Romanian Association for
Information Security Assurance

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VI
eISSN 2393-0837

CyberCon Romania
2019

THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

PROCEEDINGS
OF
THE INTERNATIONAL CONFERENCE ON CYBERSECURITY AND CYBERCRIME

Volume VI

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

CyberCon Romania
2019

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

TABLE OF CONTENTS

Issues and Challenges of Cyber Security in Social Networking

Ana-Maria COMAN
University Politehnica of Bucharest, Romania
comananamaria94@gmail.com

Abstract

In this paper will be discussed the concept of security and privacy in social media. Social networking websites such as Facebook, Instagram, Twitter and LinkedIn are the popular social sites. Social sites are the most common platform for people to communicate with their family, friends and to share thoughts, photos, videos and lots of information. Users are unaware of the privacy risks involved when they share their sensitive information on the social network sites. Security attacks continue to be a major concern of all users. This research deals with the different kind of attacks on social networks and their issues.

Keywords: Cyber attacks, Social Networking, security issues, Cyber Security

References

[1]. http://www.ic3.gov/ "Internet Crime Report 2015".
[2]. Most number of cyber crime reports. Available: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/.
[3]. National Cyber Security Policy 2013. Available: https://en.wikipedia.org/wiki/National_Cyber_Security_Policy_2013.
[4]. Security, Privacy and Trust in Social Networking Sites. Richa Garg, Ravi Shankar Veerubhotla, Ashutosh Saxena. CSI Communications ISSN 0970-647X| Volume No. 39| Issue No. 2| May 2015.
[5]. Exploiting Vulnerability to secure user Privacy on a social networking site. Pritam Gunecha, Geoffrey Barbier, Huan Lui. ACM, SIGKDD International conference on knowledge Discovery and Data Mining, August 2011.
[6]. Latest in phishing 2016. Available: https://info.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2016.
[7]. Malware statistics. Available: https://www.av-test.org/en/statistics/malware/.
[8]. Dolvara Gunatilaka, "A Survey of Privacy and Security Issues in Social Networks," www.cse.wustl.edu/~jain/cse571-11/ftp/social/index.
[9]. "Facebook Privacy Basics", [Online]. Available: https://www.facebook.com/about/basics.
[10]. Browser Security Settings. Available: http://its.ucsc.edu/software/release/browser-secure.html.
[11]. Communication Networks: Fundamental Concepts and Key Architectures by Alberto Leon-Garcia, Indra Widjaja Published July 16th, 2003, by McGraw-Hill Education (first published January 15th 2000).

[12]. Computer Networks, 5e (5th Edition) by Andrews Tanenbaum, David J.Wetherall by Pearsons Edition.
[13]. Computer Networking: A Top-Down Approach by Kurose James F. (Author), Ross Keith W. Pearsons Edition.
[14]. Data Communications and Networking by Forouza Indian Edition.
[15]. Network Processor Design: Issues and Practices: 1 (The Morgan Kaufmann Series in Computer Architecture and Design) by Mark A. Franklin, Patrick Crowley, Haldun Hadimioglu. Prentice Hall India Learning Private Limited; 5 edition (2006).
[16]. http://www.onlineschools.org/blog/history-of-socialnetworking/.
[17]. B. Stone, Is Facebook growing up too fast, The New York Times, March 29, 2009.
[18]. www.securelist.com, «"Instant" threats», Denis Maslennikov, Boris Yampolskiy.
[19]. Won Kim, Ok-Ran Jeong, Sang-Won Lee, "On Social Websites", Information Systems 35 (2010), 215-236.
[20]. Kaven William, Andrew Boyd, Scott Densten, Ron Chin, Diana Diamond, Chris Morgenthaler, " Social Networking Privacy Behaviors and Risks", Seidenberg School of CSIS, Pace University, White Plains, NY 10606, USA.
[21]. Abdullah Al Hasib, "Threats of Online Social Networks", IJCSNS, Vol. 9, No 11, November 2009.
[22]. Anchises M. G. de Paula, "Security Aspects and Future Trends of Social Networks", IJoFCS (2010) , 1, 60-79.
[23]. D. Boyd, N. Ellison, Social network sites: definition, history, and scholarship, Journal of Computer-Mediated Communication 13 (1) (2007) article 11.
[24]. Gilberto Tadayoshi Hashimoto, Pedro Frosi Rosa, Edmo Lopes Filho, Jayme Tadeu Machado, A Security Framework to Protect Against Social Networks Services Threats, 2010 Fifth International Conference on Systems and Networks Communications.
[25]. "Data Loss Prevention Best Practices", http://www.ironport.com/pdf/ironport_dlp_booklet.pdf.
[26]. "The Real Face of KOOBFACE: The Largest Web 2.0 Botnet Explained".
[27]. Hekkala, R., Väyrynen, K., & Wiander, T. (2012, June). Information Security Challenges of Social Media for Companies. In ECIS (p. 56).
[28]. Barnes, S. (2006). A privacy paradox: Social networking in the United States. First Monday, 11(9). doi:10.5210/fm.v11i9.1394.
[29]. Kumar, A., Gupta, S. K., Rai, A. K., & Sinha, S. (2013). Social Networking Sites and Their Security Issues. International Journal of Scientific and Research Publications, 3(4), 3.
[30]. Verma, A., Kshirsagar, D., & Khan, S. (2013). Privacy and Security: Online Social Networking. International Journal of Advanced Computer Research, 3(8), 310-315.
[31]. Deng, X., Bispo, C. B., & Zeng, Y. (2014). A Reference Model for Privacy Protection in Social Networking Service. Journal Of Integrated Design & Process Science, 18(2), 23-44. doi:10.3233/jid-2014-0007.
[32]. Bertot, J. C., Jaeger, P. T., & Hansen, D. (2012). The impact of polices on government social media usage: Issues, challenges, and recommendations. Government Information Quarterly, 29(1), 30-40.
[33]. Vladlena, B., Saridakis, G., Tennakoon, H., & Ezingeard, J. N. (2015). The role of security notices and online consumer behaviour: An empirical study of social networking users. International Journal Of Human - Computer Studies, 8036-44. doi:10.1016/j.ijhcs.2015.03.004.
[34]. Kim, H. J. (2012). Online Social Media Networking and Assessing Its Security Risks. International Journal Of Security & Its Applications, 6(3), 11-18.

[35]. GUNDECHA, P., BARBIER, G., JILIANG, T., & HUAN, L. (2014). User Vulnerability and Its Reduction on a Social Networking Site. ACM Transactions On Knowledge Discovery From Data, 9(2), 12:1-12:25. doi:10.1145/2630421.

[36]. Thompson, A. F., Otasowie, I., & Famose, O. A. (2014). Evaluation of Security Issues in Social Networks. Computing & Information Systems, 18(1), 6-20.

[37]. Role of Security in Social Networking, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 2, 2016.

[38]. Social Media Security Risks, Cyber Threats And Risks Prevention And Mitigation Techniques, IJSART - Volume 4 Issue 4 – APRIL 2018 ISSN [ONLINE]: 2395-1052.

[39]. Issues and Challenges of Cyber Security for Social Networking Sites (Facebook), International Journal of Computer Applications (0975 – 8887), Volume 144 – No.3, June 2016.

[40]. Cyber Security for Social Networking Sites: Issues, Challenges and Solutions, Volume 5 Issue IV, April 2017.

[41]. A General Study on Cyber-Attacks on Social Networks, IOSR Journal of Computer Engineering (IOSR-JCE), e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 19, Issue 5, Ver. V (Sep.- Oct. 2017), pp. 01-04.

Study of Cybersecurity and Notable Cyber Attacks

Cătălin-Alexandru FRONE
University Politehnica of Bucharest, Romania
catalin.frone1@gmail.com

Abstract

Since the late 1980s cyberattacks have evolved several times to use innovations in information technology as vectors for committing cybercrimes. In recent years, the scale and robustness of cyberattacks has increased rapidly, as observed by the World Economic Forum in its 2018 report: "Offensive cyber capabilities are developing more rapidly than our ability to deal with hostile incidents.

Keywords: cyberattack, Trojan, DDoS, cybercrime

References

[1]. https://securelist.com/kaspersky-ddos-intelligence-report-for-q1-2016/74550/.
[2]. https://en.wikipedia.org/wiki/Computer_worm.
[3]. https://www.kaspersky.com/resource-center/threats/trojans.
[4]. https://www.secpoint.com/top-10-worms.html.
[5]. https://en.wikipedia.org/wiki/Computer_virus.
[6]. https://en.wikipedia.org/wiki/Cyberattack.
[7]. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html.
[8]. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

Social Media and Its Data Privacy

Marius-Andrei GÎBU
University Politehnica of Bucharest, Romania
mariusgibu@gmail.com

Abstract

Digital Data Privacy is one of the biggest issues in 21st century, with ever so growing social media platforms, and so much personal information already on the Internet (credit cards, bank accounts, private pictures, etc.) the threat is real. The year 2019 comes with a big deficit of cyber security experts, so you have to do your best in keeping private data secure.

Keywords: social media, digital privacy, personal data security

References

[1]. https://turtler.io/news/data-privacy-in-social-media-who-takes-responsibility-and-data-protection-as-a-priority-feature.
[2]. https://identity.utexas.edu/everyone/how-to-manage-your-social-media-privacy-settings.
[3]. https://digitalsecurityworld.com/how-you-protect-social-media-accounts/.
[4]. https://us.norton.com/internetsecurity-privacy-protecting-privacy-social-media.html.

Firewall Technologies. Advantages and Limitations

Elena-Roxana COSTEA
University Politehnica of Bucharest, Romania
costearoxana94@gmail.com

Abstract

Currently, most businesses are based on a more or less developed IT system. For daily activities, the organization needs to be able to connect to the Internet, possibly from a local area network (LAN). But, with the benefits of using the Internet, there are also the security risks the organization needs to minimize through appropriate measures and controls. Security issues arising from Internet use include hacker attacks, virus infection, malware, and spyware. Hackers can theoretically get into the organization's network and steal confidential data, damage the organization's computers or the entire local network, use the organization's resources to be an employee of the organization, etc. Thus, a necessary security measure at the level of any organization's network is the implementation of firewalls. This paper aims to describe what is a firewall, firewall types and technologies. The paper will not present types of firewall architectures and details of their deployment, as well as details of how to configure these devices.

Keywords: security, firewall, cyber-attacks

References

[1]. Abie, Habtamu (2000). An overview of Firewall Technologies.
[2]. Godwiak, Adam (2003). Techniques used for bypassing firewall systems.
[3]. Hill, Jake (1998). Bypassing Firewalls: Tools and Techniques.
[4]. Irby, David (2005). Firewalk: Can Attackers See Through Your Firewall?, SANS Institute.
[5]. ISACA (2011). Certified Information Systems Auditor – CISA Review Manual 2011.
[6]. Noonan Wes, Dubrawsky Ido (2006), Firewall Fundamentals, Cisco Press.
[7]. Northcutt Stephen, Zeltser Lenny, Winters Scott, Kent Karen, Ritchey Ronald W. (2005). Inside Network Perimeter Security, Second Edition, Sams Publishing.
[8]. Peterson Larry, Bruce Davie (2007). Computer Networks. A system approach, Fourth Edition, Elsevier.
[9]. Scarfone Karen, Hoffman Paul (2009). Guidelines on Firewalls and Firewall policy. National Institute of Standards and Technology (NIST).
[10]. Stallings, William (2011). Cryptography and network security. Principles and Practice, Fifth Edition, Prentice Hall.
[11]. Stewart James Michael, Tittel Ed, Chapple Mike (2005). CISSP – Certified Information Systems Security Proffesional Study Guide, Third Edition, Sybex.

Analysis of Cyber Attacks Against Computers and Networks

Andrei-Marcel IONIȚĂ
University Politehnica of Bucharest, Romania
a.ionita9@yahoo.com

Abstract

A computer virus is a type of malicious software that, when executed, replicates itself by modifying other computer programs and inserting its own code. When this replication succeeds, the affected areas are then said to be "infected" with a computer virus. The term "virus" is also commonly, but erroneously, used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransomware, spyware, adware, trojan horses, keyloggers, rootkits, bootkits, malicious Browser Helper Object (BHOs), and other malicious software. This paper presents some of the existing Malware, how you can protect yourself against them and how to remove them.

Keywords: Ransomware, Trojan, DoS, CryptoLocker

References

[1]. Aycock, John (2006). Computer Viruses and Malware. Springer.
[2]. https://www.csoonline.com/article/3236183/ransomware/what-is-ransomware-how-it-works-and-how-to-remove-it.html.
[3]. https://us.norton.com/internetsecurity-malware-what-is-a-trojan.html.
[4]. https://us.norton.com/internetsecurity-emerging-threats-dos-attacks-explained.html.
[5]. https://www.supinfo.com/articles/single/5215-computer-virus.

Security of Electronic Transactions in E-commerce

Laurențiu MODRIȘAN
University Politehnica of Bucharest, Romania
lmodrisan@yahoo.com

Abstract

The shopping via an online channel has grown exponentially recently. This is closely linked to the malicious applications targeting both customers and e-commerce providers. The attackers have discovered more and more effective ways to defend the security barriers. The hackers aim at personal information, transaction's safety and also to fraud the payments. This paper's purpose is to reduce the number of cybercrimes by presenting the most common online security threats, the risks involved in online banking activities and the most famous safety measures to be considered by every internet user.

Keywords: online banking, e-commerce, security threats

References

[1]. 5 Huge WP eCommerce Security Threats and 12 Powerful Solutions, [Online]: https://wpbuffs.com/ecommerce-security-threats/.
[2]. E-Commerce Market Report in 2017, [Online]: https://www.gpec.ro/blog/en/e-commerce-market-report-2017-romanians-purchased-online-2-8-billion-euro-worth-of-products.
[3]. Why is e-commerce security so important?, [Online]: https://www.bigcommerce.com/ecommerce-answers/why-online-security-so-important/.
[4]. Pranav Patil, Study on E-Commerce Security Issues and Solutions.
[5]. Denial-of-Service attack. [Online]: https://searchsecurity.techtarget.com/definition/denial-of-service.
[6]. Candid Wüeest, Threats to Online Banking.
[7]. http://securityresponse.symantec.com/avcenter/venc/data/trojan.goldun.b.html.

Cyber Threats Related to Network Security

Constantin DUMITRU
University Politehnica of Bucharest, Romania
dumitru0constantin@gmail.com

Abstract

Network security is a method of preventing your computer network from the unauthorized user access, email spoofing, Trojan horses, denial of service, hacking, viruses, spyware and intruders etc. There are different securities mechanisms are being employed to protect the network. If a hacker gets control of your computer or network, he can send viruses or steal your company's confidential data. Similarly, if any computer in your network is infected with the viruses or spyware, all other computers will also be infected if no proper security system has been implemented. Securing a network is most important job description of the network administrators, security specialists, network engineers and IT managers.

Keywords: network, security, encryption, firewall

References

[1]. https://www.ijser.org/researchpaper/Grid-of-Security-A-New-Approach-of-the-Network-Security.pdf.
[2]. https://www.ijera.com/papers/Vol2_issue4/KB2417221726.pdf.
[3]. https://www.cpc.unc.edu/research/tools/datasecurity/computer-on-net.
[4]. https://www.lifewire.com/introduction-to-computer-network-security-817989.
[5]. https://www.gflesch.com/blog/5-simple-ways-to-help-ensure-a-secure-computer-network.
[6]. https://www.informationsecuritybuzz.com/articles/secure-computer-system-network/.
[7]. https://www.computerworld.com/article/2547589/networking/10-tips-to-secure-your-small-business-network.html.

A Study on Security of Information Systems

Georgiana BĂEȚICA
University Politehnica of Bucharest, Romania
georgiana_baetica@yahoo.com

Abstract

Alternatively referred to as cybercrime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files.

Keywords: cyber-attacks, cybercrime, malware

References

[1]. Alexander, Kent B., and Wood, Kristin L. "The Economic Espionage Act: Setting the Stage for a New Commercial Code of Conduct." Georgia State University Law Review 15 (1999): 907–939.
[2]. Baker, Glenn D. "Trespassers Will Be Prosecuted: Computer Crime in the 1990s." Computer Law Journal12 (1993): 61–100.
[3]. Branscomb, Anne W. "Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime." Rutgers Computer and Technology Law Journal 16 (1990): 1–61.
[4]. Charney, Scott, and Alexander, Kent. "Computer Crime." Emory Law Journal 45 (1996): 931–957.
[5]. Goodman, Marc D. "Why the Police Don't Care About Computer Crime." Harvard Journal of Law & Technology 10 (1997): 465–495.
[6]. Hatcher, Michael; McDannell, Jay; and Ostfeld, Stacy. "Computer Crimes." American Criminal Law Review36 (1999): 397–444.
[7]. Lederman, Eli. "Criminal Liability for Breach of Confidential Commercial Information." Emory Law Journal38 (1989): 921–1004.
[8]. Nimmer, Raymond T. The Law of Computer Technology, 2d ed. Boston: Warren Gorham Lamont, 1992. Pages 12-1–12-50.
[9]. Parker, Donn B. Fighting Computer Crime. New York: Wiley Computer Publishing, 1998.

Cybersecurity: Security of Networks and Information in the Financial Sector

Ion GURAN
University Politehnica of Bucharest, Romania
ionut_guran@yahoo.co.uk

Abstract

The primary objective of this article is to develop an economics-based analytical framework for assessing the impact of government incentives/regulations designed to offset the tendency to underinvest in cyber security related activities by private sector firms. IT financial systems are exposed to the many dangers that require consistent efforts to operate safely. In recent years, network and information security (NIS) risks have become more complex and their impact may vary from a small to very high range, including a domino effect. This paper is meant to analyze the modalities to secure and protect the financial sector firms from the many dangers in the online transactions.

Keywords: financial sector security, cyber insurance, cyber security policy, cyber regulations

References

[1]. Network and Information Security in the Finance Sector - Regulatory landscape and Industry priorities, European Union Agency for Network and Information Security: https://www.enisa.europa.eu/publications/network-and-information-security-in-the-finance-sector.

[2]. Increasing cyber security investments in private sector firms Lawrence A. Gordon, Martin P. Loeb*, William Lucyshyn, and Lei Zhou - Journal of Cybersecurity, 1(1), 2015, 3–17, http://cybersecurity.oxfordjournals.org/content/cybers/1/1/3.full.pdf.

[3]. Examining the costs and causes of cyber incidents, Sasha Romanosky, Journal of Cybersecurity, 2016, 1–15, http://cybersecurity.oxfordjournals.org/content/cybers/early/2016/08/08/cybsec.tyw001.full.pdf.

[4]. https://en.wikipedia.org/wiki/Computer_security.

Common Malware Types

Adrian-George NISTOR
University Politehnica of Bucharest, Romania
adrian.nistor3@gmail.com

Abstract

Over the last decades, there were lots of studies made on malware and their countermeasures. The most recent reports emphasize that the invention of malicious software is rapidly increasing. Moreover, the intensive use of networks and Internet increases the ability of the spreading and the effectiveness of this kind of software. On the other hand, researchers and manufacturers making great efforts to produce anti-malware systems with effective detection methods for better protection on computers. This paper presents a detailed classification of malware, specification of each type and malicious actions that cybercriminals are taking through them, in order to steal private information and damage users' information systems. In the end, there will be more about different types of defense mechanism against certain malware, that will show protection and will make the system to be immune when an attack occurs.

Keywords: cyber-attacks, malware, cybercriminal

References

[1]. Wjeb Gharibi, Studying and Classification of the Most Significant Malicious Software.
[2]. J. Markoff, Defying experts, Rogue Computer Code Still Lurks, New York Times, 2009.
[3]. What is the Difference: Viruses, Worms, Trojans, and Bots? [Online] Available: https://www.cisco.com/c/en/us/about/security-center/virus-differences.html.
[4]. M. Barwise. What is an internet worm?, 2010.
[5]. Understanding Denial-of-Service Attacks, US-CERT, 2013.
[6]. M. Prince, Empty DDoS Threats: Meet the Armada Collective, 2016.
[7]. Kiyuna and Conyers, Cyberwarfare, 2015.
[8]. S.V. Raghavan, An investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, 2011.
[9]. J. Schofield, How can I remove a ransomware infection?, The Guardian, 2016.
[10]. M. Curtin, Introduction to Network Security, 2015.
[11]. Distributed Denial of Service Attacks (DDoS) Resources, Pervasive Technology Labs at Indiana University, 2009.

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/