Data networking devices

Business

Network security is a way to address the protection of data networking devices, connections, and the contents and the ability to accomplish the communication functions. Having an effective network security will ensure that the company is safe from malicious intruders, who want to gain access to their vital information (Curtin, 1997). By using a WAN network, the Cleveland office should put in place security measures, which will ensure that its information is not accessed by unauthorized people. The office should therefore develop security policies that will ensure that the information and networks are prevented from any illegal access.

These policies would include the use of passwords, acceptable use and identification of the people using their network. This will ensure that only trusted personnel can access the network, and thus this will assure that they cannot compromise the network (Kahate, 2003). There are various ways through which the office can be able to ensure that the network is safe from being accessed by malicious people: Use of firewalls This is computer software which protects the system by blocking all unnecessary ports and only allows traffic to flow from known ports, and in the right direction. This is important software, which should be used in any organization committed to protect its network from being accessed y intruders, and gaining access to the company’s information (Qualys. com , 2010). Switch The switch should be configured in such a way, that it would allow only specific format of packets to flow in and out of it.

RoutersTheir main purpose is to provide packet routing, which can be configured in a special way. Thus, it can be used as a defense for protecting the network from the unauthorized access. This configuration will make the

router to block or filter the forwarding of certain packet types. Use of strong antivirus The Antivirus software detects viruses and ensures that they do not invade a computer or server. The antivirus should be kept up-to-date, since expired antivirus is not able to detect newer versions of viruses.

The office should be able to evaluate the best antivirus to use, as there are many antivirus software available and some maybe not effective in computer protection (Qualys. com , 2010). Use of wildcard mask This shows which part in the IP address a particular user should access. It indicates which IP addresses has been accessed. The office should ensure that the IP addresses they allow or permit are from trusted sites which might not compromise the network (CCurtin, 1997).

Access control list This is a table that instructs the operating system as to which access right every user has in a particular system object, such as the file directory. This filtering of traffic will be helpful in protecting the network, as it will ensure that the required personnel are the ones accessing the network. This should be configured for the entire routed network. If Cleveland office applies all the above mentioned measures to their network, they will be able to reduce the chances of their network being compromised by any unauthorized persons. The office should also have a network administrator, who will be competent enough to monitor the network.

This would make it possible to know when the network has been compromised and necessary measures would be taken as soon as possible in order to reduce the chances of the network being compromised any further. The protection devices and software, which are going to be put in place,

should be working properly. Any malfunction of any of the devices and software used for protection purposes will lead to the network being compromised. Thus, the office should ensure that the devices and software are working effectively, as they might be put into place and yet not function, which would lead to the deceptive illusion that the network is protected. (Kizza, 2005).