CYBER SECURITY, PROVIDING EVIDENCE IN CYBERSPACE AND SEARCHING FOR AND SECURING DIGITAL FOOTPRINTS

Markéta Brunová
Doctor of Law, Philosophiae doctor,
University of Finance and Administration Prague

Abstract. This article analyzes cyber security with regard to the occurrence, detection and provision of digital cybercrime, for the purpose of risk analysis to ensure the security of information systems and communication technologies. It briefly presents the process of risk analysis in the cyber security process, new trends in digital tracking, digital tracking issues in practice, and cybercrime detection.

Keywords*: Cybernetic security, risk analysis, occurrence, types, search, securing the digital traces, evidence, cybercrime.*

Introduction

The obligation to create and operate a secure information system can be imposed by different legal regulations, but it can also happen based on our own decision if (in fewer cases) it does not explicitly follow from the legislation. Different legislation defines different requirements. In all cases, however, at the beginning of this iterative, never-ending process, at the outset, a risk analysis is being carried out during cybercrime assurance.

Risk analysis in the process of providing cyber security

The control of cybercrime is linked to the possibilities of new technologies and hence the possibilities to abuse them; it also limits the possibilities that these technologies provide in detecting, investigating and preventing this type of crime. It follows that the process of controlling cybercrime is a continuous process that lasts as long as there are assets to be protected. The whole risk management process, from the identification and risk analysis to risk reduction methods, can be illustrated [1, 2].

Preventive security measures include tools for detecting possible cyber-attacks as well as tools to detect defects or malfunctions in the system to provide evidence of digital footprints. These traces have a dual meaning: they serve to detect the perpetrator and prove his criminal activity, but at the same time they are a feedback source for additional security measures.

From the point of view of evidence, the most important tools for us are the storage of information about users' and administrators' activities, the functioning of technical and program components, and the collection and evaluation of cyber security events. Very important is the question of the demonstration that the trace was located in a certain place and that it was not modified in any way from the process of its provision until the termination of the expert examination [1].

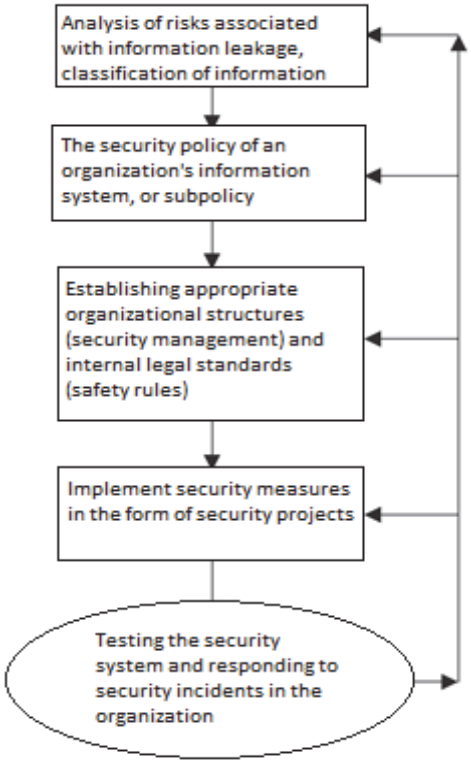

Fig. 1 Risk analysis in the process of their management (Smejkal, Rais 2013)

Digital tracks are found in computer systems and on data carriers, or anywhere in cyberspace. Their properties are in particular:

a) immateriality of digital footprints, b) digital footprint latency, c) time traceability of digital tracks, resp. manipulability with time in computer systems, d) information value of digital traces, e) very low service life of digital traces, f) preservation and quality of archival records, g) large volumes of digital data, h) high data density of digital records, i) dynamics of digital technology development, j) dynamics of information systems activity, k) complexity of the environment, l) large geographic range of digital footprint space, m) availability of quality digital data protection, n) automation options for identifying digital traces, o) the possibility of changing the identity of the culprit in cyberspace, p) digital footprint recovery, q) problem with the originality of digital footprints, r) distrust of the power of digital traces [3, 4].

Search and secure digital footprints of cyber crime

Determining the current methods of providing computer (digital) traces is of great importance for the subsequent investigation of these tracks and their probative value. The search and provision of information is derived from the basic categories of computer tracks [5]:

1. technical,
2. data.

The technical footprint is a track that can be seen directly and can be reached. These are computer sets, peripherals, and other techniques. The data track is one of the most demanding forensic tracks in the assurance process. The principle is that there is no digital footprint without the technical footprint. A very special circle of digital traces are data traces in network communication or data in information systems.

The digital footprint is relatively stable, which is directly related to the fixation of information - that is, by providing tracks. From the point of view of the noticeable value of computer tracks, we can divide them into:

1. providing technical traces,
2. providing data traces,
3. providing information from communication or information systems in the form of data.

In providing technical digital stops, we provide a technique that mainly includes all electronic, mechanical, and other computer components or peripheral components connected to them. In order to provide data traces, we must first find their carrier. The data carrier is a certain technical device capable of carrying the data. It follows that data cannot be secured directly without their

carrier. However, we cannot exclude cases where we are able to secure the data by converting data from one carrier to another without the original carrier being secured.

We can secure the data if we know this information:

1. the method of storing (recording) data,
2. the retention period,
3. process of retrieving data [6].

The method of preservation is the technical data recording solution where some of the properties of the material used for storing data on the carrier are used. We distinguish:

1. mechanical mode,
2. electromagnetic mode,
3. thermal mode,
4. electronic mode,
5. another way of recording.

The retention time is based on the ability to maintain information in time and on the electronic properties of the carrier. The information carrier may retain the data:

1. permanently,
2. temporarily.

A carrier with the ability to permanently maintain data is such a carrier that retains the data from the time the data is recorded until it is removed, deleted, or destroyed. A carrier with the ability to temporarily retain data is a carrier that stores the data under conditions that are important to its operation - e.g., memory that is capable of retaining data only for the duration of the power supply, data packet in the Internet, cache.

Retrieving data is the way we are able to:

1. develop data,
2. decode data.

In order to retrieve (read) data from a carrier, we need to know the type of communication with the carrier and the organization of the data. Organizing data on a carrier is important for decoding, recognizing, and securing data. Recall is also necessary for the data itself.

Decoding is an activity in which data from a data carrier is obtained through a precisely defined process of information stored there by a user, system, or other object whose property is reflected in the information. The data protection and technique system is related to the invocation and decoding. This includes in particular physical, communication, operational (system) and personnel protection of data or technology.

New trends in digital tracing

From the point of view of the current trends in the field of criminology related to the research of digital tracks, these areas are often visible:

- proof of the integrity of digital evidence,
- the possibility of exploring them from the point of view of their origin,
- researching portable devices such as PDAs, mobile phones, etc.,
- the issue of data decryption,
- the issue of steganography.

Cohen and others deal with issues of forensic aspects, especially portable electronic devices, CD media, and electronic communications. In nine chapters, the book focuses on MP3 Forensic, obtaining relevant information from CD and DVD media, forensic analysis of email headers, palmtop, iPod and other devices [7].

Another extensive 300-page publication focuses very closely on all aspects of obtaining criminal information from CDs and DVDs. These discs are routinely provided during house searches, and may include financial records, child pornography, etc. The authors discuss the possibilities of finding a media connection between a particular mechanic, finding the date when the medium was created and others [8]. Carvey discusses the possibilities offered by the most widespread operating system in terms of forensic science. Individual chapters concern issues such as disk space swap analysis, registry analysis, directory and file analysis and their structure, and analysis of executable files [9].

Casey deals with the issue of the admissibility of digital evidence in the courtroom, analyzing systems from a criminological point of view, whether based on Windows, Linux, UNIX or Macintosh, networking issues from the point of view of forensics, and specific examples of cybercrime investigations [10]. Kipper created one of a handful of narrowly specialized publications focused on various types of computer and other networks. The author deals with Personal Area Networks such as Bluetooth, InfraRed, Wireless USB as well as WiFi and other technologies, including mobile networks, especially in relation to SMS analysis [11].

Proof of Integrity: This is a way to prove whether a file, whether in the form of an attachment in an e-mail or for example burned on a CD medium, has not been altered since it was created by the user. The issue of

data authenticity is of interest to police and other authorities in criminal proceedings, not only for the purposes of proving the defendant, but also if, for example, part of the criminal file contains records of wiretapping or camera systems in electronic form. In this case, the authenticity of these data, such as the already mentioned MD5 sum, whose value can be written in the written material, must also be confirmed.

Steganography

Another problem with digital data is the possibility of hiding them using steganography. Steganography, unlike cryptography, does not encrypt the data, it merely changes their appearance at first glance. For example, accounting data, criminal group communications, or terrorist plans may be hidden in an innocent text, image, or audio file. Data is generally unencrypted, instead it is hidden in front of the user. But this does not prevent the user from encrypting the data before he steganographically conceals them, in case someone deliberately or accidentally during the data transfer reveals the true meaning of the transferred files [12]. In our literature the problem of steganography was described by [13].

Authenticity of the data

EXIF (Exchangeable Image File Format)[1] is a type of metadata specification that stores digital cameras in the image header. From these data, the following can be read:

1) date and time of capture,
2) brand and camera model,
3) camera settings, i.e. aperture, time, ISO sensitivity, focal length, flash usage information, camera orientation information, and so on,
4) preview of the image - because modern SLRs can capture an uncompressed image of tens of megabytes, a thumbnail image of about 10 kilobytes is stored in the header to speed up thumbnail viewing in the camera without having to open the original file,
5) in some cases, in conjunction with the GPS, you can also save the location where the picture was taken,
6) information about the author (this information allows you to insert a graphic program additionally but for some cameras you can already save these data in the settings and they will be added to each frame).

The problem of accepting digital footprints in legal practice

Digital traces in the role of evidence are not always accepted by courts. There is no wider awareness of their possibilities, characteristics, reliability, evidence, and consequently of their practical use. Uniform methodology for searching, securing, analyzing, and documenting digital footprints has not yet been developed. On a national and international scale, these procedures are researched and being developed intensively.

The open questions is also the preparation of forensic specialists, their certification, as well as the issues of ensuring standardized and certified HW and SW funds, financing. The cooperation of state and private organizations in the field of digital footprints remains problematic. The absence of uniform methodologies and standards makes it difficult to effectively exchange digital tracks between different bodies and expert teams of forensic workplaces [14].

A number of security incidents of an informational character that occur in the private sphere, in the environment of various institutions, will not reach the state institutions at all. For commercial institutions where internal security incidents have occurred, in a competitive environment, the disclosure of any sensitive information threatens to mean the losing of confidence from customers (banks, insurance companies, telecommunication companies, etc.). Investigations are conducted internally or with the help of specialized external private security or audit firms. Then there is also lack of professional publicity, sharing causes, ways of dealing with critical situations, passing on knowledge and experience. In extremely rare cases, investigations are handed over to state institutions [15]. If this occurs, then with a relatively long delay. Without mutually accepted standards, it is problematic to verify the credibility of the secured and further transmitted digital traces between different expert workplaces and authorities.

The features of digital traces further predict all the procedures and methods that need to be applied consistently when searching, securing, documenting, and analyzing digital tracks.

[1] EXIF was designed by the Japanese JEIDA Industry Association, version 2.1 was established in June 1998. Version 2.2 in April 2002. Currently no one officially manages the standard and it is not further developed. This is due to inconsistency and also to the fact that EXIF itself is only supported in JPEG and TIFF images. Other image formats, such as RAW, also store these data but differ from each manufacturer.

Considering the qualities of digital footprints, we can not only effectively conduct forensic investigations in the area of information and communication technologies but also implement very effective prevention or in a real ICT environment to set such conditions that the following forensic activity will meet all our professional expectations [3].

Possibilities of interpreting traces in the evidence process

The issue of probative value is discussed in ENFSI expert groups, particularly in recent years, very intensively. It is interesting to note that the probative value of the forensic footprints, in this case the microtraces, was already dealt with by Růža, who points out that the answer to the question of the probative value of the microstraces must be formulated only in the sense of the probability of the information of them obtained by the actual story of the investigated criminally relevant situation [16]. This statement is of great importance and concerns the issue of digital footprint interpretation in the evidence process [17].

Conclusions

1. The cyber security policy must have a guarantor responsible for the maintenance, operation and updating of security systems and networks in accordance with a tightly defined review process. In order for this basic preventive measure to be effective, a regular review of established procedures - security policy compliance - must also be part of the safety management process.

2. The security policy of an information system may be a subset of a superior security policy of information or even an organization's security policy. It is a declaration of the principles and procedures that the organization has established. The security policy of the information system is a set of standards, rules and procedures that define the way confidentiality, integrity and availability of classified information and the responsibility of the user, security administrator and the information system administrator for its operation in the information system are to be ensured.

References

1. Smejkal, L., Rais, K. Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání. Praha: GRADA, 2013. ISBN 978-80-247-4644-9.
2. Porada, V., Smejkal, L. Preventivní opatření snižujících riziko kybernetické kriminality. In Sborník konference „Bezpečné Slovensko a Európska únie“. Košice: VŠBM, 2018.
3. Porada, V. et al. Kriminalistika. Brno: CERM, 2001
4. Porada, V., Straus, J., 2012. Kriminalistické stopy – Teorie, metodologie, praxe. Plzeň: Aleš Čeněk. ISBN 978-80-7380-396-4.
5. Kothaj, L. Některé zvláštností vyšetřování počítačové kriminality ve vztahu ke kriminalistické počítačové expertize. Praha: PA ČR, 1998.
6. Kothaj, L., Porada, V. Zajišťování kriminalistických stop počítačové kriminality. Bezpečnostní teorie a praxe, 2005, p. 95-105.
7. Cohen, T., Schroader, A. Alternace Data Storage Forensics. New York: Elsevier 2007.
8. Crowley, P., Kleiman, D. CD a DVD Forensics. New York: Elsevier, 2007.
9. Carvey, H. Windows Forensic Analysis. New York: Elsevier, 2007.
10. Casey, E. Digital Evidence and Computer Crime. New York: Academic Press, 2004.
11. Kipper, G. Wireless Crime and Forensic Investigation. London: Auerbach, 2006.
12. Hosmer, C. Proving the Integrity of Digital Evidence with Time. International Journal of Digital Evidence. 2002, n. 1.
13. Smetana, M., Penkala, P. Steganografie. Kriminalistika, 2006, č. 4, s. 246-251.
14. Porada, V., Svetlík, M. (Eds.) Digital forensic forum Prague 2007. Praha: Institute of criminalistics and forensic science, College of Karlovy Vary and Risk analysis consultans Computer, Forensic Institute, 2008.
15. Straus, J. a kol. Úvod do kriminalistiky. 2. vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006.
16. RŮŽA, J. Mikrostopy. Praha: Kriminalistický ústav VB, 1983.
17. Smejkal, V., 2017. Analýza rizik jako nástroj prevence kybernetické kriminality. In: Bradáč, A, Křižák, M. (eds.). Sborník příspěvků XXVI. mezinárodní vědecké konference Expert Forensic Science 2017. ÚSI VUT v Brně: Brno, p. 504 - 515. ISBN 978-80-214-5459-0.