FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY

Assignment

BAIT1093 Introduction to Computer Security
Feb 2023 Semester

Declaration

I confirm that I have read and shall comply with all the terms and conditions of TAR UMT's plagiarism policy. I declare that this assignment is free from all forms of plagiarism and for all intents and purposes is my own properly derived work.

Name (Block Capital)	LEE WEE HARN
Registration No.	22WMR05673
Programme	RSW
Tutorial Group	G6
Number of Words	1407 Words
% Originality Report	2%
Signature	Harn
Marks	_____ / 100

Tutor's Name: Mohd Nur Rahmat Bin Mohd Taat

Date of Submission: 21 April 2023, Friday (Week 11)

Part I: 1.1

The security incident that was selected is the Kaseya Supply Chain Attack that happened on 2nd July 2021. Kaseya is an IT Management Software company that is known for their Unified Remote Monitoring & Management software platform. This type of software helps out with organizing and managing a company's IT. On 2nd July 2021, Kaseya was hit by a ransomware attack which was done by a hacker group called REvil that is based in Russia. The hacker group had encrypted the company business files and asked for $70 million in exchange for the restoration. They were also willing to negotiate a better price if the company were to entertain the idea of negotiation. The attacks not only affected their company but their clients as well. The clients would range from around 800 to 1500 businesses all around the world. Some of the businesses were merely inconvenienced for dentist's offices or accountants but the effect was felt the most by the Swedish supermarket company COOP. Hundreds upon hundreds of supermarkets were closed due to their cash registers not working. Other businesses that were affected greatly were schools in New Zealand, not having any internet (*Security, T.N. 2021*). The main classification of malware involved in this security incident is imprison (ransomware) and the main attack vector in this security incident is supply chain attack which is caused by the vulnerabilities, leaked security of the system and even fake email.

A supply chain attack, also known as a third-party attack, happens when someone gains access to your system through an external partner or provider who has access to your systems and data (*Korolov, M. 2018*). A supply chain attack can be caused by a vulnerability or flaw in a piece of software, hardware, or a system that an attacker may use to gain access, steal information, or cause other kinds of damage (*What Is the Log4j Vulnerability?*). Besides that, leaked securities, such as passwords or other sensitive data may be used by hackers to gain unauthorised access to systems or accounts. An attacker may take advantage of a leaked employee's password to access the employee's email account or workplace network(*Hanifie, S. 2017*). Furthermore, fake emails, also known as phishing emails, are intended to fool the recipient into providing personal information or clicking on a link or attachment that may infect their computer with malware. This is often accomplished by pretending to be an authoritative source, such as a bank or business, and invoking panic or haste in order to get the target to respond right away (*Gwinn, E. 2004*).

The REvil ransomware attack is a type of attack that falls under improson category and is also known as Sodinokibi. They have been involved in a number of widely known attacks on companies and organisations. It was originally identified in April 2019 and is well-known for using the ransomware-as-a-service (RaaS) model and having advanced encryption capabilities(*Constantin, L. 2021*). REvil works by encrypting the victim's files and requesting an amount of money in return for the key to unlock them. In order to avoid detection and traceability, the attackers frequently demand payment in Bitcoin or other cryptocurrencies. In addition to implementing double extortion techniques, REvil is well known for encrypting the victim's files and threatening to reveal sensitive information if the ransom is not paid (*Chong, C. 2021*).

Part I: 1.2

Recommendations to mitigate the risk of supply chain attacks happening are as follows:

- Implement security policies in companies to include the following guidelines for all employees of an organization to follow:
    - Encryption Policy
      Supply chain attacks frequently target suppliers or third-party providers who have access to private information. Data can be protected by encryption as it travels through the supply chain from one party to the next, making it more challenging for hackers to intercept or change the data. (*File-based Encryption Technology 2008*).

    - Incident Response Policy
      Supply chain attacks can be challenging to identify and may go undetected for a long time, giving attackers access to critical data and systems. A supply chain attack could result in security incidents, and an incident response policy can help make sure the company is ready to handle them by performing early detection, rapid response, coordination with third-party vendors and Investigation (*Cyberattack 2018*).

    - Patch Management Policy
      Organisations can lower the risk of supply chain attacks by setting together a patch management policy that makes sure all the systems and software involved in the supply chain are patched and up to date with the most recent security updates (*Windows Active Directory Networks 2004*).

- Physical security measures can aid in preventing unauthorised access to infrastructure and physical assets across the supply chain. This may involve taking action using technologies like security personnel, access control systems, and cameras. Organisations may minimise the risk of supply chain attacks that target these assets by making sure the infrastructure and physical assets within the chain are secure (*RAJAONAH, B. 2017*).

- Communication and network security measures can aid in protecting data and systems within the supply chain from unauthorised access or interception. This may involve taking precautions like intrusion detection systems, firewalls, and encryption. Organisations can lessen the risk of supply chain attacks that target data or systems within the supply chain by putting communication and network security measures in place (*Network Size 2005*).

Part II: 2.1 (Trends)

There is an ongoing trend of the application of fingerprint access control system as this can minimise fraudulent transactions, and protects against security breaches. Global demand is expected to increase as industry competition heats up. With the usage of passwords gradually decreasing in exchange for multimodal biometrics solutions for authentication, businesses all over the world are searching for strong security measures (*Market Research Report Database 2015*).

As for the trend in communication & network security, the use of multi-factor authentication (MFA) is rising and the factors behind this are the increasing use of digital payments via smartphones and other wireless devices, cyberattacks, and financial crimes. The use of multi-factor authentication systems will also be aided by increased investments in cloud technologies, organisational mobility, and growing BYOD usage among businesses. In addition to having a username and password for authentication, MFA offers another level of protection. Smart cards, one-time passwords, and biometric authentication are some examples of this (*Global 2019 Analysis Key Trends*).

Trends of using endpoint protection such as Zero-Trust Security is increasing due to factors like the rise in sophisticated cyberattacks. Additionally, the expansion of the worldwide zero-trust security market is being supported by the increasingly demanding government laws and regulations linked to security. It requires valid verification from both an insider and an outsider before allowing access into the network. Additionally, it has a lot of benefits like being easy to use, affordable, and providing trusted security features. Hence, these are the factors driving the demand for zero-trust security (*Adroit Market Research*).

Part II: 2.2 (Challenges/Limitations)

Even though fingerprint access control may be an effective security solution, there are some restrictions and disadvantages to take into account before using this technology. False acceptance and rejection rates indicate the probability that an authorised user will be accepted by the system while an unauthorised user will be rejected. The effectiveness of the system is based on the software and fingerprint scanner's quality. The effectiveness of the system may be compromised by higher false acceptance or rejection rates. Besides that, some organisations may find it very difficult to deploy and maintain fingerprint identification systems due to the corresponding expenses (Koolen, M. 2011).

Multi-factor authentication (MFA) comes with multiple restrictions and disadvantages, despite the fact that it can significantly improve the security of digital systems and data. For instance, Dependence on One Factor, Even though MFA uses many authentication factors, it can still be exposed if one of them is false. An attacker might still be able to access the system using the second factor, for instance, if a user's password is compromised (*Y. & Gerla, M. 2019*).

While Zero-Trust Security provides a number of advantages, organisations should be aware of some of its disadvantages as well. In particular, if the legacy systems lack connectivity for current authentication and access control standards, integrating Zero-Trust Security with them can be difficult. Furthermore, Zero-Trust Security has a risk to produce false positives or false negatives, which may result in access denials or unauthorised access. Misconfigured policies, incomplete user profiles, a lack of contextual data, and other issues can all cause this (*Ma, X. 2022*).

REFERENCES

1. Author by, J.C. & Security, T.N. 2021. Kaseya *suffers a supply chain cyber-attack resulting in up to 1,500 businesses being affected - ProQuest*. [online] Available at: https://www.proquest.com/docview/2568312108/A726360C9EF54B8APQ/4?accountid=38945 [Accessed 20 Apr. 2023].

2. Constantin, L. 2021. REvil ransomware explained: A widespread - ProQuest. [online] Available at: https://www.proquest.com/docview/2581955596/82FD96D83E5E429EPQ/3?accountid=38945 [Accessed 20 Apr. 2023].

3. Chong, C. 2021. Heard of software as a service? Now there's a hacker equivalent- ProQuest. [online] Available at: https://www.proquest.com/docview/2569584480/4796F813337D4AD3PQ/3?accountid=38945 [Accessed 20 Apr. 2023].

4. What Is the Log4j Vulnerability? What to Know. - ProQuest. [online] Available at: https://www.proquest.com/docview/2611029066/5B92531A594E416FPQ/4?accountid=38945 [Accessed 20 Apr. 2023].

5. Hanifie, S. 2017. Hackers could gain access to passwords through - ProQuest. [online] Available at: https://www.proquest.com/docview/2122203194/4BB06943E4AD439BPQ/3?accountid=38945 [Accessed 20 Apr. 2023].

6. Gwinn, E. 2004, Phishing scams reel in users with fake e-mails - ProQuest. [online] Available at: https://www.proquest.com/docview/419972458/AAB2F8ADBE334045PQ/5?accountid=38945 [Accessed 20 Apr. 2023].

7. Korolov, M. 2018. What is a supply chain attack? Why you should be - ProQuest. [online] Available at: https://www.proquest.com/docview/2021604283/C7C6C05F3DB64C6DPQ/2?accountid=38945 [Accessed 20 Apr. 2023].

8. File-based Encryption Technology Versus Full-Disk Encryption 2008. Aberdeen Group Data Loss Prevention Study - ProQuest. [online] Available at: https://www.proquest.com/docview/448575799/8E39B041EF634112PQ/1?accountid=38945 [Accessed 20 Apr. 2023].

9. Cyberattack 2018. Thycotic Releases Incident Response Policy - ProQuest. [online] Available at: https://www.proquest.com/docview/2076151728/2C4D25E3CB2D407BPQ/1?accountid=38945 [Accessed 20 Apr. 2023].

10. Patch Management Problem for Windows Active Directory Networks 2004. AutoProf Releases Group Policy-based Patch Management Solution - ProQuest. [online] Available at: https://www.proquest.com/docview/445713241/537FB06B3062415EPQ/1?accountid=38945 [Accessed 20 Apr. 2023].

11. RAJAONAH, B. 2017. A view of trust and information system security - ProQuest. [online] Available at: https://www.proquest.com/docview/2167118838/23DB43CA610643C5PQ/7?accountid=38945 [Accessed 20 Apr. 2023].

12. Company Offers Two Levels of Security Protection, Depending on Network Size 2005. Integralis Secure Watch(R) Security Service Allows Companies to Co-Manage Network Security - ProQuest. [online] Available at: https://www.proquest.com/docview/445362401/F6F46C6928934C7EPQ/1?accountid=38945 [Accessed 20 Apr. 2023].

13. Market Research Report Database 2015. Radiant Insights,Inc: RadiantInsights.com has announced the addition of "Global Fingerprint Access Control Systems Market Trends, Growth And Forecast Report Up To 2022 - ProQuest. [online] Available at: https://www.proquest.com/docview/1733313446/fulltext/D6DD8A3D93E14C01PQ/2?accountid=38945 [Accessed 20 Apr. 2023].

14. Global 2019 Analysis Key Trends. Rising financial frauds, cyber-attacks and use of digital payments is fueling the demand for the multi factor authentication 2019 - ProQuest. [online] Available at: https://www.proquest.com/docview/2239502952/678E2AF8C4B14038PQ/2?accountid=38945 [Accessed 20 Apr. 2023].

15. Koolen, M. 2011. Operational benefits and challenges of the use of - ProQuest. [online] Available at: https://www.proquest.com/docview/1034881111/AD64FDB1104A493DPQ/14?accountid=38945 [Accessed 20 Apr. 2023].

16. Adroit Market Research. Document unavailable - Zero-Trust Security Market US $38 billion by 2025. [online] Available at: https://www.proquest.com/docview/2454081761/F498997965F34E6CPQ/1?accountid=38945 [Accessed 20 Apr. 2023].

17. Y. & Gerla, M. 2019. Challenges of Multi-Factor Authentication - ProQuest. [online] Available at: https://www.proquest.com/docview/2170068047/3887362A50D94DA1PQ/19?accountid=38945 [Accessed 20 Apr. 2023].

18. He, Y., Huang, D., Chen, L., Ni, Y. and Ma, X. (2022). A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing, 2022, pp.1–13. doi:https://doi.org/10.1155/2022/6476274 .

APPENDIX 1

Kaseya suffers a supply chain cyber-attack resulting in up to 1,500 businesses being affected.

Author by Jeremiah Cristobal; Security Television Network

ProQuest document link

FULL TEXT

September 2, 2021 (Security Television Network) -- Kaseya suffers a supply chain cyber-attack resulting in up to 1,500 businesses being affected.

On July 2, 2021, Kaseya was targeted by a ransomware attack that resulted in between 800 and 1,500 businesses all around the world being affected. This ranged with their clients being inconvenienced to outright being closed down due to the seriousness of the situation.

Kaseya is an IT Management Software company that is known for their Unified Remote Monitoring &Management software platform, or Kaseya VSA. This type of software helps out with organizing and managing a company's IT whether that be a small start-up or a well-known company. The company is able to increase the efficiency of IT departments by implementing automated IT management software (Kaseya Home Page, 2021).

On July 2, 2021, Kaseya was hit by a ransomware attack that spread to not only the company but to their clients as well. The clients would range from around 800 to 1500 businesses all around the world. Some of the businesses were merely inconvenienced for dentists' offices or accountants but the effect was felt the most by the Swedish supermarket company COOP. Hundreds upon hundreds of supermarkets were closed due to their cash registers not working. Other businesses that were affected greatly were schools in New Zealand, not having any internet (Satter, 2021).

The culprits came out with a ransom note following the attack. This was targeted to the clients of Kaseya and would confuse the business owners on what to do. The ransomware attack was identified as a REvil ransomware attack, a hacker group based in Russia who encrypted businesses' files.

The hacker group had asked for $70 million in exchange for the restoration of the encrypted files and were willing to negotiate a better price if the company were to entertain the idea of negotiation (Panettieri, 2021).

The CEO of Kaseya, Fred Voccola, had stated that "I can't comment 'yes,' 'no,' or 'maybe', No comment on anything to do with negotiating with terrorists in any way. In the topic of Voccola, he also got in contact with the White House, the FBI, and the Department of Homeland Security to reassure them that the breach did not introduce any "national risk".

Fred Voccola, Source: KaseyaFrom July 6 until July 13, Kaseya had been slowly but surely getting their infrastructure back on track. They had encountered a few setbacks with vulnerability issues, leaks in their security, and fake emails.

Due to the quick response of Kaseya and help from third parties, on July 13 Kaseya was able to say to their clients that their VSA has been restored with some guidance from the Cybersecurity and Information Security Agency. Moreover REvil, the group responsible for the hack had mysteriously disappeared leaving the threat not as scary as before. Some have speculated that the U.S. Government was able to track them down or Vladimir Putin himself was able to call them off after President Joe Biden called up Putin in an effort to put an end to the ransomware group. Overall, this must have cost Kaseya and their clients millions upon millions and it is nice to see that it has been resolved. A tighter grip on their security will be needed and a sense of trust will be built right up for their clients.

References

Panettieri, J., 2021. Kaseya VSA Supply Chain Cyberattack Details, RMM Recovery Timeline - MSSP Alert. [online]

MSSP Alert. Available at: msspalert.com/cybersecurity-breaches-and-attacks/kaseya-rmm-cyberattack-warning [Accessed 13 July 2021].
Kaseya. 2021. Kaseya Home Page. [online] Available at: kaseya.com [Accessed 13 July 2021].Satter, R., 2021. Up to 1,500 businesses affected by ransomware attack, U.S. firm's CEO says. [online] Reuters. Available at: reuters.com/technology/hackers-demand-70-million-liberate-data-held-by-companies-hit-mass-cyberattack-2021-07-05 [Accessed 13 July 2021].

Dr. James Halldrhall@security20.com(202) 607-2421
By Author: by Jeremiah Cristobal, Security Television Network

APPENDIX 2

Originality report

COURSE NAME
(L) BAIT1093 - Introduction to Computer Security

STUDENT NAME
LEE WEE HARN

FILE NAME
RSW_G6_LEEWEEHARN.gdoc

REPORT CREATED
Apr 21, 2023

Summary

Flagged passages	0	0%
Cited/quoted passages	1	2%

Web matches

csoonline.com	1	2%

---

1 passage

Student passage CITED

A supply chain attack, also known as **a third-party attack**, happens **when someone** gains access to **your system through an** external **partner or provider** who has **access to your systems and**

Top web match

A supply chain attack, also called **a** value-chain or **third-party attack**, occurs **when someone** infiltrates **your system through an** outside **partner or provider** with **access to your systems and** data.

What is a supply chain attack? Why to be wary of third-party providers https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html

---