Conference Paper

Confidential Data Protection as a Means of Ensuring Information Security

Chicherov K. A.[1] and Norkina A. N.[2]

[1]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Master, Kashirskoe shosse 31, Moscow, 115409, Russia
[2]National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Candidate of Economic Sciences, assistant professor, Kashirskoe shosse 31, Moscow, 115409, Russia

Abstract

This article presents issues of protecting confidential data, ways to support information security, types of information security threats resulting in an authorized access to confidential data, countermeasures and security measures to ensure confidential data security.

Keywords: confidential data, information security, information security threat(s), personal data, information systems, data security.

Corresponding Author:
Chicherov K. A.
kirill.chicherov@me.com

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

These days there is a huge number of social activities, and each of them requires a tailored approach. Every day people all over the world encounter such problems as robberies, casual personal or business relationships with strangers, or loss of personal belongings. Informatization of our society is well on the way, the number of social networks users is increasing, and the amount of information assets is rising exponentially. Wiretapping, reading of personal information in social networks and tracking of certain individuals' personal activities are steadily growing. However, the last one represents a violation of human rights, for, according to the RF Constitution, private life of every individual is immune. It is no secret that in the vast majority of cases confidential information leakages happen in organizations and companies. Employees are not concerned with information security issues, and the number of sensitive data leakages in major organizations grows from year to year.

2. Material and Theoretical Bases of Research

Information is a set of data that needs to be stored, shared, processed and used in human activity. Information is one of the most important business resources of high value for any organization, so it needs protection.

According to InfoWatch report, 925 cases of confidential data leakage were registered in 1H 2017, or up 10% compared to 1H 2016 [4].

As a rule, information threats aim at obtaining specific information, and in most cases it is confidential information of particular organizations and individuals. If trade secrets are disclosed, the financial standing of an organization or a firm may be compromised.

The key factors contributing to an increase in vulnerability of confidential data include:

- advanced amounts of information that is accumulated, stored and processed using computer facilities;
- single databases containing information that is diverse in nature and ownership;
- growth in the number of potential users who have a direct access to data stored in the computer-based system;
- automation of machine-to-machine interaction and network information exchange.

As mentioned above, local users can be a source of confidential data leakage, however, such data may be stolen by hackers as well, who are capable of remote stealing of information that is subject to non-disclosure agreement.

In terms of law, information security can be violated by either intentional or unintentional breach of information security properties. If this is the case, management of the subject entity will be up against destruction or alteration of information.

Today not only Russian but also Western companies are increasingly suffering from external cyber attacks. Information Security compiled a rating of the highest-profile incidents for 2017 related to confidential information leakages, and in addition to other less-known companies, such global corporations as McDonald's, HTC, Microsoft, etc., are included in this rating [5].

Let's consider the issue of confidential information protection in the context of information security. The first step to solve this problem is to develop a threat model. By their nature, threats may be categorized into three groups – external attacks, internal attacks and untraceable attacks.

The use of antivirus applications only to protect an organization from unauthorized intrusions is not enough, a systemic approach to ensuring information security is required.

At the moment, Yandex.Disc, Dropbox and Google Drive cloud storages are widely used.

When choosing an easy-to-use storage, a user focuses on the amount of free space provided free-of-charge but looks past security. For example, Yandex.Disc, one of the most popular drives used by over 175 mln people, does not encrypt files uploaded to cloud storages.

Local data theft is of lesser severity as regards consequences than data theft committed from the outside. Yes, it is a case of confidential data leakage as a result of hacking into computer systems. Computer systems are hacked by highly-qualified IT professionals capable of breaking the system protection. Currently, on their personal computers users may keep materials that are not to be seen or read by their parties. Initially the hacker collects information on the object, chooses the optimal attack plan, and then attacks possible system vulnerabilities.

Today, to be on the safe side, organizations should at all times use the latest version of a selected antivirus software, update it on a regular basis and check for browser updates. Those who use routers should protect them with passwords for security purposes. Besides, for hacker-protection purposes, URLs should always be authenticated. Most commonly, it is one erroneous letter that enables hackers to obtain a password [6].

As in any other system designed to protect and prevent access to personal data, the first and foremost means of protection is the audit which involves collection and analysis of events and feedback mechanisms (critical event notifications, automatic activation of adequate protection processes).

Means of ensuring security should match the level of data confidentiality and the requirements to its protection. In some cases mandatory protection is a must, however in most cases the cost of implementing and maintaining information security systems should not exceed prospective losses that may be caused by potential incidents.

3. Conclusion

Finally, it should be noted that protection of confidential information is the most important component of data storing. If such information contains competitive data, to avoid unforeseen complications the organization should limit the number of persons who

are aware of it or have access thereto. Consolidation and compliance with all the rules mentioned above will provide the highest level of confidential information protection.

Acknowledgements

This work was supported by Competitiveness Growth Program of the Federal Autonomous Educational Institution of Higher Education National Research Nuclear University MEPhI (Moscow Engineering Physics Institute).

References

[1] Babash, A.V. Information Security. Textbook / Babash, A.V., Baranova E.K., Melnikov, Yu.N. – M.: KnoRus, 2013. – 136 p.

[2] Egorova, Yu.N. Information Security. Textbook / Egorova, Yu.N. – Cheboksary: Chuvash University Press, 2015. – 131 p.

[3] Karzaeva, N.N. Fundamentals of Economic Security / Karzaeva, N.N. – M.: INFRA-M, 2017. – 275 p.

[4] Study into Information Leakages for H1 2015 [Electronic Source] URL: http://www.infowatch.ru/analytics/reports/16340 (Access date: 20 October 2017)

[5] Highest-Profile Information Leakages for 2014 [Electronic Source] URL: https://searchinform.ru/news/world-news/ (Access date: 1 March 2016)

[6] http://perezagruzi.ru/page/kak-zashhitit-kompjuter-ot-vzloma-4