Virus Infection: Incident Response Plan (Group 2)

**Description:** A manufacturing company's network is infected with a virus, spreading rapidly across multiple systems and disrupting production operations. The infection is initiated when an employee unknowingly opens an infected email attachment or visits a compromised website.

**Objective:** Respond to the virus infection, identify infected systems, contain the spread of malware, eradicate the virus , restore affected systems from backups, and enhance network security measures to prevent future infections.

Preparation

Actions:

* Call all of the Member of the team
* Conduct Training for the employees Educate the Employees about viruses and email and also in webrowsing security
* Gather Information about the incident
* Be ready for some issues and and think of an effective solution for the Virus

Identification

Actions:

∙ SOC Team Tasks and Responsibilities

* Analyze the initial user report detailing the virus infection. Understand the specific details, such as the infected email attachment or compromised website, the nature of the disruption to production operations, and any error messages or symptoms reported.
* Gather system logs, network traffic data, and security event logs to identify the source and extent of the virus infection. Take system snapshots of affected systems to capture the state of the infection for analysis.
* Determine which systems are affected by the virus and to what extent. Evaluate the potential impact on production operations, data integrity, and network security.

∙ Security Engineering Team Tasks and Responsibilities

* Analyze the collected data to understand the behavior of the virus, including how it spreads, what actions it performs on infected systems, and any communication with external servers.
* Determine how the virus initially entered the network, focusing on the infected email attachment and compromised website. Identify any other potential infection vectors that may have contributed to the spread of the virus.
* Map out all infected systems and create a comprehensive list of compromised machines, including servers, workstations, and any other networked devices. Use antivirus and endpoint detection tools to identify signs of infection across the network.
* Assess the overall security posture of the network to identify vulnerabilities and weaknesses that the virus exploited. Document any deficiencies in security measures, such as outdated antivirus definitions, unpatched systems, or inadequate email filtering.

Containment:

* Implement temporary controls or measures to contain the spread of the virus and minimize its impact on other systems and operations.
* Isolate infected systems from the network to prevent further spread.
* Review and revoke any unauthorized access privileges or permissions associated with compromised user accounts or systems.

Eradication

* Conduct a comprehensive study of the virus's infection to determine its origin, behavior, and potential effects on the network.
* Complete scans of all infected computers for malware and remove any suspicious software or payloads.
* Describe and rectify any loopholes or weaknesses in security that facilitated the initial infection with the virus and unauthorized access to the network.

Recovery

Action:

Forensic Team

* Restore any affected data and ensure backups are clean and free from malware before restoration.
* Reconfigure the affected system and data and Identify the patch vulnerabilities that allowed the infection to occur in software and systems.

Lesson Learned:

* Eliminate the virus entirely, protect the network from additional dangers, and regrow normal operations within the manufacturing company.
* Enhance Security always Enhance and update your security and identify Then Weaknesses of the system to fix it early
* Provide additional training and awareness programs to enhance employees' understanding of cybersecurity threats and incident response protocols.
* Conduct a post-incident meeting to discuss findings, insights, and improvements with the Incident Response Team and relevant stakeholders.
* Develop and implement a plan for ongoing security improvements and incident prevention measures.