Term paper on networking

Law, Security

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Introduction

With the advancement in technology, especially with regard to information systems and online presences of services, many advantages have been realized. In fact, businesses can be transacted online fast and effectively. With these advantages also come concerns that are associated with it. Security is a major concern for these systems. Every organization is keen to ensure that their systems are security proof. Criminal hackers will always find ways to circumvent the security measures put in place by organizations. In order, therefore, to ensure that this problem is dealt with effectively, some organizations test their systems by use of in house hackers or employed hackers to do the job.

Hacking

According to Palmer (2001), hacking is described as the rapid crafting of new program or the making of changes to existing, usually complicated software in order to gain access to its resources without the authority's' knowledge. In

this paper, hacker has been defined as anyone who intentionally attacks security system of another entity for the purposes of gaining access to the systems in questions for malicious purposes.

Ethical hacker is defined by Palmer (2001) as a computer or a network expert that intentionally attacks an organizational system with the full knowledge and permission of the organization, in order to establish vulnerabilities associated with the system and hence provide effective solutions for the same. Ethical hacking therefore involves the involvement of ethical hackers by an organization to test their security systems.

Ethical hackers

An ethical hacker must have good programming and computer skills. Ethical hackers in most cases have a clear understanding of the criminal hackers' operational modes. They are patient and are willing to spend days observing the system and programming. The difference which differentiates the ethical hackers from the criminal hacker come in the sense that, criminal hackers do their hacking for malicious purposes while ethical hackers do it for the greater good.

Ethical hackers are involved in a number of activities in their daily work. In his/her work, the ethical hacker seeks to answer some questions. These questions include;

What an attacker on the system targeted can see?

How can the intruder access the information?

What can intruder do with the information?

Can an intruder’s attempts or successes be noticed in the target system?

These are some of the questions that an ethical hacker will strive to answer and provide solutions for in the system (Ec-Council, 2009)

Is ethical hacking justified?

There has been a big debate in the information sector industry concerning this question. Many have come out with the proposition that hacking is ethical if the owner of the system is aware of it and has given a go ahead to the hackers. The big questions being raised includes extend of the hacking by the hackers (Logan, & Clarkson, 2004)

Issues come out to the effect that how can a company trust a potential enemy to navigate freely in to the company’s system. By virtue, that the hacker is able to do the job makes him/her a target. Jamil et al (2011) argues that hacking is unethical. In his reasoning, Jamil notes that there is nothing to be termed as ethical in hacking. An ethical hacker gains access and increase his knowledge on the security standards and implementation of the organization systems in question. In future out of curiosity, the same hacker could hack in to the system again or if a breach of contract happens, the hacker could sell the information concerning the same to criminal hacker (Wulf, 2003). This would result in a self-inflicted problem to the company.

There is the case of risk management. An ethical hacker is mostly given a few days to work in the systems. The client on his part will expect that after the hacker goes through the system that the system will be safe. What

should happen if an external hacker gains access to the system then? Ethical hacking will introduce laxity to the management. All that will be thought is that the system is secure and that no one can hack in to it. Practices that would have been implemented daily and monitored would be forgotten. This will therefore introduce bigger vulnerabilities to the system than before (Wulf, 2003).

Considering the discussion above, it would be unrealistic to say that ethical hacking can actually be justified. Human mind is hard to control and there is bound to be cases when the ethical hackers will be tempted to reveal the secrets of the system or even hack them themselves.

Conclusion

It is prudent if proven and tested security measures are just implemented in any information system. This will call for constant monitoring of the systems and any sign of attack can be dealt with immediately. Ethical hacking is bound to create problems between the hacker and the client who might think that once a system is hacked by an employed hacker, it is safe from any other types of attack.

Reference

Ec-Council (2009). Ethical Hacking and Countermeasures: Attack Phases. New York. NY: Cengage Learning

Jamil, D. & Numan, M. A. (2011). Is ethical hacking ethical? International journal of engineering science and technology (IJEST). 3 (5), 3758-3763.

Logan, T. & Clarkson, W. (2004). Is it safe? Information security education: Are we teaching a dangerous subject? Proceedings of the 8th Colloquium for

information systems security education. West Point, NY.

Palmer, C. C. (2001). Ethical hacking. IBM systems Journal . 40 (3), 769-780.

Wulf, T. (2003). Teaching Ethics in undergraduate network. Consortium for computing

science in college, 9 (1)