Incident Response Report

Security Landscape/Background

The cybersecurity business has evolved significantly within the past few years, a new threat has hit the world: ransomware. Ransomware was involved in 23% of breaches in the most recent Verizon Data Breach Investigations Report (VDBR) 2024, through vulnerability exploitation and credential theft. Web applications and VPNs are popular gateways, combined with the ignorance of employees that contributes to 68% of cyber incidents. This shows the two main issues: the lack of technology strength and the vulnerability of the user.

Especially the healthcare sector has fallen under attack as this sector heavily depends on the functioning of its IT systems. A classic example of this trend was the 2021 ransomware attack of the Ireland's Health Service Executive (HSE). Conti ransomware gang managed to infiltrate through a phishing email they sent to the health department of Ireland and disrupted all the public health services including forcing the stoppage of all IT systems and major delay in patient care. This particular case brings out the degrees of consequence of neglecting basic cybersecurity measures in this areas of healthcare.

Scoping of the Incident

Threat Category: Ransomware

A ransomware is a form of virus that encrypts the data of the target and extorts the victim to release the lock. They have got more complex, and recent examples of such groups are Conti, which use what is known as double extortion where they also threaten to release the stolen data if the ransom demands are not met. These attacks are particularly destructive for sectors that cannot function without access to timely and accurate data – such as the healthcare sector.

Organization Type: National Healthcare Provider

The HSE is the largest employer in Ireland with a workforce in excess of 130,000 its tasked with the responsibility of providing public healthcare service across 4,000 sites; 54 of which are Acute Hospitals. Year two It had an extensive coverage of IT systems that made it even more susceptible to an organized attack.

Incident: HSE hit by Conti Ransomware Attack

Conti attack was launched on March 18, 2021, where the attackers used a phishing email containing macro-enabled Microsoft excel file. The malware in this file contaminated a workstation and gave the attackers a way into the HSE's IT system. In eight weeks, the attackers stole data, achieved privileged credentials, and deployed ransomware in systems. On the 14th of May 2021, the ransomware was triggered and this cut off all of HSE's IT networks. Major patient care databases, finance and communication systems were affected at a time that practitioners were compelled to go back to handling the systems manually.

Root Causes

The Conti attack revealed several vulnerabilities and systemic issues within the HSE's cybersecurity framework:

1. **Cybersecurity Controls Overlooked**

The HSE's IT environment lacked critical security measures, such as:

Security Monitoring: Lack of sufficient centralized function to successfully identify, investigate, and counteract security alerts.

Patch Management: Many systems were left uncovered where known exploits existed; that is, many systems had not been updated for remedial work.

Antivirus Updates: The infected workstation has not been updated with the antivirus for over one year.

2. **Network Design Flaws**

   The flat network architecture of the HSE meant that attackers were able to move from system to system. Due to the absence of segmentation, it became possible for an attacker to infiltrate one set of systems and then easily move through to other systems.

3. **Lack of Preparedness**

   The HSE failed to respond promptly to get the initial signs of a malicious attack. It is notably that no preliminary analysis of disturbances in corporate information security was started before May 14, though some signs of the attack had been previously identified; further, all the possible investigations of the cybersecurity incident were not launched, which were might be helpful for managing the threat.

4. **Governance Issues**

   Lack of appropriated focused organizational position filled by Chief Information Security Officer as well as weak structure of cyber security governance made the organization unprepared for the growing threats. Cybersecurity threats failed to gain a clear definition at the organizational strategic level and thus could not support superior planning.

Recommendations

Mitigating these risks entails reflection on technical solutions, strategic approaches and long-term resilience plans of action.

Below are detailed recommendations:

1**. Technical Measures**

a. **Network Segmentation**

Other measures such as the integration of network segmentation will reduce the opportunity of lateral movement for attackers. Apps like patient databases and finance apps should be placed in an encoded area they shouldn't be accessed normally but through authentication.

b. **Endpoint Detection and Response or EDR**

Use the best EDR to track or observe the general activity of endpoints in organizations or institutions in real-time and establish ways of preventing or mitigating threats as they arise before they progress.

c**. Automated Patch Management**

Implement automated solution in order to upgrade the software and operating systems without delays, closing the entry points attractive for the attack.

d. **Enhanced Email Security**

Introduce the up-to-date anti-phishing and email filtering mechanisms to avoid getting the dangerous attachments and links through to the end customers.

2. Strategic Governance

a. **Formulate a Cybersecurity Oversight Committee**

The next recommendation is to establish a competent panel to manage cybersecurity policy in terms of its accordance to organizational objectives. This body should comprise of executives, IT professionals, and outsiders in order to achieve diverse opinion making.

b. The very first recommendation is to set up a Chief Information Security Officer, or CISO. The roles of the CISO should be to oversee and manage cybersecurity activities on behalf of the organization, report to and enforce compliance throughout the organization and convey security risks to top officials. This role should fall under the reporting line of the Chief Technology Transformation Officer (CTTO).

Cybersecurity Strategy can be reviewed as follows:

Develop a cybersecurity strategy that is sustainable over several years based on compliance with the national initiative for cybersecurity (NIST) cybersecurity framework. One of the key factors that should herald its implementation should be risk management, training of the employees and planning on how best to address incidents in the workplace.

3. **Future-Proofing Strategies**

a. **Zero-Trust Architecture**

Take a zero-trust model to user and device access that verifies every request, be they internal or external. This reduces our reliance on the conventional zone security mechanisms.

b. **IT services**

Adopt the use of throwaway SIM cards since major threats occur within the first days after SIM card activation.

c. **Incident Response Plan**

Develop a comprehensive incident response plan that includes:

Frequency of desk-top drills on attack plans.

Defined organizational procedures of operations concerning disaster response in intersectoral functions.

Incident analysis and debriefing as a methodology of learning from the incident.

d. **Third Party Risk Management**

Be in a position to improve the scrutiny of third-party suppliers' evaluations to make certain that the sellers meet high security measures. It reduces risks, particularly those associated with software supply chain attacks.

Conclusion

The attack on the HSE through the Conti ransomware shows the serious threat facing the healthcare industry in terms of cybersecurity. To prevent further similar occurrences, organizations can mitigate the noted risks and apply the outlined technical and strategic actions. The threat landscape will keep changing in the future, making it vital for organizations to take early steps and invest in cybersecurity defence to protect crucial services and sensitive data.

References

Verizon (2024). *2024 Data Breach Investigations Report*. Available at: http://verizon.com/dbir

Health Service Executive (2021). *Conti Cyber Attack on the HSE: Full Report*. Available at: https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

Malicious Behaviour	Suspicious Behaviour	Start Packet	End Packet	Attacker IP	Destination IP	Remarks/Notes
Port scan	Connecting to website	1	91	192.168.56.1	192.168.56.101	Accessing different webpages, and the constant efforts at trying to access a given non-existent webpage.
Port scan	Ping Test	70	75	192.168.56.104	192.168.56.101	It must then be noted that unless IP 104 is an admin, it should not be capable of pinging

						another system.
Port Scan		94	48261	192.168.56.104	192.168.56.101	Port scan during all of this and the structure of packets is proved by the fact that during all of this TCP and UDP connects all the ports from 1 to 65534 is the amount of the incoming packets during all of this in 6 seconds
Port Scan		203	204	192.168.56.104	192.168.56.101	Port accessed, No. 80, HTTP port
	Ping Test	48335	48342	192.168.56.1	192.168.56.101	If the person using an IP 192.168.56.1 it is not an admin, then they shouldn't be pinging another IP system

PCAP 1

Looks more like port scanning and the attempting to telnet into the device via opened ports. As to the identified, most of it was closed but the HTTP was open and the port assigned to it was port 80.

PCAP2

Malicious Behaviour	Suspicious Behaviour	Start Packet	End Packet	Attacker IP	Destination IP	Remarks/Notes
	Server uploading and connection	10	86	192.168.56.102	192.168.56.101	Many activities are questionable as they send a file 'Confidential information.doc' to address 192.168.58.102
Password Cracking		87	157	192.168.56.1	192.168.56.101	Trying to get into accounts with phrases.

Password Cracking		165	347	192.168.56.1	192.168.56.101	Bribing server accounts, With a conspicuous fail.
Password Cracking		348	430	192.168.56.1	192.168.56.101	Does not account login, generates a zero byte file called 1.png, and logs out after three seconds.
	File storing	1359	1390	192.168.56.102	192.168.56.101	A log in is successfully accomplished and is followed by creation of a file with a name of memo, with no file extension.
Password Cracking		1392	14137	192.168.56.1	192.168.56.101	To gain access in server accounts, no success.
Password Cracking		14173	14240	192.168.56.1	192.168.56.101	Successfully gets the password, logged into the account and downloaded the Confidential Information.doc

PCAP 2

Is a password cracking attempt, connecting to one port disconnecting from port to attempt to access an account within its system.

PCAP 3

Malicious Behaviour	Suspicious Behaviour	Start Packet	End Packet	Attacker IP	Destination IP	Remarks/Notes
	Web browsing and file accessing	1	29	192.168.56.101	192.168.56.102	GET (file weblink) {'uses GET 'file', and GET 'weblink'}
Port breaching		32	88	192.168.56.1	192.168.56.102	When attempting to connect to a variety of supposedly open ports, they get denied..

Port breaching		95	133	192.168.56.1	192.168.56.102	Finds a variety of open ports.
Password Cracking		134	81189	192.168.56.1	192.168.56.102	Up to this time, that this program has been running, it has never been able to open at least one account. Password cracks having a chance to try every single letter possible.
	ICMP	1441	2044	192.168.56.101	192.168.56.102	Ping command used.

PCAP 3

Another password cracking attempt of the same kind, except is tries every possible combination there is instead of words in the dictionary. PCAP 3 fails to connect, using the filter:

```
ws.col.info == "Response: 230 Login successful."
```

Fails to show any results. We also are able to find ping attempts, these can be found when using the filter icmp portrays efforts from one or more devices being communicated with by other devices.