ASIGURAREA CALITĂȚII – QUALITY ASSURANCE
Aprilie – Iunie 2017 Anul XXIII Numărul 90

Cybersecurity – A Global Priority

Ioan C. BACIVAROV*

EUROQUALROM – Faculty of Electronics, Telecommunications and Information Technology, University Politehnica of Bucharest, Romania

Information security and *cybercrime* represent an area of international importance because the integration of information technology and communications infrastructure in the Internet is accompanied by risks of intrusion and information compromise.

Nowadays Internet is the world's largest collection of networks that reaches government institutes, commercial enterprises, universities and research laboratories in all the countries. But along with easy access to information come new risks. The number of the attacks and the frauds on Internet is increasing fast.

Computer security seeks to thwart intruders through hardware and software devices that are independent of the domain of the application or system being protected. Software security methods like authentication, access control, cryptography, antivirus, firewalls and other mechanisms used in computer security are meant to protect an underlying application by Internet attacks. Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks [1].

The most recent *cybersecurity* alert was a global one, and has – once again – drawn attention to the global importance of this issue and the need to take effective actions to counter cyber-attacks.

Indeed, on May 2017, multiple companies and organizations around the world were hit by variations of a crypto-ransomware dubbed WannaCry / WannaCrypt / WanaCrypt0r / WCrypt / WCRY (generally called WannaCry for simplicity). The ransomware also acted as a worm and once it infects a system, it then self-propagates throughout the rest of the network. The ransomware campaign caused chaos due to its massive distribution, affecting more than 150 countries and infecting over 230,000 systems. Interestingly the attack was mounted on Friday 12th May 2017, just before the weekend, making it very difficult for companies and organisations to quickly react and resolve the crisis [1].

Due to the special actual importance of the ***cybersecurity*** problem, we decided to dedicate a special section of the international scientific journal "*Asigurarea Calitatii – Quality Assurance*" to this issue, including specialized cybercrime & cybersecurity articles written by field professionals.

In the first paper published in this section, **C. Pascariu**, **I.D. Barbu** and **I.C. Bacivarov** present an analysis on *WannaCry Ransomware*, related to the recent cybersecurity alert. The authors mention that with the advent of complex techniques, tactics and procedures used by the adversaries, Information Technology professionals focus their efforts on defending environments from advanced persistent threats and highly sophisticated attacks. WannaCry ransomware came in as a caveat in this context, a way of reminding the industry that efforts should be divided into addressing the various layers of the defense in depth model.

Their paper is intended to present this type of malware on the rise that affects users in both enterprise and personal space as well by encrypting user developed content and restricting access until ransom is paid. The main focus is on the description of the virus technical details concentrating on the phases of the

* Correspondence to Prof. **Ioan C. Bacivarov**, PhD, Director of the EUROQUALROM-ETTI-UPB laboratory, President of the Romanian Association for Information Security Assurance – RAISA, e-mail: **bacivaro@euroqual.pub.ro**, **ibacivarov@yahoo.com**.

cyber kill chain. Therefore, the authors perform an analysis of WannaCry ransomware from the delivery, infection, mitigation and detection perspectives.

The long-term goal of these efforts is to anticipate threats before turning into incidents and, consequently, decrease the impact. This research represents the starting point of a process of reducing the attack surface in the case of ransomware attacks. Needless to say, the first layer worth addressing is represented by the weakest chain in the information security link, the end user.

In the second paper of this section, **M. Best** (Germany) presents some general *data protection regulation* in the focus of data leakage. Two years ago, the new General Data Protection Regulation has been published by European Commission, that will turn into nation law of all EU member states on May 25th 2018. The new Regulation will replace the existing Directive and national data protection law. In many aspects, a lot of things have changed, and more obligations and responsibilities are to respect for data controllers. Sanctions according to the new Regulation are much higher than now. In the field of data leakage, there are also several interesting aspects to consider, which are discussed in this paper, too.

Finally, **I.C. Mihai** and **I.C. Bacivarov** present a study concerning the *cyber-attacks structure*. It is important to mention that the cyber-attacks experienced during the last period a great diversification and some of them can be classified as a *global epidemics*. There are many kind of *cyber-attacks* like malware: computer viruses, worms, trojans, adware, spyware, ransomware, rogueware, Distributed Denial of Service, e-mail and web based attacks. The authors examine and classify all these cyber-attacks using the intrusion model Kill Chain, defined by researchers from Lockheed Martin.

As a conclusion, the Romania, Europe and the entire world must learn from current events regarding cybercrime and be able to respond when the next crisis arrives.

At the same time, while organizations continue to purchase and deploy technical controls, not much has been done to focus on the *human side of cybersecurity* – so named *layer 8*[**].

Consequently, is of crucial importance for all the countries, professional organizations and companies to consolidate a powerful *cybersecurity culture*. From this point of view, the contribution of specialized technical magazines, such as our journal is, could be very important.

REFERENCES

[1] **I.C. Bacivarov**, Editorial, *International Journal of Information Security and Cybercrime - IJISC*, vol.1 (2012), no.1, pp. 6-7.
[2] **https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst** (accessed June 1st, 2017)
[3] **https://securityintelligence.com/building-a-cybersecurity-culture-around-layer-8** (accessed June 1st, 2017)

[**] The term layer 8 is often used pejoratively by some IT professionals to refer to employees' lack of awareness and a weak overall cybersecurity culture. Today, it is just as important to secure human assets — layer 8 — as it to secure layers 1 through 7 [3].