

Report

by Andreea Georgiana Ruse

Submission date: 21-Jul-2023 11:13AM (UTC+0100)

Submission ID: 210503657

File name: 33295_Andreea_Georgiana_Ruse_Report_503767_916485851.docx (256.21K)

Word count: 2843

Character count: 17844

1
Networks and cyber security essentials
ACCA4024

Assignment Title:
Secure the network from common
threats and attacks

The University Of Wales Trinity Saint David
Andrea Georgiana Ruse 2108815
Network and Cybersecurity Essentials ACCA4024
BSc Applied Computing
Abida Perveen

Table of Contents

Abstract	3
Introduction	3
¹ Possible security breaches that could have led the network to this situation	4
Different types of threats, vulnerabilities, and attacks	6
Threats:	6
Vulnerabilities	6
Attacks	7
“.meds” file format attack	8
¹ Guideline for staff members, and customers to responsibly use their digital space ...	8
Conclusion, Recommendation & Future Work	10
Reference.....	12

Abstract

There is growing fear among companies, consumers, and individuals about the prevalence of malicious cyber-attacks. The ways in which hackers can penetrate a company's network are expanding in tandem with the development of new technologies. Providing clear policies for employees and customers on how to behave responsibly online can help mitigate these cyber risks. In order to cover all these concepts, this IEE format paper examines the security breaches which led to the scenario of the small cafe, owned by Mr Kermit Fogg. The cafe had 6 Sales Executives, 2 Sales Heads, and 1 Accounts Officer. By giving all users access to all of the business applications, without segregation of networks, this cafe was vulnerable to security breaches. This paper discusses the possible security breaches and reviews the various types of threats, vulnerabilities, and attacks that led to the .meds file format attack, implemented by a malicious actor. In addition, recommendations and approaches to secure the cafe's network are provided, in the form of guidance to staff and customers on how to responsibly use digital spaces.

Introduction

Cybersecurity risks and attacks are on the rise in the modern digital era, and they can have catastrophic impacts on organizations, infrastructure, and networks. Cybercriminals are always coming up with new and inventive ways to compromise systems, steal data, and cause disruptions. Cybercrime is always increasing despite the efforts of organizations, security professionals, and individual users in security networks. In order to protect that business from common threats and address these issues, a systematic approach is needed. This paper aims to provide an overview of the common threats and attacks that affect networks and offer a practical approach to secure the network from said threats and attacks. The paper herein describes the existing scenario faced by Mr. Kermit Fogg, the owner of the canteen café, where he had to take action to secure his network from a ransomware attack.

Initially, Mr. Fogg's business had 6 sales executives, 2 Sales Heads, and 1 Account Officer with limited access to the business application, such as stock, maintenance, purchase orders, sales details, accounting software, etc. Recently Mr. Fogg

¹ appointed Mr. Elmo as the Marketing Head with full access to all business applications. To further promote the business, Mr. Elmo ¹ offered "Complimentary" Wi-Fi with high-speed internet to all customers, allowing anyone to access the same network for business operations. As a result, the business income increased by 30% but the security of the network was compromised. Mr. Kermit sought help from the security consultant for solutions to how he could secure the network. The paper proposes guidelines and measures that staff members and customers should responsibly follow in order to protect the network. Further, the paper also addresses the security breach that led to the attack and provides recommendations to mitigate risks.

¹ Task 1. Possible security breaches that could have led the network to this situation.

Following are some ²² Possible Security Breach that could have led the network to this situation:

1: Unauthorized/Privileged Access

Reason: In the above scenario, all Sales Executives and Elmo ¹ (Marketing Head) were given full access to all business applications. This unauthorized and privileged access to business applications can be a security breach because it can be used to leak information or misuse the applications. It can also increase the risk of insider attacks or data breaches. Also, Kermit (owner) giving full access to Elmo, who was new to the business was a risk as there was no proper authentication process for him (Khari et al., 2017).

2: Lack of Network Segmentation

Reason: In the above scenario, Elmo provided ¹ complimentary Wi-Fi with high-speed internet to customers in order to increase business income. He didn't distinguish between the business and customer networks (Johns, 2020). Thus, this lack of proper segmentation of networks can be a security breach. By not properly segmenting the networks, the business applications and other sensitive information related to the cafe will be vulnerable to external attacks or threats to the network. This could lead to the leakage of confidential information or a potential threat to the cafe.

3: Lack of Authentication for Business Applications

Reason: In the above scenario, all ¹ Sales Executives, Sales Heads, and Elmo (Marketing Head) were given full access to all business applications with no proper authentication. This lack of authentication for business applications can also be a security breach because it makes the applications vulnerable to attacks or unauthorized access. Without proper authentication and authorization, attackers can easily access confidential information or misuse applications. This could lead to data breaches or financial losses (Carol Xiaojuan Ou et al., 2022).

4: Lack of Encryption

Reason: Data was not encrypted in the above instance. Thus, a lack of encryption can compromise security. Encryption safeguards data against unauthorized access. Without proper encryption, confidential information or data can be vulnerable to attackers or unauthorized access. This could lead to data breaches or financial losses (Fcc.gov, 2022).

5: Disgruntled Employees

Reason:

¹ Reason: In the above scenario, it was indicated that Mr. Elmo was given additional responsibilities to manage the job of the two Sales Heads. He was also not properly given authority or recognition for the additional job responsibility, which might cause dissatisfaction over time. As Elmo had full access to all the business applications, even if he is disgruntled or terminated, he can still use this access for malicious intent. This means disgruntled employees can replicate regular users' input for malicious activities. It can also be used for stealing or manipulating sensitive data (Fcc.gov, 2022).

¹⁷ 6: Social Engineering Attacks

Reason: ¹⁷ Social engineering attacks often use psychological manipulation to deceive users into providing sensitive information or taking certain actions. In the scenario given, Mr. Elmo was determined to increase the business income and offered a 20 % discount for university students and faculty, as well as free Wi-Fi to attract more customers (Verizon Enterprise, 2020). This offers employees, students, and the public an attractive incentive to access the cafe's network and could potentially be used by

attackers to perform a social engineering attack. For example, an attacker could employ phishing to acquire network access. They could also impersonate an employee to gain access (Fcc.gov, 2022).

Task 2. Different types of threats, vulnerabilities, and attacks

Threats:

Definition:

A threat is an indicator of potential danger or harm which can compromise the security of the network or system. It could be a harmful activity that damages data or systems or a potential threat. Viruses, malware, social engineering, phishing, and insider attacks are common risks (Ghelani, 2022).

Types of Threats:

Threats can fall into two broad categories: external and internal threats.

- External threats involve malicious actors who attack networks and systems from outside. These include hackers, phishers, and other data thieves (Li and Liu, 2021).
- Internal threats are the ones that come from within an organization. Examples of internal threats include malicious activity by authorized users, insiders, or careless employees who mishandle data or leave systems vulnerable (Li and Liu, 2021).

1

Significance of threats in a Network:

Threats can have serious impacts on the security of a network or system. They can lead to data leakage, data manipulation, and financial losses. It can also reduce productivity and increase cyberattack risk. According to Verizon's Data Breach Investigation report (2020), threats such as social engineering and unauthorized access and use were significant contributors to data breaches (Pritam, 2020).

Vulnerabilities

Definition:

A vulnerability is a weakness in a system's structure or design that attackers can exploit to obtain unauthorized access to the system or data. Hackers use

vulnerabilities to find and exploit various weaknesses in order to gain access to data or networks. Such networks and systems can become vulnerable if they are not maintained properly and secure patches/updates/upgrades are not applied regularly.

important of vulnerability during the network operations:

Vulnerabilities need to be taken seriously if an organization wants to maintain secure networks and systems. Vulnerabilities can lead to serious security breaches and data loss if left unchecked. Attackers can use vulnerabilities to access data and networks and commit crimes like data manipulation (Humayun et al., 2020). These activities can lead to significant financial losses for organizations.

How vulnerabilities can affect network performance?

Vulnerabilities can have serious impacts on a network's performance. They can lead to data leakage and data manipulation. Customers may lose trust if their data is compromised. Vulnerabilities raise attack risk and decrease productivity. Network vulnerabilities make malware infections and attack vectors easier for criminal actors to access data and networks (Karabacak, Yildirim, and Baykal, 2016).

Attacks

Definition:

An attack is a malicious action taken to breach a system's or network's security and gain unauthorized access to the data. Phishing, malware, man-in-the-middle attacks, denial-of-service assaults, ransomware, and distributed denial-of-service (DDoS) attacks are all potential entry points for malicious actors (Goutam, 2015). Social engineering, unauthorized network access, and data manipulation are only a few of the methods used by attackers to compromise a system or steal sensitive information.

Why attacks are important to be considered during network operations?

Attacks can have serious impacts on the security of a network or system. They can lead to data leakage, data manipulation, loss of trust from customers, and financial losses. They also reduce production and increase assault risk (Goutam, 2015). Attacks also ruin organizations' reputations. Attacks caused 28% of data breaches, according to the 2020 Verizon Data Breach Investigation Report (Burbidge, 2021).

How attacks can affect network performance?

Attacks can have serious impacts on a network's performance. They can lead to data leakage and data manipulation. They can also lead to a loss of trust from customers and stakeholders as their data may be at risk and their privacy compromised by malicious actors. Attacks also reduce production because the network must be shut down to prevent further harm (Li, and Liu, 2021).

¹ “.meds” file format attack

Definition:

A .meds file format attack is a type of ransomware attack wherein attackers encrypt the data stored on the victim's system and demand a ransom to decrypt and gain access to it (Meskauskas, 2021). It allows ²⁶ unauthorized access to a system or network to steal or alter sensitive data. Attackers utilize phishing, malware, man-in-the-middle assaults, and other methods to steal victim data.

How it affects the operation?

The “.meds file” format attack can cause sensitive data loss, which can harm an organization. reputational damage, and significant financial losses. The attackers can manipulate or steal sensitive data and demand a ransom for its release. Attackers can also take over applications and activities, disrupting operations (Meskauskas, 2021).

Are there any possible methods to recover?

A “.meds file” format attack can be recovered by numerous means. To retrieve data after an attack, organizations need a solid backup and recovery plan. To lessen attack risk, organizations should update security patches. Organizations should also use anti-virus and anti-malware software to detect and delete malicious software before an attack (Meskauskas, 2021).

¹ **Task 3. Guideline for staff members, and customers to responsibly use their digital space**

The following are some key practices and guidelines for staff members and customers at Kermit's Cafe to help prevent common threats and attacks: (University Prep, 2021)

Security Awareness

All digital space users—staff, customers, competitors, etc.—must grasp cyber-attack hazards and possibilities. Communicating effective security policies and guidelines to the users of the digital space will help them to be vigilant and understand the possible attackers and attack tactics. Moreover, users should also be aware of the methods to recognize and combat these threats (University Prep, 2021).

Secure Wi-Fi and Network Access

- Ensure the Wi-Fi router is configured with a strong password and change it periodically.
- Monitor the connection status of the router and limit it to authorized personnel only.
- Regularly check for any unauthorized access on the network (Ed.gov, 2023).
- Change the default passwords to strong passwords for all connected devices.
- Monitor access to sensitive information over the network and report any attempts of unauthorized access (University Prep, 2021).
- Educate personnel on safe network practices and identify areas where security needs to be improved.

Secure Device Usage

- Encrypt data stored on all devices including laptops, mobiles phones, and tablets.
- Disable auto-connect of devices to the Wi-Fi network.
- Implement multi-factor authentication on all devices.
- Practice frequent back-ups and prevent data loss in the event of a security breach.
- Install only enterprise-grade security software on all devices.

Physical Security

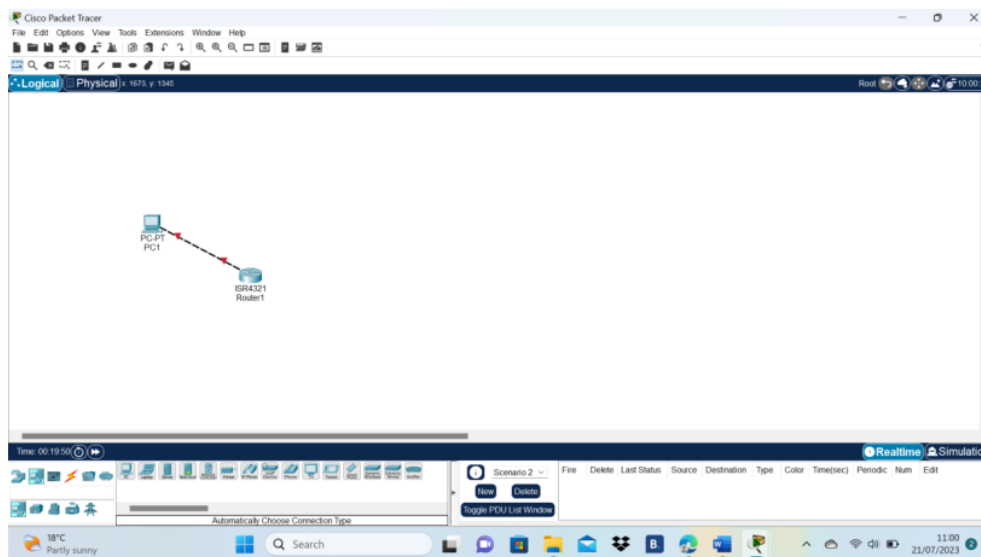
Users & all employees of the cafe must follow security measures and prevent physical access to the digital space. Users should also save data securely to avoid theft or misuse (Ed.gov, 2023).

Secure Online Interactions

- Avoid clicking on suspicious links or attachments, or engaging in communications or transactions with unknown senders.
- Use antivirus and anti-malware protection to scan any downloads.
- Make sure your browsers are updated to the latest versions.

- Install ad blockers and other preventative measures to help protect the system from malicious ads.
- Avoid opening e-mails from unknown senders and beware of deceptive links that may contain Malware executable or malicious content (University Prep, 2021).
- Use complex passwords and never use the same password twice for multiple accounts.

These best practices and guidelines are just the beginning of building a secure network. The security system should be reviewed and updated periodically to reflect environmental changes (University Prep, 2021). Firewalls, anti-malware software, spam filters, patching systems, user authentication, data encryption, and other security technologies should be part of a strong security system. Regularly educating personnel on cyber-security threats and techniques is also essential for maintaining a secure network (Ed.gov, 2023).



Conclusion, Recommendation & Future Work

Based on the scenario given, I would recommend that Kermit strengthen the security of his network by using multi-factor authentication, secure server hosting, and dedicated networks for different sets of users. Additionally, developing and implementing a password policy and raising user awareness of network security can help reduce the risk of attacks. Furthermore, Kermit should deploy a security system

that can monitor the network for malicious activity. As a future work, Kermit should have a backup plan to quickly recover from an attack and invest in advanced security solutions to further strengthen the security of his ²⁰ network. Intrusion Prevention Systems (IPS) and Intrusion Detection Systems (IDS) work together to create the backbone of a well-protected network.

de

Reference

- ¹⁰ Burbidge, T. 2021. *Cybercrime thrives during a pandemic: Verizon 2021 Data Breach Investigations Report*. [online] Available at: <https://www.verizon.com/about/news/verizon-2021-data-breach-investigations-report> [Accessed 20 June 2023].
- ¹² Carol Xiaojuan Ou, Zhang, X., Angelopoulos, S., Davison, R.M. and Janse, N. 2022. *Security breaches and organization response strategy: Exploring consumers' threat and coping appraisals*. [online] 65, pp.102498–102498. doi <https://doi.org/10.1016/j.ijinfomgt.2022.102498>.
- ⁷ Ed.gov. 2023. *Chapter 3-Security Policy: Development and Implementation, from Safeguarding Your Technology, NCES Publication 98-297 (National Center for Education Statistics)*. [online] Available at: <https://nces.ed.gov/pubs98/safetech/chapter3.asp> [Accessed 30 June 2023].
- ¹⁶ Fcc.gov. 2022. *Cybersecurity for Small Businesses*. [online] Available at: <https://www.fcc.gov/communications-business-opportunities/cybersecurity-small-businesses> [Accessed 02 July 2023].
- ¹¹ Ghelani, D., 2022. Cyber security, cyber threats, implications, and future perspectives: A Review. *Authorea Preprints*. pp. 1-23. <https://www.authorea.com/doi/pdf/10.22541/au.166385207.73483369>
- ¹⁹ Goutam, R.K., 2015. Importance of cyber security. *International Journal of Computer Applications*, 111(7). pp. 1-22. <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=5cfb7a5bd2e6c181e8a69ebd49b1dad795f493b>
- ⁴ Humayun, M., Niazi, M., Jhanjhi, N.Z., Alshayeb, M. and Mahmood, S., 2020. Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, 45, pp.3171-3189. <https://sci-hub.se/10.1007/s13369-019-04319-2>
- ⁹ Johns, E., 2020. Cyber security breaches survey 2020. *London: Department for Digital, Culture, Media & Sport*. pp. 1-22. <https://dlocal.co.uk/wp->

[content/uploads/2021/07/Cyber_Security_Breaches_Survey_2021_Statistical_Release.pdf](#)

⁶ Karabacak, B., Yildirim, S.O. and Baykal, N., 2016. A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. *International Journal of Critical Infrastructure Protection*, 15, pp.47-59. <https://fuse.franklin.edu/cgi/viewcontent.cgi?article=1034&context=facstaff-pub>

² Khari, M., Shrivastava, G., Gupta, S. and Gupta, R., 2017. Role of cyber security in today's scenario. In *Detecting and mitigating robotic cyber security risks*. pp. 177-191. IGI Global. https://www.researchgate.net/profile/Gulshan-Shrivastava/publication/326414356_Role_of_Cyber_Security_in_Today%27s_Scenario/links/5b4f2bf2aca27217ff9f80b9/Role-of-Cyber-Security-in-Todays-Scenario.pdf

³ Li, Y. and Liu, Q. 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. [online] 7, pp.8176–8186. doi <https://doi.org/10.1016/j.egy.2021.08.126>.

⁸ Li, Y. and Liu, Q., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, 7, pp.8176-8186. <https://www.sciencedirect.com/science/article/pii/S2352484721007289>

¹ Meskauskas, T. 2021. *Meds Ransomware*. [online] Pcrisk.com. Available at: [https://www.pcrisk.com/removal-guides/15820-meds-ransomware#:~:text=What%20is%20Meds%3F,in%20effect%2C%20pay%20ransoms\).](https://www.pcrisk.com/removal-guides/15820-meds-ransomware#:~:text=What%20is%20Meds%3F,in%20effect%2C%20pay%20ransoms).) [Accessed 16 July 2023].

⁵ Pritam, N. 2020. *Money makes the cyber-crime world go round - Verizon Business 2020 Data Breach Investigations Report*. [online] Available at: <https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report> [Accessed 20 July 2023].

¹³ Saber, J. 2017. *Scholar Works Determining Small Business Cybersecurity Strategies to Prevent Data Breaches*. [online] Available at: <https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=6270&context=dissertations>.

¹⁴

University Prep. 2021. *Guidelines for Responsible Use of Technology*. [online]
Available at: <https://www.universityprep.org/students/technology-resources/guidelines-for-responsible-use-of-technology> [Accessed 20 July 2023].

²⁴

Verizon Enterprise. 2020. *PCI Compliance: What to Know About Digital Payment Security*.¹⁵ [online] Available at:
<https://www.verizon.com/business/resources/articles/small-business-cyber-security-and-data-breaches/> [Accessed 20 July 2023].

Report

ORIGINALITY REPORT

27%
SIMILARITY INDEX

15%
INTERNET SOURCES

4%
PUBLICATIONS

25%
STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to University of Wales, Lampeter Student Paper	8%
2	Submitted to University of Wolverhampton Student Paper	2%
3	Submitted to Kaplan Professional Student Paper	1%
4	Submitted to Victoria University Student Paper	1%
5	Submitted to University of Sunderland Student Paper	1%
6	jsi.cs.ui.ac.id Internet Source	1%
7	myassignmenthelp.com Internet Source	1%
8	Submitted to University of Bedfordshire Student Paper	1%
9	Submitted to American Public University System Student Paper	1%

10	Submitted to The University of Manchester Student Paper	1 %
11	Submitted to Napier University Student Paper	1 %
12	Submitted to Intercollege Student Paper	1 %
13	Submitted to California Southern University Student Paper	1 %
14	Submitted to National University of Singapore Student Paper	1 %
15	Submitted to University of Teesside Student Paper	1 %
16	Submitted to Regent Independent School and Sixth Form College Student Paper	1 %
17	"HCI for Cybersecurity, Privacy and Trust", Springer Science and Business Media LLC, 2023 Publication	<1 %
18	Submitted to University of Hertfordshire Student Paper	<1 %
19	www.citethisforme.com Internet Source	<1 %
20	www.coursehero.com Internet Source	<1 %

21	cienciasforestales.inifap.gob.mx Internet Source	<1 %
22	Submitted to Swansea College Student Paper	<1 %
23	repositorio.uach.mx Internet Source	<1 %
24	Submitted to Southern New Hampshire University - Continuing Education Student Paper	<1 %
25	www.researchgate.net Internet Source	<1 %
26	bjmas.org Internet Source	<1 %
27	repositorio.ucam.edu Internet Source	<1 %

Exclude quotes Off

Exclude matches Off

Exclude bibliography Off