Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VIII
eISSN 2393-0837

CyberCon Romania
2021

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VIII

A scientific conference organized by the
Romanian Association for Information Security Assurance

CyberCon Romania
2021

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

The International Conference on Cybersecurity and Cybercrime (IC3) is an annual scientific conference, with the purpose to encourage the exchange of ideas about the evolution of cyberspace, information security challenges, and new facets of the phenomenon of cybercrime. The event provides the appropriate framework for students to present their research in this field.

The Proceedings of the International Conference on Cybersecurity and Cybercrime includes scientific papers reviewed by the *Editorial Board* that consists of experts from academic police structures and university departments, their work taking place under the guidance of the *Advisory Board*, composed of internationally recognized personalities from the academic field.

Proceedings of the International Conference on Cybersecurity and Cybercrime
Online ISSN: 2393-0837
Print ISSN: 2393-0772
DOI: 10.19107/CYBERCON
URL: https://proceedings.cybercon.ro

The International Conference on Cybersecurity and Cybercrime is part of the **CyberCon Romania** event, organized by the Romanian Association for Information Security Assurance.

CyberCon Romania brings together experts from public institutions, private companies, and universities, for raising the level of awareness and embodies the cybersecurity culture.

Website: www.cybercon.ro

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

Founded in 2012, the association started as an initiative with the aim of promoting and supporting information security activities in compliance with applicable laws and creating a community for the exchange of knowledge between the experts from the public, private, and academic environment. Its vision is to encourage the cybersecurity research and education, and to contribute to the creation and dissemination of knowledge and technology in this domain.

Website: www.raisa.org

CONFERENCE COMMITTEES

EDITORIAL COUNCIL CHAIRMAN

Professor **Ioan C. BACIVAROV**, PhD
University Politehnica of Bucharest, Romania
Faculty of Electronics, Telecommunications and Information Technology

INTERNATIONAL ADVISORY BOARD

Professor Emeritus **Alessandro BIROLINI**, PhD
ETH Zurich, Switzerland

Professor **Angelica BACIVAROV**, PhD
University Politehnica of Bucharest, Romania

Professor **Fabrice GUERIN**, PhD
ISTIA, University of Angers, France

Professor **Daniela-Elena POPESCU**, PhD
University of Oradea, Romania

Professor **Sandeep TIWARI**, PhD
Amity University, India

Professor **Ton van der WIELE**, PhD
Erasmus University Rotterdam, Netherlands

ORGANIZATION COMMITTEE

Ioan-Cosmin MIHAI, PhD
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania

Gabriel PETRICĂ, PhD
University Politehnica of Bucharest, Romania

Ionuț-Daniel BARBU, PhD
University Politehnica of Bucharest, Romania

TABLE OF CONTENTS

Security Solutions for Computer Networks

Eugeniu GONCEARUC
University Politehnica of Bucharest, Romania
eugen.goncearuc@yahoo.com

Abstract

Network infrastructure devices are the components of a network that transport communications needed for data, applications, services, and multi-media. These devices include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks. Organizations and individuals that use legacy, unencrypted protocols to manage hosts and services make successful credential harvesting easy for malicious cyber actors. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

Keywords: VMotion, Virtual LAN, network security

References

[1]. https://www.us-cert.gov/ncas/tips/ST18-001.
[2]. https://www.ntpro.nl/blog/archives/2526-VMware-vSphere-5.5-vMotion-on-EMC-VPLEX-Metro.html.
[3]. https://www.semanticscholar.org/paper/Introduction-to-Storage-Area-Networks-Schiattarella/0e09833bb64e80e8c339c1a6ab03513f713baf93.
[4]. http://www.mosaictec.com/tessera/what-is-vmotion.htm.
[5]. https://aws.amazon.com/blogs/networking-and-content-delivery/using-static-ip-addresses-for-application-load-balancers/.

Layers in Implementing Network Security

Ioana PREDOI
University Politehnica of Bucharest, Romania
ioana.predoi@stud.etti.upb.ro

Abstract

Every day, the number of cyber-attacks is skyrocketing. But what is the most frightening is the fact that their quality and complexity are increasing. Firewalls, antivirus software recognize known malware, meanwhile hackers can manipulate IT systems and steal critical information. So, enterprises need to invest more in early prevention, detection, defense methods and reaction. This paper aims to detail the main levels of network security which should be treated in order to prevent cyber-attacks, because a prevention strategy is essential to protect important data.

Keywords: firewall, network security, VPN, SIEM

References

[1]. Self-Defending Networks: The Next Generation of Network Security, Duane DeCapite, Cisco Press, Sep. 8, 2006.
[2]. "OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks" (PDF). Open Web Application Security Project. 2017. Retrieved June 30, 2018.
[3]. "Understanding and Selecting a Data Loss Prevention Solution" (PDF). Securosis, L.L.C. Retrieved January 13, 2017.
[4]. Dunham, Ken; Abu Nimeh, Saeed; Becher, Michael (2008). Mobile Malware Attack and Defense. Syngress Media. ISBN 978-1-59749-298-0.
[5]. Improving Security via Proper Network Segmentation", Nimmy Reichenberg, March 20, 2014, Security Week.
[6]. https://www.comodo.com/endpoint-protection/endpoint-security-software.php.

Cyber Attacks Analysis

Mihai-Andrei IANCU
University Politehnica of Bucharest, Romania
iancu.mihai19@yahoo.com

Abstract

A cyber-attack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Depending on the context, a cyber-attack can be labeled as a cyber-campaign, cyber warfare or cyber terrorism. Cybercrime has increased every year as people try to benefit from vulnerable business system or even personal systems. Often, attackers are looking for ransom: 53 percent of cyber-attacks resulted in damages of $500,000 or more. This paper intends to create a clear view about different type of cyber-attacks that tend to get more popular nowadays and their effects on systems.

Keywords: cyber-attacks, real-time maps, malware graphs

References

[1]. Haman AL-Mohannadi, Qublai Mirza, Anitta Namanya, Irfan Awan, Andrea Cullen and Jules Disso, Cyber-Attack Modeling Analysis Techniques: An Overview, University of Bradforn, United Kingdom.
[2]. http://www.bankofengland.co.uk/anintroductiontocbest.pdf.
[3]. https://www.information-age.com/guide-cyber-attacks-malware-part-1-123474555/.
[4]. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
[5]. https://cybermap.kaspersky.com/stats.
[6]. https://www.researchgate.net/publication/275891938_Detection_of_Trojan_Horses_by_the_Analysis_of_System_Behavior_and_Data_Packets.
[7]. https://www.secureworldexpo.com/industry-news/6-live-cyber-attack-maps.
[8]. https://www.av-test.org/en/statistics/malware/.

Data Security in Social Media

Andrada FINICĂ
University Politehnica of Bucharest, Romania
andrada.finica@yahoo.com

Abstract

Digital technology is now just a part of life. From online shopping to net banking and business to government infrastructure, digital technology plays a crucial role. Apart from the multiple advantages of digitization, cyber-attacks are a black dot. In recent years, we've witnessed many high-profile cyber-attacks. In fact, we can say that the number of cyber-attacks has grown rapidly in past few years.

Keywords: cyber-attacks, GDPR, social media

References

[1]. https://dzone.com/articles/why-is-data-security-important-for-everyone.
[2]. https://www.varonis.com/blog/data-security/.
[3]. https://blog.hootsuite.com/social-media-security-for-business/.
[4]. https://www.ecpi.edu/blog/cyber-security-for-social-media-what-information-is-at-stake.
[5]. https://www.microfocus.com/en-us/what-is/data-security.

Vulnerabilities in Computer Systems

Andreea-Ioana DRUMEANU
University Politehnica of Bucharest, Romania
andreea.drumeanu@gmail.com

Abstract

Information systems vulnerabilities can appear under several different forms and at different levels in a smart office building or on a website, including at the level of a single device, system level, network level, application level, To the level of operation and management. In this business are 2 types of hackers, on a way are black hat hackers who intent to steal your data using malicious software and exploit vulnerabilities and on the other side are the white hat hackers who put their coding power for closing security breaches and perform security evaluations for companies.

Keywords: computer vulnerabilities, standards, cyber threats

References

[1]. ***, Juridice. [Online]. Available: https://www.juridice.ro/412111/vulnerabilitati-ale-sistemelor-informatice.html.
[2]. ***, Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informaticã, Bucureşti, 2004.
[3]. Today Software Magazine, [Online]. Available: https://www.todaysoftmag.ro/article/2357/managementul-vulnerabilitatilor-si-evaluarea-riscurilor-in-domeniul-securitatii-informatice.
[4]. ANIS, [Online]. Available: https://www.anis.ro/top-10-vulnerabilitati-care-pot-aparea-intr-un-sistem-informatic.

Cyber Attacks Based on Data Injection

Alexandru-Marius SIMION
University Politehnica of Bucharest, Romania
alexandru.simion95@stud.etti.upb.ro

Abstract

Software vulnerabilities represent the most important vulnerabilities due to their impact compared to other vulnerabilities such as hardware and network ones. Throughout the years many vulnerabilities have been identified, classified, and registered by organizations such as MITRE as a CVE (common vulnerability or exposure) and assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to organizations. This paper describes, analyses, and provides solutions to the effects of the top three most dangerous system vulnerabilities such as: SQL injection and Command Injection.

Keywords: software vulnerabilities, SQL injection, command injection

References

[1]. MITRE, "CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')," 19 September 2019. [Online]. Available: https://cwe.mitre.org/data/definitions/89.html. [Accessed 30 11 2019].

[2]. MITRE, "CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')," 23 September 2019. [Online]. Available: https://cwe.mitre.org/data/definitions/78.html. [Accessed 28 11 2019].

[3]. Hack2Secure, "Understanding SQL Injection Attacks," 20 7 2017. [Online]. Available: https://www.hack2secure.com/blogs/understanding-sql-injection-attacks. [Accessed 24 11 2019].

[4]. S. I. M. M. Atefeh Tajpour, " SQL Injection Detection and Prevention Techniques," 8 2001. [Online]. Available: https://www.researchgate.net/publication/272854124_SQL_Injection_Detection_and_Prevention_Techniques. [Accessed 26 11 2019].

[5]. S. Mohanty, https://dzone.com/articles/5-important-software-vulnerability-and-attacks-tha, 2018.

[6]. C. N. C. X. Anastasios Stasinopoulos, "Commix: Detecting and exploiting command injection flaws," November 2015. [Online]. Available: https://www.researchgate.net/publication/290181384_Commix_Detecting_and_exploiting_command_injection_flaws [Accessed 1 12 2019].

[7]. How To Prevent Command Injection, [Online]. Available: https://affinity-it-security.com/how-to-prevent-command-injection/. [Accessed 29 11 2019].

Protocols and Techniques to Implement a Secure Network

Ioana-Iuliana TURCU
University Politehnica of Bucharest, Romania
iulianaturcu13@yahoo.com

Abstract

Cyber-attacks have still increased considerably last year according to Symantec Corporation and from Europol reports, cybercrimes cause annual damage of huge amount of money. In a positive way also, Europol says that last year some good things happened like: General Data Protection Regulation (GDPR), the Network and Information Security (NIS) directive and 5G technology. This paper will present the methods that ensure security communication on actual technologies.

Keywords: encryption, VPN, IPSec

References

[1]. Charles J. Brooks, Christopher Grow, Philip Craig, Donald Short, Cybersecurity Essentials, Sybex, 2018.
[2]. M. Apetrii, Introducere în securitatea rețelelor – Tehnici de bază, https://cupdf.com/document/introducere-in-securitatea-reelelor.html.
[3]. Marius Ionut Ene, https://social.technet.microsoft.com/wiki/contents/articles/6422.ce-este-ipsec-cand-se-foloseste-si-de-ce-ro-ro.aspx.
[4]. I.C. Mihai, Securitatea informațiilor, Sitech, 2012.
[5]. P. Loshim, M. Cobb, Data Encryption Standard (DES), TechTarget, https://www.techtarget.com/searchsecurity/definition/Data-Encryption-Standard.

Analysis on Cyber Attacks in Business Environment

Roxana PRUNDIȘ
University Politehnica of Bucharest, Romania
roxana.prundis@gmail.com

Abstract

Cyber-attacks hit businesses every day. Former Cisco CEO John Chambers once said, "There are two types of companies: those that have been hacked, and those who don't yet know they have been hacked." According to the Cisco Annual Cybersecurity Report, the total volume of events has increased almost fourfold between January 2016 and October 2017. Cybercrime has increased every year as people try to benefit from vulnerable business systems. Often, attackers are looking for ransom: 53 percent of cyber-attacks resulted in damages of $500,000 or more. Cyberthreats can also be launched with ulterior motives. Some attackers look to obliterate systems and data as a form of "hacktivism".

Keywords: cyberattacks, denial of service, man in the middle

References

[1]. https://becominghuman.ai/cybersecurity-and-types-of-cybersecurity-attacks-b036c6d87256.
[2]. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html.
[3]. https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html.
[4]. https://cybersecop.com/news/2019/2/16/phishing-attack-prevention-what-is-phishing.
[5]. https://tools.cisco.com/security/center/resources/sql_injection.
[6]. https://securebox.comodo.com/ssl-sniffing/man-in-the-middle-attack/.
[7]. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html#~how-cyber-attacks-work.
[8]. https://securebox.comodo.com/pos-system/zero-day-attack/.
[9]. https://www.hitechnectar.com/blogs/prevent-dns-tunneling/.
[10]. https://www.wired.com/story/facebook-security-breach-50-million-accounts/.
[11]. https://www.zdnet.com/article/predictions-2020-this-time-cyberattacks-get-personal/.

Implementing Security Measures in Online Banking

Anca-Georgiana SENCIUC
University Politehnica of Bucharest, Romania
ancaa_x@yahoo.com

Abstract

Online banking, also known as internet banking or web banking, is an electronic payment system that enables customers of a bank or other financial institution to conduct a range of financial transactions through the financial institution's website. The online banking system will typically connect to or be part of the core banking system operated by a bank and is in contrast to branch banking which was the traditional way customers accessed banking services. This paper presents the measures that the banks and the clients must follow to ensure security of electronic transactions.

Keywords: online banking, 2FA, password, OTP

References

[1]. https://en.wikipedia.org/wiki/Online_banking.
[2]. https://www.moneysense.gov.sg/articles/2018/11/understanding-online-banking-security.
[3]. https://www.which.co.uk/money/banking/banking-security-and-new-ways-to-pay/online-banking-security/how-safe-is-online-banking-ayvfj7p8cctc.

A Study on the National Cybersecurity Framework

Gabriel PETRICĂ
Faculty of Electronics, Telecommunications and Information Technology,
University POLITEHNICA of Bucharest, Romania
gabriel.petrica@upb.ro

Abstract

In an increasingly dynamic global and European context, with more and more threats and a major impact on cybersecurity, the Romanian ITC society is characterized by an accelerated technical development and harmonization of legislation for adaptation to the requirements of the European Union. In this regard, the evolution of our country has registered important steps, especially in order to harmonize the internal regulations with the commitments assumed within the European Union. This article presents the legislative and institutional context at national level in the field of ensuring cybersecurity in Romania, indicating some directions for improvement. A special chapter is dedicated to the concept of digital certificates as a solution for ensuring data and telecommunications security and authenticity.

Keywords: digital certificate, eIDAS, Certificate Authority, Romanian legislation

References

[1]. LEGEA nr. 8 din 14 martie 1996 (*republicată*) privind dreptul de autor și drepturile conexe, http://legislatie.just.ro/Public/DetaliiDocument/201472.
[2]. LEGE nr. 455 din 18 iulie 2001 (*republicată*) privind semnătura electronică, http://legislatie.just.ro/Public/DetaliiDocument/157828.
[3]. LEGE nr. 365 din 7 iunie 2002 (**republicată**) privind comerțul electronic, http://legislatie.just.ro/Public/DetaliiDocument/37075.
[4]. LEGE nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, http://legislatie.just.ro/Public/DetaliiDocument/43323.
[5]. LEGE nr. 64 din 24 martie 2004 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, http://legislatie.just.ro/Public/DetaliiDocument/51288.
[6]. LEGE nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, http://legislatie.just.ro/Public/DetaliiDocument/56973.
[7]. Banca Națională a României, Regulament nr. 6 din 11.oct.2006, http://www.bnr.ro/apage.aspx?pid=404&actId=20.
[8]. Portal legislativ, Codul Penal din 17 iulie 2009, http://legislatie.just.ro/Public/DetaliiDocument/109855.
[9]. Portal legislativ, Codul de Procedură Penală din 1 iulie 2010, http://legislatie.just.ro/Public/DetaliiDocument/120611.
[10]. MCSI, Strategia Națională privind Agenda Digitală pentru România 2020, https://www.comunicatii.gov.ro/agenda-digitala-pentru-romania-2020/.

[11]. EUR-Lex - Access to European Union Law, REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32014R0910.
[12]. European Commision, Shaping Europe's digital future, https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation.
[13]. E-SENS (Electronic Simple European Networked Services), https://www.noraonline.nl/wiki/Bestand:E-SENS_architecture.jpg.
[14]. Dawn M. Turner, Understanding eIDAS, Cryptomathic, 2016, https://www.cryptomathic.com/news-events/blog/understanding-eidas.
[15]. ORDONANȚĂ DE URGENȚĂ nr. 38 din 30 martie 2020 privind utilizarea înscrisurilor în formă electronică la nivelul autorităților și instituțiilor publice, Portal Legislativ, http://legislatie.just.ro/Public/DetaliiDocument/224709.
[16]. Oracle, CA Hierarchies, https://docs.oracle.com/cd/E19424-01/820-4811/gdzdp/index.html.
[17]. EU Trust Services Dashboard, Available at https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home.
[18]. European Commission, Romania in the Digital Economy and Society Index, 2020, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=66928.
[19]. JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Joint Framework on countering hybrid threats. A European Union response, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018.
[20]. Programul Președinției României la Consiliul Uniunii Europene, https://www.romania2019.eu/wp-content/uploads/2017/11/ro_program_ropres2019.pdf.

Author Guidelines

As an author, you are kindly advised to follow the next instructions. Reading and understanding the requirements before submittal would ensure adherence to the International Conference on Cybersecurity and Cybercrime standards and would facilitate acceptance by the scientific reviewers.

1. Papers must be submitted in English having an even number of pages (minimum 4 pages). At least 50% of the last page should be occupied by text.
2. For papers writing it is recommended the use the text processor Microsoft Word and one of the template models found on the conference website. We will do the final formatting and all necessary format conversions of your paper.
3. The papers will be submitted using our online interface. Please do not send your papers by email.
4. The papers will be reviewed by two scientific reviewers, well-known in their domains of activity. Usually, it takes 1 to 3 months between the moment you finished your submission and a response is given by scientific reviewers.
5. The papers will be sent back to the authors for corrections if the figures, pictures, or tables are not contained in the text or if the reviewers require modifications or supplementary information.
6. The papers will be rejected if their scientific content is not adequate, if they don't contain original elements and if they are not properly written in English.
7. The bibliography must show the authors adequate documentation. At least 7-10 quality references should be cited.
8. Citation standard is IEEE. Please read the IEEE Citation Reference from the website: www.ieee.org/documents/ieeecitationref.pdf.
9. The whole responsibility for the calculation exactitude, experimental data, scientific affirmation, and paper translation belongs to the authors.
10. The authors will declare on their own responsibility that the article or parts of it were not published before in other journals.

More information: https://proceedings.cybercon.ro/index.php/ic3/author-guidelines

The Romanian Association for Information Security Assurance (RAISA)

The Romanian Association for Information Security Assurance (RAISA) is a professional, non-governmental, non-partisan political, nonprofit, and public benefit association.

RAISA AIM

The aim of the Romanian Association for Information Security Assurance is promoting and supporting information security activities in compliance with applicable laws.

RAISA VISION

The vision of the Association is to promote research and education in information security field and to contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at the national level, bringing together professors and researchers from top universities and Romanian institutions, PhD, master's, and license students, as well as companies in the IT segment.

RAISA OBJECTIVES

To achieve the stated purpose, the Romanian Association for Information Security Assurance proposes the following objectives:

- Collaboration with the academic community from Romania or abroad in order to organize conferences, scientific seminars and workshops for presenting the development and implementation of effective measures to improve information security.
- Collaboration with research centers, associations, and companies from Romania or abroad, to organize informative events in information technology security field.
- To perform specific programs for education and training of personnel involved in electronic information management (data processing, storage, security).
- To ensure the dissemination of notice relating to existing vulnerabilities and nationally and internationally newly identified threats; to provide solutions for data restoration and policies to prevent and combat incidents based on the information provided by suppliers of software solutions.
- To publish scientific journals for university staff, PhD students or master's students, researchers, students, and other professional categories in the field of information security and cybercrime.
- To grant awards, scholarships, or sponsorships to people with outstanding merits in the field of information security.

Website: www.raisa.org
Email: contact@raisa.org

RAISA Members Benefits

RAISA MEMBERS

The Romanian Association for Information Security Assurance (RAISA) is an organization that consists of:

- **Founding members** - are individuals who have participated in the founding process of the Association, have agreed with the Statute of the Association at the date of establishment and are parts of the members' category, with all their rights. The founding members pay annual membership fee and have the right to deliberative vote during the General Assembly.
- **Members** - are individuals who have joined the Association after the date of establishment. The members pay annual membership fee and have all the rights, respecting the obligations stipulated in Statute of the Association. They have the right to deliberative vote during the General Assembly.
- **Honorary Members** - can be scientists, professors, cultural or religious personalities, valuable professionals, who have rendered outstanding services to the Association. They are exempted from contributions and their vote is advisory.
- **Collaborators/Volunteers** - anyone who wants to participate in Association activities without becoming a member. Their collaborations are on no-cost basis; they don't pay a membership fee and don't have the right to vote.

RAISA MEMBERSHIP BENEFITS:

- Free access to RAISA events.
- Discount to workshops and conferences supported by RAISA.
- Discount for professional courses organized by RAISA.
- Possibility to be involved in RAISA projects and campaigns, support offered for research.
- Free publishing for scientific articles in the International Journal for Information Security and Cybercrime (IJISC), indexed in international databases.
- Discount for books and scientific studies promoted by RAISA.
- The possibility of promoting the events on RAISA media channels:
    - www.securitatea-cibernetica.ro
    - www.securitatea-informatiilor.ro
    - www.criminalitatea-informatica.ro

Get the most from your membership!

www.raisa.org/raisa-members/