Management Board Newsletter

September 2013

Securing the EU's Information Society

Dear reader, welcome to our September Management Board newsletter.

ENISA's new mandate creates fresh opportunities for the Agency, and also brings challenges. We are now working to get best value out of our budget, and ensure that our staff is able to deploy their time and skills to maximum efficiency. And the demands placed on us are likely to increase further, with the EU Cybersecurity Strategy.

The challenges are great, and ENISA needs to have the full support of the Member States and all stakeholders, to ensure that we continue to deliver work of a global quality.

I hope that you will enjoy reading this Issue, which includes an overview of ENISA's Annual Incidents Reports 2012.

With best wishes, **Udo Helmbrecht, Executive Director, ENISA**

The latest news from ENISA...

Welcome Croatia! On **1st July** Croatia became the 28th Member State of the European Union, marking another milestone in the construction of a united Europe. ENISA welcomes Croatia and looks forward to working with the new EU country.

See below for more information.

On **4th July** Vice President of the European Commission Neelie Kroes made a statement on the consequences of living in an age of total information. This statement was made *after the meeting of European Cloud Partnership Board, Tallinn, Estonia.* She concluded that *"The cloud has a lot of potential. But potential doesn't count for much in an atmosphere of distrust."*

Full statement available here:
http://europa.eu/rapid/press-release_MEMO-13-654_en.htm

ENISA Executive Director, Professor Udo Helmbrecht on **11th July** took part in a special media briefing on the forthcoming European Cyber Security Month (ECSM – October 2013). The event was organised in Vienna by Digital Austria – the coordination and strategy committee of the Federal Government for eGovernment in Austria.

ENISA attended a Justice and Home Affairs (JHA) Minister's informal meeting on **18th -19th July,** where cybersecurity was a key matter to discuss. The discussion focussed on how JHA actors were contributing both domestically and in a multinational environment, to achieve synergies and to strengthen cooperation for better prevention and a more targeted response to cyber incidents. Ministers and their representatives also focussed on measures to improve cyber capacity and cooperation, where ENISA outlined on the Agency's mandate – explicitly underlining cyber capacity building.

ENISA outlined its position on the possible implications on the recent large-scale data compromise activity. For a position paper please see: https://www.enisa.europa.eu/publications/flash-notes/securing-data-in-cyber-space

Croatia in figures

Land area	56 594 km², 1,3 % of total EU area
Population	4.3 million
Capital city	Zagreb
Main language	Croatian
Currency	Kuna (HRK)

On **19th July** ENISA was visited by the Managing Director of a worldwide security company, TÜV Informationstechnik GmbH, Mr Antonius Sommer to exchange knowledge and good practices on how to make Europe a safer place.

On **30th July** a European Cyber Security Month (ECSM) Coordinators' meeting took place via online channels, targeting those who want to share a common message on the first day of the ECSM campaign – 1st October. The participants were BSI-DE; Directie Cybersecurity-NL; CERT-RO; Safer Internet-CZ; INTEL-BXL; ANSSI-FR; CERT-SI. The common message to be adapted to each specific country is "Online security requires your participation!"

ENISA issued its Annual incidents report 2012 on **20th August.** The report provides an overview of the major outage incidents in the EU in 2012. The aggregated report shows that out of the 79 incidents reported, almost 40% of the incidents affected the possibility of dialling the emergency number "112".

The Register, the leading tech portal, labelled this report as *"a must read for anyone involved in either disaster recovery or telecommunications network management"*. Here is a link to this article: http://www.theregister. co.uk/2013/08/21/enisa_comms_ outage_breakdown_report/

More information about the findings of this report is provided on p.3

On **4th September** the Head of ENISA's Core Operations Department, Mr Steve Purser, attended the Advisory Board of TREsPASS in Tallinn. TREsPASS stands for Technology-supported Risk Estimation by Predictive Assessment of Socio-technical Security. The TREsPASS project is funded by the European Commission's Seventh Framework Programme (FP7).

ENISA is looking for new colleagues!

Expert in Network and Information Security (AD 6)

Deadline for application: September 10, 2013

More information:

http://www.enisa.europa.eu/recruitment/vacancies/expert-in-network-and-information-security-4

The Expert in NIS will initially work in the Secure Infrastructure and Services Unit (COD1) of ENISA within the Core Operations Department, but must have the ability and willingness to contribute to other areas of the ENISA Work Programme as and when required.

Expert in Network and Information Security (CA)

Deadline for application: October 7, 2013

More information:

http://www.enisa.europa.eu/recruitment/vacancies/expert-in-network-and-information-security-5
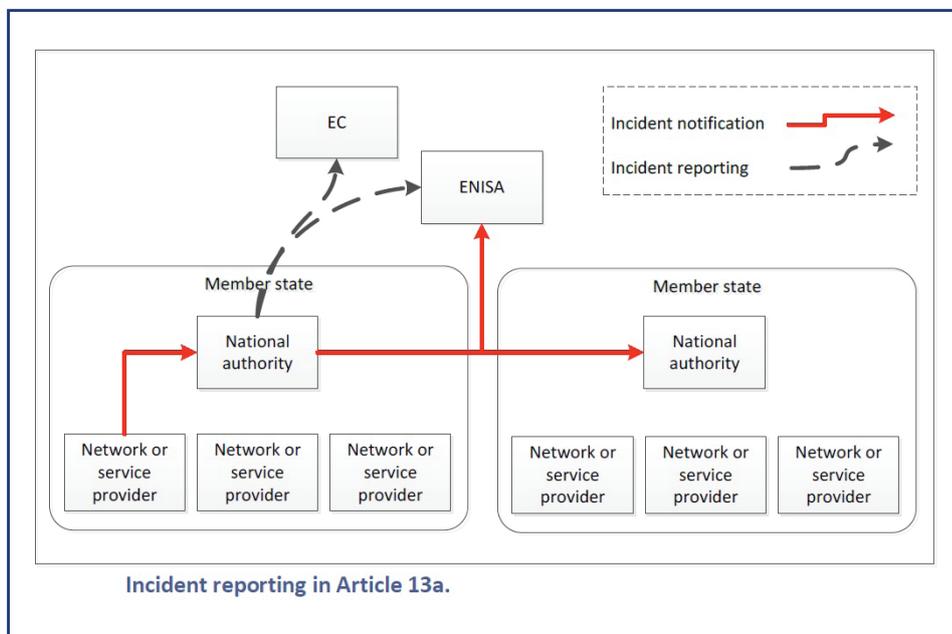
The Expert in NIS will initially work in the "Operational Security" Unit (COD3) of ENISA, but must have the ability and willingness to contribute to other areas of the ENISA Work Programme as and when required. Allocation of tasks is based on an internal work plan developed by the Unit.

Annual Incident Reports 2012

Starting in 2012 (for the 2011 reporting year) ENISA has published 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). The new report covers the incidents that occurred in 2012.

In total 18 countries reported 79 significant incidents, nine countries reported no significant incidents. Below we summarize the main conclusions that can be drawn from the incident reports.

- Most incidents affected mobile telephony or mobile Internet (about 50% of the incidents respectively). Incidents affecting mobile telephony or mobile Internet also affected most users (around 1.8 million users per incident). This is consistent with the high penetration rate of mobile telephony and mobile Internet.

- In 37% of the incidents there was an impact on the emergency number 112.

- For most incident reports the root cause was "System failures" (75% of the incidents). This was the most common root cause category also for each of the four services (fixed and mobile telephony and fixed and mobile Internet). In the category "System failures", hardware failures were the most common cause, followed by software bugs. The assets most often affected by system failures were switches (e.g. routers and local exchange points) and home location registers.

- Incidents categorized with root cause third party failures, mostly power supply failures, affected around 2.8 million user connections on average. Incidents involving the detailed cause overload affected around 9.4 million user connections on average.

- Incidents caused by natural phenomena (mainly storms and heavy snowfall) lasted the longest: around 36 hours on average.

- Incidents caused by overload followed by power failures respectively had most impact in terms of number of users affected times duration.

- Overall, switches and home location registers were the network components or assets most affected by incidents.

Incident reporting in Article 13a.

ENISA, together with the National Regulatory Authorities (NRAs) of the different EU Member States, discusses specific incidents in more detail in the Article 13a Expert Group. Where needed, ENISA drafts technical guidance for NRAs and service providers about mitigating incidents. For example, following last year's report, ENISA is now drafting recommendations on power supply dependencies and national roaming for resilience.

The full report is available here:
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2012
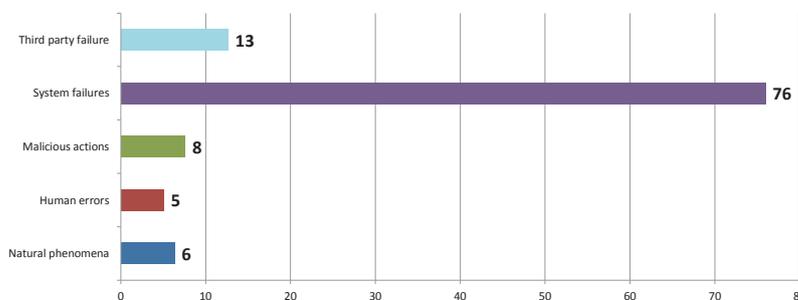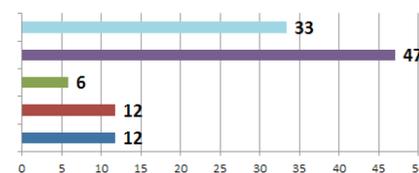
Incidents in 2012 per root cause category

Figure: Incidents per root cause category (percentage)

Most of the incidents fall in the rootcause category 'System failures' (76%). Note that the numbers add up to more than 100% because for a few incidents multiple root cause categories were indicated.

(2011)

FORTHCOMING EVENTS...

Calendar of the ENISA organised events for Q3 and Q4 2013[1]		
24 September	Brussels, Belgium	**Workshop on Security Aspects of Trust Services Providers** https://www.enisa.europa.eu/activities/identity-and-trust/trust-services/eid-workshop/workshop
24-25 September	Athens, Greece	**2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises** https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/conference/2nd-enisa-conference-on-ccc/2nd-enisa-international-conference-on-cyber-crisis-cooperation-and-exercises
1 October	Tallinn, Estonia	**Workshop on Recommendations for Harmonized ICS Testing Capability in the EU** http://www.enisa.europa.eu/activities/Resilience-and-CIIP/workshops-1/2013/recommendations-for-harmonized-ics-testing-capability-in-the-eu
2-3 October	The Hague, Netherlands	**ENISA 8th annual workshop 'CERTs in Europe'** – Part II, co-organised with EC3
16-17 October	Vilnius, Lithuania	**MB meeting**
11 October	Brussels, Belgium	**European Cyber Security Month Kick Off Event** http://ec.europa.eu/information_society/newsroom/cf/dae/itemdetail.cfm?item_id=11516
29 October	Athens, Greece	**PSG Meeting**
26 November	TBD	**Informal MB strategy meeting**
11 December	Brussels, Belgium	**ENISA High-level event.** Details will be provided in Q3

[1] For information purposes only. Dates are preliminary and might change unless the official invitations are distributed or published.

Calendar of events to which ENISA has received invitations and plans to participate in Q3 and Q4, 2013*		
5-6 September	Brussels, Belgium	**Conference "International Cyber Security Strategy"** http://test.fitce.org/downloads/ICSS%20FITCE%202013%20Program%20V1.pdf
17-19 September	Brussels, Belgium	**Cyber Intelligence Europe** http://www.intelligence-sec.com/events/cyber-intelligence-europe
9-11 September	Reykjavik, Iceland	**8th European Peering Forum** http://www.peering-forum.eu/agenda
9-11 September	Kloster Banz, Germany	**Open Identity Summit 2013** http://openidentity.eu/
12 September	Frankfurt, Germany	**FS-ISAC information sharing CERTs/Banks**
16-18 September	Amsterdam, Netherlands	**CRITIS 2013 – Conference on Critical Information Infrastructures Security**
18-20 September	Brussels, Belgium	**Digital Enlightenment Forum 2013**
24-25 September	The Hague, Netherlands	**Europol – INTERPOL Cybercrime Conference 2013**
25 September	Brussels, Belgium	**EC workshop on the EU proposal for a Regulation on "Electronic identification and trust services"**
25-26 September	Brussels, Belgium	**NIS Platform Meeting**
1 October	Prague, Czech Republic	**European Cyber Security Month kick off event in Czech Republic**
2 October	Vienna, Austria	**European Cyber Security Month kick off event in Austria**
16-17 October	Frankfurt, Germany	**German CERT-Verbund**
23 October	Riga, Latvia	**ISACA Latvia and CERT.LV annual conference 2013**
23-25 October	Amsterdam	**IT Supervision Training** – 23-25 October 2013-Amsterdam
6-8 November	Vilnius, Lithuania	**ICT 2013** http://ec.europa.eu/digital-agenda/en/ict-2013
19-20 November	Stockholm, Sweden	**2nd EU ANSA Meeting**
28 November	Brussels, Belgium	**One-day debate "The Future of Identity",** hosted by Giesecke & Devrient with the support of ENISA http://www.eu-ems.com/summary.asp?event_id=179&page_id=1484

*As notified by 01.09.2013., subject to confirmation