Cybersecurity: How to defend against potential threats

B.Sc. (Honours) in Instrument Engineering

Department of Physical Sciences

Kayleigh Dennehy

Dr. Stephen Hegarty

Background: Literature Review

What is a Cybersecurity attack?

A Cybersecurity attack is a threat on any organization that involves targeting their computer information systems, personal computers, infrastructures and or computer networks.

Types of Cybersecurity Attacks

In the last few years, Cybersecurity attack's have become more and more sophisticated. It is believed that a cybersecurity attack occurs every 14 seconds.[3] These cyber security attacks can take the form of the following:

- Malware attack– It is a malicious software that is unwanted and has been installed onto a system without consent. The most common type of malware is known as ransomware. This is when hackers steal sensitive data and or blocks the access to the data. The hackers will not release the data back and will use it as leverage in return to a sum of money being paid.. [1]
- Password Attack – Access to a password can be done by using social engineering, searching a persons desk and or just guessing the password. The most common type of password attack is known as brute force. This is when passwords are entirely guessed but can have some logic applied to it by studying the user i.e. finding out their hobbies, pets name, family member names, birthday etc and using these as possible passwords until one is correct. [1]

Cyber Security Attacks: Real World Examples

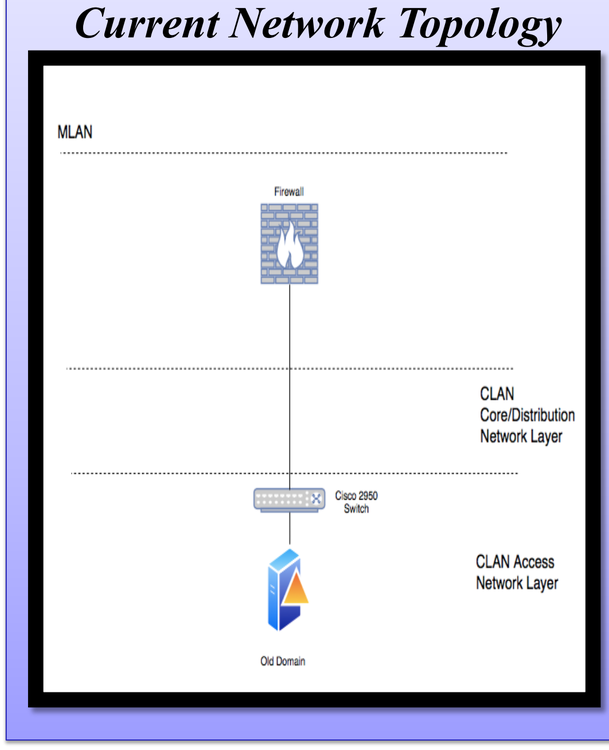
- Merck Cyberattack 2017 - NotPeyta - Crypto ransomware attack on the computers that run Microsoft windows operating systems. It blocks users from accessing their files until a lump sum in bitcoin is paid. This attack cost Merck $670 million. 4]
- NHS Hospitals May 2017 - WannaCry - Crypto ransomware attack on the computers that run Microsoft windows operating systems. It caused ambulances to be re routed leaving patients who required emergency care in need and 19,000 medical appointments were cancelled costing the NHS £92 million. [6]
- Iran Natanz - Stuxnet – Malware attack that was a worm that travelled on USB sticks and infected computers that it had access too. This virus attacked PLC computers in Natanz Uranium enrichment facility and destroyed centrifuges causing them to burn out. It ruined a fifth of their centrifuge's [7]

Introduction and Project Goal

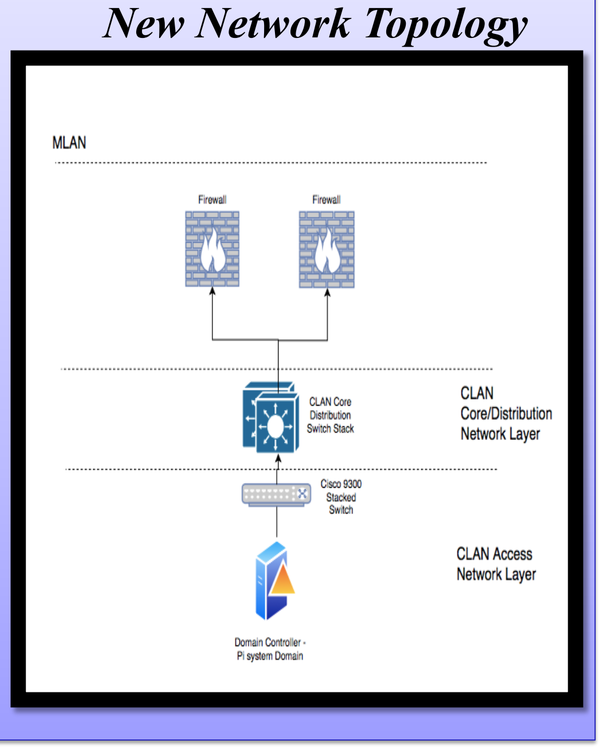
The goal of this project is to remediate against potential cybersecurity threats by upgrading and or removing assets on the network that currently reduce security at a cork based site.

The project will focus on upgrading the sites Automation system's support network infrastructure, Evaluate the DeltaV cybersecurity solutions that's provided by Emerson and also plan changeover from old firewalls to new firewalls on the system during normal

Current Network Topology



New Network Topology



A new domain controller will be configured onto a network infrastructure that will control the traffic that flows on the network that contains sensitive data that is stored in the data historian for the Cork site. A new domain will be created along with security policies for each active directory on the new domain.

A new and upgraded firewall will be placed into the network infrastructure architecture along with a new switch. These are being upgraded as new technology trends and or policies have evolved and expand the range of the current hardware that sits on the current network.

Conclusion: How to mitigate the risks of a Cybersecurity Attack

- Ensure all computer systems and or IT systems that involve hardware and software are monitored and start with the basics of having complicated passwords to ensure security within the network.[2]
- Secure organizational data with the aid of encryption [2]
- Introduce strict security policies i.e. Forbid USB keys. [2]
- Explore the option of implementing cybersecurity Insurance and cybersecurity solutions i.e. In case of ransomware.[2]
- Ensure adequate company training that will guide them to becoming aware of the vulnerabilities that will involve gaining access to company data i.e. How to avoid phishing emails [2]

References

[1] Compliance, S. and Attacks, T., 2021. Top 10 Most Common Types of Cyber Attacks. [online] Blog.netwrix.com. Available at: <https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/> [Accessed 16 April 2021].

[2] Datta, S., 2021. The grim reality of cyberattacks: How to mitigate the risks? | ITProPortal. [online] Itproportal.com. Available at: <https://www.itproportal.com/amp/features/the-grim-reality-of-cyberattacks-how-to-mitigate-the-risks/> [Accessed 16 April 2021].

[3] Builtin.com. 2021. What Is Cybersecurity? Why Is It Important? | Built In. [online] Available at: <https://builtin.com/cybersecurity> [Accessed 3 February 2021].

[4] Drug Development and Delivery. 2021. CYBERSECURITY - Why Pharmaceutical Companies Are Vulnerable to Cyberattacks & What You Can Do to Protect Your Company. [online] Available at: <https://drug-dev.com/cybersecurity-why-pharmaceutical-companies-are-vulnerable-to-cyberattacks-what-you-can-do-to-protect-your-company/> [Accessed 3 February 2021].

[5] Mcafee.com. 2021. What Is Stuxnet? | McAfee. [online] Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html> [Accessed 19 April 2021].

[6] www.kaspersky.com. 2021. What is WannaCry ransomware?. [online] Available at: <https://www.kaspersky.com/resource-center/threats/> [Accessed 19 April 2021]. ransomware-WannaCry

[7] Mcafee.com. 2021. What Is Stuxnet? | McAfee. [online] Available at: <https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html> [Accessed 19 April 2021].