Perimeter defense strategies essay

Business, Strategy

Firewall Implementation Often, the first thing people tend to think of in network perimeter defense is a firewall (Posse, 2003). In most common environments, firewalls would be placed at the terminal ends of every network segments (Cole, Crust and Conley, 2005). A firewalls basilica is to permit or stop packets from flowing into or out of a network. For perimeter security implementation, firewalls are available as a software (installed inside a route) or as a stand-alone hardware appliance (Monsoon, 2009).

Any firewall implementation will not protect the network if it is not configured properly. Thus, a strategy, suggested by Trotter (2004) is to use the “ principle of least privilege”, meaning, denying all traffic. In addition, Anon (2004) argued that the firewall must be hardened. He suggested four (4) measures to achieve this which include: 1 . Implementing authentication and authorization, allowing only authorized users to connect to and manage firewalls. 2. Hardening remote administration by turning-off web-based Telnet and SSH services.

3. Hardening firewall services and protocols such as SNAP, NTP, slog and TFTP. 4. Using redundancy to harden firewall by getting identical hardware/ footwear and configuring them accordingly. A further defense strategy is to identify how well a firewall is functioning. Posse (2003) suggested that port scanning should be performed.

A port scan is a technique by which an outside system systematically attempts to see if any TCP or LCD ports on a network are listening (open). There are many types of port scans, ranging from the very simple to the very complex (Posse, 2003). Disable Unused Ports If the port scanning identifies undesirable ports, they should be disabled. As such, this strategy is to disable all TCP and LCD ports that are not absolutely accessory through the firewall -? especially ports 135, 137, 139, and 445. An ideal arrangement, recommended by Posse (2003) would be to enable only TCP ports 80 and 443 and ports 110 and 25, the ports associated with POP and ESMTP, to have e-mail. Remote Access Server Once the firewall is secured, the next step is to turn attention to remote access servers. There are many techniques for securing remote access servers.

Some of the most common techniques include requiring callbacks to preset numbers, recording caller ID information to log files, denying dial-up access to everyone except those who have a legitimate business need for it, and limiting the times and days when employees can dial in (Posse, 2003). DMZ The next strategy is to implement DMZ (Demoralized Zones). Trotter (2004) suggested putting all internet accessible machines in the DMZ (web server, email gateway, external DNS, etc. And restricting access between the DMZ and the internal net’. Fork to source and destination IP addresses. A further strategy suggested by Monsoon (2009) is to form a DMZ by installing a host (a dedicated server) residing between the two networks.

The DMZ host can initiate sessions for web pages, email and other requests on the public network. The system cannot; however, initiate a session back into the company’s network -? it can only forward packets that have already been requested. This technique, argued Monsoon (2009), prevents unrequited and potentially destructive data from entering a company’s network. Secure VPN A VPN provides perimeter security by encrypting the data sent between a business network and remote users over the Internet. In essence, the technique creates a private tunnel through the Internet. VPN technology is ideal popular and is used by enterprises of all sizes. The approaches biggest threat is from an attacker who figures out a way of compromising an authorized user's system, then gains control of an encrypted pathway into the company network (Monsoon, 2009). Rogue Modems In most organizations, firewalls and remote access servers are the main perimeter access points (Posse, 2003).

Any PC with a modem could potentially act as a remote access server. Posse (2003) stated that " at every network administration he has worked, he discovered at least one unauthorized modem. Thus, Posse (2003) argued that unauthorized modems represent a errors security risk. Posse (2003) suggested a number of ways to spot rogue modems. One technique involves maintaining an automated hardware inventory.

The inventory software can send an e-mail message when hardware changes occur. Another technique that works well, suggested Posse (2003) is to maintain a list of every telephone number that the company owns. In doing so, a PC is configured to call every single number (preferably late at night) to search for rogue modems. Hackers typically use this technique to call every number in a company to look for modems to compromise the network, therefore it is a radical defense strategy to identify rogue modems first (Posse, 2003). Isolate Wireless Access Points Intruders get past the perimeter by going through a wireless access point (WAP).

Posse (2003) stated that Whaps present a special challenge because an intruder can access a network through one without ever having to pass through a firewall or a remote access server. Posse recommended the following defenses: (1) enabling WEEP encryption, (2) defining the clients that are allowed to use the access point and (3) a more controversial wireless defense technique is to disable DDCD of the wireless clients. By doing so, wireless DDCD would not be handing-out IP addresses to wireless hackers (Posse, 2003). Additionally, using static IP addresses for legitimate wireless clients offers one more way that you can make a hacker’s job just a little more difficult.

It also makes it a bit easier for you to spot an intruder since an intruder would have to take a guess as to what IP address to use, and would likely have to use an address that’s different from the static addresses you’ve assigned (Posse, 2003). Virus Defense Another strategy is to implement virus defenses. The network is susceptible o virus introduced in many ways. Running anti-virus protections helps to secure the network. In many IT Audits that I have conducted, this was a general security control that I have tested and usually found deficiencies because the computers were not updated with the latest definitions or servers were not installed with any.

This is a serious security threat as a network can be easily taken down by means of a single virus. Hence, it is essential to defend the perimeter this way. To demonstrate the destructive nature of virus, one caused Denial of Service of the 13 root servers in the DNS n 2003 (Krebs, 2003).