Good research paper about attack prevention article evaluation

Business, Company

Technology attackers are very sophisticated and they are continuously discovering new ways in which to attack networks. Their aim is to get access to important information that will enable them steal millions of dollars or trade secrets to sell to competitors. Today the focus of attackers is on data theft and fraud. Top on the target list of these attackers is home users. This is because most people do not see the need to put up security measures. The main reason is because installing security measures is expensive. Most people do not see the likelihood of hackers to target them. According to their perception, they do not have a lot of wealth or important data to make them potential victims of hackers (Joe, 2011).

Hackers also target companies and institutions because they harbor a lot of data. Attacks on companies lead to financial and operational losses. The total loss suffered by the affected company, in most cases, cannot be accurately determined. Surveys carried out by the Computer Security Institute reach the conclusion that most companies and institutions do not have proper plans on how to report or respond to cyber attacks (Joe, 2011).

Computer crime is categorized into three types by the Department of Justice. The three categories include using the computer to commit crimes such as credit card fraud; using the computer to attack other computers through passing of viruses; and using the computer to store stolen data (Joe, 2011). Some of the offences committed through cyber crime include damage to data and programs; computer espionage; unwarranted access; interception of data without authorization; and sabotage on the operations of a network. Small and medium sized businesses are more prone to cyber attacks compared to large companies. This is because the former do not put in place

high IT security measures compared to the latter. This is a perception by most cyber attackers and they therefore, find it easier to attack smaller companies (Joe, 2011). One of the ways that the cyber criminals use is the installation of malware which is software that silently reads and uses the user ids and passwords. The hacker gains access to the victim’s information and use it to commit fraud. People are advised to install software that will protect the computer from malware and viruses. Only one computer should be used to surf the web and read mails and the security settings should be up to standards. Systems scans should also be done regularly.

Cyber criminals are continuously looking out for small errors committed by companies so that they can gain access to the information they need. The cyber criminals affect companies through interruption of business, data theft, launching attacks on networks and compromising the companies’ computers. Some of the errors committed by companies include poor handling of data, neglect of security updates, choosing convenience over security and failing to maintain the online identifiers of a company (Joe, 2011).

The private sector of the US has been unable to protect their network information from cyber criminals. Most of these business owners have not invested in the technology and skills required to secure their network from cyber attacks. This has led to the vulnerability of areas such as financial services and the electrical grid (Joe, 2011). This has enabled attackers such as spies, organized gangs and foreign intelligence to gain access to companies, banks and government sites. The government needs to come up with regulations which will help to secure the networks of the US.

Companies need to adopt prevention measures to ensure their safety from

cyber criminals. Some of these measures include hardening of systems by configuring secure software; patching all the systems; installing firewalls; assessing the network security through port scanning; using different passwords that are hard to crack; using encrypted connections; limiting access to your servers; avoiding the installation of software from unknown sites; using Anti-Virus software; and avoiding systems that have already been compromised by hackers (Web Solutions, 2010). It is important for every person to employ attack prevention systems so as to enable them avoid huge losses due to attacks. Prevention is always better than cure.

References

Joe DePaola, (2011). Cyber Attack, Internet Crime, Hackers: Impact on Business Performance: Menace, Threat, Warfare. Retrieved from http://bizshifts-trends. com/2011/05/26/cyber-attack-internet-crime-hackers-impact-on-business-performance-menace-threat-warfare/

Web Solutions, (2010). Hacking Attacks – Prevention. Retrieved from https://www. crucialp. com/resources/tutorials/website-web-page-site-optimization/hacking-attacks-prevention. php