ENISA strategy and multiannual work programme

Steve Purser

Head of Core Operations Department, ENISA

NLO Meeting, Athens, 04/03/2015

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

ENISA activities

Recommendations

Mobilising Communities

Policy Implementation

Hands on

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

Key Points for 2014

- ENISA produced 45 deliverables – ALL WP deliverables were produced on time and in budget.
- The Agency coordinated Cyber Europe 2014 – This version of the pan-European exercise was carried out in three separate phases.
- We also assisted the Member States in coordinating the EU Cyber Security Month in October.
- We received 12 new Article 14 Requests from the EU institutions and the Member States.
- We hosted a successful High-Level Event at the beginning of October, which was kicked off by Commissioner Kroes.

Examples of achievements.
WS1 – Support EU policy building

WPK 1.1. Identifying technological evolution, risks and challenges		
	Planned deliverables (WP2014)	**Achieved deliverables/publications**
D1	Annual EU CyberSecurity Threats Landscape	"ENISA Threat Landscape 2014" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2014
D2	Identification of trends, security challenges, associated risks and required countermeasures, for emerging technologies (with special attention to selected areas/sectors)	1)"Threat Landscape and good practice guide for smart home and converged media" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/threat-landscape-for-smart-home-and-media-convergence/ 2)"Threat Landscape and good practice guide for internet infrastructures" https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/iitl

Examples of achievements. WS2 – Support Capacity Building

WPK2.1. Support Member States' capacity building		
	Planned deliverables (WP2014)	**Achieved deliverables/publications**
D1	Assisting MS in building capabilities on NCSS (workshops, Q1-Q4)	Workshop on Cyber Security Strategies organised on 27.11.2014. https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop
D2	White Paper – How to Evaluate a National Cyber Security Strategy (report, Q3 2014)	"An evaluation framework for Cyber Security Strategies" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies
D3	Good practice guide on training methodologies, etc. for operational teams and communities like CERTs ("Train the trainers handbook") derived from experiences from delivering suitable CERT training (Q4 2014)	"Good Practice Guide on Training Methodologies" https://www.enisa.europa.eu/activities/cert/support/exercise/good-practice-guide-on-training-methodologies
D4	Regular update of "Baseline capabilities" definition and status and conclusions for new training material (Q4, 2014)	""Baseline Capabilities" definition and status" https://www.enisa.europa.eu/activities/cert/support/baseline-capabilities/national-governmental-certs-enisas-recommendations-on-baseline-capabilities/
D5	New set of CERT exercise material with at least five new scenarios from the four areas of the "Baseline capabilities", including the topic of processing of actionable operational information (Q4 2014)	1) Developing countermeasures; 2)Common framework for artifact analyses activities; 3)Advanced artifact handling; 4)Processing and storing artifacts; 5)Building artifact handling and analyses environment. All available here: http://www.enisa.europa.eu/activities/cert/training/training-resources
D6	Stocktaking of achievements in the area of CERTs and a draft roadmap to plan future work in this area (Q4 2014)	"Impact Assessment and Roadmap" https://www.enisa.europa.eu/activities/cert/other-work/supporting-the-cert-community-impact-analysis-and-roadmap
D7	Assisting MS in building capabilities on national PPPs (workshops, Q1-Q4)	Panel on PPPs during the National Cyber Security Strategies workshop, 27.11.2014 https://resilience.enisa.europa.eu/enisas-ncss-project/enisa-cyber-security-strategies-workshop

Examples of achievements. WS3 – Support cooperation

WPK3.1. Crisis cooperation – exercises		
	Planned deliverables (WP2014)	**Achieved deliverables/publications**
D1	Cyber Europe 2014: Exercise Plan and Exercise (exercice, Q4 2014)	Exercise organised on 30.10.2014.
D2	Report on Cyber Crisis Cooperation and Exercise Activities and Findings (report, Q4 2014)	"Report on Cyber Crisis Cooperation and Management" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/nis-cooperation-plans/ccc-management/ccc-study
D3	EU-US Cybersecurity Exercise Plan	Was not carried out

WPK3.2. Implementation of EU legislation		
	Planned deliverables (WP2014)	**Achieved deliverables/publications**
D1	Analysis of Annual 2013 Incident Reports and Recommendations on addressing significant incidents (report, Q2/3 2014)	1)" Annual Incidents report 2013" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013 2)"Technical Guideline on Incident Reporting V2.1" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting/technical-guideline-on-incident-reporting 3)"Technical Guideline on Security Measures V2.0" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures/technical-guideline-on-minimum-security-measures 4)Secure ICT Procurement in Electronic Communications https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/secure-ict-procurement-in-electronic-communications 5)Security Guide for ICT Procurement https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/requirements-ecomms-vendors/security-guide-for-ict-procurement 6)"Protection of underground electronic communications infrastructure" https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/protection-of-underground-infrastructure

Article 14 Requests

Origin	Institution	Title	Due Date
Austria	Bundeskanzleramt Osterreich	Abusehelper Project	Completed
Croatia	Croatian Regulatory Authority for Network Industries (HAKOM)	Assistance to enhance cyber security capabilities in Croatia	Completed
Cyprus	Office of the Commissioner for Electronic Communications & Postal Regulation (OCECPR)	Participating in the pilot step-by-step guide, best practices of national risk assessments for cybersecurity	29/05/2015
Czech Republic	National Security Authority	Assistance to enhance the cybersecurity capabilieties in the Czech Republic	Completed
European Commission	DG Connect - Directorate H; Unit 4 Trust & Security	Cryptographic protection measures supporting Regulation (EU) No 611/2013 of 24 June 2013	Completed
Estonia	Estonian Information Systems Authority	Request for training on Plannning and Organising Exercises	Completed
Estonia	Estonian Academy of Security Services	Request for support for "First responders and cyber forensics" course CEPOL	28/6/2015
Germany	Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BFDI)	Cooperation in area of privacy	Completed
Greece	Hellenic National Defence General Staff	Request for support by the MoD Greece - PANOPTIS	Completed
Greece	Hellenic Ministry of Infrastructure, Transport & Networks	Request by the Hellenic Ministry of Infrastructure, Transport & Networks	Completed
Italy	Istituto Superiore delle Comunicazioni e delle Tecnologie dell' Informazione Ministero dello Sviluppo Economico	Technical meeting of the Governmental/National CERTs	Completed
Latvia	Institute of Mathematics & Computer Science University of Latvia	Organizing training courses in Latvia	Completed
Luxembourg	Le Gouvernement du Grand-Duché De Luxembourg Ministère de l'Économie Direction du	Organization of a CERT workshop in Luxembourg on the 24th of October	Completed

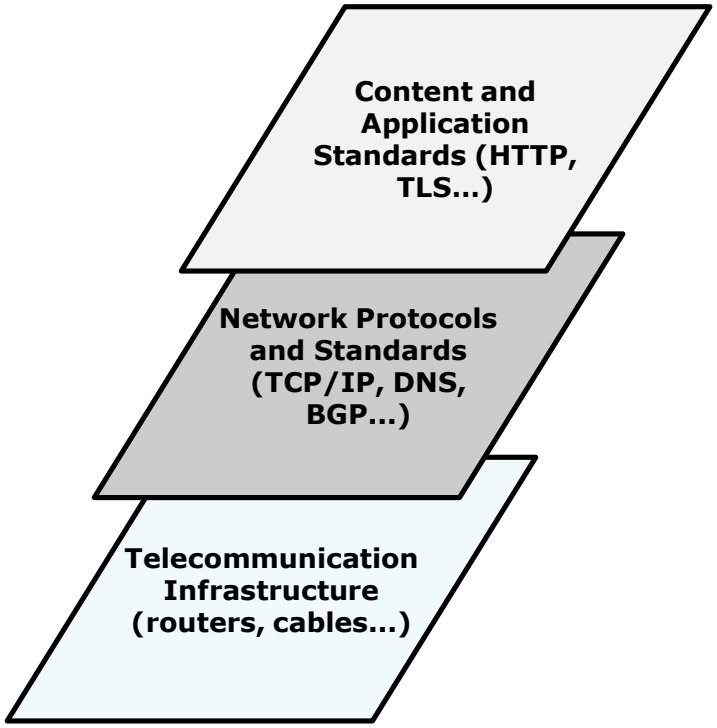
Origin	Institution	Title	Due Date
	commerce électronique et de la sécurité de l'information		
Malta	Malta Critical Infrastructure Protection Unit	Organizing training courses in Malta	Completed
Malta	Malta Critical Infrastructure Protection Unit	On-site training of ENISA CERT Training	Completed
Poland	NASK (Research and Academic Computer Network)	Honeynet Project Workshop	Completed
Portugal	CERT Portugal	Call for inputs on BEREC WP 2015	Completed
Portugal	Autoridade Nacional de Comunicações (ANACOM)	The project focuses on improving incident handling automation for CERTs	Completed
Spain	National Security Department - Spanish Prime Ministers Office	Request for seminar on NCPs and National Exercises	27/03/2015

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

Today's challenges

There is increasing reliance on communication networks

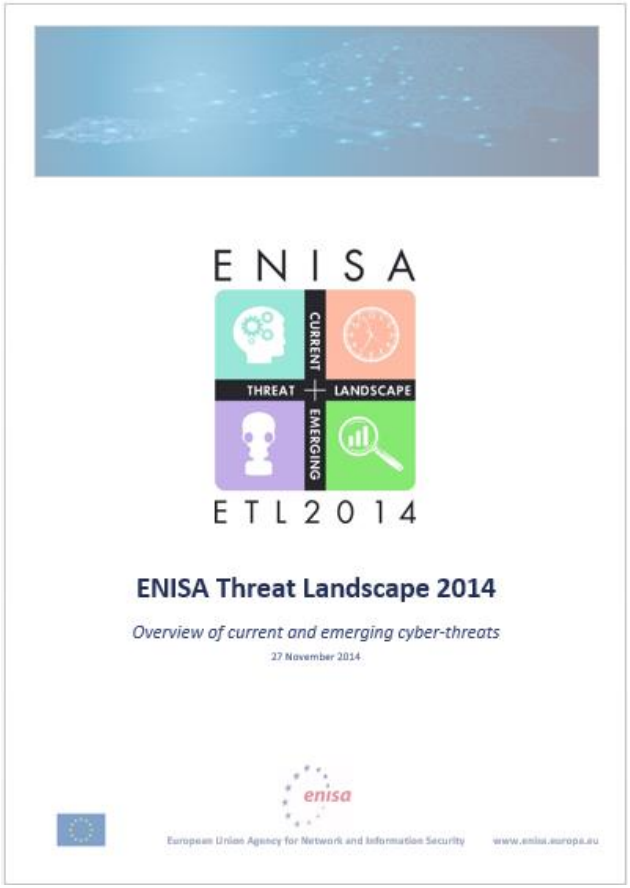


There is an emerging threat environment hampering the availability, integrity and confidentiality of networks based on:

- Infrastructure vulnerabilities
- Interdependencies
- Privacy concerns
- Growing threat landscape

The ENISA Threat Landscape

- The ENISA Threat Landscape provides an overview of threats and current and emerging trends.
- It is based on publicly available data and provides an independent view on observed threats, threat agents and threat trends.
- Over 250 recent reports from a variety of resources have been analysed.



Types of Threat Information Analysed

- **Strategic (S):** this is usually the highest level information about threats. Such information is used within forecasts of the threat landscape and emerging technological trends.
- **Tactical (T):** tactical threat information consists of condensed information describing threats and their components
- **Operational (O):** this is the most basic information about existing threats. It covers detailed technical information about threats, incidents, vulnerabilities, etc., and usually derived from detections at the level of technical artefacts.

Key Points From ETL 2014

- Threats are changing rapidly:
  - Important changes in top threats.
  - Increased complexity of attacks.
  - Successful attacks on vital security functions of the internet
- Response is getting better
  - Successful internationally coordinated operations of law enforcement and security vendors.

The Bad News

- Significant flaws in the implementation of SSL and TLS, the core security protocols of the internet, were discovered.
- Many significant data breaches occurred.
- A vulnerability found in the BASH shell may have a long term impact on older versions.
- Privacy violations have weakened the trust of users in the internet and e-services in general.
- Increased sophistication and advances in targeted campaigns have demonstrated new qualities of attacks.

The Good News

- The take down of GameOver Zeus botnet has almost immediately stopped infection campaigns.
- Last year's arrest of the developers of Blackhole has shown its effect in 2014 when use of the exploit kit has been massively reduced.
- NTP-based reflection within DDoS attacks are declining as a result of a reduction of infected servers.
- SQL injection, one of the main tools used to compromise web sites, is on the decline due to a broader understanding of the issue in the web development community.
- Taking off-line Silk Road 2 and another 400 hidden services in the dark net has created a shock in TOR community, both at the attackers and TOR users ends.

TOP THREATS

Top Threats	Current Trends	Top 10 Threat Trends in Emerging Areas						
		Cyber-Physical Systems and CIP	Mobile Computing	Cloud Computing	Trust Infrastr.	Big Data	Internet of Things	Netw. Virtualisation
1. Malicious code: Worms/Trojans	↑	↑	↑	↑	↑		↑	↑
2. Web-based attacks	↑	↑	↑	↑	→		↑	
3. Web application attacks /Injection attacks	↑	↑	↑	↑	↑		↑	↑
4. Botnets	↓		↑	↑				
5. Denial of service	↑	↑		→	→		↑	↑
6. Spam	↓	↑						
7. Phishing	↑		↑		↑	↑	↑	↑
8. Exploit kits	↓		↑		↑		↑	
9. Data breaches	↑			↑		↑		↑
10. Physical damage/theft /loss	↑	↑	↑		↑	↑	↑	↑
11. Insider threat	→	↑		↑		↑	↑	↑
12. Information leakage	↑	↑	↑	↑	↑	↑	↑	↑
13. Identity theft/fraud	↑	↑	↑	↑	↑	↑	↑	↑
14. Cyber espionage	↑	↑		↑	↑	↑		↑
15. Ransomware/ Rogueware/ Scareware	↓		↑					

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing

Table 1: Overview of Threats and Emerging Trends of the ENISA Threat Landscape 2014[1]

TRENDS

Top Threats 2013	Assessed Trends 2013	Top Threats 2014	Assessed Trends 2014	Change in ranking
1. Drive-by downloads (renamed to Web-based attacks)	↑	1. Malicious code: Worms/Trojans	↑	↑
2. Worms/Trojans	↑	2. Web-based attacks	↑	↓
3. Code Injection	↑	3. Web application /Injection attacks	↑	→
4. Exploit Kits	↑	4. Botnets	↓	↑
5. Botnets	→	5. Denial of service	↑	↑
6. Physical Damage/Theft/Loss	↑	6. Spam	↓	↑
7. Identify Theft/Fraud	↑	7. Phishing	↑	↑
8. Denial of Service	↑	8. Exploit kits	↓	↓
9. Phishing	↑	9. Data breaches	↑	↑
10. Spam	→	10. Physical damage/theft /loss	↑	↓
11. Rogueware/Ransomware / Scareware	↑	11. Insider threat	→	(NA. new threat)
12. Data Breaches	↑	12. Information leakage	↑	↑
13. Information Leakage	↑	13. Identity theft/fraud	↑	↓
14. Targeted Attacks (renamed to Cyber espionage, merged with Watering Hole)	↑	14. Cyber espionage	↑	→
15. Watering Hole (threat consolidated with other threats/attack vector)	↑	15. Ransomware/Rogueware/ Scareware	↓	↓

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

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

Strategic Objectives

- SO1. To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS).
- SO2. To assist the Member States and the EU institutions and bodies in enhancing capacity building throughout the EU.
- SO3. To assist the Member States and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security.
- SO4. To enhance cooperation both between the Member States of the EU and between related NIS communities.

Mapping of WPKs and SOs in WP2016

SO1	SO2	SO3	SO4
WPK1.1. Improving the expertise related to Critical Information Infrastructures	WPK2.1 Assist MSs capacity building	WPK3.1. Supporting EU policy development	WPK4.1 Cyber crisis cooperation and exercises
WPK1.2 NIS Threats Landscape Analysis	WPK2.2 Support EU institutions	WPK 3.2. Supporting EU policy implementation	WPK4.2 NIS community building
WPK1.3 R&D, Innovation	WPK 2.3 Assist private sector capacity building		
	WPK 2.4 Assist in improving the general awareness		

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

WP 2015 : Work Packages

Core Operational Activities: Strategic Objectives 14		Operational Activities – FTE	Total Cost of Activities ABB
SO1	**To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network and Information Security (NIS)**		
WPK 1.1	NIS Threats Analysis	2,3	245.806
WPK 1.2	Improving the Protection of Critical Information Infrastructures	6,6	688.253
WPK 1.3	Securing emerging Technologies and Services	5,3	486.603
WPK 1.4	Short- and mid-terms sharing of information regarding issues in NIS	2,7	183.301
Total SO 1		**16,8**	**1.603.963**

SO2	**To assist the Member States and the Commission in enhancing capacity building throughout the EU**		
WPK 2.1	Assist in public sector capacity building	6,6	788.253
WPK 2.2	Assist in private sector capacity building	2,4	185.971
WPK 2.3	Assist in improving awareness of the general public	2,0	167.476
Total SO 2		**11,0**	**1.141.700**

WP 2015 : Work Packages

SO3	To assist the Member States and the Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security		
WPK 3.1	Provide information and advice to support policy development	2,7	233.301
WPK 3.2	Assist EU MS and Commission in the implementation of EU NIS regulations	5,3	506.603
WPK 3.3	Assist EU MS and Commission in the implementation of NIS measures of EU data protection regulation	4,0	404.952
WPK 3.4	RandD, Innovation and Standardisation	2,7	248.301
Total SO 3		**14,6**	**1.393.157**

SO4	To enhance cooperation both between the Member States of the EU and between related NIS communities		
WPK 4.1	Support for EU cooperation initiatives amongst NIS-related communities in the context of the EU CSS	4,6	439.777
WPK 4.2	European cyber crisis cooperation through exercises	6,0	617.428
Total SO 4		**10,6**	**1.057.205**

Summary

- The ENISA model
- Looking Back at 2014
- Perspective on today's Challenges
- ENISA Strategy & Multiannual Perspective
- Summary of WP 2015
- Preview of the WP 2016

DRAFT WP2016 – Development calendar. According to new deadlines

DONE!

WP 2016 : Work Packages

	Core operational activities (Strategic Objectives 1 to 4)
SO1.	To develop and maintain a high level of expertise of EU actors taking into account evolutions in Network & Information Security (NIS)
WPK1.1.	Improving the expertise related to Critical Information Infrastructures
WPK1.2.	NIS Threats Landscape Analysis
WPK1.3	R&D, Innovation
TOTAL	SO1
SO2.	To assist the Member States and the EU institutions and bodies in enhancing capacity building throughout the EU
WPK2.1.	Assist MSs capacity building
WPK2.2.	Support EU institutions
WPK2.3.	Assist private sector capacity building
WPK2.4.	Assist in improving the general awareness
TOTAL	SO2
SO3.	To assist the Member States and the EU institutions and bodies in developing and implementing the policies necessary to meet the legal and regulatory requirements of Network and Information Security
WPK3.1.	Supporting EU policy development
WPK3.2.	Supporting EU policy implementation
TOTAL	SO3
SO4.	To enhance cooperation both between the Member States of the EU and between related NIS communities
WPK4.1.	Cyber crisis cooperation and exercises
WPK4.2.	NIS community building
TOTAL	SO4

Thank you for your attention!

For more information visit:
http://www.enisa.europa.eu

Follow ENISA: