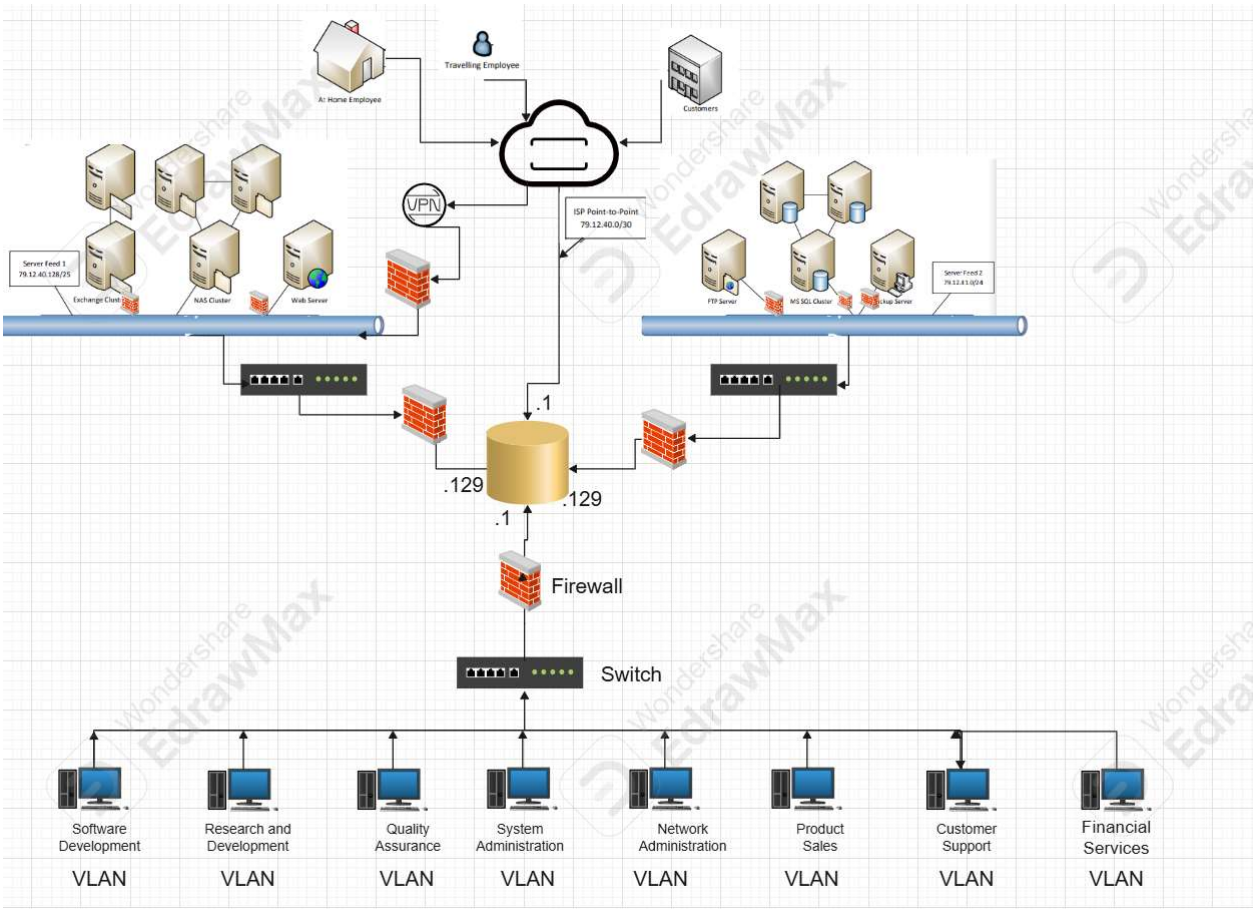
Project 4: Security Design

Alexis Fenderson

Logical Network Design



Security Implementation:

Risk 1: Lack of internal network segmentation

Problem: (co-mingling of internal and external servers on the same network)

Solution: A lack of internal network segmentation increases the risk of cybersecurity incidents since all devices share the same network. As such, if one aspect of the network is breached, that threat has access to all the other devices and information on the network. This is a high risk for the company that can be mitigated by implementing the following:

1. **Implementation of firewall**
    a. Separate different network segments with a firewall
    b. Firewall monitors traffic and can notice/alert to suspicious activity
2. **Create network segments**
    a. Have different parts of the company have different network segments using VLANs
3. **Implementation of access control measures**
    a. Creation of access policy. Determine who needs to have access to what information and limit access based on these necessities (Role Based Access Controls).
4. **Training**
    a. Regularly train IT staff in network segmentation and its importance. This implementation strategy can be used throughout the company to better limit access for safety reasons.
5. **Incident response plan**
    a. Have a plan for in the event of a breach and what to expect. Regular test IT department to understand how to deescalate a breach and mitigate damage.

Risk 2: Web server runs on ageing hardware that does not provide redundancy or resilience

Problem: Ageing hardware, no redundancy or resilience

Solution: Having no redundancy or resilience can be a large risk for any company. Downtime causes company profit loss while lack of redundancy can pose security disruption risk. To mitigate this risk the company can implement the following:

1. **Replacement of Old Hardware & Testing**
    a. Pick more reliable systems to reduce webserver performance. These implementations can be chosen by the CIO or in collaboration with a third party like CDW.
        This can include: (Based on company/system requirements)
        i. Memory
        ii. Storage Space
        iii. Processing
    b. Test the implementation of new hardware to make sure systems run properly and efficiently before phasing in.
2. **System Monitoring**
    a. Regular maintenance on new hardware and software. This mitigates this risk occurring again and keeps server runtime optimal.
    b. Implementation of monitoring software. This allows for alerts to be sent of potential issues or failures mitigating the risk of unknown issues.
3. **Create a backup policy**
    a. Create a policy regarding:
        i. How often should data backup occur?
        ii. What content is backed up?
        iii. Is the data encrypted (If yes, how?)
        iv. Who has access to stored data?
        v. Who oversees backup data?
4. **Implementation of Incident response plan**
    a. Have a plan in the event of system failure/downtime. By using load balancers, traffic can be sent to other servers reducing downtime. All departments should be included in this plan to best reduce downtime and increase fluidity of operation during downtime.

Risk 3: Backup tapes stored incorrectly

Problem: On-site, in the same room as the backup server

Solution: Storing backups in the same place as the backup server poses a significant risk in the case of an incident. In the event of a physical breach, all stored data would subsequently be destroyed. To mitigate this risk the company should implement the following:

1. **Implement Off-site storage for Backups**
    a. Connect with an offsite data backup company preferably in a different state
2. **Create a backup policy**
    a. Create a policy regarding:
        i. How often should data backup occur?
        ii. How should the data be stored (Physically, Digitally)?
        iii. Is the data encrypted (If yes, how?)
        iv. Who has access to stored data?
        v. Who oversees backup data?

3. **Regular testing of Backup data**
    a. Test the process of backing up data to ensure of fluid process before and incident occurs. By doing so, employees who are authorized to work on data storage can better recognize the process and discern if troubleshooting issues occur.
4. **Implementation of Incident response plan**
    a. Create an Incident response plan regarding what to do in the event of a breach.
    b. This plan should have elements focused on the authorized users who worked on the data as well as another section for additional employees. This is important as:
        i. A physical breach can be mitigated via training all employees on suspicious activity and how to manage seeing them.
        ii. The actions of an employee in a different department may correlate with the breach.

Risk 4: Remote and travelling users

Problem: Have no secure method of accessing the corporate environment

Solution: Remote and travelling users can expose sensitive data by connecting with public networks. This poses a large risk to the company, especially since as of the implementation of this policy, there is no network segmentation. To mitigate this risk, it is best to implement the following:

1. **Training & Awareness**
    a. Regular and active training for all remote, in-office, and travelling employees. Training should focus on developing the understanding that public networks are unsafe and could pose a risk to the company.
    b. Training on how to work while traveling. This includes how to work on sensitive information with people around you, the understanding of shoulder-spoofing, and why you should not leave devices in public or seemingly private areas.
    c. Regularly promote staff communication with the IT department. By doing so, employees feel more comfortable communicating if there was an incident they were unable to recognize as negative/impactful.
2. **Implement Endpoint Security**
    a. Implementation of (MDM) Mobile Device Management. This will allow the company or IT department to access and manage remote devices.
    b. The addition of strong security measures via MDM. Connected devices should be up to date on security standards (Antivirus software) and require detailed passwords.
3. **Usage of a VPN**
    a. Require usage of a VPN for all travelling or remote employees.
4. **Implement MFA (Multi-Factor Authentication)**
    a. All employees should use MFA to access any company websites. By doing so, the company has a strong first line of defense against any potential breaches.
    b. Multi-Factor Authentication can be set up through a third party like Okta or implemented via Cloud based service providers.

Risk 5: The MS SQL cluster running on old hardware

Problem: Purchased in 2015 and is still operating the 2015 version of software (EOL)

Solution: An MS SQL Cluster running on old hardware runs a large risk to the company. Because the version is at (EOL) End of life, Microsoft no longer provides security updates to the hardware or updates. This can leave sensitive company information vulnerable to security attacks. To mitigate this risk, the company should implement the following:

1. **Implement the newest version of MS SQL**
    a. The implementation of the newest version of SQL will ensure MS keeps SQL up to date in accordance with the latest security updates and features.
2. **Implement monitoring software**
    a. Use software like SWL Sever Audit to monitor events
3. **Create a backup policy**
    a. Create a policy regarding:
        i. How often should data backup occur?
        ii. How should the data be stored?
        iii. Is the data encrypted (If yes, how?)
        iv. Who has access to stored data?
        v. Who oversees backup data?
4. **Implementation of a Firewall**
    a. The addition of a Firewall can mitigate security risk against potential threats.