Cyber Security in a Cloud with Insight on the Slovenian Situation

PRIMOŽ KRAGELJ
Jožef Stefan Institute
Jožef Stefan International Postgraduate School
Jamova 39, 1000 Ljubljana
SLOVENIA
primoz.kragelj@siol.net

As current trends show, more and more enterprises, public administrations and home users are using cloud-based infrastructure. Thus, new challenges arise, with many questions. How is it possible to perform forensics in a new environment without having physical access to a system? Is it enough to involve local authorities where a service provider resides? How can we collect data from a network? Will forensics be performed in the same way, with the single difference that electronic devices (like hard disks) will be on a table, but connected through a network? Will service providers support a mechanism allowing remote forensics? Will a changed approach provide adequate evidence in court? Also, a review of existing methodologies and some adaptation, especially in the data acquisition process, will be needed. This paper tries to assess these issues, particularly examining the Slovenian case.

Key-words: Cyber Crime, Cyber Security, Economy, Cloud Computing, Computer Forensics, Law

1 Introduction

Computer forensics - also referred to as digital forensics - is a multi-disciplinary approach that links technology, law, economy and sometimes psychology [1]. Of course, there would be no need for real forensic and security enhancements if it were not for crime. However, forensic investigation principles can also be used for troubleshooting, due diligence and some other processes. Furthermore, we should not underestimate the economic impact and business opportunities that forensic investigation affords. This paper explains the correlation between cyber crime, cyber security and economic viewpoint by proposing different approaches closely related to the near future.

2 Current situation

The term cyber crime refers to any crime involving a computer and a network (NIST) [2]. The use of the internet creates opportunities for criminals, usually seeking assets that can be converted into money. We can separate users into three major groups: home users, business and public administration. What they have in common is that sensitive information is stored on a network attached device, while the levels of interest of attackers can vary. As reported by Detica Limited UK [3], financial damage is caused by cyber crime; while on the other hand security solutions and risk evaluations convergent with attractive IT solutions, like cloud computing.

Cyber security is defined as the ability to protect or defend the use of cyberspace from cyber attack (NIST) [2]. It is known that the number of internet users is growing; however, the numbers are distributed between home and business users, and from the data privacy perspective, public administration bodies. The need for greater security is caused by constant attacks. However, developers of malicious software are constantly improving their programs, searching for new weaknesses, and, even more important, becoming more and more organized.

In economic terms, computer system security and data privacy are not merely technical problems; however, cyber crime is better demonstrated (measured) from an economic viewpoint than explained as a purely technical issue. Research shows that cyber security is closely correlated with cyber crime. Generally speaking, if cyber crime increases, then the need for security increases, which is therefore also true for security investments. Furthermore, this is typically seen in software and

ISBN: 978-960-474-297-4

hardware enhancements, or other instruments such as insurance, which is another aspect, but also seems useful. Security levels can also be improved by appropriate policy implementations. However, this is more useful within enterprises. Financial institutions that have taken action provide good examples by implementing improvements on different levels and adding security mechanisms in order to protect their customers.
Future trends in IT infrastructure show that more and more organizations (either start-up companies or those migrating from internal IT to cloud service provider), home users and public administration are using some variant of cloud infrastructure for one of their services, which might be infrastructure as a service (IaaS), platform as a service (PaaS) or software as a service (SaaS). The attractiveness of such infrastructure is explained through different business models, referencing cash flow, stability, security, economy of scale, which finally involve new risks (operational and financial) and require deeper insight into future operations and the proper selection of a cloud service.

Computer forensics is defined as the practice of collecting, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of data (NIST) [2]. If there is a need for digital forensics, special process are executed involving law enforcement agencies or private enterprises dealing with forensics which operate on various legal grounds (at least valid for Slovenia); also, their outcomes are different. Processes involving law enforcement can conclude in court, while cases examined by private agencies - such as disciplinary action, abuse of power, competition law, violations relating to intellectual property, or data destruction - show signs of criminal activity, but the intention of the reporter is not to make accusations, but obtain reimbursement.

The prime focus of my future work relates to current trends – cloud computing – where certain things are changing relative to the current situation. The basic principles remain the same – we still have cyber crime, cyber security and computer forensics; but methodologies can adapt to new situations. Furthermore, computer forensics in a cloud is a completely new field; as it involves multiple jurisdictions, computer data can be located in many different countries, meaning that data acquisition processes vary. Furthermore, computer forensics as a discipline deals with digital evidence – facts, such as what happened, how it happened, where it happened and who made it happen, are essential for collecting reliable evidence.
On the other hand, a cloud system can be used as a computer from where crime is committed.

3 Proposed solutions

Rok Bojanc and Borka Jerman-Blažič [4] in their work 'An economic modeling approach to information security risk management' explain that the most common way of demonstrating security needs is by using risk management approaches. The goal of security risk analysis is to define and measure risks by identifying data and their value to a company. The second step is to identify and measure threats. In addition to valuation risk, minimization strategies are described:

- Avoiding threats and attacks by eliminating the sources of these risks
- Reducing asset risk exposure by implementing appropriate technologies and tools
- Transferring risk responsibility
- Accepting security measures as a cost of doing business

Another author, Shari Lawrence, RAND [5] describes cyber security economic issue. The growth in the use of digital technology in homes and in business - and therefore the storage of crucial and important data on digital devices - leads to the inevitable question: How can all this data be protected? Also, they prepare checklist helping with decision making process for different roles dealing with cyber security. Their outcome is based on multiple researches, focusing on two important questions:

- how organizations perceive the importance of cyber security
- how organizations make cyber security investment decisions

With the RAND team, Lawrence considered a framework that helps to explain researches and propose guidelines for future actions.

The authors and involved personnel produced a valuable guide, 'Security and Resilience in Governmental Clouds' [6] which can assist any organization contemplating a switch to cloud infrastructure. The RAND team covered the entire decision-making process, which includes comparative risk assessment, SWOT analysis, and evaluation of using cloud computing in public

ISBN: 978-960-474-297-4

administration (data privacy, location of data), contract details, and also forensic insight. In addition, they see forensics as an opportunity for supplier choice. Service providers offering forensics capabilities are highly ranked.
As we can see, even public administrations evaluate the use of cloud services, although they bear in mind the transfer abroad of sensitive data about their citizens.

3.1 Independent organization

Regarding the situation in Slovenia through the combined overview of law enforcement, enterprises and different educational institutions, the biggest challenges are in the following areas:

- establishing joint cooperation between the public sector, enterprises and educational institutions
- establishing an organization responsible for cyber security by monitoring, collecting and analyzing data as a prerequisite for further proactive operations
- encouraging companies to report cyber crime

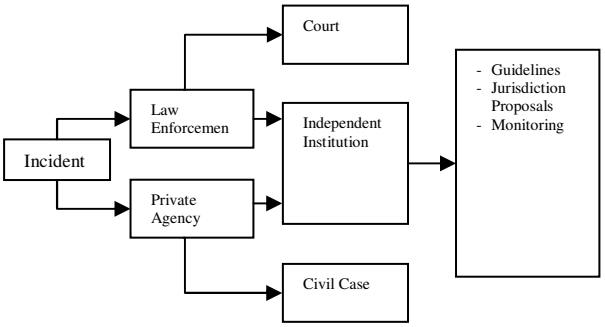

Fig. 1, Process overview

3.2 Forensic readiness

Another example of the execution of computer forensics in an enterprise. Computer forensics can be expensive for both the investigator and the subject under investigation. In order to allow for business contingencies and considering law enforcement agencies seizing core business-related equipment, we can see that forensic readiness is essential, especially for enterprises. How can be this achieved? For real implementation, there are some simple answers:

- archiving/backup
- collecting log files
- monitoring network traffic
- proactively report detected intrusions

In conclusion, a forensic ready enterprise can suffer less negative business impact in the case of some forensics requests.

3.3 Reporting cyber crime

From the economic aspect, we can also analyze why cyber crime is not reported. Usually in cases of cyber attack a company simply corrects the damage, ideally prevents recurrence, but takes no further measures. There are a few reasons why such crimes are not reported:

- Lack of time for data acquisition
- Lack of trust in law enforcement
- Understanding that the crime can not be investigated and prosecuted
- Enterprises spend much more time on security enhancements, without concern for useful data collection for possible forensic examination
- Loss of reputation

Although some reasons can be understood, inactivity does not help and the overall situation is not improved.

3.4 Forensics in cloud computing

In cloud computing, in actual cases, it is clear that there is enormous potential for use, which makes computer forensics even more difficult. Fundamentally, the methodology, (like the one published by the Department of Justice) [7], can be more or less the same, as long as in legal practice judges accept digital evidence that is treated in the same way as at present. Regarding current trends and cloud computing, new challenges have arisen, such as:

- Proving data ownership (i.e. responsibility for data)
- Proving log records validity
- Adaptation of existing methodology to a cloud
- Connecting service providers with law enforcement
- Linking data with a person
- Will service provider provide or allow forensics supportability?

Thus there are many reasons why cloud forensics challenges are attractive for further research.

3.5 Software tools

Furthermore, we can discuss tools like WMware, Eucalyptus, OpenVZ, KVM, Azures, that provide cloud infrastructure. They differ at the basic level –

ISBN: 978-960-474-297-4

how data are stored in file systems. Some use images; others have everything available as a simple file system, separated at the directory level for each virtual machine. These facts are, however, important as they can be helpful, while on the other hand they can limit an investigation. Here we actually need a set of standards and policies for forensics that will develop in parallel as part of the infrastructure.

Software developers should be connected with forensic institutions and abide by some standards. No matter what, speaking of commercial software or open source solutions, they should satisfy requirements defined by an authorized body. Furthermore, for implementation purposes, final solution can be the combination of implemented API and monitoring log files.

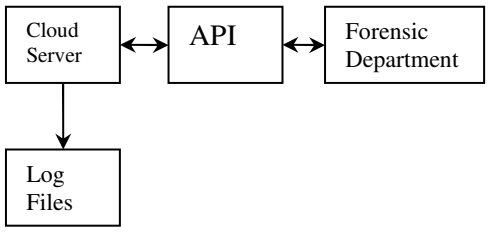

Fig. 2, Permanent access to remote system

3.6 Methodology update

Forensics as a discipline is quite standardized; however, new technologies can also reflect current methodologies and best practices. Comparing with DoJ [7] methodology, we can see that some modifications will be needed. Thus, by applying/comparing existing methodologies to cloud computing, differences become evident in the following areas:

1. Obtaining and imaging forensic data, which as a process should be performed, only the tools and approach change
2. Device seizure (like a hard drive in the case of possession of material involving child abuse)
3. Basic forensic principles - how do we duplicate and verify data integrity? Will network acquisition be treated as sustainable evidence in court?
4. Log file based forensic; however, log files are leads rather than digital evidence

4 Conclusion and Future Work

In conclusion, it is clear that, with different worlds, there is a close relationship between technical issues, technical solutions, economy and law, requiring a proactive approach for future security.

Cloud computing can be used in many different ways, which from the forensic point of view becomes even more complicated by the use of different tools for any cloud services. It will probably take some time for new industry standards for computer forensics to be accepted. However, in economic terms, the parallel development of a forensic ready system, certified service providers and proactive organizations mean we will be able to provide more reliable evidence than at present.

As it is not yet clear in which direction cloud forensics will develop, and it seems that this multi-disciplinary and complex problem makes this an attractive area of study.

My future work will focus - from the process perspective - on a methodology review; from the technical perspective, I would conduct a deeper evaluation of cloud infrastructure tools. I would also perform an evaluation of Microsoft tools such as Active Directory, Exchange Mail server and one operating system with a focus on logging. In addition, the results of the research could be transferred into best practices, either through law enforcement or through the private sector.

References:

[1] US-CERT, *Computer Forensics*, 2008
[2] NIST, *Glossary of Key Information Security Terms*, 2011
[3] Detica Limitied, *The Cost of Cyber Crime*, 2011
[4] Rok Bojanc and Borka Jerman-Blažič, An economic modeling approach to information security risk management, *International Journal of Information Management* (2008), doi: 10.1016/j.ijinfomgt.2008.02.002
[5] Shari Lawrence Pfleeger, Cybersecurity Economic Issues, *IEEE Security and Privacy*, Vol. 5, No. 3, May–June 2007, pp. 25–31
[6] ENISA, *Security and Resilience in Governmental Clouds*, 2011
[7] Department of Justice, *Digital Forensic Analysis Methodology*, 2007