COMPUTER FORENSICS IN THE BUSINESS ENVIRONMENT

Neven Bratranek, Boris Bereček
Teched Consulting Services
Radnička cesta 80/VII, 10000 Zagreb, Croatia
{nevenb, borisb}@teched.hr

Robert Kopal
Visoka poslovna škola Libertas
Kennedyev trg 6b, 10000 Zagreb, Croatia
krobert@hi.hinet.hr

Abstract. *Over recent years, computers have penetrated almost every area of business and personal life. Its resources for organizations are available 24 hours a day and enable electronic business activities between clients, other organizations or state administration during which important data is exchanged. A negative consequence for such development in technology and society is the increasing number of mobile devices, portable and desktop computers and servers from which information may leak, or which may even be used for criminal activities - whether done by malicious employees of the organisation or other malicious individuals. Thus it is important that all those who manage or administer information systems and networks be familiar with the protocols foreseen in case of security incidents together with the principles of computer forensics.*
This article explains the requirements for the implementation of computer forensics in a business environment in an efficient and legal way, whilst also providing a review of basic technical issues, indicating references for further reading. The purpose of this article is to demonstrate the idea that business implementation of computer forensics in case of security incidents is important for today's business environments and networked organizations, just as it is important to be aware of the legal background of its implementation.

Keywords. computer forensics, security incidents, computer safety, data collection and analysis, security policies, legal framework

1 Introduction

Due to constant growth in the use of information technology (IT), organizations throughout the world are faced with the challenges of protecting valuable information resources from malicious users both outside and inside the organization itself. Computers and the networks connecting them, process, store and transfer information which is important for the everyday business of the organization and consequently attract malicious users and programmes. Sometimes those malicious users are in fact disaffected employees that deliberately cause damage to the organization but more often such users are part of a group wanting to gain some form of material benefit by stealing money, information or the identity of other users. It was proved long before the computer era that criminals track money and money [1] today is increasingly transferred electronically.

As well as this, the understanding of the legal and technical framework of computer forensics helps in gathering vital data in cases when the computer and network infrastructure is compromised and for the legal chasing of those responsible when such cases are discovered.

2 Security incidents

The protection of vital IT resources requires not only the implementation of cautionary measures and security policies aimed at their protection but also the possibility of a quick and efficient reaction, should such security incidents occur. However, it is not easy to respond to security incidents. The appropriate answer to the security incident requires technical knowledge as well as communication and coordination between the staff responsible for intervention. Within organizations, often the system and network administrators are the first to face such an incident and are also the first responders, so it is essential that they know the basic areas of computer forensics and the procedures they have to take care of during interventions on the compromised computer system or network. In order to be able to react

adequately to incidents, it is necessary to be able to recognize them. In the following text there is a list and explanation of security incidents for which the correct response is to use computer forensics methods [3].

2.1 Attack by malicious programs

Malicious programs are called viruses, Trojan horses, worms and scripts by which malicious users obtain permission from the organization's computers or computer networks, to obtain possession of authorized users' passwords or to change log files for the purpose of hiding unauthorized activity. Malicious programs that are programmed to hide their presence create great problems as their presence on the computer is very hard to discover. Besides this, malicious programs such as viruses or worms have the possibility of multiplying in great numbers, so stopping their spreading is quite a challenging job to be undertaken.

2.2 Unauthorized access

Unauthorized access includes a set of security incidents, starting from irregular user log-in within the system itself, in the case when a malicious user logs into the system with the username and password of an organization employee, to the unauthorized access of a malicious user to files and directories situated on local or network disks using higher (or administrator) authorizations. Unauthorized access also includes the access to network data of some organizations by substituting an unauthorized programme that intercepts all network packages passing through a particular part of the network, and enables the malicious user free access to the data contained in those packages. In such a way he can obtain, for example, the passwords of authorized users which are transferred through the network, and use them for further malicious activities.

2.3 Malicious use of the service

Entering into possession of information within the organization can be achieved by abusing the server and programs that provide the service using the security failures within them. Examples of this are the abuse of web or FTP server services – by taking over control, the malicious user can enter inappropriate content and use the server for their further distribution.

2.4 Denial of Service – DoS

Users rely on the work of particular services that the organization provides them with through the Internet. A malicious person can upset the functioning of such services and deny access to users in several ways: by deleting the program providing the services or by swamping the server with false or invalid requests, in such a measure that the server is unable to provide services to authorized users with valid requests.

2.5 Inappropriate usage of information resources

It can be said that the inappropriate usage of information resources is using the information resource for purposes not determined by security policies, such as using the official computer for saving inappropriate (e.g. pirate) software.

2.6 Spying

Confidential information of organizations and state administration bodies can be of great value to other organizations and governments, so intrusion into information systems for the purpose of spying and stealing information is a serious security incident.

2.7 Hoaxes

Hoaxes refer to the spreading of false information regarding the presence of security errors in programs. Users are misled by false information and alerted to particular false threats and on occasion are also asked to delete important programs on the computer they are working on, thus causing damage.

3 Computer forensics

When one of the aforementioned security incidents occurs within an organization, depending on the damage caused, it is essential to investigate how the incident occurred, and then to carry out correctional actions in order to rectify the failures that enabled the damage to occur in the first place. The task of computer forensics is precisely the research of such incident details. Computer forensics can be defined as "collecting and analysing data from computer systems and networks, communication channels (e.g. Wireless networks) as well as saving media in a form suitable for the court" [2]. It is a relatively new scientific discipline but already it has a great and important application in real situations, and an ever increasing number of security investigations (criminal ones too!) within the business environment include the use of computer forensics.

4 Computer forensic procedures

When a security incident is discovered in a computer system, it is necessary to collect all clues and information that could explain how the incident occurred. There are two objectives of the initial response to a possible incident: to confirm that the

incident has actually occurred and then to collect all data not recorded on the system hard-disk and which would be lost once the system was down. During this initial response to the security incident, as few actions as possible should be performed on the compromised system, because every action may have as a consequence the modification of data, making more difficult any further collection of data.

Any program that is used for extracting data from the compromised computer should not be executed from that computer itself but rather from a specially prepared CD, DVD or USB memory stick. Professional forensic tools such as EnCase have the possibility of collecting data from compromised computers through the computer network and performing this action in such a way that the compromised system "is unaware" that such a forensic program has been started on it and that data has been collected from it. Moreover, all collected data should not be stored on the compromised system, because in this way it may influence the system and destroy the evidence. All collected data should be stored on external memory or via the computer network stored on network locations.

4.1 Verification of the integrity of collected data

If it is necessary to prove that collected data has not been changed from the moment of its collection, it would be best to create hash of the files in which the collected documents may be stored during data collection. The easiest way of doing this is by using a tool for hashing. The hash, which is usually a number, should be recorded in parallel with the file in which the collected data is stored (in another file or on paper) so it can be used later as proof that the file with collected data has not been modified. In fact, it is enough to calculate the hash number again later and compare the resulting number with the recorded number. If hashes are identical it means that the file has not been changed. It is recommended to use hashes given in standard algorithms like MD5 and SHA-1 [5].

4.2 Getting data from the live system

Regardless of whether during the initial response to the security incident, a professional forensics tool or an independently collected set of tools for a particular purpose is used, the minimum set of data that must be obtained from the live system are [1]:

- System date and time – start of collecting the data;
- A list of users currently logged into the system;
- Date and time of creation, modification and access to all system files as well as their size;
- A list of currently active processes on the system;
- A list of open network ports and applications related to those ports;
- A list of the current and recent network connections stored in the cache of network protocols;
- Event logs registered by the operative system;
- System configuration files (e.g. registry files in the Windows operating systems);
- System date and time – end of collecting data.

In the case of a serious incident, usually after turning off the system, an identical copy of the system permanent memory, i.e. the hard disk, is carried out for further forensic analysis. Prior to this, it is also necessary to store the following data from the live system:

- Names and passwords of user accounts present in the computer;
- Content of RAM (random access memory).

Names and passwords of the user accounts that will be stored from the live system will be needed later, after a forensic copy of the compromised system is completed and after the forensics expert tries to log-into such a system to make a detailed overview. Considering that it is an identical copy, he will be able to log-in using the username and password of any of the system users. It is recommended to use those with administrator authorization.

RAM content is also an important detail that should not be forgotten during forensics analysis. Computer RAM may contain different data that would disappear by switching off the computer.

Once the collection of this data is finished, the computer is usually switched off, normally by simply removing the electricity cable from the wall socket. This ensures that during the standard procedure of switching off the operating system data on that system will not be changed, deleted or rewritten and potential evidence will not be destroyed.

4.3 Forensic duplication

A copy of data stored on the hard disks of the compromised computer may be done by removing those disks and connecting them to another computer, used for forensics analysis. Such disks from the compromised computer are always connected to the second computer for analysis as secondary disks which are disks from which the operating system is not loaded. This action is necessary because the operating system, when starting up the computer, stores data on the disk and in so doing may modify and destroy evidence. When the disk is connected as a secondary disk, at the lowest physical disk level (sector by sector), it reads the content from it and stores it in the file on the disk of the computer used for analysis. Such a file containing content from the compromised computer disk is called a forensics copy [1] and will be used for forensics analysis purposes – the original disk is no longer used.

The size of the forensic copy is identical to the disk size as all the information stored on the compromised computer disk is copied. So, even if a forensic copy is made of a disk on which the files stored only occupy 1% of the space, the file for the forensics copy will be made using 100% of the size of

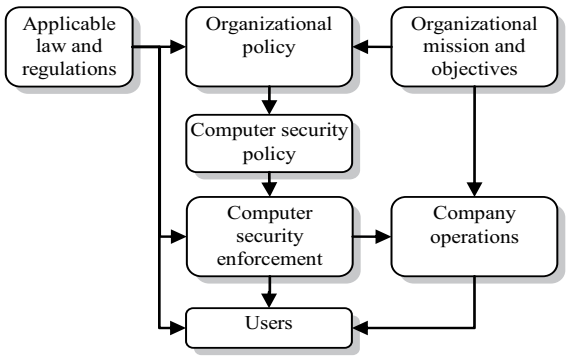
the disk. The reason for this is that it is possible that some files may have been stored on the disk but have been deleted at the last minute. As with standard deleting, the content of these files is not deleted, only the data about them, the file content can still be reached using different tools.

5 Organizational policies, security and computer forensics

Implementing adequate tools and security policies and enabling computer forensics when necessary, helps organizations to create integrity and sustainability of their infrastructure. It is important that each organization consider computer forensics as a new basic element in the so-called „defence in-depth" strategy to insure the computers and network infrastructure of the organization.

Picture 1 [7] shows the international framework of organizational structures that enables a more rapid undertaking of investigations in the case of security incidents and a higher quality of electronic evidence. During these procedures, employees are exposed to multiple authorities and must, as well as laws, respect all organizational and security policies established on the basis of the mission and targets of the organization, and which, in turn, they must reconcile with the legal regulations.

The wider definition of the aim of computer security is to ensure that the system functions as defined by the security policies. The purpose of computer forensics is to discover and explain how a particular security policy has been breached. Such a procedure of discovery can also identify errors within the security policy itself.



Picture 1. International framework relating to organizations with defined security policies that enable the collecting of electronic evidence in the case of security incidents [7].

5.1 Policies in the implementation of computer systems security and forensics

There is a specific overlap between the data that is necessary for computer systems security and that which can be used for computer forensics. Many security measures, if implemented completely, facilitate computer forensics: Event logs, computer systems access logs, error logs, traces of attempts to access computers, etc. are just some of these. Countermeasures for unauthorized access to the computer, such as smart cards for access to the computer itself, security policies for the complexity of passwords or a limited number of unsuccessful logins, together with the policy of registering the unsuccessful login, leave traces for further analysis.

Nevertheless, in practice, only minimal measures of recording are used, because of the influence they could have on the system performances. Files with event logs have configured fixed sizes in order to avoid filling up the disk space, whilst the logic of recording within them is such that the old values are overwritten with the new ones and data needed for forensics investigation is lost. Numerous security countermeasures are based on cleaning the computer system of data which is unnecessary for normal operation, such as deleting the history of web pages which have been viewed, in addition to temporary files. Procedures for accelerating system performance can also delete forensic data. One of these procedures is disk defragmentation, by which data on the disk is reorganized and disk content is overwritten in spaces where incompletely deleted files may be situated. Antivirus programs, when performing automatic virus cleaning, may also effect data, so it is important that all automatic activities are recorded in files with event logs and when viruses are found, that they are not deleted, but put, e.g. 'into quarantine'.

Managing security risks and estimating security threats are generally effective in protecting the computer system. However, as the majority of organizations are focused on prevention and system performance rather than on enabling procedures of computer forensics, it is more than obvious that due to this, data collected in the case of security incidents will be either incomplete or there will be no collected data.

Therefore, it is necessary to determine policies within the organization by which the system will work optimally and all security policies needed for the implementation of computer forensic procedures in cases of security incidents will be implemented.

6 Important legal framework necessary for computer forensics

Nowadays people are more and more conscious of protecting their privacy. However, the protection of

privacy and resolving security incidents or computer crimes are two almost conflicting activities. Legal implementation agencies have to have access to as much of the data as possible stored in an electronic form, such as for Internet banking, a list of telephone calls, electronic mail, internet connections, etc. whilst citizens are concerned about the abuse of their private data and privacy. So, one part of the law takes care of the protection of privacy and private data, whilst the other part of legislation consists of laws punishing the computer criminal and determining punishments for those who provoke security incidents. Legal regulations are different in every state. In the following text, part of the Republic of Croatia's Criminal Law referring to private information, privacy and computer security will be discussed.

6.1 Private data and privacy protection laws

In Croatia there is a Private data and privacy protection law that "regulates the protection of private data of physical persons as well as the supervision of collecting, processing and using this personal data in the Republic of Croatia" [9]. But, what is not defined is a privacy protection law which would determine which personal information may be collected. It is very possible that the aforementioned law may not have any influence on data collecting during computer forensics procedures when this computer forensics procedure is being carried out on the basis of a court order, but may influence organization security policies, particularly when this refers to recording users' activities which would thus acquire a level of privacy.

6.2 Criminal law and computer criminals

In Croatia on October 1st 2004, amendments to the Criminal Law [8] entered into force which mainly refer to the regulation of computer criminals. That is a result of the ratification of the „Convention on Cyber crime" [6] – a convention whose rulings have to be included by states in their laws. The convention was established on November, 23 2001 by the Council of Europe and was ratified by Croatia in 2002.

Article 223 of the Criminal Law, which entered into force on January 1st 1998, defines the penalties for "damaging and using data of other people". An amendment of the law has determined the more precise title of that article: "Violation of privacy, integrity and availability of computer data, programs or systems" and defined the legal articles determining punishments for particular criminal acts. Punishment will be applied to those who:

- "despite protection measures gain access to the computer system";
- "with a specific aim, disable or render more difficult work or use of computer data or programs, computer systems or computer communication";
- "without authorization, damage, modify, delete, destroy or in any other way render other computer data or programs unusable or unavailable";
- "intercept or record the non public transmission of computer data that according to the computer system are not assigned to them, either from it or in it, including the electromagnetic emission of the computer system transmitting this data, or who enable unauthorized persons to become familiar with such data".

One item of this article defines the punishment for more serious cases of criminal acts when "a criminal act is committed in relation to computer data or programs regarding administration government bodies, public institutions or companies of particular public interest or when significant damage is caused".

This article regarding the aforementioned law of major security incidents listed in Chapter 2 of the same can be seen.

The new criminal act mentioned in article 223a of the Law's amendment is computer falsification. The first paragraph of the article defines the punishment for those who "in an unauthorized way make, enter, modify, delete or make useless computer data or programs valuable for legal relations, with the aim of using them as though they were valid, or if that person himself uses such data or programs". There is also an article defining the punishment for more serious cases of criminal acts – if the injured parties are bodies of particular interest or if notable damage has been done.

Article 224a defines the criminal act of computer fraud. The first paragraph of the article defines the punishment for those who "with the aim of providing illegitimate benefit either for themselves or any other person, enter, use, modify, delete or in any other way render computer data or programs useless, or disable or render more difficult the work or use of the computer system or program, causing damage to others".

All three articles contain the item defining punishment for those who "without authorization develop, acquire, sell, hold or make available to others special tools, media, computer data or programs developed and adapted for criminal acts from the computer criminal field". The conclusion is that both those who develop and those who use malicious programs are responsible.

7 Conclusion

Computer forensics has been present for some time as a computer discipline but lately it has become more specialized and an accepted technique for providing a response to security incidents. Evidence collected in this way is also valid in court.

Computer forensic procedures are well known and defined and should be adhered to when responding to security incidents. It is particularly important to collect data from the compromised computer with as

little intervention as possible, but is also necessary to take care regarding the verification of collected data – even more importantly if they are to be presented in court. The quality of collected data will also depend on the implementation of organizational and security policies of an organization as well as computer security measures. While some of these measures are helpful, others are against the rules of computer forensics, so it is necessary to find the most favourable midpoint between computer security measures, system performances and protecting data important for computer forensics.

In order to punish malicious users discovered by computer forensics measures, a legal regulation has to exist. Croatia has foreseen in its Criminal law punishment for all those who provoke security incidents and, on the basis of these laws, compensation for committed damages can be applied for.

Although more care is being taken with computer security, undoubtedly computer forensics will be increasingly necessary, as every day faster development of new technologies and a growing number of networked organizations increase the risk of computers, information and information systems being abused.

8 References

[1] K. Mandia, C. Prosise, M. Pepe: **Incident Response & Computer Forensics**, (second edition), McGraw-Hill/Osborne, 2003, pp. XXV, 103-123, 153

[2] R. Nolan, C. O'Sullivan, J. Branson, C. Waits: **First Responders Guide to Computer Forensics**, CERT Training and Education, 2005, pp. 4

[3] Douglas Schweitzer: **Incident Response: Computer Forensics Toolkit**, Willey Publishing, Inc., 2003, pp. XXI-XXII,

[4] G. Mohay, A. Anderson, B. Collie, O. De Vel, R. McKemmish: **Computer and Intrusion Forensics**, Artech House, Inc, 2003, pp. 16-17

[5] M. A. Caloyannides: **Privacy Protection and Computer Forensics**, (second edition), Artech House, Inc, 2004, pp. 252-253

[6] Council of Europe: **Convention on Cyber crime**, 2001, available at `http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm`, Accessed: 3rd March 2008.

[7] D. S. Thomas, K. A. Forcht: **Legal Methods of Using Computer Forensic Techniques for Computer Crime Analysis and Investigation**, Issues in Information Systems, volume V, 2004,

[8] Official Gazette: **The law on amendments of the Criminal law**, available at `http://www.nn.hr/clanci/sluzbeno/2004/2026.htm`, Accessed: 3rd March 2008.

[9] Official Gazette: **Personal data protection law**, available at `http:// www.nn.hr/clanci/sluzbeno/2003/1364.htm`, Accessed: 3rd March 2008.