Security in Organizations: Assignment 1

Group number 27

Elwin Tamminga
s1013846

Lucas van der Laan
s1047485

Part 1

A

Ransomware is malicious software that encrypts data on a system without consent of the owner of the data. The data is then usually only accessible by decrypting it using a secret cryptographic key provided by the attacker in exchange for money (Al-rimy et al. 2018). This explains the word "ransom" in ransomware, because you have to pay ransom to "release" the data that is being held by the attacker (Ali 2017).

Individuals often get infected because the attacker pretended to be someone they were not, or by including the ransomware in something that people used. An individual could have received an email that pretends they are the Rabobank, when they user clicks on this mail they get instead sent to a malicious website. The email can also contain an attachment that when opened activates the ransomware on the computer (Al-rimy et al. 2018). Computers can also be infected by ransomware if they were already infected by another malware that created a backdoor into their system. This can make delivering a ransomware payload much easier without needing any user input (Zimba 2017).

Criminals that make ransomware can use the infected systems to disrupt services and ask money for financial gain. A well-known example of ransomware is WannaCry. It infected over 300,000 systems in more than 150 countries worldwide in 2017 (Akbanov et al. 2019), which also caused disruptions in important public services like hospitals (Ghafur et al. 2019). Another example is the attack on the Maastricht University in 2019, causing a disruption in their computer services. Some of their backup servers were also infected, making it more difficult to restore the services. Eventually they decided to pay the ransom to regain access to the encrypted data (*Reactie Universiteit Maastricht op rapport FOX-IT* 2020).

B

How ransomware affects us

Ransomware can affect us personally by infecting our computer and our connected devices. When you get infected, the only thing you can do that has a possibility of retrieving your lost data, is paying and hoping that the attacker can or will decrypt your data. Not paying would mean having to reformat our computer (to make sure no malware is left on there) and to be sad that our data is lost forever. Luckily we both tend to have our data on other devices as well as backups, so we would not lose as much.

How we can reduce the risks

There are some **Preventive Measures** that you can take, like double checking every link that you click on that does not come from a secure source. For example when we get a link to our Radboud address, or spam on our personal address, it's important to make sure that you are not clicking on a link like fasebook.com or another misspelling of a popular website. If you are on a "shady" website, make sure that you do not click on any advertisements or anything like and apply critical thinking to ensure that scams/traps do not get to you. This does not need to be ransomware specifically, but more broadly for any malware.

Detective Measures are very important to have. Anti-Malware software can save you a lot of trouble, for example MalwareBytes has a browser utility that informs the user that a website is unsafe before the website is loaded. This can be extremely useful when you are browsing the internet doing not so legal things, as you get saved from fake or compromised websites.

For **Corrective Measures**, there is a structure that you can do:

- Local machine
- Backup Server
- Disconnected (Off-shore) backup server, the backup to this server should only be done either manually or should have a versioning system.
- Offline backup, a physical disk that you backup to manually

This tends to be an expensive solution, so we can technically skip the Disconnected backup server and maybe even the normal backup server. It would be preferable to have the data in at least three places, every step taken will reduce the risk of losing data.

Both of us have a backup of our important files, which makes having our files encrypted by malware less of a hassle. We also do not just press on any link or attachment in our mailboxes, but ensure that the source is trustworthy and secure. Personally I also manually store a backup of my most important files encrypted in the cloud. It is not directly connected so it cannot be easily accessed by ransomware. I also use a remote git repository for my configuration files, which is shared among multiple devices (basically multiple backups).

Part 2

C

Index	Lesson Learned	Type of Lesson	Relevant to
1	Keep software up-to-date, this prevents patched exploits to be exploited.	Technical	DigiNotar
2	Security by detection, by monitoring suspicious traffic to prevent further damage	Technical	DigiNotar
3	Segregation of duties, make sure that there are different people responsible for implementing security and enforcing security	Security Mangement	DigiNotar
4	Do not blindly trust a Certificate Authority, have a backup plan to replace the certificates when the CA is compromised	Security Management	Reliant Organizations
5	Aggregate all the logs on a centralized secure server, this prevents log tampering.	Security Management	DigiNotar
6	Limit access of systems and services by hardening configuration and separating networks	Technical	DigiNotar
7	Regularly do risk assessments to identify security incidents before they can happen	Security Management	DigiNotar
8	Hire penetration testers to do audits on a regular basis	Security Management	DigiNotar
9	Detect incoming traffic to see if it comes from a (possibly) fraudulent server.	Technical	Reliant Organizations
10	Ensure that the CA is regularly audited and checked, to prevent rogue CA servers.	Security Management	Reliant Organizations

Table 1: Table of lessons learned

D

The index of the list corresponds to the lesson learned in the table above. The format is CHAPTER:Explanation, in which chapter refers to the chapter of the ISO 27002:2013

1. 12: Software should be checked to ensure that it is up to date, to ensure that it is secure and functional.
2. 12: Logs and suspicious traffic should be monitored to ensure that the systems have not been compromised.
3. 6: The organization should allocate responsibilities to it's employees and segregate these to avoid a conflict of interest.
4. 12: There should always be a documented backup procedure in place in case a CA is compromised.
5. 12: Aggregating the logs makes it so that the attacker can not access them and prevents them from being altered.
6. 13: Networks and communications between services should be secured and separated when possible.
7. 17: Risk assessments ensures that vulnerabilities can be identified to keep systems secure.
8. 18: The system needs to be audited by a third-party to ensure that it is secure.
9. 13: The network needs to be secured and validated to ensure that they are not getting attacked.
10. 15: The CA is in a sense a supplier and the users of the CA should ensure that the CA follows proper security management protocols.

E

(a) Access to the workstation was mainly gotten because it had a dual-network interface which lead to it being in two networks at the same time. Because the DIGIWS146 had a dual-network configuration, it was on both the Secure-net and the Office-net network at the same time. This gave access from the Office-net to the Secure-net.

(b) The firewall was configured to allow access to the BAPI-workstation from the main web server. This mean that it did not prevent machines on the same network from connecting to each other.

References

Akbanov, M., Vassilakis, V. G. & Logothetis, M. D. (2019), 'Ransomware detection and mitigation using software-defined networking: The case of wannacry', *Computers & Electrical Engineering* **76**, 111–121.
URL: *https://www.sciencedirect.com/science/article/pii/S0045790618323164*

Al-rimy, B. A. S., Maarof, M. A. & Shaid, S. Z. M. (2018), 'Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions', *Computers & Security* **74**, 144–166.
URL: *https://www.sciencedirect.com/science/article/pii/S016740481830004X*

Ali, A. (2017), 'Ransomware: A research and a personal case study of dealing with this nasty malware', *Issues in Informing Science and Information Technology* **14**, 087–099.

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. & Aylin, P. (2019), 'A retrospective impact analysis of the wannacry cyberattack on the nhs', *NPJ digital medicine* **2**(1), 1–7.

Reactie Universiteit Maastricht op rapport FOX-IT (2020).
URL: *https://www.maastrichtuniversity.nl/file/foxitrapportreactieuniversiteitmaastricht2pdf*

Zimba, A. (2017), 'Malware-free intrusion: a novel approach to ransomware infection vectors', *International Journal of Computer Science and Information Security* **15**(2), 317.