Management Board News

Welcome!

Dear Members of the ENISA Management Board,

Welcome to the new issue of our MB Newsletter. You will find inside a summarised overview of our activities for the period July – September 2014. I would also like to take the opportunity to thank the Board for their support and confidence in my work and for endorsing an extension of my position as executive director for the next 5 years. Our aim is to highlight some of the main topics ENISA is currently tackling. For you attention, this issue highlights the main findings of the annual incidents report 2013 ENISA has published recently. As ever, please feel free to share the newsletter with any of your colleagues or associates who may find it of use. For enquiries, or to submit news items, please contact: *Ingrida.taurina@enisa.europa.eu*.

With best wishes,
Udo Helmbrecht, Executive Director, ENISA

The latest news from ENISA...

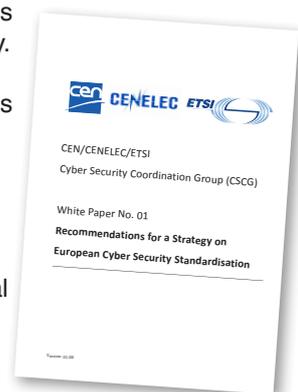**The Information Technology Security Incident Response Institution of the Republic of Latvia (CERT.LV)** and ENISA jointly organised an IT security training seminar, which took place in Riga, Latvia, on **9-10 July.** The workshop covered topics like handling incidents on mobile devices and as well touched the area of digital forensics.

In a special session of the **Industry, Research and Energy Committee (ITRE)** of the European Parliament that took place on **2 September**, the Agency's role, accomplishments, and future challenges for an open, safe and secure cyberspace were outlined by the Executive Director. The title of the Executive Director's speech was 'ENISA today and in the future', and was followed by a Questions and Answers session with the Members of the ITRE committee.

Italian Presidency of the Council of the European Union italia2014.eu

The priorities of the **Italian Council Presidency** are being outlined to the various parliamentary committees by Italian ministers on **2 and 3 September**. In the area of electronic communications these are the following: the need to complete the digital single market, improve web accessibility and remove barriers to communication such as roaming.

10 September. In response to the European Union's Cyber Security Strategy, the **Cyber Security Coordination Group (CSCG)** has published a White Paper with recommendations on digital security. The CSCG's recommendations underline the importance of Cyber Security standardisation to complete the European internal market and to raise the level of Cyber Security in Europe in general. **For the full paper:** Recommendations for a Strategy on European Cyber Security Standardisation

CEN/CENELEC/ETSI
Cyber Security Coordination Group (CSCG)

White Paper No. 01
Recommendations for a Strategy on European Cyber Security Standardisation

President-elect Jean Claude Juncker announced on the **10 September** the allocation of responsibilities in his team and the way work will be organised in the **European Commission** once it takes office. Mr Günther Oettinger is Commissioner – designate for Digital Economy and Society. The Directorate-General for Communications Networks, Content and Technology (DG CONNECT), with some adjustments, and the Directorate-General for Informatics (DG DIGIT) will report to him.

The European Commission DG Connect (Unit E2) launched a web-based Public Consultation with a view to defining future research priorities in the areas of Cloud Computing and Software, ahead of the H2020 ICT Work Programme 2016-17. All interested stakeholders (industry, research centres, academia, SMEs and users) are warmly invited to contribute by **10 October**. Consultation is available here: http://ec.europa.eu/digital-agenda/en/news/public-consultation-cloud-computing-and-software

On **16 September** the European Commission published a report (SWD(2014) 283 final) on its ambitious **science and technology Flagships**. The report draws the lessons from setting up the first two such Flagships, Graphene and the Human Brain Project, each representing an investment of EUR 1 billion. It also sets out the future working arrangements for the two Flagships underway.
Full report: https://ec.europa.eu/digital-agenda/en/news/fet-flagships-novel-partnering-approach-address-grand-scientific-challenges-boost-innovation

The European Commission (DG Connect) and ENISA organised on **19 September** a validation meeting for the work mentioned in the EU Cyber Security Strategy **"An Open, Safe and Secure Cyberspace"** regarding NIS Education and cyber security competitions. Furthermore, the report "Roadmap for NIS education programmes in Europe" continues from the previous activities, by proposing training materials, scenarios and a

way forward for the implementation of the EC roadmap for NIS education in Europe. The report "Cyber Security competitions- status in Europe" provides a general overview of existing cyber challenges competitions in Member States, as well as details of a roadmap for a future pan-European cyber challenge competition. Both reports will be published during Cyber Security Month in October.

ENISA issued its **Annual incidents report 2013** on **16 September**. The report provides an aggregated analysis of the security incidents in 2013 which caused severe outages. **More details on page 3.**

On **1 October** ENISA held its annual high-level event at the Representation of the Free State of Bavaria to the EU, in Brussels.

This year's theme "10 Years of Securing Europe's cyber security... and beyond!" marks a decade of contribution by the Agency to improving EU cyber security and looks ahead at the future cyber security challenges. Topics included using cyber security as an economic enabler, how we can secure future technologies, the need to apply standardisation and how to effectively balance security needs with privacy.

The Agency has developed training scenarios...

Under Art.14 request[1] these scenarios can be tailored for in-house free of charge training for the European Parliament, the Council, the European Commission and Member States.

The training scenarios:

• Introduction to Incident handling and procedures

• Triage and large scale incident handling

• Identification and handling of electronic evidence and digital forensics

• Network forensics

• Mobile threats incident handling

• Incident handling during an attack on Critical Information Infrastructure

[1] Requests for advice and assistance shall be addressed to the Executive Director and accompanied with background information explaining the issue. These trainings are subject to resources availability. Please consult ENISA Regulation No 526/2013 for further guidance.

Annual Incident Reports 2013

Every year, ENISA publishes an annual report about significant incidents in the electronic communications sector, which are reported to ENISA under Article 13a of the Framework Directive (2009/140/EC), by the National Regulatory Authorities (NRAs) of the different EU Member States.

This report covers the incidents that occurred in 2013 and it gives an aggregated analysis of the incident reports about severe outages across the EU. This report does not include details about individual countries or providers.

The main statistical data for 2013 are as follows:

- **90 major incidents reported:**

  This year, in total 19 countries reported 90 significant incidents and 9 countries reported no significant incidents.

- **Mobile networks most affected:**

  Approximately half of the major incidents had an impact on mobile Internet and mobile telephony.

- **Mobile network outages affect many users:**

  Incidents affecting mobile Internet or mobile telephony affected most users (around 1.4 million users and 700 000 users respectively per incident). This is consistent with the high penetration rates of mobile telephony and Internet.

- **Impact on emergency calls:**

  A fifth of the major incidents had an impact on the emergency calls (aka 112 access).

- **System failures are the most common root cause**:

  Most major incidents were caused by "System failures" (61% of the incidents).

  – Looking more in detail at this root cause category, the most common detailed causes were "software bugs", "hardware failures" and "software misconfigurations".

  – The assets most often affected were switches (e.g. mobile switching and routers) and base stations and controllers.

- **System failures affect the most user connections:**

  Incidents categorized with the root cause system failure, affected around 1.5 million user connections on average per incident.

  – Looking more in detail, the detailed causes affecting most user connections were "software misconfiguration", "software bugs", and "power surges".

- **Natural phenomena and malicious actions cause long lasting incidents:**

  Incidents caused by natural phenomena (heavy snowfall, storms, etc.) and malicious actions (arson, cable theft, etc.) lasted on average more than 50 hours.

- **Natural phenomena and system failures have most impact:**

  Multiplying number of user connection and duration, one obtains a measure for total impact, or 'total user hours lost'. Natural phenomena had on average most impact, followed by system failures.

  – Looking more in detail, Power cuts, heavy snowfall, cable cuts and storms, respectively, impacted most user hours.

- **Base stations and switches were most affected:**

  Overall, base stations, switches and mobile switching were the assets most affected by incidents.

ENISA, together with the European Commission and National Regulatory Authorities in the EU Member States, will discuss specific incidents in a more detail within the Article 13a Expert Group.

The next annual report will be published in summer 2015, for the 2014 incidents.

The European Union Agency for Network and Information Security (ENISA), the European Commission DG CONNECT and Partners are officially launching the European Cyber Security Month (ECSM) on the 1st of October, 2014. ECSM is an EU advocacy campaign that promotes cyber security among citizens and advocates for change in the perception of cyber-threats by promoting data and information security, education, sharing of good practices and competitions.

OCTOBER

EUROPEAN CYBER SECURITY MONTH

Online security requires your participation

Countries aligned for the deployment of the European Cyber Security Month

Official launch

This year, the official launch of the ECSM is taking place alongside ENISA's high-level event "10 years of securing Europe's cyber security… and beyond!" in Brussels.

At the high-level event, ECSM was addressing the issue of *"Involving the citizen"* with representatives from Code week, the Grand Coalition for Jobs, European and US partners, followed by a discussion moderated by Mr Francois Thill from the Luxemburg (LU) ECSM coordination.

Commissioner Kroes' statement for the ECSM: "The Internet and its many services bring many benefits to our society: not least significant growth of our economy and millions of jobs. But we need to build and restore trust if we really want to achieve those benefits. When it comes to cyber security, it is in our common interest to be much more responsive and resilient to cyber threats. ENISA can both play an operational and a strategic role to ensure that Europe is ready for the challenge, together with public and private parties. Each one of us must play our part in the cyber-

security challenge: every citizen, every business, every government. So I hope that the European Cyber Security Month raises more awareness – let's get people talking!"

ENISA's Executive Director, Prof. Udo Helmbrecht, statement for the ECSM: *"The internet of things, where every electronic device will be uniquely accessible and identifiable over the internet, is approaching quickly. This has a profound impact on all aspects of citizens' everyday life, as e-services are all now totally dependent on an open, safe and secure cyberspace. These are the technologies that are being built today and that will deliver the services of the future.*

"It is therefore essential for citizens to participate actively in improving information security, for ENISA to facilitate improvement processes and for Member States to ensure that security policy supports the internet based economy envisaged for Europe 2020. Year by year we have been consolidating this trust partnership for Cyber Security Month and I am honoured to see the high level of engagement from partners. On behalf of my team, thank you all!".

Action!
Happening during October at the local level

For the month of October, the community has pinpointed the following weekly Network and Information Security topics on the agenda:

1st week:
Training employees, targeting public and private organisations;

2nd week:
PC and mobile security protection and updates, targeting all digital users;

3rd week:
Coding, targeting students;

4th week:
Cyber security exercises, targeting technical expertise;

5th week:
ePrivacy, targeting all digital users.

EUROPEAN CYBER SECURITY MONTH

The full list of ECSM activities set to take place all over Europe can be found under the "Events" section of the dedicated website, which is regularly updated. This applies to both online or offline activities.

The ECSM will be followed by an evaluation meeting and the ECSM reporting.

For a complete list of collaborating partners for 2014 check: http://cybersecuritymonth.eu/partners

Calendar of events, October – December 2014 [2]

enisa

ENISA is organising, has received invitations and plans to participate[3]:

1 October	Brussels, Belgium	ENISA High Level Event 2014 and European Cyber Security Month launch
6 October	Brussels, Belgium	ENISA workshop on ICT Security Certification
6 – 10 October	Lisbon, Portugal	4th InfoSec Week, http://www.shadowsec.com/infosecweek/
7 – 8 October	Brussels, Belgium	CERT-EU Conference
8 October	London, UK	Special Workshop – Cyber Resilience Beyond IT: Crafting an Integrated and Multidisciplinary Approach to a Clear and Present Danger
9 October	Berlin, Germany	European Forum on SCADA & Cyber Sec for Utilities Industry
9 – 12 October	Portugal, Lisbon	INKOP 2014
10 October	Portugal, Lisbon	TBC Meeting with Portuguese representative(s) to ENISA MB
10 October	Geneva, Switzerland	Conference on Cyberspace, Energy and Development: Protection of Critical Energy Infrastructure
13 October	The Hague, The Netherlands	ENISA/EC3 Workshop http://www.enisa.europa.eu/activities/cert/events/9th-cert-workshop-part-ii
13 – 14 October	Budapest, Hungary	National eID and ePassport Conference https://www.eid-epass.org/
13 – 14 October	Belgrade, Serbia	TAIEX Workshop on Information Security
13 – 16 October	Mauritius	International Conference on Data Protection and Privacy Commissioners, http://privacyconference2014.org/
14 – 15 October	Brussels, Belgium	ISSE 2014
14 October	Louisenthal, Germany	Tegernseer Dialog – Giesecke & Devrient
15 October	Frankfurt, Germany	DE-CIX Customer Summit http://www.customersummit.net/home/
15 October	Brussels, Belgium	Presentation of final report on commercial mobile networks for mission critical communications
16 – 17 October	Budapest, Hungary	ETIS Meeting
17 October	Heraklion, Greece	Latvian Ministry of Defence State Secretary's visit to ENISA
21 October	Lucerne, Switzerland	Swiss Cyber Storm 2014 http://swisscyberstorm.com
22 – 23 October	Athens, Greece	14th Article 13a Expert Group Meeting
23 October	Poland, Warsaw	SECURE 2014 http://www.secure.edu.pl/
27 October	Vienna, Austria	ENISA MB Informal Meeting
27 – 31 October	Paris, France	7th Round Mutual Evaluation "Cybercrime"
28 October	Vienna, Austria	ENISA MB Ordinary Meeting
29 October	Vienna, Austria	ViS!T – Verwaltung integriert sichere Informationstechnologie, http://www.a-sit.at
30 – 31 October	Athens, Greece	Cyber Exercise 2014
3 November	Bonn, Germany	Cyber Security Summit
3 November	Venice, Italy	IEEE SmartGridComm
4 – 6 November	Fürstenfeld, Austria	IKT Sicherheitskonferenz 2014
4 – 5 November	London, UK	13th EU FI-ISAC meeting,
6 November	Amsterdam, NL	Grand Conference
7 November	Vienna, Austria	Peer-review meeting of FRA's project "National intelligence authorities and surveillance in the EU: Fundamental rights safeguards and remedies"
7 November	London, UK	1st meeting of the ENISA Internet infrastructure security and resilience reference group
16 – 18 November	Tallinn, Estonia	CEPOL Cybercrime/Digital Forensics Course
19 November	Zurich, Switzerland	IBM Zurich – Workshop on Cyber Security in Energy sector
19 – 20 November	Rome, Italy	CSA Congress event
21 November	Brussels, Belgium	Meeting competent authorities on Article 19 of eIDAS regulation No 910/2014
25 November	Brussels, Belgium	NIS platform plenary meeting
26 November	Brussels, Belgium	EFMS Meeting
26 November	Munich, Germany	TBC Forum "Finest Selection" – Baker Tilly Roelfs
27 November	Brussels, Belgium	Cyber Security Strategies workshop
1 – 2 December	Strasbourg, France	CoE T-CY Conference
3 December	Brussels, Belgium	IEEE Summit on Internet Governance
13 December	Koln, Germany	Aviation ISAC Kick-Off

[2] This calendar does not represent the events of the European Cyber Security Month
[3] This list is tentative and last minute changes may occur