CSL3207 Assignment 1 - The UK NHS WannaCry Incident

Semester 2 2022

Glen Teakle 10532981

Contents

[Introduction 2](#_Toc112137439)

[Impact on the NHS 2](#_Toc112137440)

[The Importance of Network Security 3](#_Toc112137441)

[The Vulnerability and Exploit 3](#_Toc112137442)

[Aftermath 4](#_Toc112137443)

[Mitigation strategies and Recommendations 4](#_Toc112137444)

[References 5](#_Toc112137445)

# Introduction

On Friday 12 May 2017 a cyber attack was launched using ransomware called WannaCry. The attack lasted until Friday 19 May 2017 and affected numerous systems across many countries. Within a day of the attack there were reports from Europal that more than 230, 000 computers in at least 150 countries had been affected (Smart, 2018).

One of the largest organisations most crippled by the attack was the UK National Health Service (NHS). Thousands of devices and computers throughout the NHS were locked and all files were encrypted making them inaccessible. Along with computers, WannaCry effected large numbers of medical equipment including radiology, X-ray machines and pathology devices (National Audit Office [NAO], 2018).

A large payment in Bitcoin was demanded to decrypt all files and unlock the systems (NAO, 2018). None of the affected organisations paid the ransom, and ultimately the WannaCry ransomware was stopped in its tracks by a cyber security researcher who discovered and then activated a “kill-switch”. This prevented any further damage almost instantly (Rhysider, 2020).

# Impact on the NHS

* Patient files (including emergency patients) and records became locked and inaccessible.
* Medical diagnostic equipment was disconnected.
* NHS unable to take on new patients
* Access to test results blocked
* Ambulances diverted.

The NHS initially identified 45 NHS organisations that were infected by WannaCry. Over the next few days, this number increased to a total at least 80 infected organisations across England. Out of this 80;

* 34 were locked out of their devices.
* 46 were not infected but reported disturbance. Using initiative, they shut down things like email as a precaution and had to resort to using pen and paper.
* 603 other NHS organisations, including primary care, were also infected by WannaCry, including 595 GP practices.
* 6912 appointments and operations had to be cancelled, and patients were diverted into other areas and had to travel further to accident and emergency departments.
* There were trusts that were disrupted but not infected. This was due to them sharing data and/or systems that *were* infected and had been shut down (NAO, 2018).

# The Importance of Network Security

This incident highlights the importance of a sound cyber security plan and strategy to be in place, along with contingency and disaster recovery planning. As reported by the NAO (2018), the Department of Health had developed a response plan for cyber attacks, but it had not been tested. In 2014 there were letters written by the Department Of Health to various trusts informing them of the necessity to upgrade from the older operating systems currently in use, namely Windows XP. Their suggestion was to have this completed by April 2015. Further to this in March/April 2017, NHS Digital sent out critical alerts warning organisations to patch their systems to prevent cyber attacks (NAO, 2018).

# The Vulnerability and Exploit

Most of the computers/devices that were affected at the NHS were running under Windows 7, which at the time was still under support by Microsoft. However, there is a vulnerability in the Windows file sharing communication protocol Server Message Block (SMB) that was exploited. The SMB file sharing protocol allowed the ransomware to spread automatically (NAO, 2018). The vulnerability was discovered by the U.S National Security Agency, who rather than report it to Microsoft, created code to exploit it. The code was named EternalBlue (Acronis, 2020 & Fruhlinger, 2018). EternalBlue was later stolen by a hacking group called the Shadow Brokers who published it on a website on April 8 2017 (Acronis, 2020 & Fruhlinger, 2018). Microsoft had actually discovered this vulnerability around a month prior to the WannaCry attack, and subsequently released a patch, but none of the NHS systems were updated with it (Avast, n.d; Fruhlinger, 2018; Rhysider, 2020 & Smart, 2018). NHS Digital had also advised that this patch was available on 25 April 2017 (Smart, 2018). Another step that could have been taken concerned increasing the security of the network facing firewalls in the NHS. According to NHS Digital, this would have helped guard against the infection (Smart, 2018).

The suspected threat actor for the WannaCry attack is the Lazarus Group of North Korea (Acronis, 2020). Symantec have partially linked the attack to them via tools used by Lazarus, along with shared code between Lazarus and the WannaCry ransomware (Symantec Security Response, 2017).

# Aftermath

Cancelled appointments, cost of IT support and consultants, the restoration of data and systems plus overtime worked by NHS staff are some of the costs that were incurred after the attack. The full cost of damage and to what extent however, is not known (NAO, 2018).

# Mitigation strategies and Recommendations

The most obvious mitigation strategy would be to make sure security patches are installed through automatic updates, or at the very least on a regular basis by the I.T department. Automatic patching ensures peace of mind, especially to non-technical staff who would not have to remember to do anything to their computer. The risks associated with using older, outdated operating systems should be a continued part of employee training and education.

However, this mitigation strategy being used on older operating systems such as Windows 7 and XP would not be as ideal as replacing them with newer, more supported systems such as Windows 10 or 11. Older operating systems have numerous previously discovered vulnerabilities that can be exploited easily such as EternalBlue. It would be unfeasible to think that all vulnerabilities on older systems would be and could be patched. It is more likely that through newer OS’s having more support and patching that less exploits would occur.

# References

Acronis. (2020). *The NHS cyber attack*. <https://www.acronis.com/en-sg/blog/posts/nhs-cyber-attack/>

Avast. (n.d.). *What Is EternalBlue and why Is the MS17-010 Exploit still relevant?* <https://www.avast.com/c-eternalblue>

Fruhlinger, J. (2018). *What is WannaCry Ransomware, how does it infect, and who was responsible?* <https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html>

Office, N. A. (2018). *Investigation: WannaCry cyber attack and the NHS* <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>

Response, S. S. (2017). *What you need to know about the WannaCry Ransomware.* <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack>

Rhysider, J. (2020). Darknet Diaries EP 73: *Wannacry*. <https://darknetdiaries.com/transcript/73/>

Smart, W. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack.* <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>