Douglas Roberts

010396218

C700: Secure Network Design Performance Assessment

A. Based off an internal risk analysis performed by Company A ahead of a planned acquisition of Company B, there are five moderate to high IT vulnerabilities. The first and only high risk are the Remote Desktop open ports of 88-93. In order to safely allow users to remotely access a server/machine/system over ports 88-93, precautions like multi-factor authentication (MFA), utilization of virtual private networks (VPNs), and/or network segmentation must occur. The next vulnerability (all remaining vulnerabilities are classified ‘Moderate’) is that user accounts that are no longer required are not removed. This has the potential of former employees accessing systems they no longer authorized to use or view. Another vulnerability is that every employee has full access privileges, apart from access to payroll. This violates the principle of least privilege and can have serious consequences. The fourth vulnerability is that regular password changes are not enforced. If passwords are not of sufficient length and complexity, reused, or not changed regularly, attackers can easily crack them. The final issue that needs to be remediated is the Cisco PIX 515E firewall. This product is obsolete, End-of-Life, and End-of-Support (Cisco. 2017, June 25. PIX-515E-security-appliance. https://www.cisco.com/c/en/us/obsolete/security/cisco-pix-515e-security-appliance.html). This means that Cisco no longer offers patches to fix vulnerabilities, and if any issue arises, they will not help remediate any issues, performance, security, or otherwise.

B.  See attachments.

C.  After performing Zenmap and OpenVAS scans on Company B computer at 10.10.1.3, a couple of security issues were evident. First, the system was using Windows 7 as its operating (OS) system. Just like the Cisco firewall previously mentioned, Windows 7 is past end of life and is no longer supported or patched by Microsoft. By updating to Windows10 or 11, known vulnerabilities would be remediated and Microsoft would provide support for any future usability or security issues. Secondly, TCP port 445 (SMB) is open, and the SMB server has not been properly patched. There are existing patches from the vendor (Microsoft), and if the company would install the required patches, the SMB server would be protected from a remote denial of service attack or brute force authentication.

D.  See attachments

E.

|  |  |  |
| --- | --- | --- |
| Device | OSI Layer | TCP/IP Layer |
| Firewall | 4 | 4 |
| Router | 4 | 3 |
| Switches | 3 | 2 |
| Servers | 7 | 4 |
| Cabling | 2 | 1 |
| Workstations | 7 | 4 |
| Laptops | 7 | 4 |
| Printer | 7 | 4 |

F.  In the previous network setup, there were several workstations that had RDP enabled. As RDP is not secure, the new network has disabled RDP and instead requires the use of a VPN. While not exactly the same function (RDP lets a user access a specific machine, whereas a VPN grants access to the network at large), RDP does not offer sufficient security. The end to end encryption offered by VPN tunneling will be the only authorized method of having remote access to the network.

An important and previously mentioned hardware change is the replacement of the outdated PIX 515E firewall with a Cisco Firepower 1120 ASA on/from Amazon for $2,287.20 (<https://www.amazon.com/Cisco-Systems-Fpr1120-Asa-K9-Network-Device>). With a throughput of 2.3 Gbps, centralized configuration and monitoring, and ability to filter more than 280 million URL’s, the 1120 is a significant upgrade over the obsolete PIX 515E.

Another major deletion and replacement in the network is the Cisco 2811 router. As of November of 2016, the 2811 router was past its end-of-support date (<https://www.cisco.com/c/en/us/obsolete/routers/cisco-2811-integrated-services-router.html>). For security and workload purposes, the new topology has upgraded with the Cisco ISR 4431 router with security bundle from networkoutlet.com for $2,950.00 (<https://networkoutlet.com/products/isr4431).> Capable of up to over 4 Gbps and enhanced security features like Encrypted Threat Analytics, which is able to identify malware through passive monitoring of packets as they pass through the router, the ISR 4431 is a substantial, cost effective, and size appropriate replacement of the old Cisco 2811 router.

The final major hardware change is the replacement of the three Cisco 2960 24/4 and Cisco 2960 48/4 switches. Respectively, the new ones are three Cisco Catalyst 9200 C9200L-24T-4X Ethernet Switches from neobits.com for $2,357.34 each, totaling $7,072.02 (<https://www.neobits.com/cisco_c9200l_24t_4x_a_rf_cisco_catalyst_9200_p15244138.html?atc=gbs>), and four Cisco C9200L-48P-4G-E - Cisco Switch Catalyst 9200 from router-switch.com for $4,424.00, totaling $17,696.00. Like the other hardware changes, the 2960 switches were past end-of-life, leaving serious performance and security issues that had to be addressed.

All hardware changes came in at a total cost of $30,005.22, leaving around $5,000 left to cover any incidental costs, installation, and software or support that may be required but unknown at this time.

G.  One of the biggest changes made from the existing network topology to the proposed network topology post-merger is the introduction of Virtual Local Area Network’s (VLAN). This control will keep disparate business units (and their data) isolated so that only individuals within each segment have access to data and information within their organization (i.e. Marketing is separate from sales which is separate from HR etc). That will mitigate the vulnerability of every employee being having full access privileges company wide. Also, in the event of a security compromise from a hacker, if they gain access to one VLAN, only the data in the compromised VLAN will be affected. Another noticeable change is the implementation of vigorous endpoint security. Requiring multi-factor authentication (MFA), enforcing strong passwords with lockout policy after 5 attempts, strict down/uploading policies, and screen savers requiring reauthentication will harden devices and mitigate vulnerabilities to workstations, laptops, and printers.

H.  Two secure hardware components in the new network topology are the Cisco ISR 4431 Router and the Cisco Firepower 1120 ASA. The 4431 is a far more secure route over the previous 2811 in a couple of ways. The first and most simple upgrade of the 4431 is that it is not end-of-life or end-of-service. Cisco is still issuing patches for vulnerabilities and will provide support for any issues that may arise with the equipment, performance, security, or otherwise. The other main improvement in how the 4431 addresses security needs is the Encrypted Threat Analytics (ETA). ETA is able to look into encrypted packets it is routing and detect malware. This adds another layer of security to the network on top of the firewall, enabling a greater Defense in Depth. Similar to the advantages in the upgraded router, the Firepower 1120 ASA has significant improvements over the PIX 515E. Just like the 2811, the 515E is also end-of-life and end-of-service. By virtue of current support by Cisco, the 1120 will receive patches, updates, and other services by the manufacturer. Another way to put it, there is a transference of risk. Finally, the 1120 is what is know as a Stateful (or Smart) Firewall. Instead of operating at Layer 2 and only following specific firewall rules, it operates up to Layer 4 of the OSI model, analyzes traffic for potential threats, and differentiates between outgoing and incoming traffic (incoming traffic is far more likely to contain malware and inspected more closely).

I.  As customer and employee PII are of the highest levels of sensitivity, and there are numerous laws and standards for handling such data, the proposed network topology sufficiently addresses those compliance requirements. The network maintains best practices such as network segmentation, defense in depth, and endpoint security. Those measures, in addition to updated hardware and user policies, will keep the newly merged company in compliance with standards from NIST, ISO, GDPR, etc.

J. One potential security threat is the age of the servers. The 2008 servers are outdated, and the 2012 servers are nearly obsolescence as well. They are behind multiple layers of security and access controls, but are more vulnerable to known exploits and are less likely to have current patches. Possible remediations for this are budgeting more money in a future fiscal quarter or year for new machines, or downgrading the quality or number of switches to free up capital that could be spent immediately on upgraded servers.

One potential network problem is the Cat 5 cabling. Aside from not being replaced for the merger and thus is old, it is limited in its bandwidth compared to other, more current technology. Possible remediations for this include spending the remaining $5000 in the budget for new cabling, and/or budgeting in another fiscal year for different technology like fiber optic cable or Wifi-6 access point.

**Citations**

Cisco. (2017, June 25). PIX-515E-security-appliance. Cisco. Retrieved July 31, 2022, from https://www.cisco.com/c/en/us/obsolete/security/cisco-pix-515e-security-appliance.html

Descalso, A. (2021, July 27). Open&nbsp;ports: What they are and why you need to secure them. Intelligent Technical Solutions. Retrieved from https://www.itsasap.com/blog/why-secure-open-ports

Panko, R. R., &amp; Panko, J. L. (2019). Chapter 4 Network Security. In Business Data Networks and security. essay, Pearson.

Panko, R. R., &amp; Panko, J. L. (2019). Chapter 2 Network Standards. In Business Data Networks and security. essay, Pearson

Chapple, M., Stewart, J. M., & Gibson, D. (2021). Chapter 4 Laws, Regulations, and Compliance CISSP (ISC)2 Certified information systems security professional official study guide (9th ed.).John Wiley & Sons, Inc.

Chapple, M., Stewart, J. M., & Gibson, D. (2021). Chapter 11 Secure Network Architecture and Components CISSP (ISC)2 Certified information systems security professional official study guide (9th ed.).John Wiley & Sons, Inc.

ISR4431-SEC/K9 Cisco ISR4431 router with Security Bundle. Network Outlet. (n.d.). Retrieved from https://networkoutlet.com/products/isr4431-sec-k9-cisco-isr4431-router-with-security-bundle?variant=30323145769040¤cy=USD&amp;utm\_medium=product\_sync&amp;utm\_source=google&amp;utm\_content=sag\_organic&amp;utm\_campaign=sag\_organic&amp;gclid=Cj0KCQjw852XBhC6ARIsAJsFPN3v9Z7kWjrRjVk\_rtWEw8H-QS\_iJ4XrjUyfqrP\_sQxtvMK\_ZcOKnrEaAhv7EALw\_wcB

Cisco 4000 Family Integrated Services Router Data sheet. Cisco. (2022, February 25). Retrieved from <https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/data_sheet-c78-732542.html#Productsustainability>

Amazon.com: Cisco Secure Firewall: Firepower 1120 security appliance ... (n.d.). Retrieved from <https://www.amazon.com/Cisco-Systems-Fpr1120-Asa-K9-Network-Device/dp/B085VN9VC8>

Cisco Firepower 1000 Series Data Sheet. Cisco. (2021, July 30). Retrieved from <https://www.cisco.com/c/en/us/products/collateral/security/firepower-1000-series/datasheet-c78-742469.html>

C9200L-48P-4G-e price - Cisco Switch Catalyst 9200. (n.d.). Retrieved from <https://www.router-switch.com/c9200l-48p-4g-e.html>

Neobits.com is where business goes shopping. (n.d.). Retrieved from <https://www.neobits.com/cisco_c9200l_24t_4x_a_rf_cisco_catalyst_9200_p15244138.html?atc=gbs>

Cisco Catalyst 9200 Series switches. (2022, July 1). Cisco. Retrieved from <https://www.cisco.com/c/en/us/products/switches/catalyst-9200-series-switches/index.html>