SOCIETY
ROMANIAN
SRAC
FOR
QUALITY
ASSURANCE

ASIGURAREA CALITĂȚII
QUALITY ASSURANCE

Octombrie - Decembrie 2016 Volumul XXII Nr. 88

A 15-a Conferinţă Internaţională "CALITATE ȘI FIABILITATE"

CCF 2016

15th International Conference "QUALITY AND DEPENDABILITY"

ASIGURAREA CALITĂȚII – QUALITY ASSURANCE

CUPRINS – CONTENTS

Disclaimer. Whilst every effort is made by the publishers and the Editorial Board to see that no inaccurate or misleading data, opinion or statement appear in this journal, they wish to make it clear that the data and opinions appearing in the articles, as well as linguistic accuracy, are the sole responsibility of the author.

The materials in this publication is for general information only and is not intended to provide specific advice or recommendations for any individual. The publisher disclaims all liability in connection with the use of information contained in this publication.

Cybersecurity – A Major Issue of the 15th International Conference on Quality and Dependability CCF 2016

Ioan C. BACIVAROV*

Abstract

In the first part of this paper the concepts of ***cybersecurity*** *and* ***cybercrime*** *and their importance are analyzed. It is underlined that cybersecurity is one of the biggest issues currently facing governments and businesses in the European Union (EU) and globally. In this context, a special attention is given to analysis of the European Cyber Security Strategy.*

In the second part of the paper is underlined the fact that cybersecurity was one of the main topics of the 15th International Conference in Quality and Dependability – ***CCF 2016****.*

Based on the papers presented during ***CCF 2016*** *one can conclude that one can speak of a "Romanian school in reliability field", whose achievements and representatives are recognized abroad. Judging after the papers presented by the PhD candidates in the field of cybersecurity during CCF2016, the future of this domain is "in good hands".*

Keywords*: Cybersecurity, Cybercrime, IT security, Cyber Security Strategy, CCF2016*, *International Conference in Quality and Dependability*

1. *Cybersecurity* is – according to ITU-T X.1205 – the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

Cybersecurity is one of the biggest issues currently facing governments and businesses in the European Union (EU) and globally: it is important to mention that the European Union works on several fronts to ensure cybersecurity in Europe [1] [2].

The European Commission and High Representative's *2013 Cyber Security Strategy* was the first comprehensive policy document of the European Union in this area. This Strategy covered the internal market, justice and home affairs and foreign policy angles of cyberspace. The Strategy was accompanied by a legislative proposal to strengthen the security of the EU's information systems.

The Strategy outlined the priorities for the international cyberspace policy of the European Union [3]:

- ❑ Freedom and openness: the strategy outlines the vision and principles on applying core EU values and fundamental rights in cyberspace.
- ❑ The EU's laws, norms and core values apply as much in cyberspace as in the physical world: responsibility for a more secure cyberspace lies with all players within the global information society, from citizens to governments.
- ❑ Developing cyber security capacity building: the EU engages with international partners and organisations, the private sector and civil society to support global capacity building in third countries. This includes improving access to information and to an open internet, and preventing cyber threats.
- ❑ Fostering international cooperation in cyberspace: preserving open, free and secure cyberspace is a global challenge, which the EU is addressing together with relevant international partners and organisations, the private sector and civil society.

Another important for step in the process of EU's cybersecurity assurance was the adoption by the European Parliament of a proposal for a *Network and Information Security Directive* (*NIS Directive*) in March 2014 [4].

* Correspondence to Prof. **Ioan C. Bacivarov**, PhD, Scientific Chairman of the *15th International Conference in Quality and Dependability – **CCF 2016***, e-mail: **bacivaro@euroqual.pub.ro**.

2. *Cybersecurity* 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.

Cybersecurity 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. Cybersecurity is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

Professors Alessandro Birolini and Ioan Bacivarov were the coordinators of the plenary session "*Risk and IT Security*" during CCF 2016

Three basic security concepts are important to information on the Internet: confidentiality, integrity, and availability. When information is read or copied by someone not authorized to do so, the result is a loss of confidentiality. If information is modified in n unexpected ways, the result is known as loss of integrity. Information can be erased or become inaccessible, resulting in loss of availability. While computer security has been focused on these three concepts for information, the problems of greatest concern today relate to the systems mission and the continuity of services. The new concept of survivability can be defined as the capability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures or accidents. Survivability has a very sharp mission focus: the system mission has to survive, not any particular component of the system or even the system itself. The mission must go on even if an attack causes significant damage to or even destruction of the system that supports the mission.

Professors Alessandro Birolini, Angelica Bacivarov and Ioan Bacivarov together with PhD candidates in cybersecurity during CCF 2016

3. *Cybercrime* refers to any crime that involves a computer system or a computer network. A computer can be used in the act of a crime or may be the target to an attacker. It is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he can do on the Internet, a student who has created a new software tool, an individual seeking personal gain or a paid person seeking information for the economic advantage of a corporation or a foreign country. An intruder may seek entertainment, intellectual challenge, political attention or financial gain. Intruders identify and publicize misconfigured systems; they use those systems to exchange pirated software, credit card numbers, exploitation programs and the identity of sites that have been compromised, including account names and passwords. By sharing knowledge and software tools, successful intruders increase their number and their impact.

In the context of the vulnerabilities and incident trends, developing a scientific journal for information security and cybercrime research is necessary. A robust defense requires many researches in this field that allows adaptation to the changing environment, well-defined policies and procedures, the use of different security tools to prevent and combat cybercrime.

4. The primary objective of the ***15th International Conference on Quality and Dependability*** **CCF 2016** – *a jubilee edition* – was to provide an international forum for the dissemination of recent information and scientific results in the modern domains of quality and dependability.

Cybersecurity was one of the main topics of the *15th International Conference in Quality and Dependability* [5].

In the frame of CCF 2016, 12 papers in the field of cybersecurity were presented.

Most have been included in the plenary session "*Risk and IT Security*", coordinated by Prof. Emeritus Dr. **Alessandro Birolini** from ETH Zurich, Switzerland and by Prof. Dr. **Ioan Bacivarov** – director of EUROQUALROM-ETTI – UPB and President of the Romanian Association for Information Security Assurance (RAISA). Some were included in the poster session "*Dependability*" mediated by Prof. Ioan Bacivarov, too.

In this context it should be mentioned the excellent conference "*Risk management in technical systems*" presented by Professor **Alessandro Birolini**, special guest of **CCF 2016**, considered as a "guru" of the European reliability.

Most presentations in the field of cybersecurity were made by Professor **Ioan Bacivarov** and his collaborators – PhD candidates in cybersecurity.

As a conclusion of the debates, Professor Birolini pointed out that one can speak of a "*Romanian school in reliability field*", whose achievements and representatives are recognized abroad; and judging after the papers presented by the PhD candidates in the field of cybersecurity during CCF2016, the future of this domain is "in good hands".

Extended versions of some representative papers in the field of cybersecurity presented during the **CCF 2016** will be included in this issue (as well as in future ones) of the journal "***Asigurarea Calității – Quality Assurance***" dedicated to the *15th International Conference in Quality and Dependability*.

The international journal "***Asigurarea Calității – Quality Assurance***" will continue to analyze in the future the *cybersecurity* phenomenon in all its complexity.

REFERENCES

[1] I. Bacivarov, A Regional Strategy for Cybersecurity, Editorial, *International Journal of Information Security and Cybercrime* , vol. 4 (2015), no. 1, pp. 5-8.

[2] **http://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive**.

[3] *** European Commission, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, JOIN(2013) 1 final.

[4] **http://ec.europa.eu/digital-agenda/en/news/network-and-information-security-nis**.

[5] D. Stoichițoiu, I. Bacivarov (Eds) Advances in Quality and Dependability, *Proceedings of the 15th International Conference on Quality and Dependability* **CCF2016,** SRAC, 2016.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 5-10

Quality Management in Food Industry

Srđan TOMIĆ[1], Mirjana KRANJAC[2]
[1]University „Union Nikola-Tesla", Faculty of Enginnering Management, Beograd, Serbia;
[2]University of Novi Sad, Faculty of Technical Sciences Novi Sad, Department for Transport, Novi Sad, Serbia
srdjan.tomic@fim.rs

Abstract
Management strategy is the management's answer to the changes, the way to achieve the competitive advantage, to create diversity, to introduce new methods of performing a job that others lack, to become superior, to position itself in the minds of customers as different from its competitors, with different and complete range of products for specific customer groups, which are on the one hand acceptable for customers (where it is possible to segment them), an on the other hand for competitors. Thus, strategy does not anticipate success, it anticipates competitiveness. Considering importance the food has globally, as well as profitability of food industry it is clear that food quality assurance is one of the most important areas of quality management, due to that many standards were published in this area, some causing a lot of controversies today.

Keywords: Quality; Strategic market relations; Food Quality management, HACCP, ISO 22000, Codex ALimentarius; Customers

References:

[1] FAO. (2003). Recommended international codex of practice. General principles of food hygiene, CAC/RCP 1 – 1969, Rev. 4-2003, including "Annex on Hazard Analysis Critical Control Point (HACCP) System and Guidelines for its Application".
[2] Kotler, P., Keller, K. L.(2006). Marketing Management. Twelfth Edition, Pearson Education, Inc., Prentice Hall, Upper Saddle River, New Jersey.
[3] Buncic S., et al. (2008). Vodic za razvoj i primenu preduslovnih programa i principa HACCP u proizvodnji hrane.Ministarstvo poljoprivrede, šumarstva i vodoprivrde, Uprava za veterinu, Republika Srbija, Novi Sad.
[4] Taylor E., Taylor J., (2006). HACCP: Twelve Steps to Success.
[5] Unnevehr L., (2000). The Economics of HACCP: Costs and Benefits.
[6] Codex Alimentarius: how it all began Food and Agriculture Organization of the United Nations website. Accessed 7.8.2016.
[7] Understanding the Codex Alimentarius Preface. Third Edition. Published in 2006 by the World Health Organization and the Food and Agriculture Organization of the United Nations.
[8] Acording to data taken from afficial web site of codex alimentarius, www.fao-who-codexalimentarius/standards/en/. Accessed 12.8. 2016.
[9] Tomić, S.(2013). Quality Management.Fakultet za inženjerski menadžment, Draslar partner, Beograd.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 11-16

Threat Intelligence Based Security Operations Centers

Ionuţ-Daniel BARBU, Cristian PASCARIU,
Ioan C. BACIVAROV
EUROQUALROM – ETTI, University “Politehnica” of Bucharest, Romania
barbu.ionutdaniel@gmail.com

Abstract
With the advent of complex techniques, tactics and procedures used by the adversaries, Security Operations Center are starting to become obsolete. This paper changes the focal point to an advanced model that leverages intelligence to understand and anticipate threats targeting the organization. One of the most important aspects of this model is represented by this ability of anticipating threats before turning into incidents and moreover it highlights the proactive vs. reactive approach towards cybersecurity. Using this format, in the following pages the authors intended to build a comparison between a Security Operations Center and Security Intelligence Center by analyzing the impact of and steps needed for such a transition to both processes and people. Needless to say, it is critical to dedicate numerous and valuable resources to the automation aspect of such a migration. In this way management will enable the analysts and engineers to separate from routine activities, allowing them to focus on performing threat hunting against the intelligence gathered. As the enterprise oriented tools from various vendors are intended to work for everyone but are optimized for no one, the authors highlight the importance of deploying custom tools supported by knowledgeable engineering teams. Based on the authors’ research one of the initial steps and perhaps one of the most effective projects on this matter would be the implementation of a honeypot environment for obtaining tailored IoCs.

Keywords: IT Security, Cyber-Security, SOC, SIC, Threat Intelligence, APT, HoneyPots

References:

[1] SOC vs. SIC: The Difference of an Intelligence Driven Defense Solution, Lockheed Martin Corporation – Reviewed 2nd of March 2016.
[2] The Six Stages of Incident Response, Dark Reading, 2007 – Reviewed 14 of May 2015.
[3] http://www.lockheedmartin.com – Reviewed 28 of March 2016.
[4] https://en.wikipedia.org/wiki/Advanced_persistent_threat– Reviewed 2nd of May 2016.
[5] https://technet.microsoft.com/dynimg/IC78017.jpg.
[6] https://en.wikipedia.org/wiki/Honeypot_(computing) – Reviewed 3rd of June 2016.
[7] Naveen, Sharanya. “Honeypot” – Reviewed 1st of June 2016.
[8] Lance Spitzner(2002). Honeypots tracking hackers. Addison-Wesley. pp. 68–70. ISBN 0-321-10895-7 – Reviewed August 2014.
[9] Barbu, I.D., Petrică, G. (2015). Defense in Depth Principle to Ensure Information Security. International Journal of Information Security and Cybercrime, 4(1), 41-46. Retrieve from http://www.ijisc.com.
[10] Mihai, I.C., Prună, Ş., Barbu, I.D. (2014). Cyber Kill Chain Analysis. International Journal of Information Security and Cybercrime, 3(2), 37-42. Retrieve from http://www.ijisc.com.

[11] An introduction to threat intelligence, CERT-UK – Reviewed July 2015.
[12] http://www.honeyd.org/concepts.php – Reviewed September 2015.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 17-21

A Graph-driven Approach to Data Loss Prevention

Michael BEST
Bensheim, Germany
mb@michael-best.de

Abstract
Today, one threat to cybercrime is data leakage. Examples for this are the Snowden publications, theft of financial data or wikileaks. In this paper, a concept is shown to visualize the path between the asset and an actor who might leak the data. To prevent data loss, this path must be secured.

Keywords: Cybercrime, Security, Data, Data loss prevention, Graph-driven approach

References:

[1] European Union Agency For Network And Information Security, „ENISA Threat Landscape," ENISA, Brussels, 2016.
[2] Intel Security, „Data exfiltration study: Actors, tactics, and detection," Intel Security, 2015.
[3] PwC, Turnaround and transformation in cybersecurity, 2016.
[4] E. Comission, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995.
[5] PCI-Council, PCI DSS Standard Version 3.3, PCI, 2016.
[6] L. Kohnfelder und G. Paerit, „The threats to our products," 01 04 1999. [Online]. Available: https://blogs.msdn.com/cfs-filesystem file.ashx/__key/communityserver-components-postattachments/00-09-88-74-86/The-threats-to-our-products.docx. [Zugriff am 16 07 2016].
[7] B. Scheier, „Attack Trees," 12 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html [Zugriff am 16 07 2016].
[8] A. Shostack, threat modeling, Indianapolis: Wiley, 2014.
[9] W. Stallingsund L. Brown, „Computer Security Principle and Practice," Pearson.
[10] Ernst & Young, „Data Loss Prevention," Ernest & Young, 2011.

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 22-26

A Reliable Architecture for a Massive and Continuous Scanner of Web Vulnerabilities in Internet

Eugenie STĂICUŢ, Radu BONCEA, Carmen ROTUNĂ
Romania Top Level Domain, National Institute for Research and Development in Informatics-ICI Bucharest
estaicut@rotld.ro

Abstract
In recent years, the Web has become one of the major vectors for transmitting malware and computer viruses. As a response, nations around the world have established Computer Emergency Response Teams with the purpose of countering the next generation of cyber threats. One such solution is for CERTs to pro-actively scan the Web for vulnerabilities and notify the right persons before malicious users could exploit the vulnerable application. Another solution is to search the Web for compromised and vulnerable applications and take appropriate actions, such as sending simple notifications to application's owner. Either way, continuously scanning of the Web is a complex task which requires a reliable architecture. In this paper we propose a data-centric architecture, with focus on a distributed streaming processing system. We will define a virtual process bus as a group of data channels where a process can take its input from a specific channel and write the result to an output set of channels.

Keywords: cybersecurity, stream processing, distributed processing, messaging, ETL, Kafka, vulnerability

References:

[1] Huseyin, Birendra Mishra, and Srinivasan Raghunathan. "The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers", International Journal of Electronic Commerce 9.1 (2004): 70-104.
[2] Powers, J., Anderson, R., Trueblood, N., & Ciruli, D. (2005). U.S. Patent Application No. 11/245,952.
[3] https://access.redhat.com/documentation/en-US/Fuse_Message_Broker/5.3/html/Getting_Started/files/FuseMBStartedKey JMS.html.
[4] http://www.jonathanbeard.io/blog/2015/09/19/streaming-and-dataflow.html
[5] https://www.datadoghq.com/blog/monitoring-kafka-performance-metrics/
[6] https://owasp.org
[7] https://dzone.com/articles/kafka-logs-and-the-policy-of-truth
[8] https://kafka.apache.org
[9] http://tools.kali.org/

Asigurarea Calitatii - Quality Assurance, ISSN 1224-5410
Vol. XXII, Issue 88, October-December 2016
Pages 27-32

Reliability Tests for Switches Used in Telecommunication Networks

Dragoş VÂRŞESCU[1], C. PATRICHE[2], N. DUMBRĂVESCU[1], M. BÂZU[1], I. BACIVAROV[2]

[1]Reliability Lab., National Institute for R&D in Microtechnology – IMT-Bucharest, Romania;
[2]Faculty of Electronics, Telecommunications and Information Technology, University Politehnica of Bucharest, Romania
dragos.varsescu@imt.ro

Abstract
The results of several reliability tests concerning switches used in telecommunications networks are presented. Tests were combined ones: temperature and humidity, and the experiment was conducted step-by-step, with failures analysis carried out after each test step, so as to simulate actual operating conditions. An analysis of the results was performed, finally making a series of recommendations on changes in manufacturing technology switches in order to increase their level of reliability.

Keywords: Reliability, Reliability tests, Accelerated tests, Failure analysis, Switches, Telecommunication networks

References:

[1] Cisco Corporation, Netacad Routing and Switching Courses, Course 3. Switching, Cap. 2, p. 6.
[2] Hai Liu, "Reliability of copper wire bonding in humidity environment," Samsung Semiconductor (China) R&D Co., Ltd, Singapore 9.12.2011, pp. 53-58.
[3] Tarja Rapala-Virtanen, Erkko Helminen, and Timo Jokela, "Next-Generation Ultra-Thin HDI PCB Manufacturing Challenges", Iconnect 007, April 2015, p. 8.
[4] http://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/12027-53.html, April 2009.

The Journal «ASIGURAREA CALITĂŢII - QUALITY ASSURANCE»
wishes all our readers, authors and members of the Editorial Board
a happy and prosperous New Year 2017!

May the year 2017 be for you a set of 365 wonderful days,
personally as well as professionally!

Dan STOICHIŢOIU

Ioan BACIVAROV

Happy New Year 2017 !

ISSN 1224-5410