Establishment of firewall and related findings

Technology, Information Technology

Running Head: Week 5 Group Week 5 Group: Personal Firewall Week 5 Group: Personal Firewall Establishment of Firewall and Related Findings Establishing the Firewall I use the Windows Firewall, which has been provided with the Windows 7 operating system as an inbuilt tool. After turning on my personal computer (PC), I clicked on the Start button located at the lower left corner of the desktop screen. Next, I clicked on the Control Panel located in the right pane of the Start menu. Step 1: Screenshot 1 In the Control Panel, I clicked the System and Security option. Step 2: Screenshot 2 In the System and Security console, I clicked on the Windows Firewall. Step 3: Screenshot 3 Next, in the Windows Firewall console, I clicked on the option Turn Windows Firewall on or off located in the left pane. The Customize Settings console appeared. Here, I selected the radio buttons for turning on Windows Firewall for both the private and public networks; I also checked the checkboxes for notifying me whenever Windows Firewall blocks a new program. Findings Screenshot 4 In the Windows Firewall console, I found several options like those for changing the notification settings, turning the firewall on or off, restoring defaults, etc. As I clicked on the option for Advanced settings, the console window of Windows Firewall and Advanced Security appeared as shown in the next screenshot. Screenshot 5 Using this console, I found that the user could further set the inbound rules, outbound rules, connection security rules, and monitoring techniques. I also found that the firewall had arrangements to select from different user profiles with respect to the domains, workgroups, public networks, etc. and provided for importing/exporting system and network security policies to devise suppler and tighter protection schemes. Personal Firewall What Can Personal

Firewalls Do An ideal personal firewall is generally inexpensive and uncomplicated to establish and utilize. Personal firewalls are generally based on the PC operating system and/or third party applications. It can hide all the ports to make a PC indiscernible to scans. By selecting external contacts with the help of its inbuilt or user defined safety parameters, a firewall can protect the system from external attacks. A firewall can also diagnose the potential and genuine threats and immediately alert the user in the case of serious attacks. The firewall establishes a sort of filter when the PC is connected to an external network and/or the Internet. (Markus, 2012) What Can Personal Firewalls Not Do Firewalls are not invulnerable. It can protect the PC from external threats and not from the internal ones. Sometimes, firewalls may put restrictions on the user of the PC and create considerable annoyance. It may block even the reliable and safe external programs and/or codes to run via the Internet. Indiscriminate selection/rejection of software protocols may cause downtime, frequent reconfigurations, and network congestion. Also, without a correlated or third party antivirus software or toolkit, firewalls cannot eliminate or quarantine the malicious codes found inside the system, in the external network, and/or in the different storage devices. (Zwicky, Cooper, and Chapman, 2000) Important Benefit Windows Firewall lets the user to set rules for either inbound traffic or outbound traffic. The rule can be intricately configured as per the user’s security needs. While most of the personal firewalls can help the user to select/reject certain programs, ports, services, and/or protocols only, Windows Firewall also lets the user to detail which sort of network adapters the rule might be implemented to and how the PC’s external environment connections might

be controlled. The network or external environment might be a LAN, a VPN, a Wireless Network, the RAS, Bluetooth, or the Internet. Without Windows Firewall, I think it is almost impossible to obtain such sort of hassle free network protection provided free of any hidden cost. Also, the high degree of customizability of this tool makes it apt for more intricate security setting and establishment for the PC. (Microsoft Corporation, 2012) Interaction with Third Party Software Antivirus and anti-spyware software applications are also interrelated with the firewall. Some advanced antivirus software applications provide firewall protection too. However, they generally provide as holistic protection schemes as the firewall with regard to external attacks. For example, antivirus software on a PC may focus on Internet security and provide for filtering the different websites, programs run on Web, monitor threats during browsing, and so on. But it is not likely to secure the Remote Assistance Services (RAS) or accept/reject Remote Desktop Protocol (RDP) requests. A firewall scrutinizes these utilities and applications too in conjunction with Internet security and warning system. Mueller (2011, p. 7-130) has rightly remarked, “ Users install third party firewalls and virus protection products in many cases, so you’ll also need to consider these third party products as part of an overall application strategy.” List of References

Markus, H. S. (2012), Personal Firewall Reviews, Firewallguide. com. Available at http://www. firewallguide. com/software. htm. Last accessed on 6th August, 2012. Microsoft Corporation (2012), Understanding Windows Firewall settings, Microsoft Corporation, Redmond. Available at http://windows. microsoft. com/en-IN/windows7/Understanding-Windows-Firewall-settings. Last accessed on 6th August, 2012. Mueller, J. P. (2011),

Professional Windows 7 Development Guide, Hoboken: Wiley. Zwicky, E., Cooper, S. and Chapman, B. (2000), Building Internet Firewalls, Sebastopol: O’Reilly.