi-factor authentication, unique passwords, regular network monitoring, and employee training to detect and respond to threats early. This incident serves as a lesson for companies to strengthen access controls, conduct routine security checks, and establish backup and recovery plans to prevent future cyberattacks.

THANK YOU SO MUCH!

REFERENCES

[1]Y. Li and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; emerging trends and recent developments,” Energy Reports, vol. 7, no. 7, pp. 8176–8186, Nov. 2021, doi: https://doi.org/10.1016/j.egyr.2021.08.126.

[2]“Colonial Pipeline | EBSCO,” EBSCO Information Services, Inc. | www.ebsco.com, 2021. https://www.ebsco.com/research-starters/business-and-management/colonial-pipeline

[3]INSURICA, “Cyber case study: Colonial pipeline ransomware attack,” INSURICA, 2024. https://insurica.com/blog/colonial-pipeline-ransomware-attack/

[4]J. Easterly and T. Fanning, “The attack on colonial pipeline: What we’ve learned & what we’ve done over the past two years,” Cybersecurity and Infrastructure Security Agency, May 07, 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

[5]S. Kerner, “Colonial Pipeline Hack explained: Everything You Need to Know,” TechTarget, Apr. 26, 2022. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know

[6]L. Gawazah, “To Pay or Not to Pay: The US Colonial Pipeline Ransomware Attack,” Aug. 2024. Available: https://www.researchgate.net/profile/Lazarus-Gawazah/publication/383206534_To_Pay_or_Not_to_Pay-_The_US_Colonial_Pipeline_Ransomware_Attack/links/66c1b6bf8d007355925dd805/To-Pay-or-Not-to-Pay-The-US-Colonial-Pipeline-Ransomware-Attack.pdf