International Journal of Information Technology and Knowledge Management (ISSN: 0973-4414)
July-December 2012, Volume 5, No. 2, pp. 462-464

SAFE COMPUTING IN THE ERA OF CYBER CRIME

Hitesh Ahuja, Dr. Rajesh Verma
Research Scholar,CJM University, Shellong
Deptt. of Comp. Science & Engineering, KITM, Kurukshetra
kurukshetracallhitesh1977@gmail.com

Abstract: Life on the internet is a different experience. There are many parties who are interested in who you are and what you do on the Web, all with different intentions. It is because of this that initiatives such as the Electronic Privacy Information Center (EPIC) and the World Wide Web Consortium (W3C) Platform for Privacy Preferences (P3P) were launched. Among the many examples of potential intrusions on your personal privacy include. Details of your hardware and software configuration, the browser you use, your assigned IP (Internet Protocol) address are readily available to the websites you visit. The IP address is usually sufficient to give an indication of your physical location. The owner of a Website will want to know, for example, when you access the Website, what pages and documents you look at, whether you download items or not, whether you look at advertisements, etc. To do this, they place cookies on your computer, and employ spy-ware and other devices to track such use.

Introduction

Who is reading your e-mail" Tools which are used to monitor the contents of e-mail messages (such as Carnivore and Echelon) may also used by an employer to monitor the content of messages for abusive or improper language, personal rather than business use, etc. Not all employers have clearly articulated policies about their rights and yours, and without such policies, many problems can arise, largely influenced by the national legislation concerning the rights of individuals.

Policies for staff monitoring

What you to do in your home, through your personal access to the Internet and the Internet Service Provider of your choice, is usually your own business, unless your employer has advised you otherwise. Using your employer's corporate network from your home, or surfing the Web, downloading software and doing your personal e-mail, may be in conflict with the employer's security policies and practices. These policies should normally be clearly disclosed to all staff.

Privacy at work is a major topic in its own right, for which there are no fixed rules. Legislation on this matter is either incomplete or ambiguous with the exception of criminal or civil investigations when there is "sufficient cause". Otherwise, it is a matter for very clear communications between management and employees. It's wise to assume that there is NO privacy at work, and that this applies no only to computer systems, e-mail, etc., but also to the use of telephones and fax machines.

User IDs/Passwords or physical devices

It is always a good idea to protect your computer, particularly notebooks and other small devices to prevent access by others. Such protection can take many forms ranging from a well designed

User ID and password to the use of physical devices such as Smart Cards or small pieces of hardware (commonly referred to as "dongles") that need to be physically plugged in, usually in a parallel port.

Cryptography is the second mechanism for ensuring privacy since the invention of writing and has been in used in many different forms. Cryptography is usually reserved for the most highly confidential messages and has a counterpart in Cryptographysis, the process of braking ciphers – something that is not always possible at present).

Credit card number details should never be disclosed without making sure first that the connection is in fact encrypted – this is usually indicated by an icon such as a closed lock or padlock or an unbroken key as well as by a web address (URL which begins with https//) – if the web address does not have this "s" at the end of the "http" is not a secure site.

Safe Computing Practices

Ensure that you have all the material necessary to rebuild your software and:

1. Consider not being "permanently connected" as you are with DSL and cable modems. Such connections use a static IP address that makes them especially vulnerable to potential hackers.

2. Ensure your Internet browser is sufficiently recent to incorporate security features and make certain these are correctly configured in your computer.

3. Keep copies of all original and licensed software, together with appropriate ID codes and documentation needed to obtain updates and technical support.

4. Ensure that your freeware is from a reputable and recommended source and that your shareware meets the same criteria as freeware AND is registered with the provider.

5. Look for an install updates to virus definitions, personal firewalls, browsers and other software on which the security of your computer depends.

6. Monitor alerts and development in malicious software from the Press or appropriate websites. Take appropriate action immediately if a patch is required for your computer.

7. Consider upgrading your software to a newer version or major new release if it contains features that will enhance your confidence in the security of your arrangements.

8. Enable anti-virus software and personal firewalls to operate in the background all the time. Moreover, test for the presence of viruses, Trojan horse and other malicious software on a regular basis: this vigilance malicious software on a regular basis: this vigilance should reflect the value of the software and data in your computer to your personal life.

Conduct intrusion detection tests

Some 15 years ago, a leading IT journal, Datamation, carried on its cover the following text: "How good is your I.T. shop? Find out before your boss does." This message remains valid today, and in the particular case of information security, it is strongly recommended that regular and serious tests be carried out to validate security arrangements before someone else exploits any weaknesses. Such tests may include one or all of the following:

- Pre-announced tests carried out by staff
- Pre-announced tests carried out by a trusted third party
- Unannounced tests by staff and/or a trusted third party
- Intrusions detected by an unknown and thus untrusted third party (hacker)
- Security tests performed during a test of the disaster Recovery Plan.

It needs to be recognized that successful tests do not constitute a guarantee. They simply mean "so far so good". At the end of such tests, any successful security breach regardless of its nature virus attack, Denial of Service attack, intrusion leading to access to data, or other, should be the subject of a detailed review of the technical and procedural weaknesses in the arrangements.

Restore systems and facilities

This action is needed to restore a compromised system to normal operation and allow staff to have access to that system again, possibly even before a full analysis is completed and all corrections are made. In this case, the risk of doing so needs to be managed and monitored, in particular focusing on continued analysis of the incident, elimination of any intruders' access, and acknowledge the vulnerability to similar types of intrusion.

One of the purposes of a response process is to eliminate vulnerabilities that allow a security incident to occur and to return affected systems to full operational status. The first step towards restoring a system is the determination of the requirements and timeframe for returning the system to normal operations. This cannot be achieved without the involvement of senior management.

References

1. http://www.ccrduindia.com/
2. D. Smith, and W. T. Rupp, "Issues in cybersecurity: understanding the potential risks associated with hackers/crackers," Information Management and Computer Security, vol. 10, no. 4, pp. 178-83, 2002.
3. Castells, M. (1996) The Rise of the Network Society, The Information Age: Economy, Society and Culture, Vol. I. Oxford: Blackwell.
4. D. MURALI AND GOUTAM GHOSH Security is an ongoing process pg23.
5. Nosworthy, J. D. (2000). Implementing information security in the 21st century- Do you have the balancing factors? Computer & Security, 19, 337-347.