Bellevue University

Eric Wellmaker

M11 Written Assignment

CYBR515: Security Arch & Design

May 26th, 2022

Utilizing a network whether it be home or business needs safety protocols in place to prevent a security breach. From Milestone 1 project, J&L Coffee, a fictitious company that suffered from a breach in security. In this essay, I will give my final architectural design utilizing the security protocols that were learned throughout course. I will discuss how zero trust will be implemented into J&L Coffee framework design, how the updated architecture thwarts threats and explain how compliance addresses vulnerabilities while using a SaaS (Software as a service) framework. In the next section, I will discuss ZTNA (Zero Trust Network Access) and how I implemented into J&L Coffee security network.

Approaching Zero Trust Architecture

Zero Trust Network Access automatically assumes that all aspects of a digital world that utilizes a platform to transmit and receive data are considered untrustworthy. ZTNA is a source that monitors data transmission between users in real time while having protocols in place to limit access to servers, networks, etc. (Embracing a Zero Trust Security Model, 2021). NIST Special Publication 800-207 mentions three core components which are policy engine (PE) which grants or deny access to data and resources. Policy administrator (PA) and Policy enforcement point (PEP) while similar have key differences. PA makes the determination to startup or shutdown communications between the source of information and the user. While PEP monitors connections between users and resources to determine whether to terminate the connection. (Rose, S. et al, 2020). PEP is a great example of Endpoint Threat Detection because it continually monitors users and resources.

Zero Trust would be fitting for J&L Coffee because the company deals with sensitive credit card data which is transmitted over company servers. Implementing Endpoint Initiated ZTNA on the 400 Dell Optiplex 3080 workstations, the office computers in the Off Campus Coffee Shops and the Virtual PC would stop unauthorized breaches because Endpoint Initiated ZTNA forces the end user to initiate access to the application, which in turn would be verified before access can be granted. Identity Governance would be implemented here as user management and access control is a direct result of utilizing ZTNA. I would also recommend using the Service Initiated ZTNA on both the 2 Point of Sale Computer Systems (Clover) and the File Transfer Protocol which is accessible from the home residence. Service Initiated ZTNA on the other hand, a third party completes the connection as long as the requestor is vetted with the provider before data can be transmitted (What Is a Zero Trust Network Architecture?, 2022). In the next section, I will discuss the updated architecture design and how potential threats can be mitigated.

Updated architecture and Threat Mitigation

It was previously identified that J&L Coffee had numerous shortfalls in their framework design. Here, I will discuss my updated architectural framework which I will present to the fictitious company based on a multi-tier management design. The first to be identified was password history, requirements and complexity were disabled. Sandy written down her credentials which were soon compromised and finally employees also documented their credentials around the workplace. As previously discussed in the beginning of this essay, I would utilize ZTNA as it would mitigate access and only allow entry when needed through an administrator. Next was their Aruba 7000 Mobility

Controller which was still configured with default parameters and no firewall being enabled. For the Aruba 7000 I would implement the use of a stateful inspection firewall which would only allow entry for packets that match the profile of entries from the outbound and inbound directory (Stallings, W., 2016). The other firewall I would use would be an application-level gateway which would be used on all internal firewalls throughout the J&L Coffee framework.

The Wireless system for J&L Coffee is configured with open access points so workers can BYOD (Bring Your Own Device). If J&L Coffee implemented a SaaS (Software as a service) network, then devices can connect via router to the internet/cloud over a secure network server (Stallings, W., 2016). Along with the BYOD and SaaS, the use of different public and private servers for webpage usage is just as important. For this, a DMZ network will be utilized which will house the DNS, web and email servers. The 802.11 or Wi-Fi routers will be configured by disabling the SSID broadcasting or the name that is displayed when searching for an 802.11 network to connect with. Changing the default passwords with the access point or AP and renaming the SSID so only employees can find and connect with the router. As for the public router, same rules apply but the SSID name will be changed more frequently. For the router configuration will be the WPA2 program under the Wi-Fi Alliance (Stallings, W., 2016). Lastly when dealing with 802.11 connections, a point-to-point tunneling protocol (PPTP) VPN should be used. PPTP routes network traffic over the unsecure internet (Point-to-Point Tunneling Protocol (PPTP)., 2022).

For email protection, it was previously identified that software updates were not being accomplished and firewall security appliance were configured to allow traffic in both directions. Utilizing a S/MIME (Secure/Multipurpose Internet Mail Extension) platform here would be a valid solution. S/MIME has four services which are authentication or verifying a digital signature for authenticity, confidentiality or content-encryption key, compression encrypts messages in any order and email compatibility which acts like a translator for the conversion of 8-bit binary stream to ASCII characters or Base64 conversion (Stallings, W., 2016). Along with S/MIME, symmetric encryption can be used here as it shares data between authorized users whose systems have the encryption and decryption keys (Symmetric Key Algorithm., n.d.).

The Virtual machines were not running antivirus software, so incorporating a SaaS network here would also mitigate software missing important updates and patches. File transfer protocol servers or FTP while increasing convenience of use also increases the likelihood of a security breach if measures are not implemented to prevent attack. In my final architecture design for the FTP, I opted to use both a Service Initiated ZTNA and a PPTP as routes network traffic over the unsecure internet.

It was identified that J&L Coffee was still using IPv4 on their network browsers. Upgrading to IPv6 and utilizing the current TLS version 1.2 will secure the web browsers while using the internet. The final shortfall was the credit card software from Clover was being processed through open networks. In my final design I implemented a PPTP protocol and a SaaS network to transmit the credit card data over the internet to the J&L Corporate HQ. In the final section, I will discuss whether compliance and monitoring will be successful in this network infrastructure.

Compliance and Monitoring. The network redesign addresses the vulnerabilities that were previously identified in the beginning of Milestone 1 assignment. The use of the security appliances will affect users' connectivity speed when they connect to the free Wi-Fi network that is secured using SaaS and PPTP. These security protocols job is to encrypt data that is transmitted and received over a secure network, so upload and download speeds on devices will be slightly affected. I've identified only one potential risk with this entire network design. SaaS is updated, patched, etc. through a third-party vendor. If their system has any discrepancies, then it would directly affect the customer being J&L Coffee Inc. and they would have to wait until all discrepancies are mitigated. As for the new design, I believe its technically sound as I addressed all discrepancies that were identified. When it comes to cost, having a secure network is important. Since J&L Coffee Inc. conducts transactions using customers credit card data, having a network design that will protect the customer and company is important. Like I previously mentioned, internet connectivity will be affected as this network infrastructure is designed on the security of data transmission. As for this new system, I would implement it because it has the necessary checks and balances required to conduct business with consumers.

The final network infrastructure design of J&L Coffee Inc. will reduce the likelihood of a security breach by implementing zero trust protocols in its organizational foundation. The updated architecture design mitigates the identified vulnerabilities while utilizing the internet from a SaaS network. Compliance was identified and was discovered that one vulnerability exists from the SaaS network itself. In my opinion, preparation and understanding from the employees of J&L Coffee Inc. will reduce the chances of a security breach.

References

Embracing a Zero Trust Security Model. (2021). National Security Agency. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Point-to-Point Tunneling Protocol (PPTP). (2022). Network Encyclopedia. https://networkencyclopedia.com/point-to-point-tunneling-protocol-pptp/

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Stallings, W. (2016). Network Security Essentials Applications and Standards (6th ed.).

Symmetric Key Algorithm. (n.d.). NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/symmetric_key_algorithm

What Is a Zero Trust Network Architecture? (2022). Zscaler. https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust-network-architecture