Digital Security Case Project: NotPetya

Viyanka Moodley (300565283)

6 June 2024, 23:59

Statement on use of generative AI:

I acknowledge the use of *ChatGPT, Gemini and ChatPDF* in this report, to help my understand elements of the case, improve my academic writing and enhance the quality of my own ideas.

Table of Contents

Summary

The NotPetya cyberattack began when the Russian military group, *Sandworm,* hacked into the update servers of *Linkos Group*, a Ukrainian software company that developed the M.E.Doc accounting software. M.E.Doc was widely used for tax filing and business operations in Ukraine. After compromising the M.E.Doc update servers, Sandworm embedded the ***NotPetya*** malware into a software update, which was then distributed to all users of M.E.Doc.

The malware initially spread through a single infected computer at a Maersk office in Odessa. Once installed, NotPetya exploited network vulnerabilities to move laterally across systems. This rapid spread was amplified by Maersk's outdated systems and poor network segmentation. Leveraging EternalBlue for remote code execution on unpatched Windows systems and Mimikatz for password extraction from memory, NotPetya quickly moved through Maersk's network, compromising even patched systems.

The consequences for Maersk were severe. The spread of the malware disabled their global network, including 4,000 servers and 45,000 PCs, effectively making the bulk of their computers, servers, and communication systems inoperable. This led to a complete shutdown of their shipping infrastructure which halted their operations worldwide. Maersk’s inability to manage ports, ships, and cargo logistics resulted in significant disruptions, with 17 out of their 76 freight terminals being affected. Ports in major cities were reduced to standstill, unable to process freight, take new orders, or manage the contents of containers.

The NotPetya attack highlighted the interconnectedness and vulnerability of global infrastructure to cyber threats. It was a wakeup call on the far-reaching and devastating impacts a cyberattack can have on critical infrastructure and global commerce, emphasising the necessity for robust cybersecurity measures to prevent such widespread disruptions and financial losses.

Attack Analysis

Managerial Layer(People Related):

1. ***Lack of prioritisation of cybersecurity:*** Despite warnings from IT executives about the need for a security redesign of Maersk's global network, the initiative was not considered a key performance indicator for senior IT overseers. This lack of emphasis on cybersecurity at the managerial level led to delays in implementing security measures.
2. ***Inadequate Security Policies:*** Maersk's managerial layer seems to have lacked robust cybersecurity policies and procedures, including regular cybersecurity audits and comprehensive incident response/disaster recovery plans. This hindered the organisation's ability to detect and contain the attack.

Operational (Process-related)

1. *Insufficient Patch Management Process*: The failure to implement a rigorous patch management process left Maersk's systems vulnerable to known exploits like EternalBlue.
2. ***Inadequate backup strategy:*** While Maersk had backups for individual servers, the oversight in not having a backup for domain controllers, which are crucial for network functionality, exposed a critical flaw in their

operational processes. The decentralised backup strategy did not account for the scenario where all domain controllers are wiped simultaneously, leading to significant challenges in recovery.

3. ***Insufficient Incident Response:*** The company did not have a robust, actionable incident response plan in place. They only formed an incident response team, after the incident had already happened. The chaotic and ad-hoc nature of the response(such as physically unplugging computers, makeshift recovery centres) indicates that procedures were either lacking or not effectively communicated and practised.
4. ***Disaster Recovery Gaps:*** The process for backup and recovery was insufficient. The failure to anticipate and plan for a scenario where all domain controllers could be simultaneously wiped was a detrimental oversight.
5. ***Operational Dependencies:*** Maersk's operations were heavily dependent on its IT infrastructure. The inability to process shipments, manage port operations, and communicate with customers due to the IT shutdown demonstrates an over-reliance on digital systems without adequate manual fallback procedures.

Technical / Data

1. ***Centralised Data Systems:*** Maersk's reliance on centralised data systems meant that once the malware infiltrated the network, it could access and encrypt vast amounts of critical data. Decentralising data storage and employing robust data segmentation could have reduced the attack's impact.
2. ***Credential Theft Vulnerability:*** The domain administrator's credentials were stolen using the pass-the-hash method, providing the attackers with

administrative access (Ashford, 2019). This allowed the malware to propagate rapidly across the network.

3. ***Data Recovery Delays:*** The recovery process was hampered by slow data transfer speeds from remote locations. This indicates a lack of preparedness for restoring data from remote backups swiftly and securely.

Technical / Application

1. ***Compromised Third-Party Application***: The attack vector was an automatic update to the M.E.Doc software, which Maersk was obligated to use for tax purposes in Ukraine. This backdoor provided an entry point for NotPetya, demonstrating the risk of relying on third-party applications without adequate security measures.
2. ***Vulnerability to Malware:*** The applications used by Maersk were outdated and susceptible to malware attacks(Microsoft 2000). The ability of NotPetya to lock and corrupt systems indicates that application-level security measures, such as endpoint protection and real-time threat detection, were insufficient.
3. ***Interconnected Systems:*** Maersk's applications were deeply interconnected, meaning that the infection of one system quickly spread to others. This lack of segmentation and isolation allowed the malware to propagate rapidly throughout their network.

Technical / Infrastructure

1. ***Network Vulnerabilities:*** The malware was able to spread quickly across Maersk's global network, suggesting weaknesses in network segmentation and access controls. More rigorous network security measures, such as

firewalls, intrusion detection systems, and segmented networks, could have mitigated the spread.

2. ***Legacy Systems:*** The reliance on potentially outdated systems and infrastructure that were not designed with modern cyber threats in mind contributed to the attack's success. Ensuring that all systems are up-to-date with the latest security patches is critical.
3. ***Poor Network Segmentation***: The lack of adequate network segmentation allowed the malware to spread rapidly across Maersk's global network. Implementing strict network segmentation can contain malware spread and limit the damage to isolated sections.
4. ***Outdated Infrastructure:*** The use of outdated operating systems (Windows 2000) and network infrastructure contributed to the ease of the malware's spread. Regular upgrades and maintenance of IT infrastructure are essential to mitigate the risk of such attacks.
5. ***Insufficient Endpoint Security:*** The malware's rapid spread was facilitated by insufficient endpoint protection measures, such as outdated antivirus software and lack of automated threat detection mechanisms on individual devices.

The NotPetya attack's devastating impact on Maersk was influenced by a combination of managerial, operational, and technical factors across various layers of their digital security architecture. The lack of cybersecurity awareness, inadequate incident response protocols, and insufficient patch management processes, combined with vulnerable applications, centralised data systems, and outdated infrastructure, created an environment perfect for exploitation by the malware

Security Controls - Improvement Proposals

The NotPetya attack's devastating impact on Maersk was influenced by a combination of managerial, operational, and technical factors across various layers of their digital security architecture. At the managerial level, the lack of prioritisation of cybersecurity was evident. Despite warnings from IT executives about the need for a security redesign of Maersk's global network, the initiative was not considered a key performance indicator for senior IT overseers. This lack of emphasis on cybersecurity led to delays in implementing critical security measures. To address this, establishing an ***Incident Response Plan (IRP)*** is essential. The IRP, classified as a recovery control affecting the applications, network, and data layers, would ensure that cybersecurity becomes a managerial priority and is integrated into the organisation's KPIs.

Inadequate security policies also played a significant role in Maersk's vulnerability. The company's managerial layer likely lacked robust cybersecurity policies and procedures, including regular cybersecurity audits and comprehensive incident response plans. These deficiencies hindered the organisation’s ability to quickly detect and contain the attack. Implementing a ***Secure Software Development Lifecycle (SDLC)*** can address this issue. The SDLC, both a preventive and corrective control affecting applications and data layers, promotes the development of strong cybersecurity policies and ensures that regular audits and incident response plans are in place, thereby enhancing the organisation's overall security posture.

Operationally, Maersk faced issues such as an insufficient patch management process and an inadequate backup strategy. The failure to implement a rigorous patch management process left Maersk's systems vulnerable to known exploits like EternalBlue. ***Regular vulnerability scanning and patching***, which are detective and corrective controls, can ensure timely updates and mitigate the risk of such exploits. This control impacts the applications, operating system, middleware, and runtime environments layers.

Moreover, Maersk's decentralised backup strategy did not account for the scenario where all domain controllers were wiped simultaneously, exposing a critical flaw in their operational processes. Enhancing the backup strategy through ***automated security configuration management***, a preventive and corrective control affecting the same layers as patch management, would ensure that critical components like domain controllers are backed up and that these backups are both centralised and resilient. Implementing robust backup and recovery protocols is crucial for minimising data loss and ensuring quick recovery post-attack.

On the technical front, the reliance on centralised data systems allowed the malware to access and encrypt vast amounts of critical data once it infiltrated the network. Implementing ***network segmentation***, a preventive control affecting the network/infrastructure layer, could have contained the malware spread and limited the damage to isolated sections. Additionally, the lack of data backups furthered the data loss. Continuous monitoring and logging, a detective and corrective control affecting the infrastructure, applications, and data layers, would ensure regular and secure backups are created and stored in isolated environments, enabling data recovery post-attack.

Maersk's reliance on third-party applications without adequate security measures also contributed to the attack. The compromised application update vector highlighted the risk of using third-party software. Ensuring third-party applications undergo rigorous security checks through a ***Secure Software Development Lifecycle*** (SDLC) can mitigate such risks. ***Multi-Factor Authentication (MFA)***, a preventive control affecting the applications and network layers, can further enhance security by adding an extra layer of protection against credential theft, which allows the attackers to gain administrative access using the pass-the-hash method.

Finally, outdated infrastructure and insufficient endpoint security facilitated the malware's rapid spread. ***Regular vulnerability scanning and patching***, as well as ***continuous monitoring and logging***, are essential to address these vulnerabilities. These controls ensure that IT infrastructure is regularly upgraded and maintained, and endpoint protection measures are updated to prevent malware spread.

In conclusion, addressing these managerial, operational, and technical issues through enhancing patch management, implementing robust backup and recovery protocols, improving network segmentation, and establishing better access management and automated threat detection systems can significantly mitigate the risk of future cyber-attacks. These measures ensure a more resilient cybersecurity posture, protecting Maersk from similar attacks in the future.

Contingency Process: Mapping

Incident Management

Incident Detection:

- The detection phase began as employees realised they couldn't reboot their systems and saw that the malware had locked their screens. Panic spread as the scale of the attack became apparent within half an hour.

Activation of the Incident Response (IR) Plan:

- IT staff began a physical response to contain the malware. They ran through hallways, conference rooms, and offices, unplugging machines and shouting to others to disconnect from the network. This impromptu and chaotic response was the initial activation of the incident response plan.

Incident Reaction:

- The immediate reaction involved a physical disconnection of computers from the network to halt the malware's spread. Employees were ordered to turn off their computers and leave them at their desks.
- The network shutdown, including digital phones, was a critical step in containing the incident.
- By 3 pm, a Maersk executive instructed employees to go home, acknowledging that the IT systems were beyond immediate recovery.

Escalation to Disaster:

- By 3 pm, a Maersk executive instructed employees to go home, acknowledging that the IT systems were beyond immediate recovery.
- As it became evident that IT staff could not contain the issue and the entire network was deeply corrupted, the incident escalated to a disaster.

This recognition led to the next phase of the contingency management process.

Disaster Recovery (DR)

Activation of the DR Plan:

- The disaster recovery plan was activated as the scale of the attack was confirmed. An emergency operations centre was established in Maidenhead, England, to coordinate the global recovery efforts.
- Maersk engaged Deloitte to manage the disaster recovery, effectively giving them a blank check to resolve the issue.

Decision on DR Restoration:

- Maersk had to decide whether the disaster recovery plan could restore operations quickly. Initial attempts showed that the damage was extensive, and normal operations could not be resumed immediately.
- The discovery that all domain controllers were wiped out indicated that restoring operations would not be quick. The IT staff searched for backups, realising that a critical layer of the network's infrastructure was missing.
- Focus shifted to salvage operations. This included the search for backups of domain controllers, which were eventually found in Ghana due to an unrelated power outage. This discovery was a significant breakthrough.

DR Operations:

- The disaster recovery operations involved transporting the backup from Ghana to the UK. This required coordination of a relay race involving multiple staff members due to visa issues, demonstrating a significant logistical effort to ensure data transfer.

- In Maidenhead, the IT team, alongside Deloitte, began rebuilding Maersk's network. This also involved purchasing new laptops, setting up fresh systems, and confiscating old equipment to prevent reinfection.

Salvage and Recovery:

- Recovery operations focused on restoring basic functionalities at Maersk's ports and terminals. Temporary solutions included paper documents and personal communication tools like Gmail and WhatsApp to continue essential operations.
- Maersk's core services started coming back online gradually, with port operations regaining the ability to read ships' inventory files within a few days.

Business Continuity (BC)

Activation of the BC Plan:

- With disaster recovery expected to be lengthy, Maersk activated its business continuity plan to maintain operations. This included setting up a centralised recovery centre in Maidenhead.
- Staff from around the world were brought to Maidenhead, turning the office into a 24/7 emergency operations centre. Maersk booked all available accommodations in the area to house the influx of personnel.

Operations at Alternate Sites:

- Temporary operations were established using new laptops and prepaid Wi-Fi hotspots. Staff worked from makeshift setups, maintaining business operations through unconventional methods.
- Communication was key during this phase, with staff resorting to using personal email accounts, WhatsApp, and Excel spreadsheets to manage operations and communicate with customers.

Crisis Management (CM)

Crisis Management Activation:

- The crisis management plan was activated due to the significant operational and reputational impact of the incident. Deloitte was brought in to manage the crisis, providing expertise and resources to ensure effective communication and efficient recovery operations.
- Despite initial failures, communication improved, with staff using personal channels to keep operations running.

Communication and Operational Aspects

- *Internal Communication:* IT staff communicated recovery plans and instructions internally, leveraging emergency setups in Maidenhead.
- *Customer Communication*: Initial communication with customers was poor, with limited updates. Ad hoc methods (emails from personal accounts, WhatsApp) were used to handle critical operations.
- *Operational Issues:* Port operations were halted, causing global supply chain disruptions. Manual processes (e.g., paper documentation) were temporarily used to manage cargo and bookings.
- *Technical Recovery:* The primary focus was on rebuilding the network, restoring domain controllers, and reissuing clean systems to employees.

Shortcomings of Maersk's Contingency Management Process

1. **Inadequate Incident Detection and Response Preparation**
    - *Delayed Detection:* The initial recognition of the malware's presence was slow, leading to employees manually disconnecting computers.

- *Chaotic Response:* Employees were seen running through hallways and manually disconnecting machines, which indicates the absence of an organised and well-rehearsed incident response plan.

2. **Ineffective Communication**
    - *Internal Communication Issues:* During the early stages of the attack, communication among employees and IT staff was disorganised. Many staff members were left without clear instructions and had to vacate the premises in confusion.
    - *External Communication Failures:* Customers received minimal to no communication in the crucial initial hours and days of the incident. The use of personal emails and messaging apps like WhatsApp for business communication underscores the lack of an effective communication plan.
3. **Flawed Backup Strategy**
    - *Backup Shortcomings:* The central backup strategy for domain controllers was insufficient, as it did not anticipate a scenario where all domain controllers would be simultaneously compromised. The reliance on finding a single surviving domain controller in Ghana illustrates the lack of a robust and redundant backup system.
4. **Insufficient Business Continuity Planning**
    - *Delayed Activation:* Business continuity measures were not immediately put into action. It took several days before new booking processes were established and basic port operations could resume.
    - *Reliance on External Consultants:* The heavy dependence on Deloitte and giving them a "blank check" indicates that Maersk's internal business continuity and disaster recovery plans were not sufficiently comprehensive or well-practised.

5. **Technical and Operational Unpreparedness**
    - *Complete Network Shutdown:* The total shutdown of Maersk's global network and the confiscation of pre-existing equipment highlight a lack of preparedness for maintaining operations using alternative systems.
    - *Manual Operations:* The need to revert to paper documentation and personal communication channels suggests that Maersk lacked effective manual or semi-automated fallback processes for critical operations.

Contingency Improvement Proposals

1. **Improved Incident Detection and Response:**

   For Maersk, implementing real-time monitoring and automated incident detection tools is crucial to enhance response times and safeguard their global operations. This would involve deploying advanced Security Information and Event Management systems capable of analysing network traffic and system activities across Maersk's extensive network infrastructure. Automated tools can detect anomalies in real time, such as unusual login attempts or unauthorised data access, triggering immediate alerts to the security team.

   Moreover, establishing clear incident response protocols tailored to Maersk's operational context is essential. These protocols should include detailed steps for containment, mitigation, and communication during a cyber incident. Regular training sessions and simulated drills should be conducted to ensure all employees, from IT staff to senior management, understand their roles and responsibilities. This preparedness is vital for

Maersk, considering its vast and complex logistical network, to ensure a swift and coordinated response that minimises operational disruptions.

2. **Enhanced Disaster Recovery Planning:**
   Maersk should conduct regular testing and validation of their disaster recovery plans to ensure the availability of critical backups. This involves routine drills simulating various disaster scenarios, verifying that backups can be restored quickly and effectively. Regular testing helps identify weaknesses and gaps, allowing Maersk to address them proactively.

   Implementing geo-redundancy for essential systems is particularly important for Maersk due to their global operations. By having multiple backup locations across different geographic regions, Maersk can ensure that if one site is compromised, others can seamlessly take over. This approach mitigates the risks associated with single points of failure and ensures business continuity, even during large-scale disruptions

3. ***Effective Crisis Management Framework:*** Defining clear escalation paths and communication channels is essential for effective crisis management at Maersk. This involves creating a structured approach for escalating incidents to higher levels of management and external stakeholders as needed. Clear communication protocols ensure that everyone knows who to contact and what information to share during a crisis.

   Regular crisis management drills and simulations are necessary to test the effectiveness of response strategies. These exercises help identify potential weaknesses in the crisis management plan and provide an opportunity to refine and improve the approach. By simulating different

crisis scenarios, Maersk can ensure they are prepared for a range of potential incidents, from cyberattacks to natural disasters affecting their ports and logistics operations.

4. ***Communication and Coordination:*** Establishing a centralised communication platform is critical for communicating during incidents. This platform should be accessible to all relevant parties and provide a single source of truth for updates and instructions. For Maersk, having a centralised system ensures that all employees, stakeholders, and partners receive consistent and accurate information, reducing confusion and miscommunication. Regular communication updates to stakeholders, employees, and customers are also essential. Maintaining transparency and trust during a crisis involves keeping everyone informed about the situation and the steps being taken to address it. Timely and accurate updates help manage expectations and maintain confidence in Maersk's ability to handle the incident effectively

Discussion

The statement that "companies cannot protect themselves against cyber attacks by nation states" reflects the immense challenges posed by state-sponsored cyber threats in today's interconnected world. It is particularly interesting in this case, as Maersk became collateral damage in a Russian military attack on Ukraine. Nation states possess vast resources, advanced cyber capabilities, and highly skilled operatives, often greater than those available to individual companies. These adversaries employ sophisticated tactics like advanced persistent threats (APTs), zero-day exploits, and targeted social engineering to exploit vulnerabilities in global

supply chains and interconnected systems, causing significant disruptions across industries.

Additionally, state-sponsored actors frequently utilise strategies designed to evade conventional cybersecurity defenses and exploit weaknesses in legacy systems or outdated infrastructure. Legal and diplomatic constraints further complicate companies' responses, limiting the effectiveness of retaliatory actions and international legal recourse.

However, despite these challenges, companies *can* strengthen their cybersecurity posture through proactive measures. This includes investing in robust cybersecurity technologies such as advanced threat detection systems, encryption protocols, and regular security audits. Collaborating with industry peers, government agencies, and cybersecurity experts for threat intelligence sharing and incident response planning is crucial. Adhering to cybersecurity regulations and standards provides a fundamental framework for protecting against both state-sponsored and criminal cyber threats.

While achieving complete immunity from nation-state cyber attacks may be unrealistic, proactive defense-in-depth strategies significantly mitigate vulnerabilities and potential impacts. By continuously evolving cybersecurity practices to address emerging threats and embracing collective defense approaches, companies can enhance their resilience against sophisticated adversaries, safeguarding their operations, data, and stakeholders in today's complex digital environment.

Bibliography

References

Ashford, W. (2019, June 7). *NotPetya offers industry-wide lessons, says Maersk's tech chief*. ComputerWeekly.com. https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief

Capano, D. E. (2021, September 30). *Throwback Attack: How NotPetya Ransomware Took Down Maersk*. Industrial Cybersecurity Pulse. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

CEO Monthly. (2019, April 9). *Incident response takes centre stage at Infosecurity Europe 2019 with keynote speakers from Maersk*. CEO Monthly. https://www.ceo-review.com/2019-incident-response-takes-centre-stage-at-infosecurity-europe-2019-with-keynote-speakers-from-maersk-and-uk-law-enforcement/

Chandra, V. (2022, August 8). *Lessons Learned from NotPetya*. Wattlecorp Cybersecurity Labs. https://www.wattlecorp.com/lessons-learned-from-notpetya/

Harner, C., Beck, C., & Fleisher, B. (2020, March 2). *The law of unintended consequences: When companies are collateral damage in a cyberattack*. Milliman.

https://www.milliman.com/-/media/milliman/pdfs/articles/the-law-of-unintended-consequences.ashx?la=&hash=7B401048147E5FAC439285826384595B

Martin, E. (2019, June 26). *Protect and survive: how Maersk learned from the NotPetya cyber attack*. Riviera. https://www.rivieramm.com/news-content-hub/news-content-hub/protect-and-survive-how-maersk-learned-from-the-notpetya-cyber-attack-55284

Milne, R. (2017, August 13). *Maersk CEO Soren Skou on surviving a cyber attack*. Financial Times. https://www.ft.com/content/785711bc-7c1b-11e7-9108-edda0bcbc928

Palmer, D. (2019, April 29). *Ransomware: The key lesson Maersk learned from battling the NotPetya attack*. ZDNET. Retrieved June 5, 2024, from https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/

Perez, R. (2017, October 20). *NotPetya Ransomware: Lessons Learned*. Infosecurity Magazine. https://www.infosecurity-magazine.com/magazine-features/notpetya-ransomware-lessons-learned/

Poireault, K. (2023, July 11). *What Have We Learned from NotPetya Six Years On?* Infosecurity Europe. https://www.infosecurityeurope.com/en-gb/blog/threat-vectors/learnings-from-notpetya-cyberattack.html

Red Goat. (2023, April). *Maersk incident response*. Red Goat Cyber Security. https://red-goat.com/why-you-should-test-your-incident-response-a-review-of-the-maersk-incident/

Schwartz, M. J. (2019, May 31). *11 Hot Sessions: Infosecurity Europe 2019*. BankInfoSecurity. https://www.bankinfosecurity.com/blogs/x-hot-sessions-infosecurity-europe-2019-p-2750

Schwartz, S. (2018, March 6). *How Maersk proved its 'herculean resilience' after malware devastation*. CIO Dive. https://www.ciodive.com/news/how-maersk-proved-its-herculean-resilience-after-malware-devastation/518421/

VinciWorks Group. (2018, October 15). *NotPetya: The World's Worst Cyber Attack*. VinciWorks. https://vinciworks.com/blog/notpetya-the-worlds-worst-cyber-attack/

Walton, H. (2020, October 26). *The Maersk cyber attack - How malware can hit companies of all sizes*. Kordia. https://www.kordia.co.nz/news-and-views/the-maersk-cyber-attack

Wingrove, M. (2017, June 29). *Maersk should have avoided cyber attack*. Riviera. https://www.rivieramm.com/news-content-hub/news-content-hub/maersk-should-have-avoided-cyber-attack-28071