Vulnerable areas of perimeter protection security essay

Business, Management

1 IntroductionPerimeter security deals with the security threats that arrive at the enterprise boundary via a network.

The current network-centric approach of computing reinforces the requirement of boundary line, which divides the line between the internal and external so that inherent weaknesses, mis-configuration, and other vulnerabilities in various components are hidden behind the controlled interface of the perimeter device (Bosworth, Kabay, 2002, p. 5). Perimeter devices are considered to be the most vital part of the security of a network if the network is connected to another less secure network. However, despite the level of security it offers, perimeter protection security is still vulnerable to threats. This paper presents such risks and vulnerabilities in the perimeter production technology.

The paper starts with a description of the term ‘ perimeter protection’, what it entails and the different types of the technology. After this the possible vulnerabilities of the protection technology are discussed along with some ways to mitigate the issues. 2 Perimeter protectionPerimeter security, according to the definition, has to “ handle user authentication, authorization, and access control to the resources that reside inside the perimeter” (Berson, Dubov, Dubov, 2007, p. 160).

As mentioned earlier perimeter devices control the flow of information between les secure outer networks and inner networks. In other words perimeter devices “ protect the information at the production system of inner systems” (Carvalho, da Silva, 2006, p. 69). Perimeter security

protection solutions are basically a collection of border routers, firewalls and proxy servers to protect networks from external attack.

There are three types of perimeter detection systems: a. Firewalls – This is the primary technology employed to achieve perimeter security. A firewall is placed at the network node where a secure network i. e.

internal enterprise network and an insecure network such as the internet, meet each other. Firewall basically restricts the incoming traffic from the external to the internal network based on some parameters. Once a firewall is configured it filters the network traffic, examines packet headers, and determines which packets would be allowed to enter and which would be rejected (Berson, Dubov, Dubov, 2007, p.

160). b. Intrusion Detection Systems – These types of systems primarily sound an alarm when all is not well with the network security. When all the network security mechanisms are working properly, intrusion detection information is really the threat level information, useful in maintaining knowledge of the background levels of hostile activity directed at the protected network (Thomas, Thomas, 2004, p. 203, 204). c. Content Inspection Devices – These types of devices such as Cisco IOS Firewall feature set or FFS, allows for the inspection of a packet’s contents which is extremely helpful while securing a network. This is the latest type of perimeter protection product.

The content inspection gateway sits on the network between the internet and the exchange server. The security is defined here on a per-physical

interface level. After the inspection the packet is filtered accordingly (Thomas, Thomas, 2004, p.

203, 204). 3 Vulnerabilities of Perimeter protectionA network perimeter consists of all the external most points of the internal network. Each connection to another network creates an entry point in the perimeter that must be secured. Perimeter security is only as strong as its weakest link. Without adequate security on each external connection, the security of the network automatically becomes dependent on the security of these other connected networks.

For instance, if a firewall is 100% effective, and if external traffic entering the network is the only attack vector, there would be no need for any other computer or network security on the internal network or the computers inside the firewall. However, this is not the case as the firewalls and intrusion detection systems do not protect the network from every possible computer attack. Some instances of vulnerability even after using perimeter protection are presented here: 3. 1 ModemsModems these days have become very cheap and in fact many manufacturers ship their computer system with a high speed modem installed as a part of their configuration. This is actually one of the biggest security threats to a network as modems allow users to create uncontrolled access points into the network.

If the modem is improperly configured, it can bypass of the network’s perimeter protection mechanisms and directly access the network resources (Stewart, Tittel, Chapple, 2005, p. 389). The only way to mitigate this

problem is the correct configuration of the modem, and restriction of access to the physical modem in case of an enterprise network3.

2 Internal v/s External boundaryThe perimeter approach is not effective if the network is extremely large. For instance just before AT&T split into three companies, it had as many hosts inside the perimeter as the entire internet user in the year 1988, In addition to this, not one individual knew the location, policies, security or the connectivity of all the hosts. Lacks sheer size of the network, combined with lack of knowledge is more than enough to question a perimeter defense. In addition to it, there is the additional problem with the systems which are used as the point for information sharing. These systems operate with the other internal enterprise networks on a transient trust basis i. e.

using internal login to access resources. If such systems are not adequately protected, the firewall on the rest of the network is merely superficial (van der Linden, 2007, p. 19, 20). 3. 3 Unmanaged backdoor connectionsEvery network in the world has a variety of backdoor connections that network administrators use or even some that the software developers build in. When unmanaged, these connections can create security problems for the entire network infrastructure. Some of these even have the capability to bypass the perimeter security systems, and hence are extremely problematic (van der Linden, 2007, p. 19, 20).

3. 4 Lollipop model of defenseMost of the perimeter protection systems operate on a lollipop model i. e.

with a hard exterior and softer vulnerable interior (Figure shown in APPENDIX). The main vulnerability of such a system is obviously that once an attacker has breached the perimeter defense, the network inside is completely exposed. Another closely related limitation of the lollipop model is that it does not provide for different levels of security. On a computer network, as is mentioned earlier, firewall is limited in its abilities, and hence it should not be expected to be the only line of defense against intrusion. Hence, many network experts suggest the layered Onion model of defense as against the perimeter protection security (Bragg, Rhodes-Ousley, Strassberg, 2004, p. 38).

3. 5 Impact of Wireless technologyNetwork perimeter security is only useful if there are adequate physical security controls to prevent an unauthorized user from simply walking up to and plugging into the internal network. Thus without physical access to the network, a malicious user is required to use the weakness of the corporate perimeter security controls to gain access. With the advent of wireless technologies, a new set of threats to perimeter security is emerging.

There are major risks to perimeter security for companies that have not actually deployed a wireless solution. Companies that deploy wireless solutions must recognize and mitigate the risks associated with an unauthorized individual gaining connectivity to the corporate LAN via wireless signal leakage outside of the corporate control premises. By simply getting physically close enough, a malicious user with a laptop and a wireless LAN card may be able to get an IP address on the network. It is

possible to mitigate such risks by configuring wireless access points to only accept authorized wireless cards. However, such configuration requires extra administration work and do not scale beyond a limited number of users (Bragg, Rhodes-Ousley, Strassberg, 2004, p. 201, 202). 3. 6 Insufficient trainingRegardless of the computerized barriers a perimeter protection offers, it can always be breached by people on the inside, if they are so inclined.

Simply buying and installing software and hardware does not solve the problem if the security policy runs counter to the organizational culture and in the absence of training and policing. For instance an employee may dial his or her own dial up service provider while connected to the corporate LAN, which would obviously be more vulnerable to outside threats, making the entire network vulnerable. Hence, clear security and usage policies are just as important while implementing perimeter protection.

The protection system also must not be too tight, to tempt employees to deliberately look for breaching the systems using external proxy servers etc. (van der Linden, 2007, p. 22). 4 ConclusionAlthough perimeter protection is the most basic and common forms of network security, it is by no means complete. The risks of threats in the present day organizations are both internal and external. In addition to this, a continuous upgrading and evaluation mechanism is also required to keep the companies on par with the security required. The access to internet is perhaps the single most important place where the security breaches usually take place; hence this point of access must be closely guarded as well as administered.

With the advent of wireless technologies, the safety of the network has not only become more difficult, it has also become more necessary. Care must always be taken so that the perimeter security is not the only security measure available with the network, and that the security system is leyered which offers additional protection against malicious attackers. 5 ReferencesBerson A, Dubov L, Dubov L, (2007), " Master Data Management and Customer Data Integration for a Global Enterprise", Published: McGraw-Hill Professional, NewYorkBosworth S, Kabay ME, (2002), " Computer Security Handbook", 4th Edition, Published: John Wiley and SonsBragg R, Rhodes-Ousley M, Strassberg K, (2004)," Network Security: The Complete Reference", Published: McGraw-Hill Professional, CaaliforniaCarvalho FD, da Silva, 2006 EM, " Cyberwar-Netwar: Security in the Information Age", Published: IOS Press, AmstredamStewart JM, Tittel E, Chapple M, (2005), " CISSP: Certified Information Systems SecurityProfessional: Certified Information Systems Security Professional Study Guide", 3rd Edition, Published: Wiley_Default, CaliforniaThomas TM, Thomas T, (2004), " Network Security First-step", Published: Cisco Press, Indianapolisvan der Linden MA, (2007), " Testing Code Security", Published: CRC Press, Florida 6 APPENDIX6.

1 Lollipop Model of Defense diagram(Bragg, Rhodes-Ousley, Strassberg, 2004, p. 38)6. 2 Research paper is a piece of academic writing that requires a more abstract, critical, and thoughtful level of inquiry than you might be used to. Writing a research paper involves (1) first familiarizing

yourself with the works of “ experts”–for example, on the page, in cyberspace, or in the flesh through personal interviews–to build upon what you know about a subject and then (2) comparing their thoughts on the topic with your own