A brief on network and its security essay examples

Law, Security

Organization

Proposal Argument For Network Secuirty

Abstract

Network Security is an issue whose adverse effects on the society is often undermined. Although the past few years have witnessed a steady rise in the awareness of network security, the issue still has not gained enough importance (Ciprian, 2012). The government is trying to imbibe measures of information and network security but, the efforts are still half-hearted and not well-researched. The whole world today makes extensive use of the “ network”, however what people do not pay any attention to is the importance of maintaining the security of the network.

In this proposal paper, the significance of maintaining information and network security would be discussed in length. The paper would present definite means through which the government can increase the network security for students and well as professionals.

Before we get on to discuss further on the importance of increasing network security, detailing on the exact nature and working of a network is critical. A network is the system of several computers interconnected with each other. The basic fundamental behind the working of a network is to enable computers across different locations to be connected with each other without the necessity of physical presence of the users.

In the 21st century, the people have become completely dependent on the internet and the World Wide Web for conducting business, maintaining personal relationships and for imparting education. Online/distance learning programs have been possible only through the use of network (Whitman et al, 2009). Students share their personal and educational information on the network in order to gain access to the online resources.

Now, this network and its components, on which the students and professionals share their confidential data, is vulnerable and prone to misuse and unauthorized attacks. These unauthorized attacks can significantly compromise the confidential and private information, leading to adverse consequence for the user.

For example, according to a recent study, out of the 50 students pursuing an online learning course from a reputed organization, the accounts of 15 students were compromised. Some unauthorized hackers had compromised the passwords of the online account of these 15 students and were using it for their own illegal research. This example clearly shows how why network security becomes important. Instead of being a high-tech principle, network security is simply the process of protecting any network from an unauthorized access.

Lack of Network Security: A Threat to Modern Society

Many people argue that network security, though important, is not significant enough to be given international concern as it does not pose any immediate threat to the society. However, I would like to argue that network security issues may not pose direct threat but, they definitely have the capability of wreaking havoc on the society (Adesanya, 2012).

Network is the backbone of all activities around us. From maintaining personal relationships through social media platforms to conducting oversees business and developing the economy of a nation, network is the underlying process. There are various threats to the network security such as -:

- Resource Attacks-: These attacks attempt at collapsing the network completely. A resource attacks forces the whole system to crash, thereby making it open to access. Malware and information flooding is the most common way to plant a resource attack on vulnerable system (Hayden, 2009).

Now let us take, for example, an online database containing personal information as well as marks statement of the students studying in a particular university. Each students has his/her personal account on the online portal, through which they upload their assignments and tests and communicate with their teachers and class-mates (Pandey, 2012). If such a network is not secure, a resource attack can lead to manipulations and compromise on the students’ marks, attendance and assignments. Through this example the need for network security and its breach can be established.

Though the consequence of network security may seem far-fetched, if a network is compromised it can shake the basics of a modern society.

- Logic Attacks-: The logic attacks attempt to enter the system by finding any weak gates or entries. Logic attacks are much more harmful than resource attacks because the network users do not even get to know that their information and data is being compromised, in most cases (CERT, 2012).

Cyber warfare is one of the latest and the most upcoming ways of international security breaches opted by nations to gain access to private information which can help then in gaining an edge over the rival nation (Dipert, 2010). Cyber warfare is considered moral by a few leader, but it is the most immoral method of war. Lack of network security in such a scenario not only poses threat to the government, it poses a huge threat to the safety and security of the entire nation.

Strategy for Implementing Network Security

It would be impossible to ensure complete network security unless and until the user of the network is aware and knows how to protect his/her network from compromise. The government is responsible for making strict cyber laws and policies. However, all these policies and laws would fail if the users themselves are not trained. Thus, the government needs to establish a Network Security Training Program to Create Awareness (Adesanya, 2012). This program would focus on making network users, through computers and mobiles, aware about how to maintain security of their network.

The government should make it mandatory for every business organization and personal computer user to undergo this network security training so that they understand their role in protecting their network from malware. The program would include the four basic steps of Secure, Examine, Test and Enhance.

In the first step, the user needs to ensure that their network is well-guarded. Adequate training would be provided on the various anti-viruses and policies that the user can employ to guard their network. The next step is to constantly keep on examining the network activities and regularly check the various safe-guards. The third step is to train the users on the various ways through which the hackers can attack (Adesanya, 2012). Then the users would be trained to test their own networks by getting the network compromised through some trusted source. The last step is to make the user comfortable with the various techniques through which they can upgrade the security of their system.

The Network Security Training Program to Create Awareness would be the most logical and cost-effective way to ensure that each network user maintains the security of his/her network.

Conclusion

Network security is an issue that needs immediate attention from both the government and the users of the network in order to protect the society from any cyber catastrophe. To implement greater network security, the government needs to spread awareness and provide training.

References

- Adesanya, Ahmed. “ How to Improve Corporate Network Security”. ISACA News. 15 Aug. 2011. Web. 25 Jan. 2012.

- CERT Coordination Center. “ Home Network Security”. CERT. com. Carnegie Mellon University. 27 Feb. 2006. Web. 27 Jan 2012.

- Ciprian, Boldea. " Scada Security in the Context of Corporate Network Integration." Analele Universitatii Maritime Constanta (2012): 159-164. Web. 23 Jan. 2012.

- Dipert, Randall R. “ The Ethics of Cyber Warfare.” Journal of Military Ethics 9. 4(2010): 388-40. Web. 23 Jan. 2012.

- Hayden, Lance. “ Designing common control frameworks: A model for evaluating information technology governance, risk, and compliance control rationalization strategies”. Information Security Journal. (2009). 18(6), 297-305. 07 Dec. 2009.

- Pandey, Shailja. “ Modern Network Security: Issues and Challenges.” International Journal of Engineering Science & Technology 3. 5(2011): 4351-357. Web. 23 Jan. 2012.
- Whitman, Michael E., Herbert J. Mattord, Richard D. Austin, and Greg Holden. Guide to Firewalls and Network Security: Intrusion Detection and VINs. 2nd ed. Australia: Course-Cengage. 2009.