Company Case Study: Luigi's

A Luigi's Inc. employee brought a personal laptop into the facility infected (albeit unknowingly) with PSL and connected it to the corporate network via a wireless access point (AP). The system obtained an IP Address using Dynamic Host Configuration Protocol (DHCP) address provided by the core corporate network services. Upon connection, the infected system made an Internet connection to the command-and-control server.

Once connected, the threat actor provided the command for the system to scan the local network for available services. While the user noticed that the machine was running slowly, it was late on Friday before a three-day weekend. The user left the machine powered on with plans to look at it again on Tuesday. The scan identified an open File Transfer Protocol (FTP) service on the internal network that allowed anonymous access. The threat actor, still using the compromised machine, logged into the FTP server, compressed the contents and then transferred the data to the control server (over the internet) using an encrypted outbound VPN connection.

Over the weekend, the Network Operations Center (NOC) tracked a large amount of data over an encrypted channel. While they were able to identify both the source and destination, without the encryption keys, they were unable to decrypt the traffic to identify the content. The destination was not on the current list of known malicious sites (the list was out of date by four months). The help desk technician then opened a work ticket for the local desktop services to investigate.

Early Tuesday morning the user noticed that the machine was still acting erratically, even after a reboot. The user then called the help desk to open a ticket. The help desk technician was able to tie IP address of this machine to the traffic identified over the weekend. When the desktop technician arrived, it was determined that the machine in question is not a corporate machine and does not have all the standard protection software. A quick scan using a boot time tool found the PSL signature. At this point, the technician confiscated the machine for forensic investigation and the ticket was closed.

The forensics team determined a known malware tool named PSL compromised the machine. They also found a temporary file, left over by the scanning, that included the directory listing of the FTP site. Many of the folders within the directory were named after previous high-value programs. These files included parts lists, price quotes and even proprietary drawings. Included in the information were patents from the current Chief Executive Officer (Ms. J. Rabbit) as well as legal documents describing the purchasing and legal aspects of these programs.

Clearly state all of the issues that need to be addressed at Luigi's. (How did the attack occur?)

- **Unauthorized Device –** An employee's personal device was being used within the workplace without proper security implementations. It then got infected while being on the corporate network. There was no policy or mechanism in place to prevent a personal or unauthorized device from connecting to the company's network.
- **Insecurely Configured Services –** Having an FTP server which allows anonymous access is an extreme risk. This exposes sensitive data and was used in this attack to steal data critical to the company.
- **Outdated Threat Detection –** With outdated threat detection the destination of the encrypted data wasn't flagged. This is due to the malicious site list not getting updated to include all malicious sites.
- **Delayed Detection and Response –** The user who was experiencing issues with the device waited to report it to staff days later. The employee may not have been security aware, which may have caused the lack of communication.

Which CIS Controls v8 could have helped to prevent the attack that is detailed in the case study? (Why is the Control Important?)

List the Safeguards for each of the Controls, that should have been implemented to prevent the attack. (Why is the Safeguard Important?)

- **Control 1:** Inventory and Control of Enterprise Assets
    - This control helps ensure that all devices connected to the network are authorized. This prevents unknown or infected devices from gaining access to the network.
    - **Safeguard 1.1:** Establish and Maintain Detailed Enterprise Asset Inventory
        - In this scenario, being able to detect a device that wasn't part of the enterprise could have helped detect the vulnerability sooner.
    - **Safeguard 1.2:** Address Unauthorized Assets
        - Once the unauthorized asset was discovered, making sure it hasn't been taken advantage of yet is extremely important. Then remove it from the company's network completely.
    - **Safeguard 1.4:** Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory
        - Having better DHCP logging could have prevented the unknown asset from getting an IP address. If the device was not assigned an IP address, it wouldn't have access to the network preventing this issue.

- **Control 2:** Inventory and Control of Software Assets
    - This control helps ensure that only authorized software is installed and operating within the organization. Overall, it prevents unauthorized or malicious software from being executed within the organizations network.
    - **Safeguard 2.1:** Establish and Maintain a Software Inventory
        - Establishing and maintaining an accurate inventory of all software allows the organization to identify unauthorized or malicious applications that may introduce vulnerabilities much quicker.
    - **Safeguard 2.3:** Address Unauthorized Software
        - Ensuring that only authorized software is installed and preventing the use of software that may introduce vulnerabilities would help prevent issues such as the one in the case study.

- **Control 3:** Data Protection
    - This control helps ensure that sensitive data is protected through processes and technical controls. This will help prevent unauthorized access or exploitation
  - **Safeguard 3.6:** Encrypt Data on End-User Devices
    - Encrypting sensitive data stored on devices ensures that, even if compromised, the data cannot be easily accessed without first being decrypted.
  - **Safeguard 3.10:** Encrypt Sensitive Data in Transit
    - Encrypting data in transit prevents data exfiltration as when the data was transferred over the VPN tunnel it would have been encrypted.

- **Control 4:** Secure Configuration of Enterprise Assets and Software
    - This control is extremely important as not having securely configured systems can allow attackers to easily gain access and steal critical information.
  - **Safeguard 4.7:** Manage Default Accounts on Enterprise Assets and Software
    - Securing or disabling default accounts is extremely important as it minimizes the risk of attackers exploiting them. Default account information is common knowledge to attackers.
  - **Safeguard 4.**8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software

- **Control 6:** Access Control Management
    - This control focuses on identifying and addressing vulnerabilities with account privilege, zero trust, and least privilege. Overall, ensuring that all sensitive data is not accessible to just anyone.
  - **Safeguard 6.3:** Require MFA for Externally Exposed Applications
    - Having MFA for remote access is extremely important due to the nature of remote access. With the ability to access the system from anywhere having this extra safeguard ensures it is the trusted person accessing the system.

- **Control 7:** Continuous Vulnerability Management
    - This control ensures that there is a focus on identifying and addressing vulnerabilities proactively. Identifying these vulnerabilities early allows for fast patching not giving adversaries the chance to take advantage of these vulnerabilities.
  - **Safeguard 7.1:** Establish and Maintain a Vulnerability Management Process
    - Having regular scans can help identify vulnerabilities early and prevent adversaries from having the opportunity to take advantage of them. This can prevent major breaches such as the one in the case study.

- **Control 8:** Audit Log Management
    - Having detailed log management can help detect issues when they arise which helps ensure fast mitigation of attacks. It can also help us understand what attacks occur most within the organization.
  - **Safeguard 8.11:** Conduct Audit Log Reviews
    - Being on top of the logs is vital to having a fast remediation process. Some logs that come through will be false positives although fishing through those to find real breaches is extremely important.

- **Control 10:** Malware Defenses
    - Ensuring that proper virus protection is in place to detect malware and mitigate it quickly is essential to prevent many major attacks which could include exfiltration, ransomware, and more.
  - **Safeguard 10.1:** Deploy and Maintain Anti-Malware Software
    - Ensuring that all devices have a Anti-Malware software on it before it is allowed to interact with the network is extremely important. If this was in place it could have prevented a unauthorized device from connecting to the network causing this breach.

- **Control 14:** Security Awareness and Skills Training
    - The first point of contact about any attack is your employees and staff. It is critical that they are aware of common attacks and understand the reporting process in place.

- **Safeguard 14.6:** Train Workforce Members on Recognizing and Reporting Security Incidents
    - Teaching workforce members on how to recognize and report security incidents could have prevented the breach in this case study. Having a direct and comfortable way for staff to report security incidents can help prevent breaches earlier preventing prolonged damage.