Chapter 1

Introduction:

On June the 20th, 2024, a group called ‘Brain Cipher’ based on the ransomware Lockbit 3.0 attacked Indonesia's National Data Centre. The attack disrupted 282 public services, including immigration, airport services and online student registration. The hackers demanded a US$8 million ransom; however, the group later revealed it would be sharing the decryption key for free (Nugroho, 2024).

Initially, the attack was detected on the 17th of June, when Windows Defender security features were being disabled. Within 3 days later, on June 20th, the suspicious activities increased and malicious files and the deletion of crucial system files, well as the deactivation of essential services, happened within the data centre (Setyawan, 2024).

Lockbit 3.0 is a ransomware malware software that encrypts data stored on a device, preventing user access. The attackers then demand a ransom for the decryption key or threaten to steal, delete, or leak data (Anon., n.d.).

Threat Analysis:

The attack on Indonesia portrayed many threats to the National data centre, national security and public services. The attack targeted public services, immigration, airports and online student registration; if the attackers threatened to **release this data**, it could cause significant privacy issues as well as the potential for **identity theft**. Furthermore, the disruption to public services and personal, financial and government data caused substantial disruptions, and the government had to rely on emergency measures for functionality; this could have impacted the **citizens day to day lives** as well as their **trust** and the **national economy** (Nugroho, 2024).

The attack highlighted the underlying security issues and Indonesia's poor lack of digital security and protocols. The problem is that it could **promote future attacks**, and attackers could see the **data centre as a target.** This could **prevent the public from trusting their personal data** to be stored if no cybersecurity improvements are made (Azhar, 2024).

After the attack was noticed, the data was quickly transferred to an Amazon web server. This caused more system downtime, and although the data centre was expected to recover by late July, the data within the national data centre is classed as lost and unusable, causing significant downtime (Bella Evanglista, 2024), (Azhar, 2024).

Vulnerability Assessment:

Because Indonesia's priorities are to expand its digital access instead of ensuring proper security, many vulnerabilities have been exploited by criminals. Multiple variables contributed to the attack on Indonesia's National Data Centre. Software, lack of misconfigured and poorly managed firewalls and encryption protocols, and social engineering could all be linked to the leading cause of the hack.

What the Vulnerability is:	Why is it a Vulnerability:	Severeness Risk (1-10):
Unpatched and Old Software.	Government systems tend to run on older software, which could be missing the latest update or patch. This could lead to open vulnerabilities to gain access. If the data centre relied on old software, it could have opened opportunities for the attackers (Anon., n.d.).	9/10
Weak Access and Configuration Control.	Weak access control or misconfigurations could have allowed the attackers to grant unauthorised access to multiple systems across the data centre and access sensitive data easily. For example, if an employee has excessive privileges, the hacker could take advantage (Anon., n.d.).	8/10
Security Awareness	Unintentional and accidental employee actions could have helped the attackers because of human error, making people more susceptible to mistakes without adequate training, phishing scams, weak passwords, or social engineering, all of which can lead to vulnerabilities (Noonan, n.d.).	6/10
Lack of an Incidence Response Plan	Without a proper incident response plan, it can lead to delayed threat response to the attack, increasing the downtime and the amount of ransomware spread. It can also leave the team in the dark about the protocols to take during an attack (Anon., n.d.).	7/10
Lack of Threat Detection and Prevention	Without proper threat detection, there is a possibility that there is an open port or a piece of misconfigured security or other potential vulnerable back doors for attackers (Sweeney, n.d.).	7/10

Countermeasures:

To enhance Indonesia's National Data Centre and prevent future attacks, we could implement these countermeasures:

Improving Software and System Security:

- **Regular Software Updates and Patch Management**: Up-to-date software provides the latest security and software issue patches, decreasing the potential for vulnerabilities and software errors. The primary aim of patch management is to minimise vulnerability by regularly identifying, testing, and constantly installing software updates against weaknesses that an attacker could penetrate with.
- **Vulnerability scanning and penetration testing:** A vulnerability scan can prevent known weaknesses and security issues such as known malware, open ports, weak passwords, and misconfigured software or hardware (Anon., n.d.). Penetration testing helps identify weaknesses, simulate attacks, and find known and unknown vulnerabilities (Anon., n.d.).

Improving configuration and access control:

- **Implement multi-factor Authentication:** MFA on critical systems can help protect the organisation against brute-force attacks, even with the username and password (Kinza-Yasar, n.d.).
- **Strict access control policies:** Limit system access only based on the user's role and responsibilities, minimising access levels to the user's requirements and increasing security integrity (Anon., n.d.).

Improving Human Security Awareness:

- **Comprehensive security awareness training:** Educating employees about cybersecurity risks, including phishing and social engineering tactics, and how to respond and report decreases the chance of manipulation by an attacker (Anon., n.d.).
- **Phishing simulations and drills:** A phishing simulation helps identify vulnerabilities within employees and offer training, which helps close the vulnerabilities before an attacker does (Effect, 2023).

Develop and Test an Incident Response Plan:

- An incident response plan is a set of instructions for responding to an attack. It can help reduce an attack's financial and reputational damage and limit the amount of damage. Testing the plan with real-world attacks can additionally ensure that the team knows and can respond to an attack promptly and correctly (Kirvan, 2024).

Threat Detection and Prevention:

- Threat detection works by monitoring network traffic, endpoints, user activity and applications by revealing suspicious activity. Physical threat detection products automatically monitor traffic patterns, system logs, suspicious files, user access attempts and other trends. Having adequate threat detection is crucial as it aims to block potential entry points into the database (Sweeney, n.d.).

Table of Contents