# ABOUT CYBERSECURITY – AN IMPORTANT ISSUE IN OUR TIME

**BOGDAN ŢIGĂNOAIA**

***ABSTRACT:*** *This paper is a short review article that speaks about cybersecurity – general aspects and protection rules. Another treated subject is about new issues regarding cybersecurity.*

***KEYWORDS:*** *cybersecurity, protection rules, new issues.*

### *General aspects*

Information can be accessed anytime, anywhere - this is one the features of the twenty first century. Security in the cyberspace must be assured both for individuals and for companies.

In this context, it is very important to know aspects regarding:

a) the security risks in cyberspace, vulnerabilities and threats of informational systems;
b) the actual technologies, systems and mechanisms used for security assurance in cyberspace;
c) the actual international standards and settlements regarding information security assurance;
d) the ability to implement models for security assurance in cyberspace or to use secure systems.

The concept of cybersecurity is related to cybercrime or computer-crime. Computer crime refers to any crime that involves a computer and a network [1]. According to D. Halder and K. Jaishankar (2011) [2], cybercrimes are defined as the offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).

The virtual medium is a free space where a lot of security incidents can appear. The most common types of threats are presented below (based on [3]):

- *Computer viruses / Worms / Trojans;*
- *Spyware / Adware / Spam;*
- *A rootkit;*
- *Identity theft;*
- *Spyware and adware programs;*
- *Cyber stalking;*
- *Phishing;*
- *Illegal access and interception;*
- *Data interference / system interference;*
- *Misuse of devices;*
- *Computer-related fraud;*
- *Offences related to child pornography and offences related to copyright and neighbouring rights.*

### *Protection rules in cyberspace*

Based on the exploratory researches, on the author experience and on [4], some general rules for security on the cyberspace are presented below:

- Do not open attachments and do not click on links in spam.

- Never use public computers for banking transactions or other online purchases. These computers might contain programs that can collect personal information such as trojans.
- Do not install software from sites you are unsure about, especially software that appears to be codec. Instead, go to the manufacturer to download this type of program.
- Use programs with licenses.
- Never send your passwords through e-mail or attachments. Any service provider should not request such information.
- Avoid to do online shopping when you are connected to a public Wi-Fi hotspot, such as those in airports, coffee shops or malls. Usually, the information exchanged between you and the online store are not encrypted and can easily be intercepted by an attacker.
- Do not open the attachments from emails with unknown source / don't run programs with unknown or unverified source.
- Do not access links via email which ask you for personal data.
- Deactivate the option of Bluetooth when you do not use it.
- On the social networks your personal data or images can be used against you, anyone can see your public profile in order to collect data about you.
- Do not use/allow untrusted applications on social networks.

Cyber security programs need also to take into account how the organization and its people, processes and technologies interact, and how organizational governance, culture, human factors and architectures support or hinder the ability of the enterprise to protect information and to manage risk [5]. Some security measures for companies (based on the author experience and on the [4]):

- Install a security solution (that is permanently updated) that provides protection at least antivirus, anti-malware, anti-spam and anti-phishing;
- A good configuration of the network architecture;
- Unauthorized access points (hot spots) should be prohibited;
- A reserved attitude towards BYOD (bring your own device);
- Specialized security courses for the employees;
- Whitelisting software has better results than the blacklisting.

These protection rules can be useful for the entire online community. There is no 100% security; even if there are effective protection rules, the human factor plays an important and sometimes a decisive role. This paper tries to highlight the importance and the necessity of security in the cyberspace both for the individuals and for companies. If we refer to organizations, the necessity of investments for companies' security against cyber attacks should be a priority. Persons and companies can protect themselves if they are aware of some rules to assure their security in the cyberspace. Updated protection rules in cyberspace are necessary (a simple reason is the dynamic evolution of the cyber crime). We can see in the next figure the distribution of exploits used in cyber attacks, by type of application attacked, 2015 [7] (Kaspersky Security Bulletin 2015).

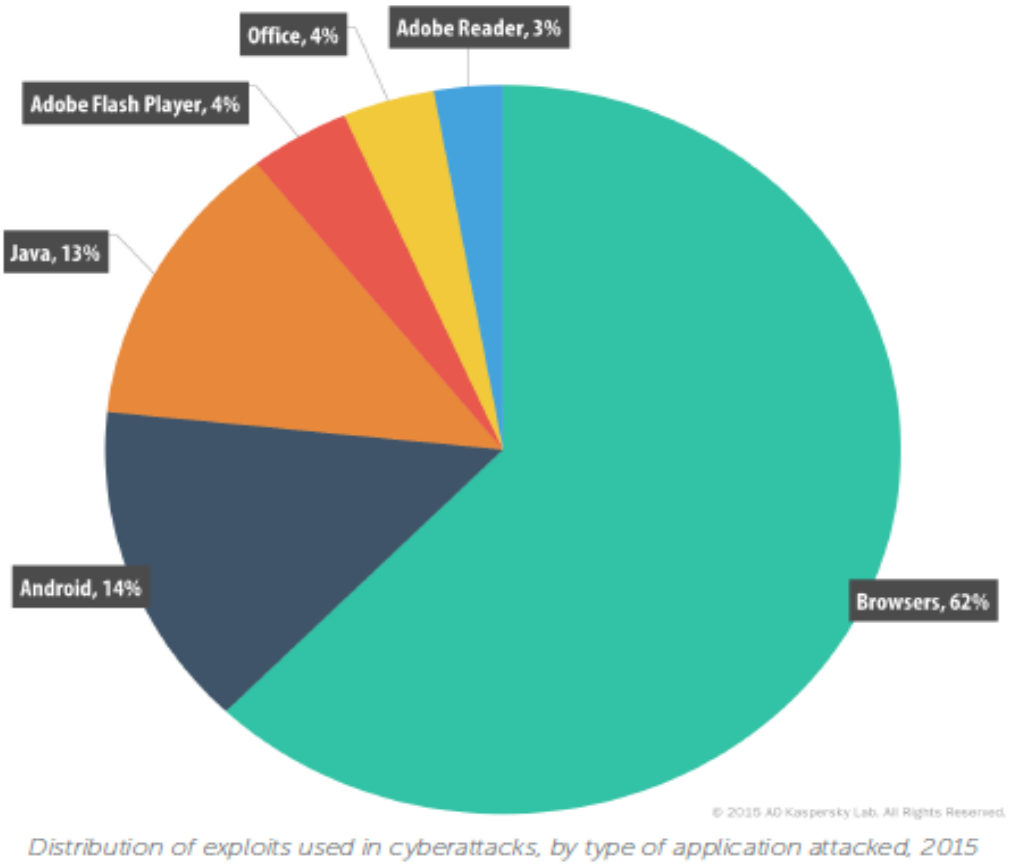


**Figure 1. The distribution of exploits used in cyber attacks, by type of application attacked - 2015**

***New issues regarding cyberspace***

Regarding the cyber security some new issues must be in our attention:

- In the next period, a lot of vulnerabilities can be exploited by criminals in the social networks: identity and data theft, viruses and worms, industrial espionage etc;
- Hacktivism will grow in the next years; hacktivism (a portmanteau of *hack* and *activism*) is the use of computers and computer networks to promote political ends, chiefly free speech, human rights and information ethics [6]; some definitions of this term include cyber-terrorism acts;
- The growth and development of viruses and worms; / The prevention of Zero-Day attacks;
- New viruses for mobile devices and platforms will be developed; a major problem can be with the threats regarding identity and data theft;
- The payments, announced to be made by using a smartphone in supermarkets for example, can be a serious problem and security gaps can be exploited by criminals in order to obtain financial benefits;
- What are the obligations of authorities and public institutions, but also juridical persons which have cyber structures;
- The cooperation between public, private and academic sectors regarding the cyber security issues;

- Measures for awareness and prevention at a local, regional and global level;
- The role of cyber security legislation and the necessity of sectorial CERT;
- A good management of the cybersecurity incidents;
- Critical infrastructure (the vulnerabilities) vs the last cyber attacks;
- Global and local cyber threats / terrorism at a global level;
- New cyber weapons;
- Trends for next years;
- (New) Methods for data protection;
- New approaches regarding information security and cybersecurity.

***Final aspects***

This paper speaks about some general aspects and protection rules in cyberspace and new issues related to the subject. Updated protection rules in cyberspace are necessary (a simple reason is the dynamic evolution of the cyber crime). New issues regarding cybersecurity must be permanently in our attention.

ACKNOWLEDGEMENTS

*I would like to thank very much Prof. Stanimir Stanev and Hristo Paraskevov for our productive cooperation!*

**REFERENCES**

[1] **Moore R**., *Cyber crime:Investigating High-Technology Computer Crime*, Cleveland, Mississippi: Anderson Publishing, 2005.
[2] **Halder D., Jaishankar K**., *Cyber crime and the Victimization of Women: Laws, Rights, and Regulations.* Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9, 2011.
[3] **Guide** - How to stay away from viruses, worms and trojans, *Available from* http://www.cert-ro.eu/articol.php?idarticol=788, *Accessed:* 2015-05-27.
[4] **Guide** - How to stay away from viruses, worms and trojans, *Available from* http://www.cert-ro.eu/articol.php?idarticol=788, *Accessed:* 2015-05-27.
[5] **ISACA Report** - An Introduction to the Business Model for Information Security, Printed in the United States of America (2009), *Available from* http://www.isaca.org/knowledge-center/bmis/documents/introtobmis.pdf, *Accessed:* 2015-05-27.
[6] **Krapp P.,** *Terror and Play, or what was Hacktivism?*, Grey Room, MIT Press Fall, pages 70-93, Retrieved 2013-02-28., 2005.
[7] **Overall statistics for 2015**, Kaspersky Security Bulletin 2015.