2017 NHS WannaCry Attack

CYBER ATTACK ANALYSIS

Network Security Fundamentals - CSI3207.4

Marco Cavani 19/08/2022

Student ID: 10570027

Bachelor of Computer Science (Y89)

Contents

Introduction

In 2017 the WannaCry Cyber Attack had a significant impact on many organizations around the globe, especially in England where the National Health Security was taken down by a crypto worm. The report is to analyse the facts that determine the attack and the consequences that it has had on society, moreover, it is questioning how a similar attack can be prevented in the future. This report aims is to outline important aspects of one of the biggest cyber-attacks ever faced and discuss what should have been done and what can be learned from it.

WannaCry Crypto worm

The WannaCry malware is a ransomware crypto worm or crypto-ransomware that targets Windows-based computers. The Crypto-Worm encrypts data using Cryptography, with the aim of blocking access to computers unless a ransom is paid to the hackers. Like many ramson attacks, WannaCry relies on complex techniques specifically designed to infect, persist in the system, and prevent eventual recovery attempts (Akbanov et al., 2019). The infection was spread in more than 150 countries showing high infection rates among various sectors including Manufacturing, oil and gas, healthcare, Information technology, media, food and beverage, education, and government. More than 300,000 windows base computers between XP and the Windows 8.1 version were affected all-round the globe (National Audit Office, 2017). WannaCry did not target a specific sector but specific unpatched operating systems. In fact, the National Health Services (NHS) in England was one of many enterprises affected by the crypto worm as its system was mostly relying on an unpatched version of windows 7 and other older and unsupported versions like Windows XP (Smart, 2018)

WannaCry Impact on NHS

The NHS provide care for over 1 million people every day and it is composed by 236 thrusts and more than 7,000 GP practices. With 83 National Health Services (NHS) thrusts, 603 primary care centre and 596 GP practices compromised, the services provider has impacted badly duo to the crypto worm (National Audit Office, 2017). The NHS suffered temporary disruption and struggled to keep the operations going in a way that was difficult for them to provide care for many patients. However, the NHS kept the operation going by cooperating with other NHS facilities. Some patients in demand for emergency treatments had to travel to other hospitals, many appointments urgent referrals and emergency cases were prioritized (Smart, 2018). Fortunately, no cases of death can be linked to the incident (National Audit Office, 2017). Permanent data loss, money loss, time loss, and reputational damage were also consequences of the impact. Data was lost as the worm deleted and blocked data and data access on the affected Windows computers, Time as the attack caused an unwanted delay on the services as many appointments were cancelled, money lost estimated at 92 million pounds and last but not least reputational damage as the attack could have been easily prevented by updating the operating system (*The NHS Cyber Attack*, 2020). The head of the National Audit Office (NAO) said *"It was a relatively unsophisticated attack and could have been prevented by the NHS following basic IT security best practices. There are more sophisticated cyber-threats out there than WannaCry, so the Department and the NHS need to get their act together to ensure the NHS is better protected against future attacks."* (*The Guardian*, 2017).

The aftermath of the Infection

The National Audit Office (NAO) outlined that more than a third of NHS facilities suffered from disruption with 80 out of 236 organizations involved in the incident divided into 34 facilities that were completely infected and 46 partially infected. Another 603 primary care along with 595 out of 7,454 GP Practices and clinics equivalent to 8% of the total. 21 additional NHS clinics registered suspicious network activities linked with the crypto worm that could have compromised facilities' internal devices (Smart, 2018). Process of supportive cooperation among the organization facilities was also enacted to maintain the operations going. Almost 7,000 booked appointments were rescheduled. Also, to be noted is the political aspect that the incident upstretched (*The Guardian,* 2017).

Political debate

The incident raised political conflicts with the accusations blaming on the health department that should have update the operating systems earlier with minor costs. The attack was predictable, and the impact of a potential attack underestimated (BBC, 2017). As reported from The Guardian, the labour and the liberal party claim that unappropriated conservative austerity has result in vulnerable services. The British politician Jonathan Michael Graham Ashworth wrote a letter to the health committee, Jeremy Hunt, saying that the issue was persistently disputed but no action was taken to address it. Also, the labour leader Jeremy Corbyn expressed his disappointment about not having renewed the security package on the Windows systems and demanded further explanation. While the liberal democrat's deputy Brian Paddick, declared: *"We need to get to the bottom of why the government thought cyber-attacks were not a risk when a combination of warnings and plain common sense should have told ministers that there is a growing and dangerous threat to our cybersecurity,"*. Considering the money lost it would have been far fewer resources consuming to invest in technology updates before facing the consequences of the attack (*The Guardian,* 2017).

Network and Cyber Security Reflection

The NHS relied on an articulate network called N3 that connects different hosts to communicate and store sensitive data among NHS facilities and other social services providers (*The NHS Cyber Attack*, 2020). The N3 was a broadband network designed by BT to address the needs of the NHS and was utilized by NHS until 2018 when it was replaced by the National Health Social and Care Network or HSCN (British Telecommunications, 2010). The N3 network was configured without encryption, no firewall, and no suspicious activity detection software to guard the communications. Additionally, there was no system to prevent unwanted communications to the SMBv1 or a mechanism to log SMBv1 activities (British Telecommunications, 2010). Furthermore, the NAO has confirmed that the infection spread over the internet including the N3 network (National Audit Office, 2017). However, the NHS incident could have been prevented in the first place by updating or patching the operating systems(BBC, 2017).

NHS WannaCry Attack

The fact that the NHS system was set on many unpatched computer systems made the National Health Service a target (Smart, 2018). Recent dynamic analysis verified the two crypto-worm main components: the worm component and the Cryptographic component. The worm component allowed the spread of the virus and the Cryptographic component encrypted data on infected computers using public-key cryptography (Akbanov et al., 2019). The attack was launched by exploiting the Server Message Block (SMB) using a computer exploit developed by the National Security Agency (NSA) called EternalBlue which was leaked

by a hacker group known by the name Shadow Brokers on April 14, 2017 (*The NHS Cyber Attack*, 2020). Even though the security vulnerability exploited was outlined a month before the leaking by Microsoft in the Security Bulletin MS17-010 that cited *"The most severe of the vulnerabilities could allow remote code execution if an attacker sends specially crafted messages to a Microsoft Server Message Block 1.0 (SMBv1) server" (Microsoft, 2017)*, on the 12th of May 2017, a massive attack victimized the NHS in England along with many enterprises in 150 different countries (BBC, 2017). In fact, during the attack, specific code was sent remotely to the SMBv1, and illegal connections were established through TCP ports 139 and 445. Furthermore, the malicious figures used EternalBlue along with DoublePulsar to have guaranteed remote access and bypass credentials on the unpatched systems (Akbanov et al., 2019). As a consequence, the worm infected 83 NHS trusts, 603 primary care canters and 596 GP practices (BBC, 2017). Originally developed by NSA as a communication protocol to share access to ports, printers, and files, EternalBlue was used to exploit the SMBv1 Windows file sharing protocol along with DoublePulsar which was used to deploy the WannaCry malicious code (AVAST, n,d).

Factors that Contributed to the Incident

The NHS was a victim of WannaCry as their system vulnerabilities were matching to the ideal target of the cyber-worm. Additionally, the lack of cyber-security measures and lack of cyber-security leadership at the management level contributed to the incident. It is responsibility of the cyber-security management to address the vulnerabilities of the network especially if the service provider is an essential service like the NHS (National Audit Office, 2017). The lack of measurements that could have prevented or mitigated the attack is a clear sign of inadequate support from cyber security professionals. Furthermore, none of the facilities infected had the Microsoft updated patch even if it was advised on 25 April 2017 by NHS Digital's CareCERT bulletin(BBC, 2017). Moreover, the attack was easy to prevent by following cyber security standards and the network security standard e.g., firewall or network monitoring technologies applied. However, the effects of the incident could have been far greater if a cyber-security researcher did not find the "kill switch" in the crypto worm (National Audit Office, 2017).

The Kill Switch

The attack was contained by Marcus Hutchins a self-thought cybers security expert which found the "kill switch" inside the malware logic as WannaCry used a link to initiate the encryption in the infected computers in a way that if the domain is not found online the encryption began. This link was simply an unregistered URL. Marcus Hutchins, mitigate the attack by registering the domain (BBC, 2017).

Attack Attribution

The British cyber-security centre pointed the finger at North-Korea as responsible for the 2017 WannaCry attack, soon later the US join the accusation on the Kim Jong-un regime which was also believed to be responsible for the 2014 Sony corporation hack. Research conducted by the Russian group Kaspersky lab and the US group Symantec outlined similarities on the code used in the 2014 Sony hack which was attributed to a group close to the north Koreans known by the name of Lazarus Group. However, there is a need for more investigation on this case as there is insufficient evidence to incriminate the North Korean which denied all accusations (USA Department of Justice, 2018).

Technical, Social, and Political recommendations

Technically speaking there were implementations that would have mitigated the 2017 NHS attack. Because the SMB was known to be vulnerable to EternalBlue exploitation, The Cyber-Security team should have considered the following actions to prevent or mitigate the attack:

- Conducting relevant risk assessment on the network
- Patching and updating the operating systems
- Monitoring the communication sent to SMB
- Constantly analysing and evaluating Network vulnerabilities
- Providing employees with adequate cyber-security training
- Having define both redundancy and contingency plan

The risk assessment is used to identify, prioritize, and target potential vulnerabilities on the system, whereas the Cyber security management should have taken the actions suggested by Microsoft as preventative measures against the worm that was known to target Unpatched Microsoft windows operating systems (Microsoft, 2017). Additionally, they could have embraced effective software products for analysing and monitoring network activities, also beneficial would have been to have a method in place to log SMB activities capable of generating warnings under specific suspicious activities (British Telecommunications, 2010). Last but not least, the lack of policy that defines certain behaviours and best practices to adopt during a cyber-attack could have had a positive impact on containing the malicious nature of the WannaCry crypto worm, e.g., the staff could have unplugged certain devices from the N3 network or the source power during the attack (CISA, 2018). The NHS governance should have predicted or mitigate the disruption of the service and the avoided the disbursement of money spent to recover from the attack by observing common cyber security practices (Hern, 2017). Common security practice refers to updating the system in a regular base, Analysing, and maintaining network security, reviewing, and enforcing training for the employees (How to Protect Your Networks from Ransomware: Technical Guidance Document, 2016). Considering that the NHS provides health services that are in part delivered using computer systems linked to a greater network of database and information related to important and confidential information about people health, the system should have been reviewed and secured periodically ensuring the Confidentiality, Integrity, and the availability of the information (CISA, 2018). Moreover, patients who are in hospital should be able to access data even if the system is under attack, with an appropriate redundancy plan that defines the use of multiple servers to both mitigate the disruption of the service and to protect the information on the server (How to Protect Your Networks from Ransomware: Technical Guidance Document, 2016).

Lesson Learned

Now days, many services are dependent on information technology as many activities are driven by computers systems that can handle data in a way that is convenient to use them over conventional methods. Reason why, the security of IT systems plays a crucial rule among the majority of organizations (Tansey et al., 2010, pp. 29–33). Particularly, when the service provided is an essential service like the NHS is a good practice to invest in preventative measurement. The 2017 NHS attack put the attention on how vulnerable the system could be and how the human factor can determinate the failure of an essential service. The cooperation between the NHS facilities was remarkable as they managed to keep the operation going resulting in zero cases of death linked to WannaCry. However, the NHS case outlined how vulnerable can be the system without appropriate policy and best practices that can prevent or mitigate a cyber-attack(Smart, 2018). In fact, The NHS made the poor decision to keep the system unpatched even if the risk was noted the year before even if the cost to updating the system would have been less than the cost of recovering from the attack (Hern, 2017). In saying that would have been more convenient investing on cyber-security rather than paying the consequences of a cyber-attack (*The NHS Cyber Attack*, 2020). In my opinion this concept can

be apply to many organizations that would rather invest money to prevent and mitigate malicious activity rather than facing the consequences of an incident like the 2017 NHS WannaCry.

References:

1. Akbanov, M., Vassilakis, V., & Logothetis, M. (2019). *WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms* (pp. 113–118). Journal of Telecommunication and Information Technology. https://www.il-pib.pl/czasopisma/JTIT/2019/1/113.pdf
2. BBC. (2017, October 27). NHS "could have prevented" WannaCry ransomware attack. *BBC News*. https://www.bbc.com/news/technology-41753022
3. British Telecommunications. (2010). *N3 Network User Guide | Manualzz*. Manualzz.com. https://manualzz.com/doc/4167334/n3-network-user-guide
4. CISA. (2018). *WHAT IS WANNACRY/WANACRYPT0R?* CISA. https://www.cisa.gov/uscert/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_WannaCry_Ransomware_S508C.pdf
5. *Cyber-attack sparks bitter political row over NHS spending*. (2017, May 14). The Guardian. https://www.theguardian.com/technology/2017/may/13/cyber-attack-on-nhs-sparks-bitter-election-battle?CMP=gu_com
6. Hern, A. (2017, October 26). *NHS could have avoided WannaCry hack with "basic IT security", says report*. The Guardian; The Guardian. https://www.theguardian.com/technology/2017/oct/27/nhs-could-have-avoided-wannacry-hack-basic-it-security-national-audit-office
7. *How to Protect Your Networks from Ransomware: Technical Guidance Document*. (2016). https://www.justice.gov/criminal-ccips/file/872771/download
8. Microsoft. (2017, October 11). *Microsoft Security Bulletin MS17-010 - Critical*. Microsoft.com. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010
9. National Audit Office. (2017, October 27). *Investigation: WannaCry cyber attack and the NHS - National Audit Office (NAO) Report*. National Audit Office. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/
10. *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. (2018, September 6). Justice.gov. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
11. Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack* (pp. 1–42).
12. Tansey, S. D., Wateridge, J., & Darnton, G. (2010). *Business, information technology and society* (pp. 29–33). Routledge, Taylor & Francis Group, Dr.
13. *The NHS cyber attack*. (2020, February 7). Acronis; Acronis. https://www.acronis.com/en-sg/blog/posts/nhs-cyber-attack/
14. *What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant?* (n.d.). What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? Retrieved August 19, 2022, from https://www.avast.com/c-eternalblue#:~:text=The%20NSA%20allegedly%20spent%20almost