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) addressing 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 The destination was not on the current list of known malicious sites (the list was out of date by four months).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.

1. **Clearly state all of the issues that need to be addressed at Luigi's.**

    - A device was connected to the server without permission. An employee from Luigi's brought in their own personal laptop and used it on the corporate network. This shows that either a) there are no guidelines in place for outside devices on the network or b) these guidelines are not enforced.

    - By allowing a random laptop on the network (that, according to the case study, seems to be a fairly open network), it is apparent that access control is a problem. Least privilege should be instituted on the network.

    - Said laptop was infected with malware (PSL, to be more specific) that was allowed to connect to Luigi's network without any endpoint protection. This allowed the network to be infected with the malware as well. This malware also extracted sensitve data on a VPN and an encrypted channel through an open FTP. This led to data loss.

    - The user noticed that the computer was running slow both on the day that it was (unknowingly) infected and two days later. It was not until then that he called the help desk. This delayed responded very well could have caused additional issues.

    - For lack of a better term, the user was ignorant to attach a personal device to the network and Luigi's was ignorant to allow such events to happen. This shows a lack of simple awareness and training on basic cybersecurity.

2. **Which CIS Controls v8 could have helped to prevent the attack that is detailed in the case study?**

    - ***CIS Control 1: Inventory and Control of Enterprise Assets***
        - By keeping a thorough inventory of enterprise assets (the hardware, essentially speaking) Luigi's would be able to know what is and is not allowed on their network. This includes the laptop that the user brought without permission.

    - ***CIS Control 2: Inventory and Control of Software Assets***
        - The same thought process applies for CIS Control 2 as it did for CIS Control 1. Luigi's should have a running audit of what software is and is not allowed on the network that should be extensively monitored. That way, the PSL would have been noticed much sooner.

- ***CIS Control 3: Data Protection***
    - Any sensitive data should be held to known standards (such as PCI DSS for credit card standards). All data that is stored on Luigi's network should be classified and protected accordingly, thus mitigating extraction attempts.

- ***CIS Control 4: Secure Configuration of Enterprise Assets and Software***
    - While keeping an inventory on both hardware and software is important, it's also important to make sure that Luigi's assets are both secure and "locked down" in case of cyberattacks mentioned in the case study.

- ***CIS Control 5: Account Management***
    - With account management in place, the user who works at Luigi's would have to sign in using their username and password. This would potentially - and hopefully - happen on an approved device, thus making sure that only approved accounts are allowed to access the network in a particular fashion through trusted endpoints.

- ***CIS Control 6: Access Control Management***
    - While "Account Management" and "Access Control Management" sound similar, there is a difference in scope. While everyone at Luigi's needs an account, the access to everything on the data should be limited to least privilege. If this had been implemented, the attack through the PSL could have been mitigated.

- ***CIS Control 7: Continuous Vulnerability Management***
    - Every asset - whether it is software, hardware, part of the network, etc - has some form of weakness. A system at Luigi's should have been put in place to recognize and mitigate these weaknesses, thus lessening or completely illuminating the PSL attack.

- ***CIS Control 10: Malware Defenses***
    - Malware defenses are an integral part of vulnerability management. Items such as antivirus software and malware sandboxing systems should be put in place. With these items, attacks such as the ones mentioned in the case study can be avoided.

- ***CIS Control 11: Data Recovery***
    - As the attack was (unfortunately for Luigi's) a success, it is important that they have a plan to recover all of the stolen data that they are now missing. A backup of all sensitive information should be on hand, ready to be restored.

- ***CIS Control 14: Security Awareness and Skills Training***
    - The first line of defense should have been the employer who (unbeknownst to him) started the issue. If there was security awareness and training taking place at Luigi's, the employees would have been aware of attacks like phishing, social engineering, and the importance of keeping unauthorized devices off of the network.

- ***CIS Control 18: Penetration Testing***
    - A proactive approach to mitigating cyberattacks (as opposed to a reactive approach - which is what it seems happened with Luigi's) is essential to mitigating cyberattacks.

3. **List the Safeguards for each of the Controls that are listed in question 2, that should have been implemented to prevent the attack.**

    - ***CIS Control 1: Inventory and Control of Enterprise Assets***
        - ***Safeguard 1.1: Establish and Maintain Detailed Enterprise Asset Inventory:*** First and foremost, having an inventory of all devices (hardware, software, network, etc) would help mitigate attacks like this for Luigi's. Knowing what should and should not be on the network and tracking this thoroughly would help - at the very least, it would keep tabs on unauthorized devices such as the user's computer.
        - ***Safeguard 1.2: Address Unauthorized Assets:*** Let's be very clear - while "keeping tabs" is a good start, it is not enough. Policies should be in place that would address instances where unauthorized devices such as this laptop. This would stop the data breach and malware attack before it even started.
        - ***Safeguard 1.3: Utilize an Active Discovery Tool:*** Setting up these policies and procedures to mitigate unauthorized assets can be daunting. Thus, having an active discovery tool such as NinjaOne may be very beneficial for Luigi's.

    - ***CIS Control 2: Inventory and Control of Software Assets***
        - ***Safeguard 2.1: Establish and Maintain a Software Inventory:*** Luigi's should have a listing of all software that they use. This software should be licensed and registered. That way, Luigi's would know for certain what unauthorized software (such as the malware in the case study) is on the network.
        - ***Safeguard 2.3: Address Unauthorized Software:*** When unauthorized software is on the network (such as the malware), Luigi's should have a system in place that will address it. This should mitigate malicious attacks before they even begin.

- ***Safeguard 2.4: Utilize Automated Software Inventory Tools:*** An automated software inventory tool such as ManageEngine would be of great benefit to Luigi's. Not only would it keep the store up to date, but it would make the inventory process slim and well organized, thus saving Luigi's time and money.
- ***Safeguard 2.5: Allowlist Authorized Software:*** Similar to automated software inventory tools, having an allowlist that authorizes or denies software automatically (again, akin to what ManageEngine can do) would help streamline Luigi's efforts.

- ***CIS Control 3: Data Protection***
  - ***Safeguard 3.1: Establish and Maintain a Data Management Process:*** When it comes to an establishment such as Luigi's, there is a lot of sensitive data that needs to be managed (and, as we have seen, has the potential to be stolen). A process should be created that handles the data - how sensitive it is, how to handle it, how to dispose of it when the time comes, etc. This will be some of the first steps when it comes to mitigating attacks on data.
  - **Safeguard 3.2: Establish and Maintain a Data Inventory:** Knowing the data is an integral part in protecting it. By keeping tabs on the data, Luigi's would be well aware of how sensitive each piece of it is and how to protect it.
  - ***Safeguard 3.3: Configure Data Access Control Lists:*** Having a user access to the network in such a way was (as we have seen) a mistake. Luigi needs access control with least privilege in place. This will be another aspect of defense that mitigate attacks by limiting what each particular user can do and have access to.
  - ***Safeguard 3.6: Encrypt Data on End-User Devices:*** Once our users are no longer allowed to use their own personal devices on the network, Luigi should still encrypt data on all devices that they have in inventory. This would allow an extra layer of security - even if the attacker got on the network, the data would still be inaccessible.
  - ***Safeguard 3.10: Encrypt Sensitive Data in Transit:*** Encryption is not only important on end-user devices. It is also important when data is going from device to device. Having this encryption in transit would protect the data from any sort of eavesdropping or interception from one place to the other.
  - ***Safeguard 3.11: Encrypt Sensitive Data at Rest:*** Encryption is crucial on user devices and during transit, but it is also crucial when data is at rest on a server. If an attacker was to have access to where the data is stored, keeping it encrypted would add an extra layer of protection.

        - ***Safeguard 3.12: Segment Data Processing and Storage Based on Sensitivity:*** It appears as if Luigi's had all of their data in one location, which made it easier for the attacker to access it. Having their data (especially their most sensitive data) segregated on separate servers would allow for an extra layer of protection that it seems like Luigi's needed.

- ***CIS Control 4: Secure Configuration of Enterprise Assets and Software***
    - ***Safeguard 4.1: Establish and Maintain a Secure Configuration Process:*** The case study proves that there isn't a process to "lock down" any of Luigi's assets. Luigi's needs to create this process to ensure that their hardware, software, and their network is secure and safe from cybersecurity threats. These processes and procedures need to be tested at least every six months to ensure security.
    - ***Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets:*** According to the case study, it seemed like the laptop was allowed to run continuously over three days. Having an automatic locking session (such as locking the computer after 15 minutes of inactivity, for example) may have helped mitigate some of the attack.
    - ***Safeguard 4.5: Implement and Manage a Firewall on End-User Devices:*** While session locking is important, it is not a sure fire way to stop attacks. Once the attacker is in the network, session locking is of very little to no help. Thus, having firewalls in place that have default deny rules in place could help mitigate the damage done to an attack surface by limiting where the attacker can go in the network.
    - ***Safeguard 4.7: Manage Default Accounts on Enterprise Assets and Software:*** Many assets (such certain software or routers) have default usernames and passwords that are easily accessible with a Google search. If Luigi's changed the usernames and passwords, it could assist in the prevention of a cyber attack.
    - ***Safeguard 4.8: Uninstall or Disable Unnecessary Services on Enterprise Assets and Software:*** Various software and other assets have services and features that are unnecessary, particularly to Luigi's business in this case study. If Luigi's disabled these services and features, it would minimize the attack surface and help limit how the attacker can access the network.

- ***CIS Control 5: Account Management***
    - ***Safeguard 5.2: Use Unique Passwords:*** Once we have established that only authorized users with authorized devices are allowed on the network, it is essential that all accounts use unique passwords (preferably with MFA). By using passwords that are hard to guess, the attacker would have a hard time getting on the network and causing data breaches (again, it would be extra challenging with MFA installed as well).

- ***Safeguard 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts:*** To retirate, least privilege should be established. Having too many accounts enabled with too many permissions (whether it be through scope creep or any other lack of cybersecurity awareness) is detrimental to Luigi's. As proven, it allows attackers to have too much access to the network.
- ***Safeguard 5.6: Centralize Account Management***: If Luigi's had a centralized account management system, this would provide consistency for all users when it comes to lockouts, password length and complexity, etc. This would further help mitigate attacks by making sure all users were uniform in their account management practices.

- ***CIS Control 6: Access Control Management***
  - ***Safeguard 6.1: Establish an Access Granting Process:*** While keeping least privilege in mind, an access granting process needs to be uniformly accepted for all employees of Luigi's. This would help mitigate access that is unauthorized. This process can be done automatically.
  - ***Safeguard 6.2: Establish an Access Revoking Process:*** Accordingly, an access revoking process needs to be in place at Luigi's, as well. This can take place when an individual leaves or changes their position (which would avoid scope creep). This allows for protection from insider threats and any other access that is not authorized.
  - ***Safeguard 6.3: Require MFA for Externally-Exposed Applications:*** MFA (otherwise known as multi-factor authentication) has been previously discussed in this case study. Requiring MFA for externally exposed applications could mitigate the risk of unauthorized access, which would have prevented this attack.
  - ***Safeguard 6.4: Require MFA for Remote Network Access:*** As previously stated, having multi-factor authentication turned on is extremely important. This is also true for remote network access (if this form of access is needed at Luigi's). Have MFA turned on for this could have stopped the attack from the word go, seeing as the attacker was not in the physical location.
  - ***Safeguard 6.5: Require MFA for Administrative Access:*** It is probably becoming apparent that multi-factor authentication is important for Luigi's, but it must be said that having additional MFA for administrative access allows for better control and protection. With this in place, parts of the network would be inaccessible for the attacker if he was able to get on in the first place.

- ***CIS Control 7: Continuous Vulnerability Management***
    - ***Safeguard 7.1: Establish and Maintain a Vulnerability Management Process:*** Luigi's would benefit from making sure they know what their vulnerabilities are through a vulnerability management process. It would also benefit them to prioritize their vulnerabilities by risk. This vulnerability management system should cover all of Luigi's assets.
    - ***Safeguard 7.2: Establish and Maintain a Remediation Process:*** Once a vulnerability management process has been established, a remediation process to counteract said vulnerabilities should be put in place as well. This will further establish a plan that Luigi's has in case they are ever attacked.
    - ***Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:*** Part of vulnerability management and remediation process should include vulnerability scans of all internal servers, devices, and other assets that Luigi's has in their inventory. This will help keep Luigi's "on guard" against any threats or attackers.
    - ***Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets:*** In the same manner that internal assets are scanned for vulnerabilities, external-exposed assets (such as servers that are public facing) should be scanned as well. This will allow for a holistic approach in vulnerability management.

- ***CIS Control 10: Malware Defenses***
    - ***Safeguard 10.1: Deploy and Maintain Anti-Malware Software:*** Anti-Malware software is imperative to have for any establishment that has any part of their business online. As is shown in the case study, this is especially true for Luigi's. With anti-malware software established, there may have been a good chance that the PSL malware would have been detected and quarantined before it did any major damage.
    - ***Safeguard 10.2: Configure Automatic Anti-Malware Signature Updates:*** Anti-Malware software is important. But if the software becomes out of date, it is essentially useless very quickly. New malware threats happen all of the time. It is essential to keep the software up to dte to catch them.
    - ***Safeguard 10.6: Centrally Manage Anti-Malware Software:*** Simply put, the anti-malware software should be managed from one central location and should be used across all assets evenly. This creates a uniform approach to anti-malware services for Luigi's.

- ***CIS Control 11: Data Recovery***
  - ***Safeguard 11.1: Establish and Maintain a Data Recovery Process:*** Even if Luigi's had everything in place, data loss, corruption, attacks, and breaches can still happen. There should be a clear process in place for recovery that is easily understandable in the unfortunate event that data is destroyed or stolen.
  - ***Safeguard 11.2: Perform Automated Backups:*** As part of the data recovery process, automated backups of all the data should be performed. These backups should take place often - preferably every week. That way, data can be restored quickly in case of an attack such as the one in the case study.
  - ***Safeguard 11.5: Test Data Recovery:*** The data recovery process can have its own issues and may not work as well as Luigi's needs it to. Thus, the process should be tested every three months to ensure that it is in working order.

- ***CIS Control 14: Security Awareness and Skills Training***
  - ***Safeguard 14.1: Establish and Maintain a Security Awareness Program:*** Employees can not be held responsible for what they don't know. It is Luigi's responsibility to train them on all security measures needed to prevent attacks such as the one in the case study.
  - ***Safeguard 14.2: Train Workforce Members to Recognize Social Engineering Attacks:*** While the case study does not explicitly state it, the user may have received the malware through a social engineering attack such as phishing with the attacker knowing that they connect their device to Luigi's network. Having the users trained on recognizing social engineering attacks would be beneficial to the company.
  - ***Safeguard 14.4: Train Workforce on Data Handling Best Practices:*** As mentioned before, the data needs to be inventoried and categorized based on sensitivity. With that in mind, users of the data need to be trained on handling the data based on the sensitivity level. Once they are trained, this should help in mitigating attacks and data breaches.
  - ***Safeguard 14.6: Train Workforce Members on Recognizing and Reporting Security Incidents:*** The user should have noticed that there was an issue as soon as he noticed that the machine was slow on Friday. By reporting it quickly, the attack may not have happened over three days. Thus, employers of Luigi's should have training to feel empowered to report these types of instances.
  - ***Safeguard 14.8: Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks:*** While it is obvious by reading the case study that connecting to the network from an external device was wrong, it is not fair to assume that all users are tech savvy enough to recognize this mistake. Thus, they should be trained on how connecting external devices may cause nefarious attacks.

- ***CIS Control 18: Penetration Testing***
    - ***Safeguard 18.1: Establish and Maintain a Penetration Testing Program:*** By creating a penetration program (possibly with a third party vendor) that focuses on where Luigi's is and where they should be in terms of security, they can begin to be aware of their vulnerabilities and what should be done about them.
    - ***Safeguard 18.2: Perform Periodic External Penetration Tests:*** Once a penetration program is established, periodic penetration tests should be established. This will provide a "real world" example of their vulnerabilities that were previously mentioned.
    - ***Safeguard 18.3: Remediate Penetration Test Findings:*** Simply knowing what the vulnerabilities are will not necessarily help Luigi's. Once they are known, there should be a plan to remediate them in case of a real world attack.