Free computer security threats case study example

Law, Security

Personal Computer Security

Personal Computer Security

Computers have made lives better and complex tasks easier to perform. Internet services on computers make one connected virtually to the almost any part of the world. Along with the convenience, efficiency and ease of information available through the computer networks, the exposure to security threats has tremendously increased. Cyber criminals popularly known as hackers are persistently trying to devise new ways to breach user privacy so as to gain access to sensitive information such as credit/debit card details and personal information .

Virus

A virus is a program with the ability to replicate itself inside the computer . A computer virus may spread through the internet, computer networks, and removable media such as CDs . An infection of a computer system with a virus may result in data loss, deletion of files, hard disk reformatting, frequent system crashes, and decreased system performance .

Spyware

Spyware is a software program installed secretly without the consent of the user to gain access to user sensitive information . A spyware intends to monitor a user’s online activity . Spyware programs installed on computers may cause web browsers to be redirected to some hostile websites or may alter system settings .

Trojan horse

Trojan horses are software programs which install “ back door programs” into a user’s system without user’s knowledge . These “ back door programs” are used by hackers to gain access secretly into the computer system of the user . Trojan horses can erase or overwrite data on a computer, corrupt files, install a malicious program such as virus and worm, deactivate or interfere with the antivirus or firewall of the system, and provide remote access to user's computer .

Common Techniques Employed by Hackers to access Information

SQL Injection

Taking advantage of the improper coding of the web applications, hackers inject SQL codes for their execution in the backend database . This is possible only in the fields where user input allows the SQL codes to pass through and query the database directly . Through this technique, hackers gain access to the sensitive information stored in the database .

Phishing

Cyber criminals create a fake web page which looks like an exact replica of the original website . Spam emails are sent to recipients with a link to the spoofed malicious website attached in the mail . When a user accesses such a dummy website thinking it to be original by clicking the malicious link, the sensitive information such as user name, passwords, credit / debit card details are captured by the hackers . The hacked data can then be used for

creating fake accounts, making bank transactions, thereby ruining the victim’s credit rating

Botnets

Botnets are a collection of bots or “ zombie computers” that run malicious programs such as virus, worms, Trojan horse or backdoor programs over the internet . They are commonly used to launch Denial of Service attack against the website servers .

Denial of Service Attack

Denial of service attacks is targeted to crash or hang up a server by redirecting large volumes of traffic to the server, thereby making the service unavailable to the legitimate users . Botnets and network of zombie computers are used to institute such an attack .

Conclusion

With the development of new technologies, internet has evolved tremendously over the years. Various anti-virus programs and ethical hackers have worked hard to develop programs which make computer networks safe and secure. But with time, the hackers have also developed new and innovative techniques to break into secure networks by identifying the loopholes in the security mechanisms. The onus is on users to adopt the latest security mechanisms and indulge in safe practices to avoid security thefts in this technological era.

References

Acunetix. (2014). SQL Injection: What is it? Retrieved June 2, 2014, from Acunetix: https://www. acunetix. com/websitesecurity/sql-injection/

Aloe, S. (2011, June 20). Why Do We Need Computer Security. Retrieved June 2, 2014, from hubpages: http://saraalgoe. hubpages. com/hub/Computer-Security2

Douglas, T. L. (2010, July 16). Is Internet Security Really That Important? Retrieved June 2, 2014, from Ezinearticles: http://ezinearticles. com/? Is-Internet-Security-Really-That-Important?&id= 4683951

Garber, L. (2000). Denial-of-Service Attacks Rip the Internet. Computer, 12-17.

Kaspersky. (2014). Internet Security Center. Retrieved June 2, 2014, from Kaspersky: http://usa. kaspersky. com/internet-security-center/#. U4yMJfkbWtm

Norton, S. (2014). The 11 most common computer security threats. Retrieved june 2, 2014, from symantec-norton: http://www. symantec-norton. com/11-most-common-computer-security-threats_k13. aspx

Webroot. (2014). Computer Virus Information. Retrieved June 2, 2014, from Webroot: http://www. webroot. com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses