Performance Assessment: Secure Network Design (DHN1)

Skerdilaid Hoti

College of IT, Western Governors University

Yolanda W. DuPree

January 6, 2024

Performance Assessment: Secure Network Design (DHN1)

A

While company A's infrastructure and security are strong certain vulnerabilities still become apparent. Based on the given scenario, and the two given documents, the network map and risk analysis, company A suffers from an infrastructure problem including the open ports, and the devices that end of life. The second issue is the end-of-life devices still being used. The issue with end-of-life devices is that software lacks security updates. Without these updates, a system is exposed to potential security breaches, leaving sensitive data and information at great risk. Two security risks include that all users use eight characters passwords, and that regular password changes are not reinforced. The issue with every user using the same number of characters is that it becomes much easier for hackers to force themselves into the system since they know the length and they can use different software to brute force their way in. Another issue is that regular password changes are not reinforced. Due to this a breached account can linger for unknown amounts of time and cause significant damage.

Two infrastructure issues for company B include end-of-life operating system, and there PostgreSQL admin is reachable from internet. Two security problems are rlogin Password less Login, and that All users have local administrative privileges.

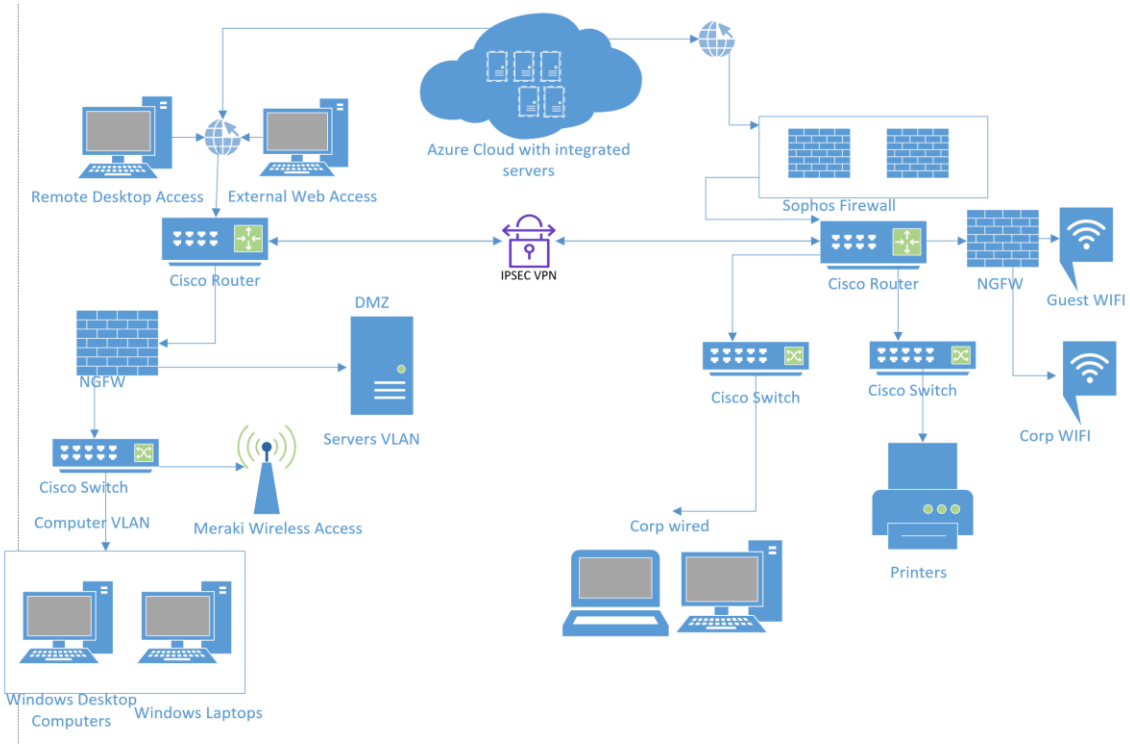
B

For company A two existing vulnerabilities include the open ports 21-90, 3389, and that all users have local administrator privileges. The open ports create a significant issue because they allow passage in for attackers, especially some of the insecure ports that are open such as 20, 21, 80. Also Port 3389 is the default port for Remote Desktop Protocol (RDP). If open to the internet without proper security measures, it could be a target for brute-force attacks, unauthorized access, or exploitation of RDP vulnerabilities. Attackers can use these ports as a gateway to the network and begin lateral movement. Based on the chart the likelihood of this happening is high. Due to the potential damage based on these open ports the risk, and impact of such a vulnerability is also high. The second is that all users have local administrator privileges. The issue with this risk is that users with local administrator privileges can make significant changes to system settings and installed software. Users can cause system instability, disruption in service or unintended configuration that compromises security. Another issue is that malicious software or attackers who gain access to the system will now have elevated privileges and can cause significant damage to the system, and other systems. Based on the chart the likelihood of this happening is moderate. This, however, is outweighed by the fact that the risk and impact is critical.

Company B has many more vulnerabilities which include MFA not being enforced on all devices, and FTP Brute Force Logins Reporting. The first issue is with the MFA not being enforced on all devices. Without MFA it becomes much easier for an attacker to exploit a weak or compromised password to gain unauthorized access to user accounts. Unauthorized access can lead to data breaches, compromised sensitive information, and result in unauthorized actives on the accounts. One of the biggest issues with this is that the attackers can escalate their privileges

to gain access to the network which also becomes much easier since company B also suffers from the issue of their accounts all having local administrative access. The chart says that the severity and likelihood of the vulnerability is high, but the impact would also be high in this case due to the potential damage it may cause. The second vulnerability is the FTP brute force logins reporting. A successful brute-force attack can lead to unauthorized access to the FTP server which will compromise sensitive files and data stored on the server. Another issue that can be caused by this is that brute force attacks can cause user lockouts. This will cause inconvenience for authorized users impacting business operations. The severity and risk are high, and because compromised sensitive files for this company include credit card information, the impact is also high.

C



D

Device	OSI LAYER	TCP/IP Layer
Firewall	Application	Application
Router	Network	Internet
Servers	Application	Application
Wireless Access	Physical	Network Interface
Printer	Application	Application
Cabling	Physical	Network Interface
VPN	Network	Network
Laptops and Workstations	Applicaiton	Application
Switch	Network	Network

E

One of the first things done when merging the two companies was merging the servers into the Azure cloud system. This was done for many reasons. The first reason was that Azure provides scalable infrastructure, which is very important during a merger, and for future growth. It also keeps the budget under control by offering a pay-as-you-go service which only charges the company for the services they use. It provides redundancy and reliability, security and compliance but most important it provides remote access so that both networks can have access to it. For company B I added a Fortinet 800D NGFW, priced at $9,841.12, (https://4tekgear.com/fortinet-fortigate-800d-network-security-firewall-appliance-only.html), the same that was present in company A, between the wireless access points and the network to filter traffic coming in and ensure the security of the network. From company A I removed two switches because they are no longer needed since the servers are on the cloud, and one from

company B for the same reason. To connect the networks of the two companies a VPN was used this time provided by Amazon's AWS. The estimated cost of this VPN would be 0.05 per hour per client.

F

To ensure the security of this network Zero trust was implemented, and scalability. To implement zero trust the network was segmented, especially in company B. Wi-Fi is now separated behind a firewall, and each system is separated. The benefits of this include that if one section is breached it becomes much more difficult for threats to use lateral movement to gain access to other systems. Also, another important feature when implementing zero trust is MFA. Both companies possess financial and healthcare information. MFA would be required for all users to access their devices and the network. MFA gives an extra layer of authentication which reduces the risk of unauthorized access. The second network principle is scalability. Scalability ensures that a network can adapt and grow to accommodate the increased demands that will arise as the two companies are merged. The first step was cloud migration of the servers in which Azure was used. Azure enables resource allocation, is cost effective, offers scalability, and improves redundancy. We would also be implementing load balancing for servers in the cloud to distribute traffic evenly. This allows for increased performance, prevents bottlenecks, and supports a growing number of users.

G

To ensure regulatory compliance two main policies were used in the proposed network topology diagram. One was GLBA, and HIPAA. Both are applicable since both companies contain financial information, and company B has health information. GLBA mandates the protection of consumers personal financial information (Groot, 2023). The proposed topology diagram uses robust security measures to protect customer PII. The use of NGFW, segmentation for isolating

critical systems, and data encryption all align with GLBA. Also new access controls to limit who has administrative controls and DLP systems are implemented to ensure only authorized personally have access to this information. The second policy is HIPAA. Since company B offers specialized software for medical providers and handles medical data it is essential to follow these guidelines. The topology map implements strict access controls and encryption for healthcare data. The cloud-based infrastructure ensures secure storage and processing of medical information while also providing redundancy and scalability. Company B would also be using secure communication protocols and continuous monitoring to detect and respond to potential security incidents. Also isolated segments for healthcare-related systems help prevent unauthorized access.

H

During the merger various challenges and potential threats arise. One would be operational disruption. When integrating two systems it is important that business operations continue as much as possible due to issues that can arise such as customer trust and damage the reputation of the newly formed company. Business continuity is important to maintain a constant and reliable experience for customers. Also, an issue between these two companies is some systems are out of date, and compatibility becomes a big problem when companies are using different software and OS. This was fixed by implementing similar technologies in both companies and removing end of life or updating old systems. Another big issue that can arise is insider threats. A critical problem during an acquisition is a disgruntled employee unhappy with the merger acting as an insider threat. To prevent this, it is essential to actively monitor the systems, conduct security awareness training, and implementing least privilege.

F

In order to justify the costs of this secure network map it's important to understand the risk if such expenses were not implemented. Some changes included upgrading on premise infrastructure of company B such as the switch, and firewalls, and segmentation of the system. This allows for continued use of the existing infrastructure to save money but also upgrading it to ensure it is secure. Another cost was implementation of the cloud system, costs include subscription fee to the cloud service, migration cost, and some training costs for staff to learn the new technology. This was done to provide redundancy, overall will cut down expenses to do pay as you go model, and it will centralize security management and monitoring. Some indirect costs to the merger include Downtime, operational disruption, reputational damage, time and internal resources, and legal and non-compliance fees. (Shackleton, 2023).

References

Shackleton, T. (2023, March 23). A cost-benefit analysis approach to cyber security. Six Degrees. https://www.6dg.co.uk/blog/cost-benefit-approach-to-cyber-security/

Elliot, J. (2022, Feb 23). Important Governance: GDPR [Video]. PluralSight. https://app.pluralsight.com/library/courses/information-governance-gdpr/table-of-contents

Juliana De Groot on Saturday May 6, Brook, C., & Lord, N. (n.d.). What is GLBA compliance? (understand requirements). Digital Guardian. https://www.digitalguardian.com/blog/what-glba-compliance-understanding-data-protection-requirements-gramm-leach-bliley-act