Topic: Firewall and Network Security

RQ: How could improved firewall and antivirus strategies have mitigated the impact of the WannaCry ransomware attack on NHS's Windows-based systems in 2017?

Computer Science HL

Word Count: 3998

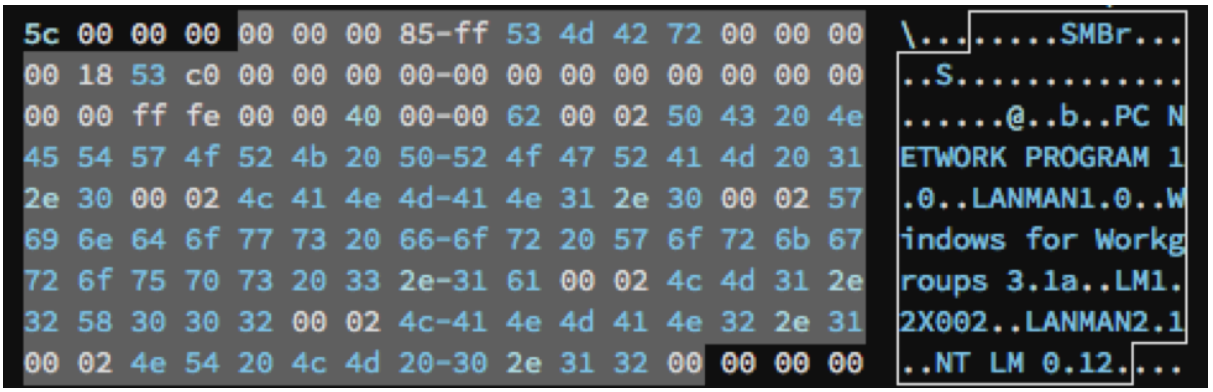
Table of Contents

1. Introduction

The 2017 WannaCry ransomware attack was one of the most significant cybersecurity incidents in recent history, with far-reaching consequences that showed the vulnerabilities in modern digital infrastructure. This attack devastated the UK's National Health Service (NHS), where outdated and unpatched Windows-based systems were exploited, leading to widespread operational disruptions. Over 230,000 computers in 150+ countries were affected, but the NHS suffered significantly due to its essential services, experiencing cancelled appointments, delayed treatments, and service breakdowns due to weak cybersecurity. The attack exploited a vulnerability in the SMB (Server Message Block) protocol via the EternalBlue exploit, leaked by the hacker group Shadow Brokers after it was stolen from the NSA. Despite Microsoft having released a patch for this vulnerability months before the attack, many NHS systems still needed to be updated, mainly due to the reliance on older, unsupported versions of Windows. This situation questions the adequacy of the cybersecurity measures at the time, specifically in regard to the deployment and management of firewalls and antivirus solutions, which are foundational components of security infrastructure. This essay explores **how improved firewall and antivirus strategies could have mitigated the impact of the WannaCry ransomware attack on the NHS's Windows-based systems**. If properly configured, firewalls could have played a critical role in blocking the malicious traffic that allowed WannaCry to spread rapidly across networks. Additionally, up-to-date antivirus software could have detected and neutralised the ransomware before it encrypted critical files. The lessons learned from WannaCry are pertinent to understanding the need for continuous improvements in cybersecurity practices, particularly in sectors where the cost of failure can be measured in human lives. This

study will also be connected to the United Nations Sustainable Development Goals (SDG), particularly Goal 9, which emphasises the necessity of building resilient infrastructure.

2.Technical Analysis of WannaCry's Propagation



(Figure 1.) A Hex Dump of the SMB Packet Sent to Exploit the PC (LogRhythm)

WannaCry exploited a bug in the SMB v1 Protocol, used by Windows for file-sharing. During its 7-hour attack from May 12, 2017, 7:44 - 15:03 UTC, it infected over 300,000 computers at 750 infections per minute, a rate contributing to its success. Figure 1 is a sample of the SMB v1 packet sent from an infected computer to other devices on the network, which is how the ransomware was propagated.

EternalBlue

The NSA discovered this bug and created its own exploit titled "EternalBlue", which used the bug to detect other vulnerable devices on the network. It would then connect to those, meaning only one computer had to get infected for the rest of the network to also be at risk without the other computers needing to do anything. A hacker group titled "Shadow Brokers" were the original group that claimed they hacked the "Equation Group", known to be a sub-division of the NSA, and attempted to auction off a large lot of zero-day exploits and other malware that the NSA developed. On April 14, 2017, The

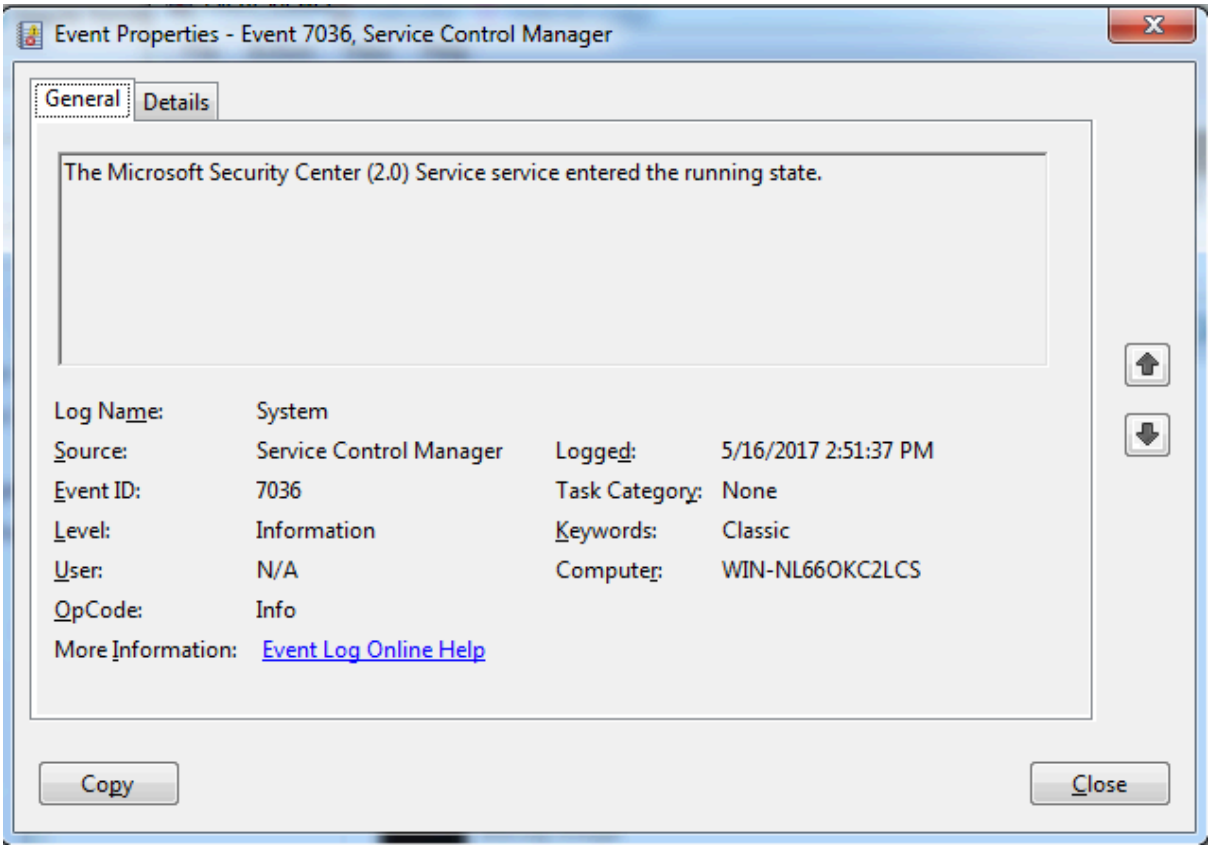
Shadow Brokers released, amongst other things, the tools and exploits codenamed: “DANDERSPRITZ”, “ODDJOB”, “FUZZBUNCH”, “DARKPULSAR”, “ETERNALSYNERGY”, “ETERNALROMANCE”, “EXPLODINGCAN”, “EWOKFRENZY”, “ETERNALBLUE”, and “DOUBLEPULSAR”, for the public after a failed auction in which they attempted to sell it on the darknet.

DoublePulsar/DarkPulsar

Two of these tools were used and combined to construct and propagate the WannaCry virus, EternalBlue and DoublePulsar/DarkPulsar. EternalBlue was used to exploit the network and enabled WannaCry to spread so quickly through the network to all vulnerable devices. DoublePulsar was used as a backdoor, which enabled WannaCry to gain full control over the infected devices. On Tuesday, 14 March 2017, Microsoft issued a security bulletin MS17-010 to all devices still being supported, which was an entire month before the exploits were leaked. This played a huge role in lowering the infection rate because all newer Windows versions that were still supported and updated before May 12, 2017, weren't vulnerable to the WannaCry virus. DoublePulsar allowed WannaCry to spread through the network, bypassing firewalls and other defenses to control compromised machines. WannaCry then scans through the network in search of the other vulnerable machines and uses DoublePulsar to install itself on those machines without requiring additional interaction from users or administrators making it autonomous.

Propagation through the NHS

The ransomware spread autonomously through the NHS's network, creating a cascading effect that shut down offices and vital machines. The NHS hasn't updated their operating systems on their newer machines and is using many machines that are too old to receive firmware or software updates, leading to them being known as "dead" machines and making them susceptible to the WannaCry ransomware. Better patch management and updated security protocols could have closed the vulnerabilities that DoublePulsar exploited. Additionally, stricter internal firewalls and network segmentation could have slowed or prevented the spread by preventing the infected machines from communicating freely with the rest of the NHS's internal network. The major problem was the NHS's reliance on outdated and unsupported versions of Windows, such as Windows XP and Windows 7, which were used on over 40% of their machines. This was a significant issue as the legacy systems were used in the NHS's network for critical medical and administrative functions.



(Figure 2.) System Event Log of Wannacry starting the Program “The Microsoft Security Center 2.0”

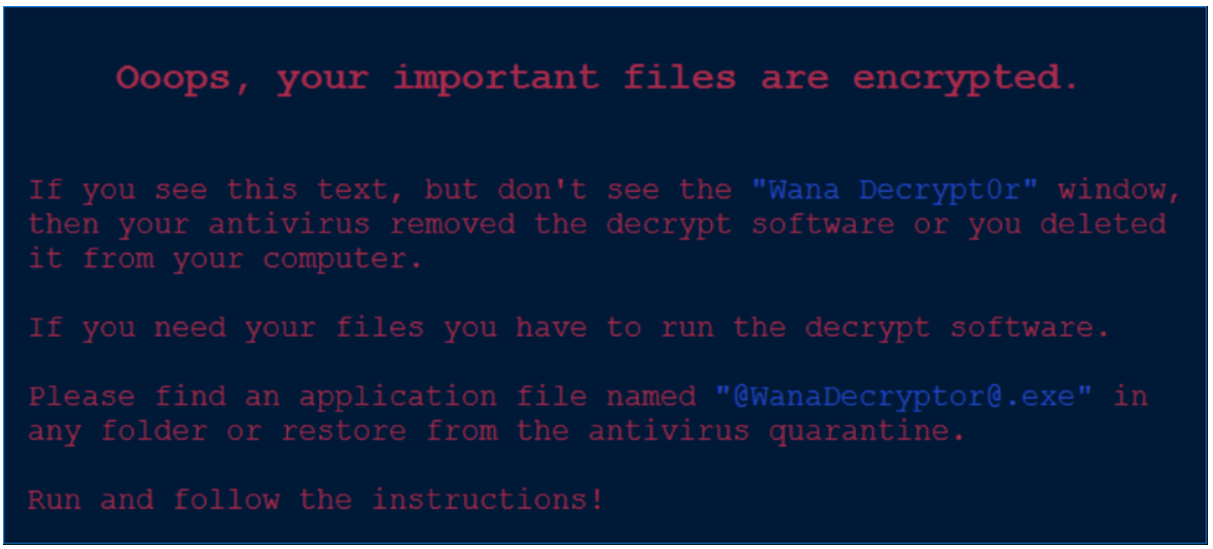
```
push    offset aGlobalMswinzon ; "Global\\MsWinZonesCacheCounterMutexA"
lea     eax, [ebp+Dest]
push    offset aSD      ; The sprintf format "%s%d" appends a "0" to the end of the mutex name
push    eax             ; Dest
call    ds:sprintf      ; Global\\MsWinZonesCacheCounterMutexA0
xor     esi, esi
add     esp, 10h
cmp     [ebp+arg_0], esi
jle     short loc_401F4C

                        ; CODE XREF: check_mutex+4B↓j
lea     eax, [ebp+Dest]
push    eax             ; lpName
push    1               ; bInheritHandle
push    100000h         ; dwDesiredAccess
call    ds:OpenMutexA   ; Check for existence of mutex
test    eax, eax
jnz     short loc_401F51 ; If this mutex exists, the malware exits
push    1000            ; dwMilliseconds
call    ds:Sleep
inc     esi             ; Increment the counter
cmp     esi, [ebp+arg_0] ; Compares the incrementer to the value 60, effectively
                        ; performing this mutex check each second for one minute
jl      short loc_401F26
```

(Figure 3.) Encrypter Checks to See if the Mutex “MsWinZonesCacheCounterMutexA0” Exists

```
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset CommandLine ; "attrib +h ."
call    sub_401064
push    ebx             ; lpExitCode
push    ebx             ; dwMilliseconds
push    offset aIcacls_GrantEv ; "icacls . /grant Everyone:F /T /C /Q"
call    sub_401064
add     esp, 20h
```

(Figure 4.) Execution of “attrib +h .” Followed by “icacls_GrantEv” to Hide the Downloaded Files and then Grant Full Permissions to Itself

(Figure 5.) The Wana Decrypt0r 2.0 Application used to Alert the Victim and Give the Instructions for the Ransomware



(Figure 6.) The Changed Background of Devices Affected

What happened once a device was infected?

Once the ransomware infected a device, it executed the "dropper" which attempted to make a connection to the domain "http://www[.]iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com" and stops the attack if the connection is successful. The domain was previously unregistered, causing the query to fail and meant that it would continue. The developers put this in place as a "Kill Switch". However, on May 12, a security researcher named "MalwareTech" inspected a sample of WannaCry and saw it constantly query the unregistered domain. He registered it and, in turn, activated the killswitch, stopping all new infections from happening and halting the spread of the world's largest ransomware. If the connection was unsuccessful, the "dropper" attempts to create a service named "mssecsvc2.0" with the display name "Microsoft Security Center (2.0) Service". This can be seen in the System event log as event ID 7036 in Figure 2. The dropper would then extract the encrypter's binary code from its resource R/1831, and write it to the hardcoded

filename “%WinDir%\tasksche.exe”, then execute it. Once executed, the encrypter checks to see if the mutex “MsWinZonesCacheCounterMutexA0” exists, and if present, it would not proceed with the infection if it is present. This can be seen in the ransomware code in Figure 3. The encrypter binary also contains a password-protected zip file containing a directory names “msg” containing Rich Text Format (RTF) files with the extension “.wnry”. These files are the equivalent of a readme file and is used by the decrypter program named “@WanaDecryptor@.exe” and contains instructions in a text format for the user to know that their files are encrypted and instructions on how to get the decrypted and how to transfer the bitcoin (BTC) to the perpetrators. Additionally there was the file “b.wnry”, a bitmap file which also contains instructions for the decryption of the files, “c.wnry”, which contained five links to the darknet with “.onion” extensions and a zip download file for the tor browser, the browser used to open “.onion” links and access the dark net. “r.wnry”, which contained additional decryption instructions in English, “s.wnry”, a zip file with the Tor software already installed, t.wnry, which is an encrypted file using the “WANACRY!” encryption format, where “WANACRY!” is the file header, “taskdl.exe”, a file deletion tool, “taskse.exe”, which enumerated Remote Desktop (RDP) sessions on the machine and executed the ransomware on each session and “u.wnrx” which contained the “@WanaDecryptor@.exe” decrypting software. After downloading all the files to the working directory, it attempts to hide the files and grants full administrator access to all files in the directory and any directories below it. It does that by executing the commands ““attrib +h .”, followed by “icacls . /grant Everyone:F /T /C /Q” which you can see in the ransomware’s code in Figure 4. Following this, WannaCry encrypts all files on the system searching for a range of standart extensions, encrypting the files using the WANNACRY! Encryption method and

renaming the file extensions to ".wnry". After the encryption was successful, it launches the "Wana Decrypt0r 2.0" program, which you can see in Figure 5, which shows the instruction files in different language options, 2 countdown timers labeled "Payment will be raised on" and "Your files will be lost on", aswell as the instructions to send 600$ worth of bitcoin to one of 3 addresses which were also hardcoded into the binary. The ransomware also changes the users background to the bitmap image contained in the file "b.wnry" which can be seen in Figure 6. This was used as a "backup" incase the WannCry decryptor software didn't automatically launch. If the ransom was not paid before the first timer ends, the ransom price would have doubled and after the second timer expires, the malware "readme" states that the files would be unrecoverable. Once the files were encrypted by the ransomware, it would have been realistically impossible to decrypt it without the decryption key as it would take over 600,000,000 years to crack/brute force the decryption key. This is because the ransomware utilised the Microsoft Enhanced RSA and AES Cryptographic Provider libraries to encrypt the files. After the files are encrypted, the decrypter program attempts to delete any Windows Shadow Copies via the hardcoded command: "cmd.exe /c vssadmin delete shadows /all /quiet & wmic shadowcopy delete & bcdedit /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog –quiet"

Role of Firewalls in Mitigating WannaCry

Firewalls in Cybersecurity

Firewalls, as hardware or software, control network traffic by examining data packets against predefined security rules. Firewalls act as a barrier between an internal and an external network. It creates a protective layer that shields the system from external threats such as hackers, viruses, malware, DDoS attacks and more. By controlling and filtering the traffic, the firewalls help ensure only authorized users and data can access a network. They can be used by cybersecurity specialists to block specific types of traffit such as those using certain ports or protocols known to be vulnerable such as SMB traffic on port 445 which was exploited by WannaCry. This could have mitigated the attack.

Types of Firewalls

Network firewalls are hardware or software devices that were installed and the boundary of an organizations network to inspect the traffic that enters or exits the entire network. They usually filter traffic based on predefined rules such as IP, ports, or protocols. Host based firewalls are software programs installed on individual devices or servers to control the incoming and outgoing traffic of that specific device. Host-Based firewalls provice a more granular level of control, protecting the device even when its outside the main network. Modern firewalls also include features such as deep packet inspection (DPI) which lets them examine the contents of the data packets for malicious payloads aswell as intrusion detection and prevention systems (IDPS) which can alert or block suspicious activity in real-time.

Importance of Firewalls in Network Security

Firewalls control traffic to prevent unauthorized access, malware, and network-based attacks, like DoS and port scanning. Firewalls are effective in controlling access to vulnerable systems and blocking exploits targeting specific protocols such as the SMB protocol that WannaCry used to spread. In WannaCry's context, firewalls could have been configured to block incoming and outgoing traffic over port 445, which the malware used to spread via the SMB protocol. This would have significantly reduced the ransomwares ability to propagate across the NHS's network. With proactive firewall monitoring by the network administrators, they can identify potential threats early, giving network administrators the ability to respond quickly to prevent the spread of the malicious software. Monitoring for abnormal SMB traffic could have alerted NHS Digitals network administrators of the presence of WannaCry, allowing for a quicker response and neutralization.

How Firewalls Could Have Mitigated WannaCry

Blocking Malicious Traffic

The WannaCry ransomware primarily propagated throught the exploitation of the SMB protocol's vulnerability in which its meant to be used for sharing files and printers across the network but the EternalBlue exploit took advantage of a flaw in the protocol. Properly configured firewalls could have blocked all incoming and outgoing SMB traffic, specifically traffic on port 445 from external sources or across internal network

segments. This would have prevented WannaCry from exploiting this vulnerability and spreading to the other machines on the network. By blocking SMB traffic at the firewall level, the NHS could have limited of entirely prevented the ransomware from moving laterally across the network, isolating any infected machines and containing the attack. In a network like the NHS, firewall rules at multiple layers could have helped limit the attack.

Examples of how firewalls succesfully protected companies

Telefonica, a telecommunications company in Spain, was one of the first high-profile victims of the WannaCry ransomware, However, the spread of the attack was largely contained within their internal network. Telefonica's firewall configurations blocked SMB traffic from the internet, containing the ransomware to internal systems.
Another good example of the succesfull use of firewalls is in the case of Renault-Nissan automotive group when they experienced disruptions due to WannaCry, especially in its production facilities. However, they were able to minimize the impact by having their firewalls configured to limit internal network traffic, which helped contain the ransomware and prevent it from spreading. By segmenting their network, they ensured that infected systems couldnt spread.

Network Segmentation

Network segmentation refers to the practice of dividing a larger network into smaller, isolated segments, each of which operates independently and has its own security controls. This prevents the attack from spreading so when one segment is compromised,

the damage is limited to that segent leaving the other parts of the network unaffected. If the NHS had employed network segmentation, the spread of WannaCry across its systems could have been significantly reduced. In a segmented network, critical systems such as medical equipment, admin computers and patient records would completly be seperate. WannaCry quickly spread laterally between devices on the same network which network segmentation would have limited.

Advanced Firewall Features

Deep Packet Inspection (DPI) is an advanced firewall feature which allows for the inspection of the actual contents of data packets beyond just the header information. DPI features can detect the malicious content or patterns in the data being transmitted may be associated with malware such as ransomware. If DPI was emplosed, it could have examined the SMB traffic the WannaCry used and would have been able to identify and block it. Intrusion Detection and Intrusion Prevention Systems (IDPS) are commonly integrated and monitor and prevent suspicous traffic.

Because the EternalBlue exploit used by WannaCry was already known at the time of the attack, an IPS equipped firewall could have detected the ransomware exploiting the SMB vulnerability and automatically have blocked it. A layer 7 firewall could have also been employed to inspect the network traffic based on more than just IP and ports and would have also detected specific requests and responses made by applications which could have allowed the firewall to detect abnormal requests associated with the EternalBlue exploit and block the traffic without affecting legitimate SMB communication.

How Antivirus Software can Mitigate WannaCry

Whats an Antivirus

An antivirus is software developed for the cybersecurity market. Its primary function is detecting, preventing, and removing malware, including ransomware like WannaCry. Antiviruses typically have 2 detection methods for malware and viruses:
Signature-Based and Behavior-Based Detection.

Signature-Based Detection

Signature based detection is the traditional method used by antivirus software, inwhich the program scans files and compares them to a database of known malware signatures. These are a large database of already detected malware which helps the antivirus recognize sequences or code patterns that are associated with known malicious programs. When the software detects a file that matches a known virus, it flags it as a threat and either quarantines or removes it from the system. This is a highly effective method for recognising malware as long as the antivirus database is up-to-date. If the NHS would have had the latest updated version of their antivirus software, it could have potentially recognised WannaCry's signature early in the attack preventing it from spreading.

Behavior-Based Detection (Heuristics/BBD)

Behavior-based detection, also known as heuristic analysis, is an advanced method used by antivirus software to identify new or unknown malware based on how it behaves rather than matching specific signatures. This method monitors applications in real time, flagging suspicious activities like file encryption or abnormal traffic and taking preventive measures if detected. Therefore, when WannaCry attempts to encrypt files or exploit the SMB vulnerability, BBD detects it, allowing NHS Digital's team to intervene before it spreads.

Challenges of Antivirus Software

Zero-day exploits, or unknown security flaws, are a significant threat since attackers exploit them before antivirus vendors create detection signatures. While WannaCry exploited a known vulnerability in the SMB protocol, future ransomware attacks may take advantage of zero-day vulnerabilities that antivirus programs relying on signature-based detection couldn't recognise. If WannaCry had been a zero-day exploit, the results of the attack on the NHS and the rest of the world would have been more drastic and extreme as it would have bypassed traditional antivirus defences, leaving them vulnerable to it even if their antivirus software was up-to-date.

Organisational and Human Factors

The Importance of Strong IT Governance

It governance refers to the structures, policies, and processes that ensure that an organisation's IT resources are effectively managed and aligned with the organisational goals. In the context of cybersecurity, strong IT governance is applied, risks are assessed, and there are clear protocols for handling threats. IT governance involves clear accountability for cybersecurity, including patch management, updates, and deploying advanced firewalls and antivirus tools. In large organisations like the NHS, with decentralised structures, IT governance becomes even more critical as it ensures that all departments or trusts within the organisation follow uniform cyber security protocols.

NHS's IT Governance Challenges

IT Governance prior to the WannaCry attack has several weaknesses. Many NHS trusts were using outdated systems and lacked a unified approach to cybersecurity, making the network more vulnerable. Patching and updating these existing systems were often delayed due to resource constraints, fragmented management, and competing priorities within individual departments and trusts. There was very little oversight and coordination across NHS trusts, meaning some departments where better protected than others. Without centralised control or standardised cybersecurity policies across the organisation, certain areas of their network became weak points that WannaCry was able to exploit. The lack of centralised IT governance within the NHS significantly contributed to the scale of the WannaCry attack. A stronger governance framework

would have mandated that all NHS trusts apply critical security patches when they were released, especially for known vulnerabilities like the one WannaCry exploited. Instead, the fragmented governance structure allowed vulnerable systems to persist, which enabled the ransomware to spread rapidly across NHS networks.

NHS Staff and Cybersecurity Awareness

Human Behavior in Cybersecurity

Human behaviour is a critical factor in maintaining cybersecurity within the network and organisation, as many cybersecurity exploit human error, also known as “social engineering” rather than technical vulnerabilities. Even robust defences can fail if staff aren’t trained to recognise common cybersecurity threats. In large organisations like the NHS, where thousands of employees interact with IT systems daily, cybersecurity awareness among staff is essential. Without proper training, employees may unknowingly become entry points for malicious software.

Why the NHS couldn’t implement neccesasary security features to protect its network.

This decision was often due to budgetary constraints as it is a publicly funded system and the complexity of upgrading hospital IT infrastructure. Many compatibility issues with medical devices and software also depended on older operating systems. The NHS also struggled to prioritise their investments into their IT infrastructure because they

focused their resources on direct patient care and medical equipment, which led to it overlooking the need for continual upgrades in cybersecurity infrastructure. Due to logistical issues, the NHS didn't upgrade to Microsoft's patch, which would have rendered EternalBlue useless on its machines. Applying updates can be very complex in a healthcare environment like the NHS. It often requires coordination across multiple departments and running through multiple testing stages to ensure everything works, which may interrupt critical services. The failure to apply these patches in a timely manner is what left the NHS's systems so vulnerable. The use of the outdated systems not only created vulnerabilities to ransomware but also hindered them from implementing modern cybersecurity solutions, which could have detected the encryption of files and blocked it immediately, aswell as having multi-layered firewalls and intrusion detection. The NHS had disruptions in over 80 NHS trusts, representing almost a third of the NHS in England. Additionally, 603 primary care and other NHS organisations, including walk-in centres and GP surgeries, were affected by the attack. It was estimated that at least 19,000 appointments were cancelled, including surgeries and diagnostic procedures, aswell as an alert telling people not to come to the hospital unless there is a life-threatening issue. Over ten hospitals had to divert ambulances and shut down ER rooms as they couldn't access patient records or run essential equipment. CT Scanners, MRI machines and other equipment were rendered inoperable due to their integration with the infected Windows-based machines. This directly impacted the ability to conduct medical scans and diagnostics, further delaying patient care. Certain hospitals also reverted to using paper-based systems because they couldn't access their digital records, drastically slowing down the process and increasing the risk of medical errors due to the lack of real-time patient information. The National Audit Office (NAO)

stated that the attack demonstrated the NHS's widespread vulnerability to cyber threats and that NHS Digital had issued a warning about the vulnerability before the attack started. Still, many trusts and hospitals hadn't acted on these warnings due to the resource limitations and operational risks with taking their systems offline for the update. The NAO report also pointed out that the NHS organisation lacked proper business continuity plans that would allow them to maintain their services in the case of a cyberattack. Barts Health NHS Trust, one of the largest healthcare providers in the UK was one of the branches severely affected by WannaCry. Barts had to shut down several systems, including diagnostics and medical imaging tools, and switch to manual processes, which delayed their services. Another example is the Royal London Hospital, where some departments were forced to cancel appointments and elective surgeries as the hospital's systems couldn't function properly for several days, severely disrupting patient care. Following the attack, NHS England reviewed its cybersecurity measures comprehensively. The review emphasised the need for improved cybersecurity and patch management aswell as better coordination of its security across trusts and investment in upgrading their legacy systems and medical tools/software. NHS Digital was tasked with ensuring that future vulnerabilities would be addressed more swiftly and that critical updates which had a major impact on the organisation would be applied uniformly across all NHS organisations and branches. The NHS also implemented stricter protocols for the incident response and recovery including better network segmentation and stronger backup solutions to ensure that medical data could be restored much faster in the case of another attack. The NHS's struggle to implement the necessary features such as intensive firewalls and updated anti virus software was a driving factor in the extreme infection of their network.

Works Cited

BBC News. “Massive Ransomware Infection Hits Computers in 99 Countries.” BBC News, 13 May 2017, www.bbc.com/news/technology-39901382.

County Durham and Darlington NHS Foundation Trust (CDDFT). NHS England » NHS England business continuity management toolkit case study: WannaCry attack. 21 Apr. 2023, www.england.nhs.uk/long-read/case-study-wannacry-attack.

Inagaki, Kana. “Honda Plant Hit by WannaCry Ransomware Attack.” Financial Times, 21 June 2021, www.ft.com/content/a0f5d047-2e20-3db9-b258-565d3be17bba.

LogRythm. “A Technical Analysis of WannaCry Ransomware.” LogRythm, 15 May 2017, logrhythm.com/blog/wannacry-ransomware.

ManageEngine, communications@manageengine.com. How to disable SMB v1 (Server Message Block). www.manageengine.com/vulnerability-management/misconfiguration/legacy-protocols/how-to-disable-smb-v1.html#:~:text=Server%20Message%20Block%20(SMB)%20is,to%20a%20number%20of%20attacks.

Miridakis, Vicky. “WannaCry: Die Technische Analyse - Onlineportal Von IT Management.” Onlineportal Von IT Management, 19 May 2017, www.it-daily.net/it-sicherheit/cybercrime/wannacry-die-technische-analyse.

NAO [Comptroller and Auditor General]. “Investigation: WannaCry Cyber Attack and the NHS.” NAO, HC 414, NAO, 25 Apr. 2018, www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

“Ransomware WannaCry: All You Need to Know.” , 8 June 2020, www.kaspersky.com/resource-center/threats/ransomware-wannacry.

"WannaCry Cyber Attack Highlights Dilemma in Fight Against Malware." Financial Times, www.ft.com/content/bf29e8e0-3985-11e7-821a-6027b8a20f23.