The New Global Challenges in Cyber Security

7-8 October 2019, Bucharest, Romania

Conference report

CERT-RO

Contents

- Summary
- Sessions Insights
- Participants’ feedback
- Attendance stats

CERT-RO

Dear partners, supporters and guests,

On behalf of Romanian National Computer Security Incident Response Team –CERT-RO, I would like to thank you all for attending the 9th edition of the Annual International Conference "The New Global Challenges in Cyber Security"- #certcon9.

The primary goal of the conference was to bring together stakeholders and experts in cyber security, so we are glad to mention this edition has been the largest yet, as it brought together over 400 cyber experts, government officials and policy-makers, as well as representatives of private companies from across all sectors and industries, NGOs and Academia. Moreover, the event achieved the global reach that we had hoped for, proving that Romania can become an important regional actor on cyber security area.

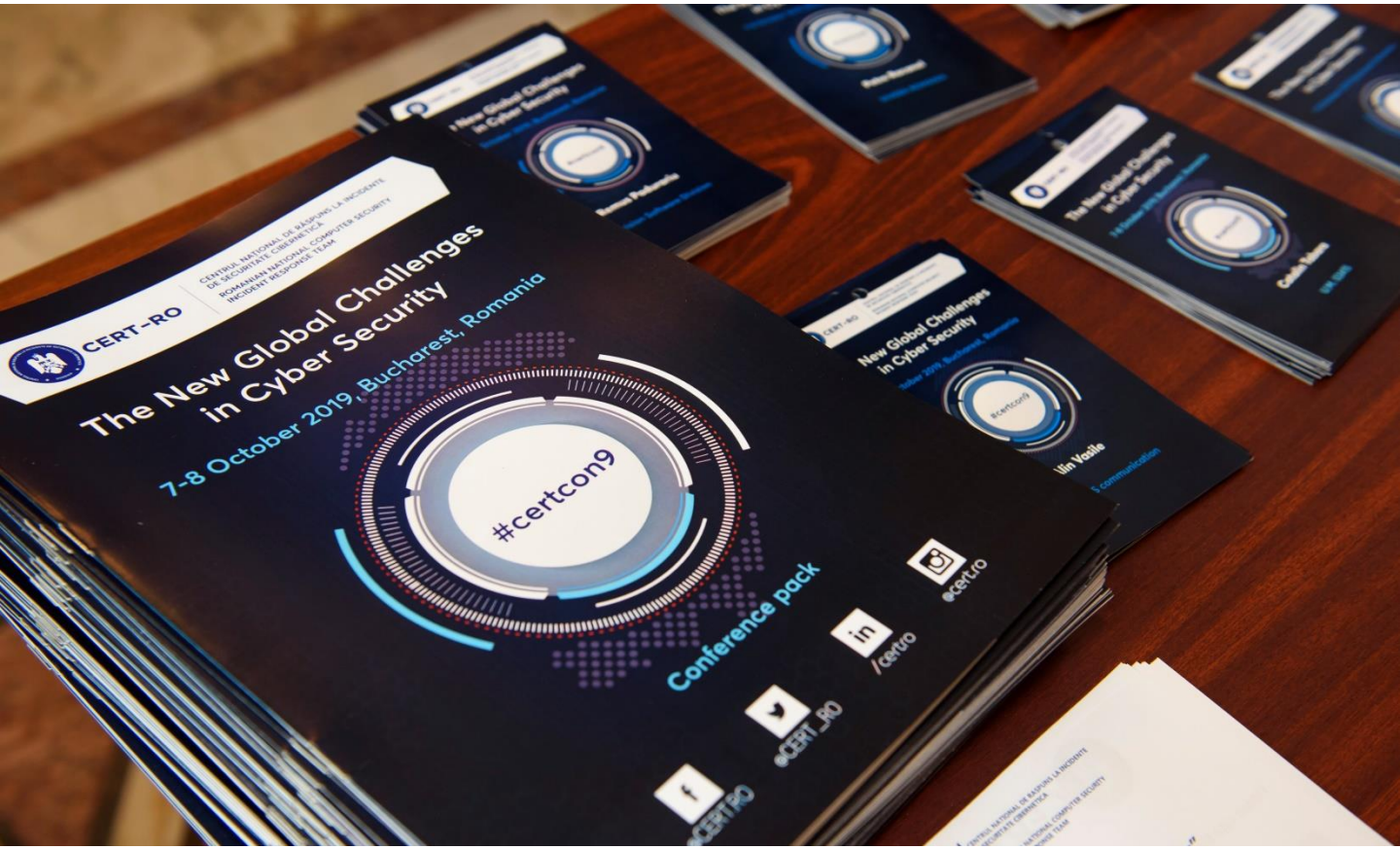
We hope that you found the conference informative and an opportunity to extend networks and to enhance cooperation. We believe that our diverse and dynamic group of speakers provided in-depth insights into policy developments at European and International level, capacity building tools and initiatives, implementation of new technologies in the cyber security field, as well as insights into the global threat landscape.

We plan to have at least the same global impact with the 2020 edition and we hereby extend the invitation to have you as partners, supporters and / or guests both for the event and throughout the year!

Sincerely,
Cătălin Aramă
Director General CERT-RO

CERT-RO

Summary



Every year, the „New Global Challenges in Cyber Security" conference tackles the most pressing cyber security issues on the public agenda and looks at both the latest challenges in this field and ways to overcome them together with cyber security experts from private companies across all sectors and industries, government officials, policy-makers, NGOs and Academia.

This year's edition of the CERTCON addressed some of the most critical subjects of cybersecurity, ranging from policy and law enforcement to technical aspects. We will discuss the challenges of 5G Networks from cybersecurity perspectives, the action and the counteraction against cybercrime, education and awareness necessary to maintain the population alert, lessons learned and the challenges of the NIS implementation, the vision and the challenges of artificial intelligence, but also the research and development in cybersecurity.

In the context of intensifying the dynamics and complexity of cyber threats, as well as the steps taken for ensure a high common level of cyber security of network and information systems, the event offered the opportunity to share ideas and good practices with Romanian experts, representatives of EU member states/European officials.

In the opening session, we had the honor of having Mr. Alexandru Petrescu, Minister of Communications and Information Society who stressed the importance of promoting a safer digital society, an effort in which Romania plays an important role by participating in different formats of international cooperation.

Cyber security affects all domains, reason why it is necessary to develop communication, cooperation and an appropriate common response to cyber threats.

Alexandru Petrescu
Minister of Communication and Information Society

"Romania plays an important role in promoting a safer digital society in the Central and Eastern Europe."

Cătălin Aramă
Director General, CERT-RO

Mr. Cătălin Aramă, the General Director of CERT-RO presented the three main pillars created with the entry into force of the Law no. 362/2018 on ensuring a high common level of security of computer networks and systems. The novelty elements are the designation of CERT-RO as nationally competent authority, Single Point of Contact and CSIRT team.

The volume of data we produce and the level of digitization is increasing, development which brings opportunities and challenges alike. We must resist these vulnerabilities and threats by increasing the capacity of accountability, developing digital skills and updating the curriculum to new realities.

"CERT-RO has acquired a triple quality, respectively of national competent authority for the security of the networks and information systems, single point of contact at national level and national CSIRT."

The public institutions are among the most vulnerable entities affected by cyberattacks, as the smallest breach can have a great impact. The public institutions have a big responsibility in assuring the population that the state offers secure electronic public services. In Romania, this process has already begun with the Operational Competitiveness Program which aims to digitalize 36 most common life events.

In the current security context, cooperation and reciprocity in confronting the threats that have no border is of extreme importance. The Memorandums of Understanding concluded by Romania with other states in the field of cyber security is the starting point in this endeavor.

For a country to be considered a cyber power it has to safeguard the cyber health of its citizens, businesses and institutions, and to foster public thrust. In the same time, it must have the legal, ethical and regulatory regimes and when the security of the state is threatened, it has to have the capability to disrupt the adversaries.

CERT-RO

Sessions Insights

Session 1 - The challenges of 5G Networks from cybersecurity perspectives

In terms of connectivity and expansion of services, 5G means an increase in the number of devices connected to the core network and to other devices, at extremely large speeds, with a very low latency. The technological advancement will pave the way to new services and the digital experiences will increase in quality. Edge computing will move the processing power from the core of the network towards to the consumer. The main vulnerability we will have to face is the expansion of the attack surface.

This digital transformation will bring the cloud closer to the consumer, a phenomenon called by some "fog computing". The opportunities of the new technology can provide an increased security if we take the correct decisions. Among the security risks we have to consider with the transition to 5G are supply chain, deployment, system security, privacy, loss of competition and choice, management plane. 5G brings a management and orchestration system that has multiple opportunities for security risks and challenges.

We need to create a holistic and versatile strategy to confront the ever-changing vulnerabilities characteristic to 5G network. Apart from these vulnerabilities, we have to keep in mind that 5G comes with a number of key enhanced security properties compared to earlier generations.

James Travis
Ministry of Defense Cyber Advisor at
Defense Security Cooperation Agency

"5G brings new cyber security opportunities for Romania."

5th generation (5G) deployment of network technologies is a major enabler for future digital services and a priority for the Digital Single Market strategy. Thus, the Commission adopted the 5G Action Plan to ensure the cybersecurity of the 5G networks. Among the points of the Plan is the assessment of the cybersecurity risks affecting 5G networks at national level and take necessary security measures and develop jointly a coordinated Union risk assessment that builds on the national risk assessment. The Objective is the creation of a common Union toolbox of appropriate, effective and proportionate possible risk management measures to mitigate the identified cybersecurity risks at national and Union level.

Romania has established an interinstitutional group to discuss the risk assessment of cybersecurity of 5G networks and attended to the works of NIS Cooperation Group.

Dean Kinsman
Assistant Legal Attaché assigned to
Cyber investigations for the FBI in U.S. Embassy to Romania

Session 2 - Cybercrime – Action & Counteraction

Cybercrime increased exponentially over the last 15-20 years, having in mind the temptation of huge amounts of money that can be gained through hacking or scamming activities in cyber networks.
Internet Crime Complaint Center from USA have revealed that only in the course of a week there are almost 12mil. USD gained in business email compromise attacks.
In this context, it is expected an increase in the number of attacks being identified a strong relation between the attacks and the powerful development of social and commercial activities in cyberspace.

Ionuț Stoica
Senior Project Officer, C-PROC,
Council of Europe

"Cyberattacks represent the common area between cybercrime and cybersecurity."

Cyberattacks represent the common area between cybercrime and cybersecurity. Cybersecurity refers to security, trust, resilience and reliability of ICT, while cybercrime focuses on the rule of law, criminal justice and human rights. The Budapest Convention on Cybercrime (Budapest Convention), the Cybercrime Convention Committee and the C-PROC are the basis of the necessary legislation to protect the individuals and their rights in the cyberspace. The means of fighting cybercrime include reporting mechanism for criminal activities, international cooperation channels and data shared by public and private parties.

Among the foremost consequences of the increase of the number of cyber attacks are alert fatigue and too many false positive verdicts requiring far too much manual action which is time consuming. The solution is to surface the most advanced attacks with machine learning to speed up investigations.

The first challenge is the detection of advanced threats, many of them are hidden, unknown and emerging.

Cyber Threat Hunting is the act of aggressively intercepting, tracking and eliminating cyber adversaries as early as possible.

The primary objective of threat hunting is gathering actionable intelligence, which include information on individuals, organizations, institutions, infrastructure and geography. One issue in assuring cybersecurity is being underequipped, the obsolesce of security instruments, focus on the wrong direction or a lack of process and procedures.

Tudor Cristea
Regional Sales Manager, Bulgaria and Romania, Palo Alto Networks

"We continue to see an escalation in the volume, sophistication and impact of data breaches, which only seem to be getting worse."

Iulian Alecu
Deputy Director General

Session-3 - Education & Awareness

We need more cooperation between the state, private sector and academia/education in order to prepare the future generation for the emerging cybersecurity challenges. In this endeavor, we only need to use the real assets that Romania already has. The three parties are complementing each other in meeting the need for a well-trained human resource. The need for preparing the population of all ages is increasing with the development of sophistication, frequency and impact of the attacks.

The public institutions and agencies that have top-expertise in the field of cybersecurity should be involved more in the training in schools and universities. In order to prepare for the emerging challenges, we have to establish an appropriate curriculum with a vision on the future. The training program should focus on three key-elements: awareness, education and offered services. The public-private-education cooperation should be developed in order to foster exchange of information and know-how. Furthermore, we should involve the top-level practitioners in teaching.

The employment of resources has to be done wisely to the programs with good results and stop the ones that do not perform well. In addition, we have to project strategies for no more than 3 years in order to always have a vision that matches reality.

Andrei Nagy
Head of European Sales, AlphaBlock

Considering the dynamic evolution of the cyberspace, the need for continuity and cooperation between the state, the private sector and education in this field is greater than ever. This cooperation must be based on ensuring an optimum level of preparedness to face the technological and geopolitical challenges, as well as to face one of the most delicate challenges of nowadays: identification, adequate preparation, motivation and the preservation of human resources in the field of cyber security.

In this context, after CERTCON9 debates, it was issued a draft of an White Paper on State, Private Sector and Education Cooperation which will constitute the basis of a national synergy of action between the three mentioned fields (state, private, education) that will be focused on the training and the education of human resources.

Marnix Dekker
NIS Directive coordinator, ENISA

"The NIS Directive provides member states with considerable margin of discretion, which could lead to a divergent application across the EU."

Session 4 - NIS implementation, lessons learned, challenges

The NIS Directive lays down measures to achieve higher level of security for network and information systems. To achieve this goal, it created a cooperation group with strategic role and brings together the CSIRTs of MS via CSIRTs Network. Starting with NIS national strategies, the NIS Directive's provisions also establish incident notification and security requirements for DSPs (such as cloud provides, online market players and search engines) and OES (such as transport, energy, water, health, finance and digital infrastructure).

The NIS Directive is the first piece of the EU cybersecurity legislation. Cybersecurity is a necessity and is no longer optional. Many companies viewed cybersecurity in terms of costs and preferred to give it a low priority. This resulted in a lack of specialization to meet all the security needs. It will take time to implement all the security requirements. Risk evaluation is necessary and can be done through security audits and testing methods. In order to build this capacity, we need to see which detection and protection mechanisms are missing.

In the process of NIS implementation, the law subjects have to increase awareness and assessments throughout the organization, consider risks, define internal policies and procedures, implement technical security solutions, manage security incidents, stay compliant-monitor, prevent and respond.

The NIS Directive has three main objectives: improving national cybersecurity capabilities, building cooperation at European Union level, promoting a culture of risk management and incident reporting among key economic actors.

The NIS Directive is one of the most important topics, not only for Romanian, but also for Europe. The core of the NIS Directive is to assure a framework for collaboration between stakeholders. In this regard, ENISA, the member states and the private sector are working together to fulfill the cybersecurity measures.

One of the first steps in implementing the NIS Directive is to define and understand which are the essential services.

In Romania 76 essential services have been identified by July 2019.

Toma Cîmpeanu
Executive Director, National Association for Security of Information Systems

"The core of the NIS Directive is to assure a framework for collaboration."

Session 5 - Artificial Intelligence-challenges and vision

In 3 to 5 years, the technological landscape will be completely different and will have a huge impact on cybersecurity. Artificial Intelligence will play an important role, both for personal security and for organizations' security.

We are witnessing an increase in the sophistication of the instruments employed by the cyber criminals. One of the instruments used by these malicious actors is hacking the human, or social engineering.

The cyber criminals are using our lack of attention or our lack of skills to try to scam us. Machine learning and AI will help us in fighting cyber crime. The cyber criminals are using algorithms to create and spread botnets and we can use the same instrument to identify the malicious code and try to disrupt it or take legal actions against it.

CERT-RO

Magda Popescu
Outside Legal Counsel,
Microsoft Corporation Digital Crimes Unit,
Central and Eastern Europe

"AI technology helps us to quickly track fast-moving scammers and devote investigator time to higher value work that could lead to finding criminal networks."

We are in the middle of an arms race in terms of cybersecurity threats.

Machine learning and behavior analysis can be used to identify, at a very early stage, the patterns that are out of the ordinary. The natural language processing and image recognition can be used to recognize the methods (such as pop-ups) which are employed in the scamming activities.

Information exchange on our findings and ideas are the key-method in increasing our efficiency in fighting common threats.

Machine Learning is important for defense. Algorithms are helping us to identify which are the false alarms and which are the actual attacks.

Using AI technology, we are able to quickly track fast-moving scammers and devote investigator time to higher value work that could lead to finding criminal networks. The objective is to improve accuracy and reduce false negatives.

Security Operations Centers will be more and more automated processes based on AI and machine learning.

We must collaborate in order to better defend ourselves. There will always be challenges in sharing data. There technical mechanisms which allow different entities to work on the same data which have been cryptographically secured.

There is a need for a standardization of the malware naming convention in order to have a better picture on the threat landscape.

The European Union put forward a series of proposals within the Digital Single Market strategy, such as the Regulation on the free flow of non-personal data e-Privacy Regulation and the Cybersecurity Act.

Peter Elmer
Security Expert, Check Point

"Provide data to algorithms and have these working on selected features."

Session 6 - Research & Development in cyber security

The core-elements of R&D is asking questions, building consortium and groups of interest, cooperation and exchange of knowladge and experience. The Memorandum of Understanding in the field of communications and information society between CERT-RO and CERT.PL is only the first step in fostering cooperation. The idea of an eastern partnership would be a great ocasion to start new R&D initiatives in the future.

Cyber criminals are organized and are collaborating in sharing information. They develop and sell exploit kits on the darknet, which makes it very cheap and simple for anybody to launch a cyber attack. The reality is that cybersecurity remains a business activity and is often difficult to justify the investment necessary to protect.

The three biggest challenges we have to face is the high quantity of false positives and poor quality of data, lack of scalability and massive volumes of data, skills shortage and the lack of collaboration and information sharing. There are information sharing, collaboration and trust channels in place, but sharing critical information and collaborate is still hindered by the lack of trust.

Security Analysts' capacity to make informed decisions is limited by time, personal knowledge, organization's service legal agreement, lack of context and scalability issues. AI and Blockchain can be employed to limit these shortcomings. There is a way to encapsulate intelligence into a blockchain in order to allow people to share information in a trusted way.

What we need to do is to be at least as much creative as the attackers are, in order to be capable to assure the security measures through infrastructures.

Dany Gagnon
Cyber Security Advisor, AlphaBlock

"Cybersecurity remains a cost of doing business."

Andrei Bozeanu
Coordinator of Information Security
and Monitoring Department, CERT-RO

There are Romanian companies focused on deepening the research on using the machine learning to detect malicious activities in the cyberspace, with a special attention to attacks that are very dangerous, but not so common.

Some of the attacks are so dangerous that even though the systems have state-of-the-art security solutions in place, the attackers still succeed to reach their goals.

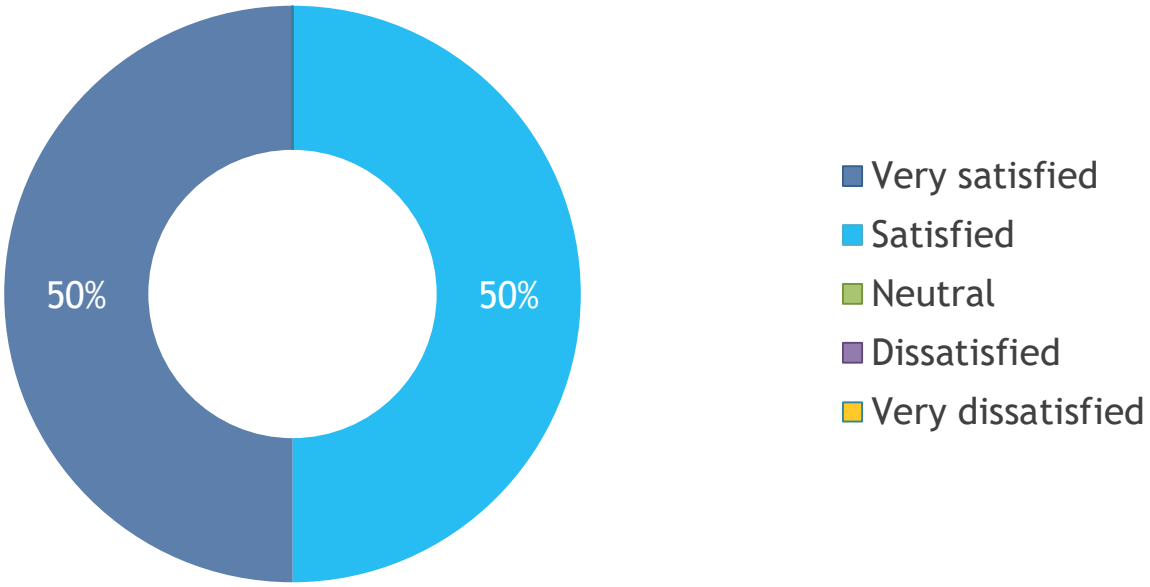
Through activities of research, there were identified cybercriminal campaigns, state sponsored attacks and crypto jacking attacks.

CERT-RO

Participants' feedback

CERT-RO

Overall satisfaction with the conference



General comments

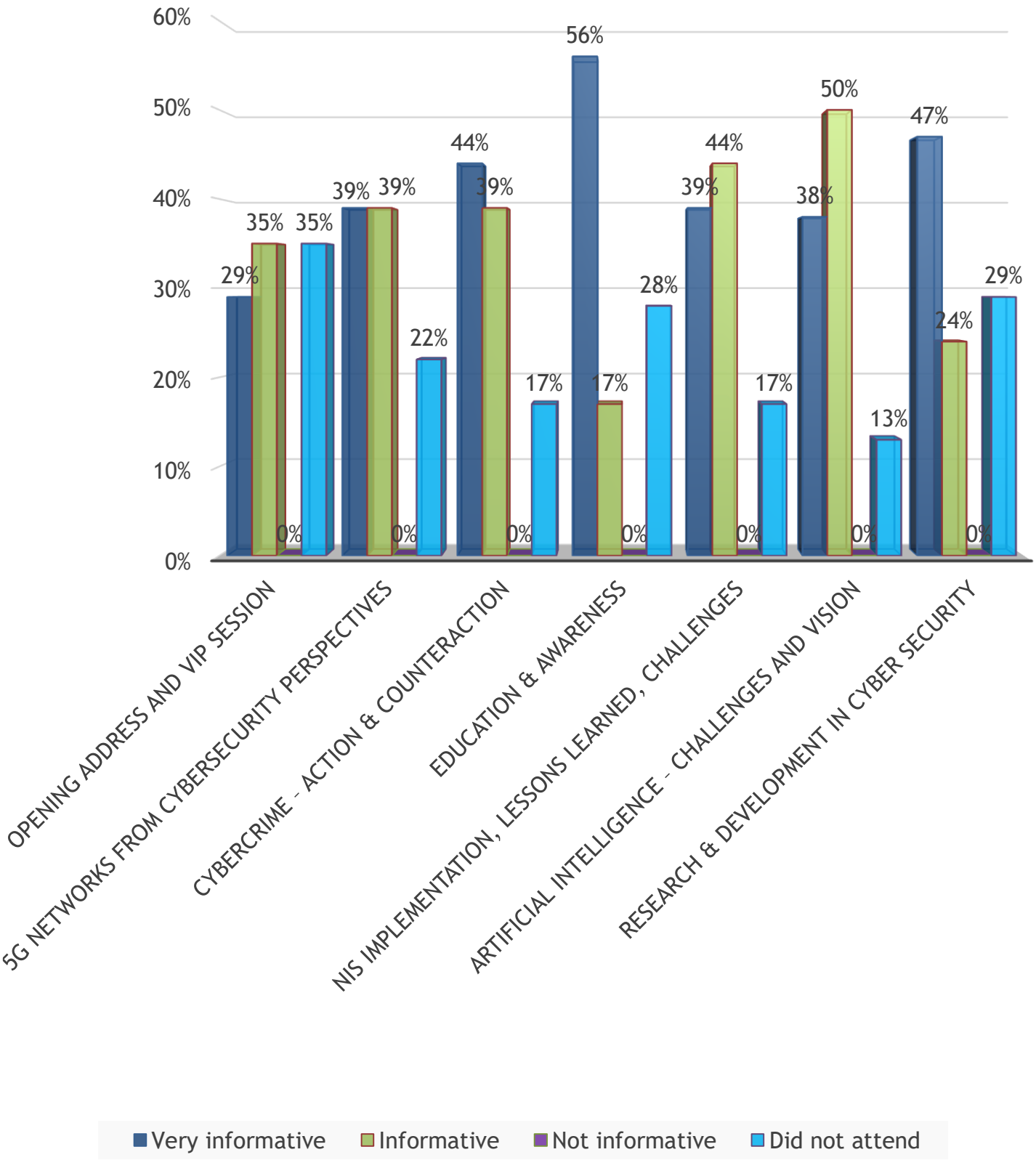
"Organize Round Tables or Forums as preparatory or follow up events to discuss some of the topics of the conference."

"I would like to see more subjects regarding cybersecurity of IOT."

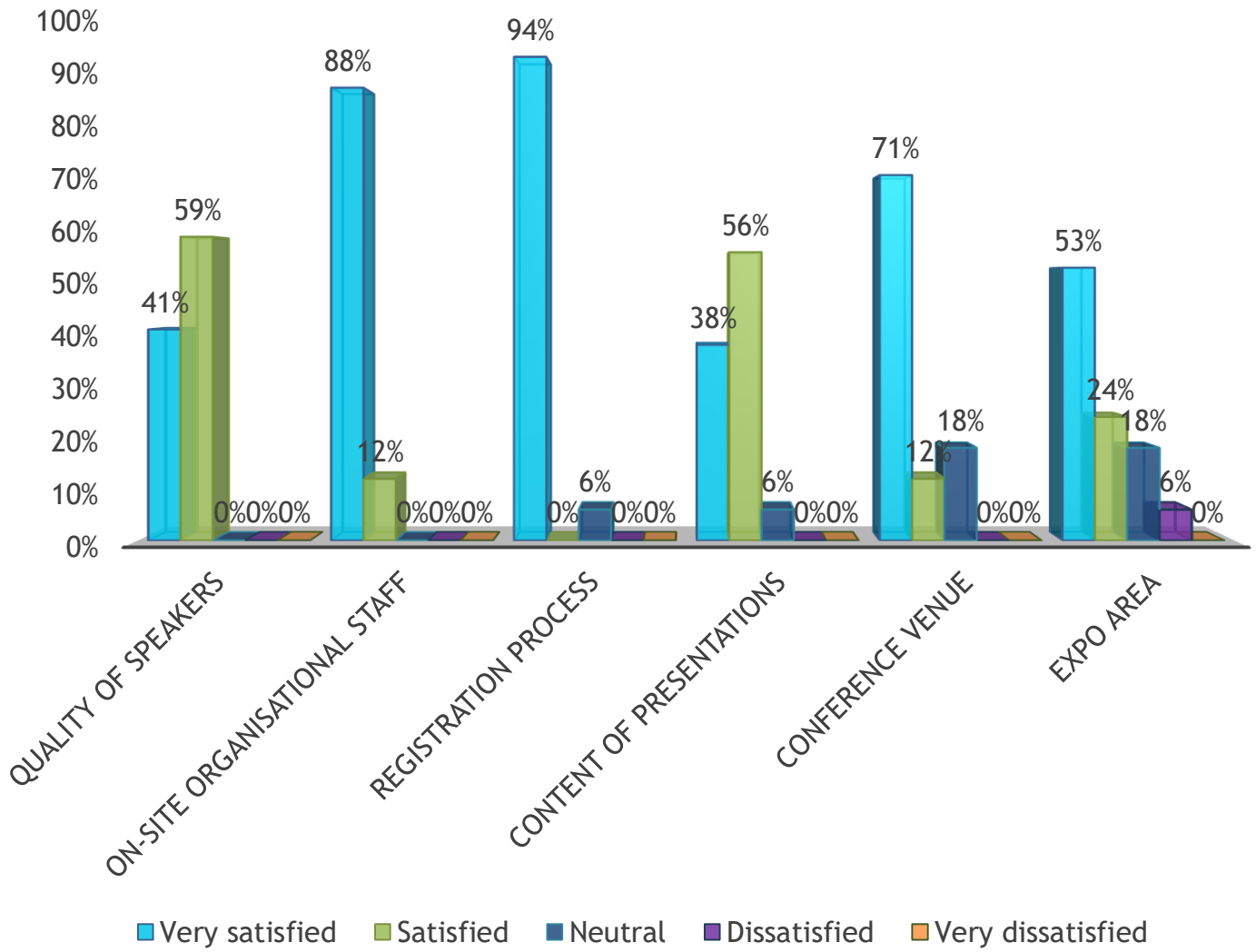
"Include parallel sessions to cover more subjects."

"The chosen topics were very interesting and the overall organization was great."

The most informative session



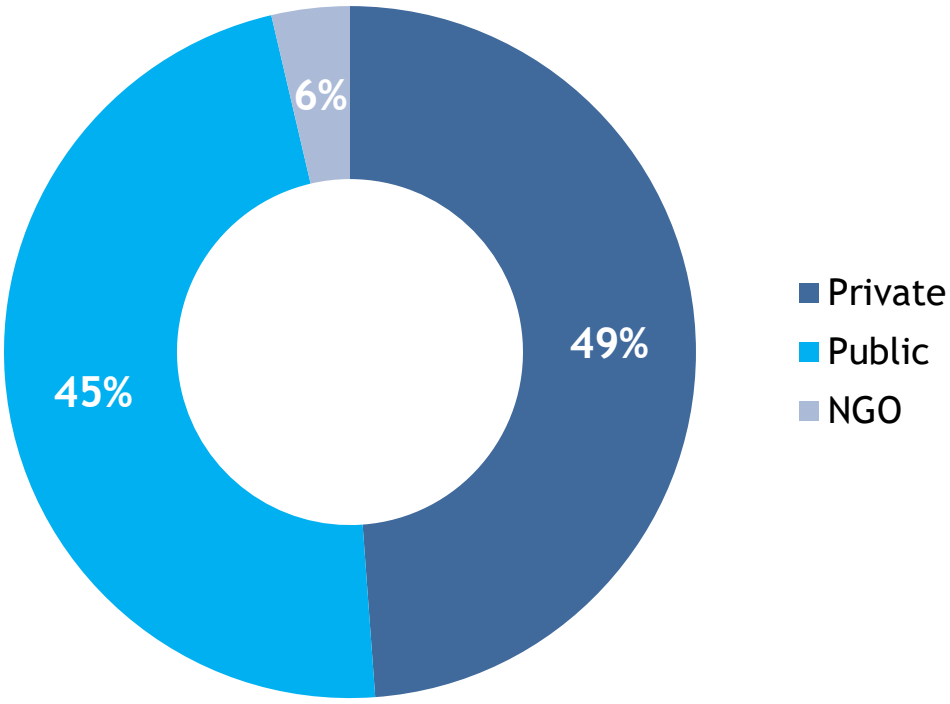
Other aspects



CERT-RO

Attendance stats

Sector Overview



Key stats

Participants	Private	174
	Public	158
	NGO	20
	Total participants	**352**
Speakers		**56**
Press		**7**
TOTAL		**415**

Organised by

CERT-RO

CENTRUL NATIONAL DE RASPUNS LA INCIDENTE DE SECURITATE CIBERNETICA

ROMANIAN NATIONAL COMPUTER SECURITY INCIDENT RESPONSE TEAM

With the support of

MINISTERUL COMUNICAȚIILOR ȘI SOCIETĂȚII INFORMAȚIONALE

Our Partners

paloalto NETWORKS

Check Point SOFTWARE TECHNOLOGIES LTD.

orange

FIREEYE

s&t 25 TWENTY FIVE Years of IT EXCELLENCE

kapsch

CLICO

IBM

CISCO

Microsoft

safetech Your trusted security partner

Bitdefender

FORTINET

ERICSSON

VERINT

ixia A Keysight Business

pwc

www.cert.ro
+4031-6202187
cooperation@cert.ro
8-10 Mareșal Averescu Blvd., 011455 Bucharest, Romania
22 Italiana Str., 020976 Bucharest, Romania