Data Breach Incident Analysis

Assignment 2

Adrianne Crouse

ac4119@mynsu.nova.edu

NOVA Southeastern University

Yair Levy, Ph.D.

ISEC-615 Winter 2021

4/11/2021

Table of Contents

Data Breach Incident Analysis

NotPetya, described by Cisco's Talos division as "the fastest-propagating piece of malware we've ever seen" (Sandberg, 2019, p. 183) is estimated to have cost some $10 billion dollars in damage (Smith, 2019). NotPetya, delivered to desktops as a tailgater on legitimate program updates, spread quickly through networks via a combination of known Windows vulnerabilities. Since NotPetya's initial delivery mechanism was a piece of Ukrainian software, the more popular of two accounting programs permitted for use in filing Ukrainian tax returns, other cybersecurity experts note the extent of damage that might have been seen if NotPetya had targeted a more developed nation (Smith, 2019). The prolific analysis immediately following the attack includes a theory that NotPetya might have been released with a bug that limited its value as ransomware (Heller, 2017). For all the damage caused, a bitcoin account associated with NotPetya only saw some $10,000 transferred out of it a week after the outbreak at which time a message was sent via the dark net that 100 bitcoins would decrypt hard drives but not master boot disks allowing for only a partial restoration (Leyden, 2017). One of the largest companies affected, Maersk, had recently undergone a cybersecurity review and approved financing for a large number of upgrades, but in the wake of WannaCry, the specific upgrades that could have prevented some of the NotPetya damage, including network segmentation, were not yet undertaken (Greenberg, 2018). The Linkos Group family run software business that was patient zero, however, was described as any easy target, and the MEDoc tax filing application that carried the worm to users across the world was said to be outdated and poorly written (Greenberg, 2019). According to Greenberg and Cybereason's Ran

Levi, only one machine in the vast Maersk network had MEDoc installed. Modern tools such as those incorporating system audits, uniform change managements, and sandboxing as well as a periodic professional review with penetration testing would have significantly reduced the chances of the Linkos Group company being used as a vehicle for a global disaster.

Data Breach Overview

The MEDoc malware invasion of June 2017 was given a number of nicknames related to Petya, an earlier ransomware incident, and chiefly became known as NotPetya as the intention appeared to be more destructive than financial (Schwartz, 2017). A cybersecurity expert with the Slovakian firm ESET, while working to find a method of stopping NotPetya, recovering disks encrypted by NotPetya, and building an antivirus update to protect vulnerable machines, discovered the file used to trigger the worm was associated with the Ukraine approved tax return software called MEDoc. As reported in Bank Info Security and Tech Target, as well as the Wired excerpt from Sandworm, Anton Cherepanov was familiar with the software, and the file, from a lesser outbreak the previous month. Cherepanov quickly downloaded all MEDoc updates for the May/June 2017 timeframe for further analysis. Within a week, the worm's origin was tied to the MEDoc software, and the Ukranian police retrieved the stack of company's servers from the Linkos Company office in Kiev (Goodin, 2017).

Meanwhile, another cybersecurity expert working for Cybereason heard about NotPetya panic and studied the worm's code in hope of finding a solution such as the "kill-switch" discovered for WannaCry earlier that year. Amit Serper of Cybereason found an if/then statement that seemed to prevent the NotPetya encryption process. The solution was to create a file on every Windows machine that could potentially be affected (Sandberg, 2019, p.208); the information was released, but the infected machines still could not be decrypted. Cybereason staff was hired to analyze the servers retrieved from Linkos to determine how the penetration occurred and how the worm was delivered. ESET's and Cybereason analysis found the NotPetya worm was spread so quickly as a result of two known and somewhat previously developed vulnerabilities working together; EternalBlue allowed remote code execution on unpatched Windows machines via Server Message Block (SMB), and Mimikatz exploited a Windows flaw regarding passwords stored in RAM. The NotPetya analysts saw that NotPetya infected entire networks by the combination of remote code execution and administrative password discovery. The worm then proceeded to wipe data and master boot records depending on the presence of other system files. The study of the Linkos server's confirmed Cherepanov's theory that NotPetya was distributed by legitimate copies of MEDoc application updates; furthermore, the Linkos's group servers had been penetrated for months (Sandberg, 2019).

Security Failures

Amit Serper of Cybereason, hired by authorities in Kyiv to analyze the Linkos Group server infrastructure, saw a significant discrepancy in the sophistication of the attack and the preparedness of the defense. "These agile, innovative intruders were strolling through holes in MEDoc's server software that was years old, poorly configured, and shoddily patched" (Sandberg, 2019, p.208). The failures on the part of Linkos group occur in all three McCumber Cube dimensions. Chiefly, failures are seen in provisioning of security for data integrity in all states, provisioning of cybersecurity technologies, and use of cybersecurity policies and procedures.

Serper, from his analysis of the Linkos Group servers, found that a component of the company’s webserver had been breached, and the hackers had set up an administrative shell directly on the server. From this foothold the attackers were able to breach the server that managed software updates (Greenberg, 2019). ITPro further states that the Linkos Group servers had not been updated since 2013 (Shepherd, 2021). The integrity of the data on these servers was severely compromised, not only by lack of updates but by failure to detect changes. Amit Serper discovered a hidden web shell in use as early as November 2015 (Greenberg, 2019). The integrity of the MEDoc updates themselves was compromised by the failure to check what data was sent out to customers against what programmers prepared; at some point, during the preparation of an update, a programmer would be able to detect what Cybereason discovered: lines of code creating a backdoor. Such a discovery should have provoked investigations, delays, and warnings. The attacks, on 3 occasions, took place several days following an update release (Schwartz, 2017).

The Linkos Group failed to make use of available cybersecurity technologies, the most obvious being audit logs and sandbox mechanisms to test their own software. A plethora of change management programs exist to audit application changes; the MEDoc application could have been checked both at rest on the servers and following transmission to a test machine. Analysis of the processing of the update would have shown tax ID numbers sent in cookies back to the server, a process put in place by the hackers to, presumably, identify the companies utilizing the Ukrainian software for further penetration (Schwartz, 2017).

Appropriate policies and practices surrounding the release of software updates should have alerted Linkos Group staffers to a problem, even if the technologies had not been implemented. Policies and procedures require multiple checks and generally, heavy documentation. Such practices can result in expertise being called in where an event seems inappropriate or suspicious. Many months passed from the onset of the servers' compromise and the final mind-blowing NotPetya attack. In an interview with Greenberg, the Linkos Group proprietor said she did not willfully neglect security; she just considered their effort too insignificant to warrant making them a target (Greenberg, 2019).

Cybersecurity Posture

In an unsourced interview on their website Linkos Group CEO, Olesya Lynnik, notes their survival of the NotPetya disaster as well as the strides they've taken to provide security. In a 2018 publication, Aleysa Belousova notes cooperation with companies such as Enjoy security and Berezh Security as well as other companies in continuing the MEDoc platform. Regarding Cybersecurity posture, outsourcing is increasingly relied upon and required for an accurate picture of a company's cybersecurity status. Areas of improvement possibly included a robust intrusion detection system, change management policies and audit trails of such, as well as improved patching procedures for production servers and employee workstations given the now high profile work of Linkos Group in the region. Costs for security related improvements in hardware, software, and services could be monthly or annual or a combination. More than likely, some fixed costs would include a powerful IDS in combination with a next generation firewall, plus a platform for an event manager with professional services. The fixed cost could be anywhere from $10K to $20K just for these items; monthly costs for endpoint security and network monitoring could be $1000 per month assuming some 50 devices at a minimum. Professional services for penetration testing and additional training would have a wide range depending on whether the services were dedicated in person visits or remote access; an additional $5000 to $20,000 annually for periodic professional services would bring the company's annual total to a minimum of $40 to $60K which is considerably less than the salary of even one full time security employee.

Business Continuity Plan

Successful business continuity plans are often highly detailed. The Linkos Group, as a relatively small operation providing a widespread service, would likely benefit from engaging outside help to review their business process and the infrastructure required to maintain operation. Documenting lists of potential disasters and how each might affect their ability to deliver service to customers as well as maintain structure for continuing development is essential. Lists and procedures should be highly detailed referencing locations, property, and specific contacts including how to reach them day or night. A password management solution should be referenced. Sensitive data should be encrypted and under lock. Business continuity plans should be reviewed with all involved as well as a trusted 3rd party for clarity. The plan must be maintained securely with appropriate confidentiality and integrity checks, and the plan must always be available (McNeal, 2020).

Conclusion

Reports of the NotPetya disasters as experienced in hospitals and other companies across the globe vividly describe the havoc created by cyber terrorist groups. Hundreds of businesses shut down; gas stations, banks, power companies, hospitals, airports, and the federal government in Ukraine freeze due to a single business application. When the office of the shipping giant Maersk reboots to a black screen, the outbreak paralyzes 17 of 76 worldwide ports nearly instantaneously. A internet photo shows streams of 18-wheelers bringing in their loads for the Maersk containerships backed up for miles. Writers allude to Hurricane Katrina regarding the vast damage, such as large number of unidentifiable containers stuck for months. Reports of potential criminal neglect were made concerning the Linkos Group role, but still, according to press releases on the medoc.ou website, Linkos Group CEO Olesya Linnyk and the MEDoc application received awards for their success in 2019. The vehicle for NotPetya, despite neglect for good cyber practices, was prey to applications developed by cyber engineers in the U.S. and France for the purpose of protecting against such acts of malfeasance. The hackers in their sophistication might have thought it a riot other than for the damage to Russian industry. In IT, progress is made by testing and development. Consumers on the business stage must protect themselves and their customers to whatever extent possible to maintain viability. Several articles concerning NotPetya promoted non-Windows platforms or full time sandboxing strategies for malware avoidance, but as the Linkos Group success demonstrates, a product must also be usable, even user friendly, or it is useless for the common good.

Reference List

Ashford, M. (2017, September 25). *NotPetya attack cost up to £15m, says UK ad agency WPP.* Computer Weekly. https://www.computerweekly.com/news/450426854/NotPetya-attack-cost-up-to-15m-says-UK-ad-agency-WPP

Edroso, R. (2018). NotPetya and ransomware: Six steps to help you beat hackers. *Patient Safety Monitor Journal*, 19(1), 8-10.

Goodin, D. (2017, July 5). *Backdoor built in to widely used tax app seeded last week's NotPetya outbreak.* Ars Technica. https://arstechnica.com/information-technology/2017/07/heavily-armed-police-raid-company-that-seeded-last-weeks-notpetya-outbreak/

Greenberg, A. (2018, August 22). *The Untold Story of NotPetya, the Most Devastating Cyberattack in History.* Wired. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenberg, A. (2019). *Sandworm: A new era of cyberwar and the hunt for the Kremlin's most dangerous hackers.* Anchor Books.

Heller, M. (2017, July). *Tax software backdoor allowed NotPetya ransomware attacks*. TechTarget. https://searchsecurity.techtarget.com/news/450422320/Tax-software-backdoor-allowed-NotPetya-ransomware-attacks

Levi, R. (2021, March 3). *Inside NotPetya, Part 1*. Security Boulevard. https://securityboulevard.com/2021/03/malicious-life-podcast-inside-notpetya-part-1/

Leyden, J. (2017, July 5). *Ker-ching! NotPetya hackers cash out, demand 100 BTC for master decrypt key*. The Register. https://www.theregister.com/2017/07/05/notpetya_hackers_cash_out

McNeal, A. 2020, August 26. *Cybersecurity Disaster Preparedness 101*. ID Agent. https://www.idagent.com/cybersecurity-disaster-preparedness-101-business-continuity-planning

MEDoc. (2018). *Modern technologies to help business*. https://medoc.ua/media/linkos-group-sovremennye-tehnologii-v-pomoshh-biznesu

Obozrevatel. (2019, June 5). *Engine for business: what EDO products are used by retail leaders*. https://news.obozrevatel.com/ukr/tech/dvigun-dlya-biznesu-yaki-produkti-edo-vikoristovuyut-lideri-ritejlu.htm

Proven Data. (2020, June 25). *How Much Does Cyber Security Cost? Common Cyber Security Expenses & Fees*. https://www.provendatarecovery.com/blog/cyber-security-cost-expenses-fees/

Schwartz, M. (2017, July 4). *NotPetya patient zero: Ukrainian accounting software vendor*. Bank Info Security. https://www.bankinfosecurity.com/notpetya-patient-zero-ukrainian-accounting-software-vendor-a-10080

Shepherd, A. (2021, March 26). *What is NotPetya?* ITPro. https://www.itpro.com/malware/34381/what-is-notpetya

Smith, K. (2019, June). *Going dark: NotPetya paralyzed businesses and put cyber on the map as an emerging catastrophe risk.* Best's Review. http://news.ambest.com/ArticleContent.aspx?pc=1009&altsrc=158&refnum=285596

Williams, M. (2017, July 5). *Wannacry, Petya, NotPetya, Vault 7, Dark Matter, Show Numerous Key Flaws in Popular Devices.* EIN Presswire. https://www.einnews.com/pr_news/390642204/wannacry-petya-notpetya-vault-7-dark-matter-show-numerous-key-flaws-in-popular-devices

College of Computing
and Engineering
NOVA SOUTHEASTERN UNIVERSITY
NSU
Florida

Certification of Authorship of Assignment

Submitted to: Yair Levy

Student's Name: Adrianne Crouse

Date of Assignment: 4/11/2021

Title of Assignment: Data Breach Incident Analysis

Certification of Authorship: I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this course.

Student's Signature: Adrianne Crouse