The usage of the internet by a number of people

Technology

Network Security Introduction 'Every computer is a Network' - So the saying goes. Every computer because it is connected to the internet or to the local intranet has become a part of the network. This makes the PC as much susceptible to the vulnerabilities of the network as any other network might be. The nature of the vulnerabilities that a location is exposed to is remarkable. The usage of the internet has multiplied manifold. This by itself leads to a number of ways by which the world might find ways of cheating or robbing an honest person. While vulnerabilities are exploited mostly by people who want to make money there are also others, who do it for the entertainment. The internal vulnerabilities are to be countered so that possession of one is not used by the other.

The need for the Security
The PCs in the school are used by a number of people including students and staff. But there are at least ten times more students who use the computers compared to a staff. Students in a school are to be exposed to learning exercises in the internet and not to the other derogatory experiences that one might get on the internet. Internet is a source of both good and bad. It is the duty of the person to segregate them and use them as he deems fit. However, in the case of the students, on many occasions, they may not be in the right position to identify whether what they are doing is right or wrong. Therefore, the responsibility lies with the staff to ensure that they educate themselves appropriately and not in any other way.

The security in School
The security in school is therefore, very important. One, to ensure that no

viruses or worms come into the system; secondly, this is also to ensure that there is no unsolicited visitor into the network. Thirdly, the security should also ensure that the students are provided access to those that they are allowed to see and are not provided permission for those that they are not allowed to. This security is implemented in the school using the following:

1. Hard firewall has been provided at the entry of the internet in to the school campus. This protects the network from unsolicited visitors over the network; hacking is stopped by this process. There is no intrusion detection software that has been put in place since the vulnerabilities foreseen does not show a large probability of people making unsolicited visits breaking through the firewall.

2. An online anti-virus, anti-worm and anti-Trojan system has been implemented on the network. This works on one of the servers and uses a thread to keep track of the file transfers and communications to ensure that there is no virus movement or signature.

3. The firewall also provides for settings to stop access to specific certifications in the sites accessed. This is set appropriately to ensure that the students do not access the unwanted web sites. In the school, the students are not allowed to access even the mail based websites since that would start off a new communication channel.

4. Internal vulnerabilities are countered by employing appropriate password protected network and continue maintaining it that way.

Conclusion

Therefore, school is also vulnerable and might get hacked; spoofed or such other damaging mechanisms might be employed to collect information from

the school and its students / staff. The security in the school with regard to the virus, worms and Trojans would be to counter them with the utmost severity to stop them when they do occur. For the others, adequate security depending upon the level of protection sought.

References

1. Equiinet, 2005, Network Security in schools, available at: http://www. equiinet. com/securepilot/networksecurity/Equiinet_Security %20Report_colour. pdf

2. Robert Brumfield, 25 Oct 2005, Schools need Improved IT Security, eSchool News online, available at: http://www. eschoolnews. com/news/showstory. cfmArticleID= 5923