Security Architecture Report and Recommendations

Subject:

Mid-Sized E-commerce Company

Robert Ajegbo

Lighthouse Labs Cyber Security June 26 Cohort

Week 10 Secure Architecture Project

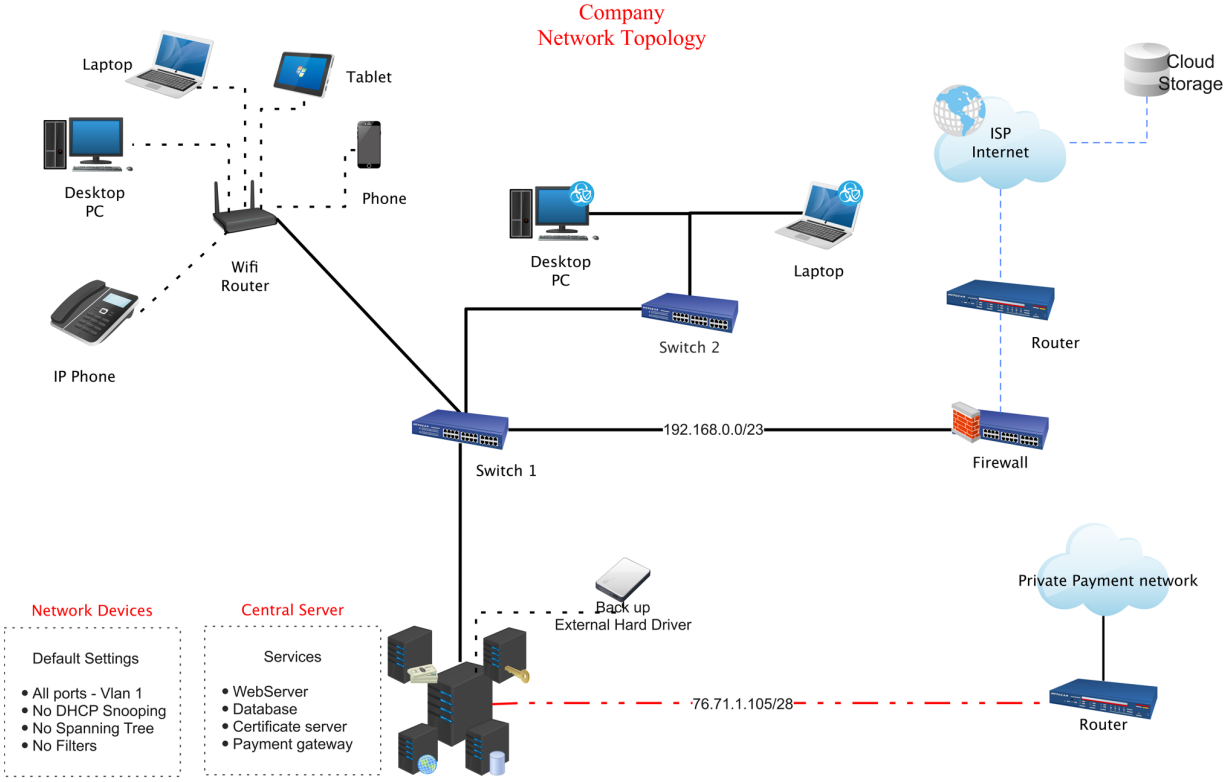
Table of Contents:

1. Introduction:

The purpose of this report is to identify and assess the security architecture of a mid-sized e-commerce company. Following the initial analysis, I will make some recommendations on techniques and strategies to improve the overall security landscape.

2. Current Security Landscape:

Upon an initial assessment of the security infrastructure for this company, it is evident that some clear weaknesses must be improved to better protect valuable assets and data. To me, the most obvious flaw is within the network topology where we can see that all of the organization's endpoints are located on VLAN 1. This would make it significantly easier for an attacker to potentially gain access to valuable data by breaching a low-privilege system and moving laterally to the web server. There is no firewall between the private payment network and the company servers. There are no port filters on the network meaning that cybercriminals can exploit insecure ports such as FTP ports with default credentials. There is also no spanning tree which leaves an opportunity for network loops.



3. Security Architecture Goals:

Due to their business industry, the company has made it clear to us that its main priority is the protection of personally identifiable information. Through any transactions made on the company website, there will be access to lots of private information that must be kept secure. However, considering that they are an e-commerce company in Canada, some key regulations may need to be considered when implementing measures. Some of these regulations include PIPEDA, PCI DSS, CASL, Canada's Digital Privacy Act, consumer protection laws, and other provincial privacy legislations. The Personal Information Protection and Electronic Documents Act or PIPEDA is potentially the main regulation to consider, It is Canada's federal privacy law that governs the collection, use, and disclosure of personal information. This ensures that companies are responsible for handling customer data and they must notify individuals in the event of any data breaches. As well as the customer information, it is essential that the personal details of the company's employees are kept as secure as possible. In the next section, I will outline some recommendations that will help to meet these security goals.

4. Security Architecture Recommendations:

I will address the above statements where I have already stated that there are some flaws in the network topology that should be improved to secure the systems. I will also outline some effective preventative techniques and measures that should be implemented to improve the overall security infrastructure. Due to the size of the company, they may not have the resources to use the absolute best systems for their new security architecture. For example, there are lots of different IPS/IDS systems and monitoring solutions that they could implement but their executive team would need to come together to make decisions about what their budget is for implementing these recommended tools and techniques.

<u>Network Segmentation:</u>

Isolate critical systems from less secure areas of the network. This may be done by implementing multiple VLANs rather than the current network with only one. These systems include the private payment network, web server, and customer databases.

Firewalls:

Implementation of multiple robust firewalls will protect against unauthorized access and stop potential cyber threats. Ensure web application firewalls are used to protect against web-based attacks. The deployment of firewalls will also allow for port filtering where we can control what network ports are open and accessible. This will minimize the potential for exploiting vulnerabilities.

Intrusion Detection/Prevention Systems:

On top of the firewalls, the use of IDPS will help to detect and prevent unauthorized access and malicious activities. It is important to use a system that will notify the admins of any unusual behaviour.

Secure Access Control:

Implement strong access controls such as role-based access control to ensure that individuals only have the access required to complete their tasks. You should also use techniques such as multi-factor authentication and strong passwords (At least 12 characters with a mix of letters, numbers and special characters).

Data Encryption:

Ensure that all sensitive data is encrypted so that only authorized parties can read it even if the data is stolen.

Regular Patch Management:

Ensure that all systems are regularly maintained and updated with the latest security patches. This will decrease the likelihood that a software vulnerability may be exploited.

Regular Security Training:

The job of securing the company's data is not only the responsibility of the security team. It is important to ensure that all employees are made aware of the importance of keeping their data safe and protecting the organization. In some cases, it only takes one naive user to breach an entire company's database through phishing and other attacks.

Incident Response Plan:

Develop an effective plan for handling security incidents in the case of cyber attacks.

5. Implementation Plan:

Network Segmentation:

1. Define Goals and Scope:
    - Clearly state the objectives of network segmentation
    - Determine which parts of the network need segmentation
2. Segment the Network:
    - Divide the network into zones (by security needs) based on defined objectives
    - Assign IP subnets or VLANs to each zone
3. Implement Access Control:
    - Establish strict access control policies between segments
        - Employees should only have the minimum access necessary to complete tasks
    - Use firewalls, IDS and IPS systems, and network policies to enforce security
4. Monitoring and Testing:
    - Set up network monitoring tools to track traffic between segments
    - Regularly test segmentation to identify any vulnerabilities or misconfigurations
5. Constant Maintenance:
    - Document segmentation strategy and configurations
    - Continuously update and improve network segmentation
        - Security threats are always evolving
6. Timeline:
    - This will be conducted by the IT Team and the security team and it could take anywhere from 3 to 6 months to implement as they may need to completely redesign the network configuration

Data Encryption Implementation:

1. Identify and Prioritize Sensitive Data:
    - Identify types of data that need encryption
        - This can include customer information, employee records, and payment data
    - Prioritize data based on sensitivity and security needs
2. Choose and Implement Encryption Methods:
    - Select suitable encryption methods based on security needs
    - Implement encryption across relevant systems
3. Key Management and Compliance:
    - Develop a robust key management strategy, ensuring secure storage and periodic key rotation
    - Regularly test the encryption solution for effectiveness and compliance with relevant regulations and standards
4. Timeline:
    - This will be done by the network administrators and the security team and it could take anywhere from 1 to 4 months depending on the complexity of the encryption

Security Awareness Training:

1. Assess Training Needs:
    - Identify roles and departments where security awareness is most crucial
    - Conduct a risk assessment to pinpoint areas with highest security vulnerabilities
2. Develop Tailored Training Content:
    - Create customized training programs based on needs
    - Develop materials that address specific security threats and practices relevant to your business
3. Deliver Comprehensive Training:
    - Variety of training methods to fit various learning styles:
        - Online modules
        - In-person workshops or seminars
        - Simulated security incidents
    - Cover essential security topics

4. Measure and Assess Progress:
    - Implement assessments and quizzes to measure the effectiveness of training
    - Track progress and identify areas for improvement
5. Continuously Reinforce Security Awareness:
    - Maintain ongoing security communication plan to reinforce training
    - Regularly send security reminders, newsletters, and updates to employees
    - Encourage reporting of security incidents and guide incident response
6. Timeline:
    - The security training will be conducted by the HR department and the security team (for their expertise and guidance) and the initial training could be anywhere from 1 to 3 months but there should be more training implemented later also (threats are always evolving)

<u>Incident Response Plan:</u>

1. Preparation and Assessment:
    - Identify relevant company stakeholders and form an incident response team
    - Conduct thorough risk assessment, prioritize assets, and set clear security objectives
2. Implementation:
    - Deploy security measures, listed above in the recommendations section
    - Test and validate each measure to ensure effectiveness and make changes wherever necessary
3. Monitoring and Maintenance:
    - Establish constant monitoring for e-commerce operations before and after any security incidents occur
    - Review and update incident response plan wherever necessary
4. Compliance and Reporting:
    - Maintain comprehensive documentation and any other necessary data, to maintain compliance with regulations
    - Conduct regular compliance audits to meet requirements

5. Review and Improvement:
    - As stated previously, you must always review the security architecture to maximize the organization's security
    - Conduct incident response tests/simulations for company operations
    - Share progress reports with executives and stakeholders
6. Timeline:
    - The IR Plan will be developed by the security team and the relevant stakeholders chosen for the incident response team (CSIRT). This will be a long process and it can take anywhere from 2 to 6 months. There will also have to be constant testing and revisions to the plan as things go on.

Task Prioritization:

In this section, I will outline the recommended security measures in order of priority. I will be taking into factors such as the risks they protect against and the feasibility of implementing them.

1. Regular Security Training:
    - I believe this should be the highest priority. Regardless of any security measures, your systems and data will not be as secure if the employees do not understand the need for data protection. It is also relatively easy to implement.
2. Regular Patch Management:
    - Unpatched software and outdated systems are some of the most common vulnerabilities in any kind of business, let alone an e-commerce company. Applying regular patches can address these known vulnerabilities and reduce the risk of hackers' exploitation of others.
3. Incident Response Plan:
    - I put this in the middle priority because a proper incident response plan may be the most important security measure for an organization but it also requires dedicated resources and time for its development, testing, and training. If resources allow, companies could employ the help of dedicated cybersecurity teams for this.

4. Data Encryption:
    - Data encryption is important for protecting sensitive data, but it can be more complex and resource-intensive to implement compared to the tasks above. This company may still desire to encrypt their most sensitive data to maximize the safety of their customers' information.
5. Network Segmentation:
    - Network segmentation is valuable for enhancing security but it can be more complex and time-consuming to implement compared to the other tasks. This can require significant planning and network infrastructure changes. I do believe that it would be beneficial for the company to deploy a more robust firewall and more secure access control even if they do not have the resources for maximum segmentation.

References

Commercial Facilities Sector Cybersecurity Framework Implementation Guidance. (2021, January 7). CISA. Retrieved September 6, 2023, from https://www.cisa.gov/resources-tools/resources/commercial-facilities-sector-cybersecurity-framework-implementation

Enterprise Security Architecture Requirements and Best Practices for Sustained Growth. (2022, February 8). RSI Security. Retrieved September 6, 2023, from https://blog.rsisecurity.com/enterprise-security-architecture-requirements-and-best-practices-for-sustained-growth/

Full-scale Mapping. (2022, October 2). LHL Compass. Retrieved September 6, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w10d5/activities/3227

Implementing the NIST Framework. (2022, October 2). LHL Compass. Retrieved September 6, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w10d1/activities/3202

Jennings, M. (2022, November 8). *8 Steps to Implement a Cyber Security Awareness Training Program*. SymQuest Tech Talk. Retrieved September 13, 2023, from https://blog.symquest.com/steps-to-implement-a-cyber-security-awareness-training-program-at-your-company

Network Segmentation best practices & implementation. (n.d.). NordLayer. Retrieved September 13, 2023, from https://nordlayer.com/learn/network-security/network-segmentation-best-practices/

Secure Architecture Report and Recommendations. (2022, October 2). LHL Compass. Retrieved September 6, 2023, from https://cyber.compass.lighthouselabs.ca/projects/secure-architecture-report#

Sheldon, R. (n.d.). *What is Spanning Tree Protocol?* TechTarget. Retrieved September 7, 2023, from https://www.techtarget.com/searchnetworking/definition/spanning-tree-protocol

What is VLAN? How VLAN Works and Common Examples. (2019, July 8). N-able. Retrieved September 6, 2023, from https://www.n-able.com/blog/what-are-vlans