The Incident Report Summary

Student Name

Instructor

Course

Date

The Incident Report

Below is a network latency and sluggishness incident report on the Pro-Engineer application conducted on 13 December 2023. The security team investigated the incident, and the compromised system is the WIN-6JNN6RLT6IL, hosting the Pro-Engineer application. The security found that the malicious software miner.exe was installed on the system, causing high CPU utilization and network latency.

The security team responded to the incident by terminating the malicious process, restoring the antivirus functionality, and updating firewall policies. They also blocked the unauthorized outgoing traffic to the compromised port.

The attack incident occurrence

The attack incident was reported at 10:00 a.m.; by 5:30 p.m., the attack had been fully mitigated, and the system was returned to work. At 10:00 a.m., Maya Patel reported network latency and sluggishness in the Pro-Engineer application; at 3:14 p.m. and 3:20 p.m., Diego Martin and Alex Lee reported network latency and sluggishness, respectively. At 3:30 p.m., the security team is notified of the incident and starts their investigation. At 4:00 p.m., the security team identified the system and began remediation by 5:00 p.m. They successfully removed the malicious software and installed security patches into the system. At 5:30 p.m., all the impacted systems had been returned to work.

The attack compromised the Pro-Engineer system, executing a Denial of Service attack over the internet. The incident slowed down the system application, showing a high functional impact, hence the need for incident response priority.

Lessons learned

The above incident report displays the importance of an incident response team in an organization. The incident response team is responsible for:

1. **Detect**

   In the report, we identify the hostname of the Impacted System(s) as WIN-6JNN6RLT6IL, the IP Address of the Impacted System(s) as 10.10.20.10, and the Operating System of the Impacted System(s): Microsoft Windows Server 2019 Standard, this helps in detecting a cyberattack incident.

2. Investigate

The team can investigate the destination Port of Malicious Traffic: port 3333

Other observations to consider

High CPU utilization signals the possibility of a cyber-attack. The remote network connections to unknown IP addresses signal to the security team the potential unauthorized access into the network, and an email phishing attempt warns the company against a potential cyberattack.

Actions to restore Network Security

The security team blocks suspicious IP addresses, reviews the firewall rules, and implements network monitoring tools to ensure no network intrusion (Pearlson et al., 2022). The incident report shows the significance of implementing email security measures and the need to schedule updates of security patches.

Reference

Pearlson, K., Thorson, B., Madnick, S., & Coden, M. (2021). Cyberattacks are inevitable. Is your company prepared? Harv Bus Rev.