Interview with Ms. Daria CATALUI

Ms. Daria CATALUI is currently dealing with Network and Information Security in Education, stakeholder management and outreach strategies @ENISA. Her work focuses on communicating towards the end user.
Graduate in public policy from the University of Bucharest, further advanced academic qualifications in education: global education, virtual learning, youth studies; security: security studies, information security, data communication; trainer. Her professional background includes working with the EC and the CoE on youth and educational policies, social entrepreneurship and community development initiatives. During the past years she has been working and learning from skilled professionals @Chelgate consultancy @IER & ANPCDEFP public administrations @CTR & EYF volunteering. For current work you may consult www.cybersecuritymonth.eu and ENISA's Education reports.

1. You are currently dealing with Network and Information Security in Education at The European Union Agency for Network and Information Security (ENISA). Can you tell us about the role of ENISA in education in the field of cybersecurity?

Indeed, and thank you for the invitation to write about ENISA's work in the International Journal of Information Security and Cybercrime. It is very important for us to reach a large audience with our work and now at the beginning of 2016 we may develop on many reports freshly published on our website, www.enisa.europa.eu. Education is an essential element since through our work we support in developing capabilities of technical teams and not only. At ENISA we deal with education in a lifelong learning context, encouraging professionals from different walks of life to update their skills in cybersecurity, Network and information security- NIS, data protection, incident handling, cloud computing, assessing the threat landscape and mitigation techniques. In this sense we develop a quiz that may be accessed here https://cybersecuritymonth.eu/references/quiz-demonstration/intro.

2. Do you think that cyber-security strategies should focus also on education as part of the overall strategy?

As an European broker of best practices ENISA is promoting cybersecurity education as part of cyber-security strategies developed by different member states actors. Moreover, ENISA has listed all the documents of National Cyber Security Strategies in the EU but also in the world on the website. This information is based on publicly available material, and consulting the documents one may see that education is already an integral part of many strategies. Interactive map here: https://www.enisa.

europa.eu/activities/Resilience-and-CIIP/…/national-cyber-securi ty-strategies-in-the-world.

3. How do you see the role of academic environment in cybersecurity? Does ENISA have plans to involve university professors in scientific research projects?

The academic stakeholders have an important role in developing the knowledge in NIS. With the help of the ENISA-NLO network we disseminate and consult many of them for our projects. In 2014 we have developed an interactive Education map where we list courses from different providers for a good overview of what happens in Europe in the sector. Interactive map here: https://cybersecuritymonth.eu/references/universities.

4. How important is Public Private Partnerships in information security education?

Public Private Partnerships-PPPs in NIS are recommended to advance the approach "doing more, with less resources". We published a report with recommendations in this sense that all point to the usefulness of PPPs. This report focuses on the brokerage of best practices between the public and private sectors aimed at all members of the Network and Information Security Education community in Europe. ENISA is committed to taking the lead in encouraging the exchange of NIS best practices and it follows a strong community-building process for NIS Education stakeholders. In this report we recommend reading the case studies with special attention to the methods used to build partnerships, the approach to working together and setting the right metrics. The case studies include: CISCO's networking Academy dedicated to professionals; Cybersecurity education in Finland describing academic programmes from universities and the link to the national cybersecurity strategy; The US National Cyber Security alliance and their approach on working together for achieving common results; Trend Micro's Internet Safety for Kids and Families Programme that shows the commitment towards community education; Intel's training programme and their integrating approach on education. The recommendations mention:

1. EU and national policy makers should ensure that current education approaches are enhanced by a set of actions to improve cybersecurity know-how in the whole of society, and security should be incorporated as a supporting theme that plays throughout the computing curriculum;
2. Schools and institutes offering higher education should ensure that research and education programmes holistically integrate the perspectives of technology, information, and organizations, business and people;
3. Educators should consider deploying a blended learning model, which combines classroom instruction with online curricula, interactive tools, hands-on activities and online assessments to provide immediate feedback;
4. Find better ways of working directly with the community in creative ways, advocacy work and empowering the users;
5. Use as a case study the Finnish model of Triple Helix Cooperation: business, academia and public authorities.

Overall stepping up the European and national effort on networks and information security education and training are the main priorities! More for the report here:

www.enisa.europa.eu/activities/stakeholder-relations/…/public-private-partnerships-in-network-and-information-security-education.

5. European Cyber Security Month is a project started by ENISA 3 years ago. Last year ENISA succeeded to involve 30 countries in this project, including Romania. How ENISA will support this project in the future?

The European Cyber security Month is an EU advocacy campaign that promotes cyber security among citizens and advocates seeking to change the perception of cyber-threats by promoting education, sharing of good practices and competitions in data and information security. ENISA, the European Commission and partners from public private organizations deploy the campaign every October month. It has a dedicated website on www.cybersecuritymonth.eu. The engagement model that ENISA uses is depicted in the graphic below. It represents the stakeholders that are involved in the ECSM and the way the Agency implements the brokerage role.

ENISA Engagement Model

Indeed in 2014 we had 30 countries involved and in 2015 there were 32 countries, including active organizations from Romania that were supported by CERT-RO. For example the highlights that we can report are the following:

- In total there were 242 activities encoded in the official calendar from public and private stakeholders in 32 countries. The NIS Education Map registered an increase of courses registered, currently with 417 courses in 22 countries.
- The outreach on social media on the 1st of October alone, was 718,967 accounts reached. Number of visitors for www.cybersecuritymonth.eu peaked in October with 52,574 page views, with 71% corresponding to new visitors from all around Europe.
- Numerous trainings for multipliers and online calls for coordinators were supported by ENISA.
- The kick-off event had a global partnership organized in the presence of ITU Secretary General, general deployment with partners from the United States

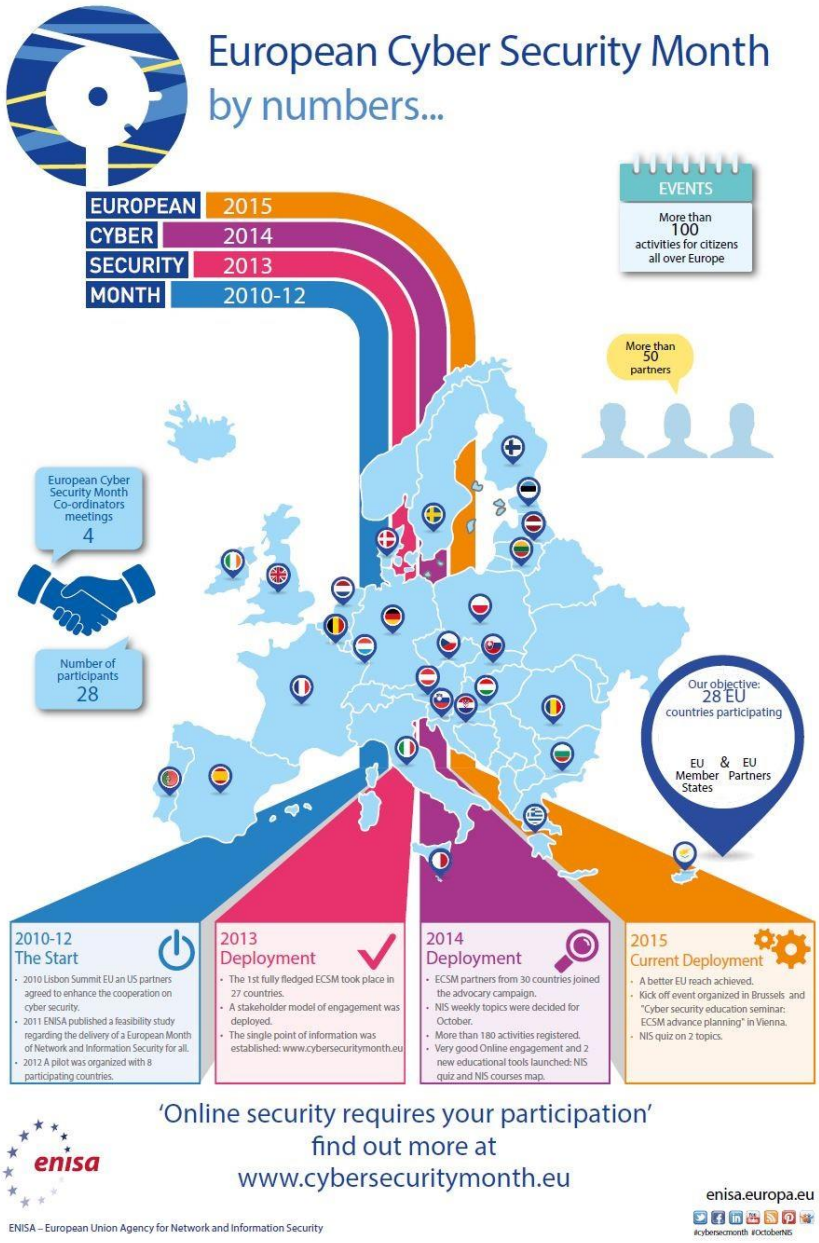
(such as NCSAM and DHS), and coordinators from Member States, all supported by ENISA and European Commission DG Connect.

ENISA is committed to continue in 2016 and 2017 supporting the European Cyber Security Month and will encourage the active involvement of member states organizations in the coordination and deployment. From the deployment of the 2015 edition, the following should be emphasized regarding outcomes:

1. Member States and EU partner countries are interested in working in partnership on cyber security education. The number of countries involved reached a stable dimension with a tendency for steady growth. With this edition the maturity level was successfully attained, furthermore there is work to be followed to increase the content distribution and content co-ownership between MS' organizations with the support of ENISA.
2. The European Commission, other EU bodies such as EESC, Agencies continued to get involved and maintain their participation at high level. The campaign created a good environment for European but also international cooperation for cyber security PPPs.
3. The community building process around the campaign is an important win. The EC, MSs and ENISA may choose to further develop this aspect and extend its use to content distribution on cyber security education and more. The European Cyber Security Month had developed a model of engagement that makes possible a multi-stakeholder governance approach, main benefits being reaching to a large number of European citizens through numerous activities organized by stakeholders. ECSM will be further developed following its basic principles, namely:
    - Support the multi-stakeholder governance approach;
    - Encourage common public-private activities;
    - Assess the impact of activities, optimizing and adapting to new challenges.
    - It is about "Building together a joint EU advocacy campaign on Cyber Security topics!".

6. Nowadays, many social networks and websites have implemented tracking techniques. How important is the awareness of the existence of the online tracking ecosystem?

Users should be aware of it in order to take informed decisions. ENISA has published a study in the area of Privacy Enhancing Technologies for the protection of online privacy (online privacy tools) with two main objectives: a) to define the current level of information and guidance that is provided to the general public and b) to provide a proposal for an assessment model for online privacy tools that could bring more assurance in their use, supporting their wider adoption by internet and mobile users. More here: www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-tools-for-the-general-public. Also another recommendation for the readers is the solution developed by CNIL in France "Cookieviz", more here www.cnil.fr/vos-droits/vos-traces/les-cookies/telechargez-cookieviz/.



ECSM by numbers

7. What solutions ENISA has for raising the awareness in cybersecurity field? How important is social media in this domain?

Most important is the training material that ENISA developed (video herewww.enisa.europa.eu/activities/cert/media/multimedia/enisa-csirts-training), Euro pean Cyber Security Month and the information brief in all EU languages https://cybersecuritymonth.eu/press-campaign-toolbox/ecsm-material/tips-and-advice.

We form communities of multipliers and work with them in order to disseminate the good practices and the new developments information in NIS.

8. Lately, the number of cyber-attacks has increased in Europe. How do you think these attacks will evolve next years?

To reply to this question I will mention a flagship report that ENISA is publishing annually, namely "The Threat Landscape report" (www.enisa.europa.eu/media/press-releases/enisa-draws-the-cyber-threat-landscape-2014). In 2014, major changes were observed in top threats: an increased complexity of attacks, successful attacks on vital security functions of the internet, but also successful internationally coordinated operations of law enforcement and security vendors. Many of the changes in cyber threats can be attributed exactly to this coordination and the mobilization of the cyber community. However, the evidence indicates that the future cyber threat landscapes will maintain high dynamics. 2014 can be characterized as the year of data breach. The massive data breaches identified massive attacks to main security functions of the Internet, demonstrating how effectively cyber threat agents abuse security weaknesses of businesses and governments. Main lessons learnt of the ETL highlight that "sloppiness" with regards to cyber security – is the number one reason for breaches accounting for 50% of the cases. Additionally, a positive development was reflected in the increase of both the quality and the quantity of the collected information, resulting in better threat assessment and more detailed material for end-users. The Emerging Technology that will impact the Threat landscape are: Cyber Physical Systems (CPS), Mobile and Cloud computing, Trust Infrastructure, Big Data, and Internet of Things. CPS – has an important impact within the protection of Critical Infrastructure Protection – represents a distinct opportunity creating competitive advantages for European industry and research.

Furthermore in 2015 (report www.enisa.europa.eu/activities/…/enisa-threat-landscape/etl2015) edition of the cyber-threat landscape features a number of unique observations, the main one being the smooth advancement of maturity. As a matter cyber-space stakeholders have gone through varying degrees of further maturity. While the friendly agents – the good guys – have demonstrated increased cooperation and orchestrated reaction to cyber-threats, hostile agents – the bad guys – have advanced their malicious tools with obfuscation, stealthiness and striking power. On the defenders' side, improvements have been achieved in coordinated campaigns to disturb operations of malicious infrastructures, strengthen the legal/governmental cyber-defense framework and develop more efficient products.

To understand the broader context the table below with comparative data 2014vs 2015 is handy.

Top Threats 2014	Assessed Trends 2013	Top Threats 2015	Assessed Trends 2014	Change in ranking
1. Malicious code: Worms/Trojans	↑	1. Malware	↑	→
2. Web-based attacks	↑	2. Web based attacks	↑	→
3. Web application /Injection attacks	↑	3. Web application attacks	↑	→
4. Botnets	↓	4. Botnets	↓	→
5. Denial of service	↑	5. Denial of service	↑	→
6. Spam	↓	6. Physical damage/theft/loss	⊃	↑
7. Phishing	↑	7. Insider threat (malicious, accidental)	↑	↑
8. Exploit kits	↓	8. Phishing	⊃	↓
9. Data breaches	↑	9. Spam	↓	↓
10. Physical damage/theft /loss	↑	10. Exploit kits	↑	↓
11. Insider threat	⊃	11. Data breaches	⊃	↓
12. Information leakage	↑	12. Identity theft	⊃	↑
13. Identity theft/fraud	↑	13. Information leakage	↑	↓
14. Cyber espionage	↑	14. Ransomware	↑	↑
15. Ransomware/ Rogueware/Scareware	↓	15. Cyber espionage	↑	↓

Legend: Trends: ↓ Declining, ⊃ Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Overview and Comparison of Cyber-Threat Landscape

I would like to end by giving the reader the channels that we use for sending updates and useful information, below. I wish you all a secure 2016!

Website: www.enisa.europa.eu

Twitter: @ENISA_eu @CyberSecMonth

Interview made by Ioan-Cosmin MIHAI
Vice President of RAISA