**CYBR515 Milestone 4b**

Alice Mace

Cybersecurity, Bellevue University

CYBR 515: Security Arch & Design

Professor Scott Christiansen

November 13, 2022

The J&L Coffee IT network has been modified to include additional security parameters and functions for greater capability and safety. New recommendations to policies and procedures will also be documented and an overview of system components and their functions in creating a Zero Trust Environment for J&L will be detailed. The associated diagram distinguishes these zero trust components in pink.

The most apparent addition the J&L’s network architecture is the addition of intrusion detection system (IDS) servers at both on and off campus locations. These will alert if a malicious or abnormal intrusion is detected to prompt the IT professionals to investigate and determine if an attack is occurring. The Software-as-a-Service (SaaS) provided by a third party has also added an IDS to notify of any threats coming from or going to the third-party provider servers. The internal IDS are for redundancy within the internal network, as it is possible for intrusions to generate from any point of entry to the network. Being alerted sooner is always better so that action can be taken in a timelier fashion to reduce potential damage. SaaS applications will also include email and secure messaging services, in addition to the distributed file sharing and data storage capabilities. This works in concert with the mail servers on campus and creates a record of all message traffic on the third-party servers. Previously we activated the firewall controls for the mobility controllers for wireless access points, but they will also be linked with the active directory servers to require users’ logon with their credentials before network access is granted.

Ensuring policies and procedures are in place is key to properly structuring an organization around security and knowing how to respond in the event of an attack. The implementation of Information Security Continuous Monitoring (ISCM) processes and instilling the risk management framework for all system architecture components is one step J&L should take to keep their systems and personnel functioning properly. A Computer Incident Response Team (CIRT) and CIRT plan should also be established which encompasses policies and procedures to follow in the event of an attack and identifies individual’s roles in the response. This team can quickly react to an attack and establishing a CIRT plan helps an organization focus on the critical business functions and restoration of those services first. Another key piece of data that will be recorded on J&L’s servers are auditing records. This helps to establish when, where, and how an attack took place or a virus entered the system. It is also critical when addressing an insider threat concern and being able to track back to an individual based on their login credentials who may be responsible. Companywide compliance and monitoring are necessary components to a successful security architecture and must be enforced through policy and leadership, even when not convenient.

Zero Trust is assuming that there is already a breach in all networks and requires authentication of all files, emails, and access. NIST explains that “Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary.” Each of the following briefly describe the component’s role in establishing the zero trust network for J&L. Firewalls, both on and off campus, scan for potential threats based on the configuration implemented by the IT staff and do not permit traffic in or out if it does not adhere to secure parameters. IDS, both on and off campus, actively monitor for intrusions and alert IT staff to potential risks to the network. The Barracuda servers acts as an additional protection for email traffic and functions similar to a firewall in this instance. The email server assists in credential verification and encryption/decryption processes to ensure message traffic is coming from the intended sender and has not been altered. The active directory servers constantly verify credentials of all traffic from users and do not allow activity on the network if the user is not registered and using proper credentials to login. The wireless access controller works in complement with the active directory requiring login before network access is granted. These components reflect aspects of a zero trust environment and instill multiple checks on all data and network traffic.

References:

Gibson, D., & Igonor, A. (2020). Managing Risk in Information Systems (Information Systems Security & Assurance) (3rd ed.). Jones & Bartlett Learning.

National Security Agency. (2021, February). *Embracing a Zero Trust Security Model*. Media Defense. https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI\_EMBRACING\_ZT\_SECURITY\_MODEL\_UOO115131-21.PDF

Stallings, W. (2016b, July 28). *Network Security Essentials: Applications and Standards* (6th ed.). Pearson.