MANAGEMENT BOARD NEWSLETTER

THE LATEST NEWS FROM ENISA

ENISA's Cyber-Threat overview 2015

On 27 January ENISA published its Threat Landscape 2015 report. This is a consolidated overview to the 15 top cyber threats together with detailed threat assessments in the emerging areas Software Defined Networks and Big Data. More information is available on page 4.

The call to join the Cyber Europe 2016 has been published

Cyber Europe 2016, the next European cyber crisis exercise, is under preparation. For European public and private organizations eager to test their cybersecurity capabilities it is the one event in 2016 not to be missed. More information is available online: https://www.cyber-europe.eu. Watch the Cyber Europe 2016 promo video: Are you ready for the next cyber crisis? For your information the After Action Report of the previous pan-European cybersecurity exercise Cyber Europe 2014 is available as well.

EC launched a public consultation

In line with the Digital Single Market (DSM) Strategy, the European Commission launched a public consultation on how to best set up a Public-Private Partnership (PPP) on cybersecurity. The public consultation will be open until 11 March 2016 and will be primarily concerned with where to focus efforts for establishing the PPP (which is expected to become operational in the course of 2016).

Udo Helmbrecht
Executive Director

European Union Agency for Network and Information Security

Dear Members of the ENISA Management Board,

Welcome to the new issue of our MB Newsletter. We have challenging year ahead in view of the upcoming regulatory changes which include the NIS directive and other policy initiative. The Amending Work programme 2016 is now being prepared to reflect these changes. Nevertheless we are pleased to provide you with a summarised overview of our latest activities. As ever, please feel free to share the newsletter with any of your colleagues or associates, who may find it of use.

ENISA calls for partners for the European Cyber Security Month

EUROPEAN CYBER SECURITY MONTH

ENISA invites public and private organisations to show their interest to take part in this year advocacy campaign by filling in this web-form.

ENISA plays its part for a better internet!

Safer Internet Day was celebrated on 9 February, with this year's theme being 'play your part for a better internet'. ENISA played its part for a better internet by sharing some of its work in the field of education and awareness as a central broker of best practices in terms of NIS materials and tools. Four new posters are released and available online as part of our educational campaign (#Netiquette) for all EU citizens interested in a secure and safe digital life in all EU languages, available here: https://www.enisa.europa.eu/media/news-items/enisa-plays-its-part-for-a-better-internet

ENISA - Telefonica Workshop on Big Data

On **2 February** the workshop on the use of big data in critical sectors hosted by ENISA in the venue kindly provided by Telefonica in Madrid. The invitation only event welcomed participants from the private sector, banks and cloud service providers. The workshop aimed at providing valuable insights on the current status of big data security and privacy, and identified challenges and risks and the potential ways to address the expressed concerns. ENISA's experts gave an overview of the findings as identified in its upcoming report on 'Big Data Security" and the recently published 'Privacy by design in Big Data' report.

Cryptographic tools are important for civil society and industry

ENISA's paper on the subject looks into several aspects of crypto regulation and their difficulties from a technical perspective. Key points ENISA focuses on are:

- The use of cryptography might make lawful interception harder and by this less efficient or even ineffective. While key recovery and escrow might enable lawful interception, it introduces new technological risks to IT infrastructure and it might even damage the gathered evidence.
- It is easy to bypass systems that allow key escrow or recovery; evidence for bypassing will only be found during investigation.
- Vulnerabilities that where left from legacy policy have been abused to attack systems. Further, policy that limits the use of cryptography in commercial products can damage IT industry.

#APF16: Call for Papers open until March 15th

ENISA's Annual Privacy Forum (APF) is to be held on the 7 and 8 September 2016 in Frankfurt, at the Goethe University Frankfurt am Main. This year's edition is organised in the light of the agreement on the data protection regulation and the European Digital agenda.

The call for papers is open until 15th March. To submit your paper you are requested to use the following link. The programme committee will provide extensive feedback to all authors. For more information visit http://privacyforum.eu

Annual Privacy Forum

E-learning platform by ENISA on National Cyber Security Strategies

The National Cyber Security Strategies e-learning platform has been provided by ENISA. Such platform is appropriate for experts involved in the process of creating or implementing a strategy at a national level. The platform aims to provide interactive training courses in order to facilitate the process of:

- designing a national cyber security strategy
- implementing a national action plan
- evaluating the cyber security awareness after the end of the timeframe
- raising awareness on cyber security topics
- offering advice to the public bodies that need to take over the initiative

To receive access to ENISA's tool please register here: https://resilience.enisa.europa.eu/ncss-training-tool/express-interest

Defending the smart grid – how to protect networks and devices from cyber attacks

ENISA report on „Communication network interdependencies in smart grids" focuses on the evaluation of the interdependencies and communications between all the assets that make up the new power grids, their architectures and connections in order to determine their importance, threats, risks, mitigation factors and possible security measures to implement. The recommendations of this report are addressed to operators, vendors, manufacturers and security tools providers in the EU and they include the following:

- foster intercommunication protocol compatibility between devices originating from different manufacturers and vendors
- develop a set of minimum security requirements to be applied in all communication interdependencies in smart grids
- implement security measures on all devices and protocols that are part, or make use of the smart grid communication network.

ENISA - CEER 1st Workshop

On **22 January** ENISA hosted the meeting of the experts from the Council of European Energy Regulators (CEER) IT security subgroup. Participants from the European Commission Directorate General for Energy, the Agency for the Cooperation of Energy Regulators (ACER), as well as representatives from Austria, Hungary, Greece, Italy, Slovenia, Ireland and the Netherlands were also present and discussed the status of cyber-security in the energy sector, future steps and collaboration. Among other things:

- The European Energy Cyber Security Platform (EECSP),
- ENISA's activities regarding security in the energy sector,
- The NIS Directive and The information sharing initiatives were presented and further discussed.

JRC Members visit ENISA

On **25 January** the Technology Assessment Unit (STA) from the Institute for the Protection and Security of the Citizen (IPSC) Security of the Joint Research Centre (JRC), visited the ENISA premises in Athens.

The objective of the meeting was to exchange experiences with ENISA's Secure Infrastructure and Services Unit, discuss technical topics and create synergies on common working areas.
In more details, the meeting focused on discussions, exchange of experiences and future collaboration on common topics of interest:

- IACS (Industrial Automation Systems) security and certification,
- eHealth,
- Smart infrastructures and
- IPSC's tools to secure businesses and the society.

Cybersecurity priority of Dutch presidency

The Dutch presidency aims to strengthen cybersecurity in the EU and in member states. The Netherlands will actively promote discussions on current and future developments in the EU since digital innovations continue to develop rapidly. Specific attention will be given to the following themes: public-private cooperation, cooperation between CSIRTs, coordinated vulnerability disclosure, standards and education/e-skills. An informal kickoff meeting of the CSIRT network created under the NIS directive will take place in the Netherlands during the One Conference on 5/6 April.

Calendar of Dutch Presidency events on cybersecurity:

- One Conference 5/6 April (CSIRTs representatives and policy advisors)
- High Level meeting on the future of cybersecurity in the EU 12/13 May (high-level senior officials and CEOs or board members)

The Dutch presidency is looking forward to welcome our European partners at these meetings. For more information on the up-coming events, please contact the Dutch presidency team at NL-EUPresidency-cyber@nctv.minvenj.nl

TOP 10 DOWNLOADS IN 2015

List with top 10 file downloads from ENISA website

In 2015 the following deliverables were among the most popular downloads from the ENISA website:

1. Good Practice guide for incident management
2. Cloud computing security risk assessment
3. Privacy and Data Protection by Design – from policy to engineering
4. ENISA threat landscape 2014
5. Cloud computing risk assessment in Spanish
6. Risk Assessment and Risk Management Methods: Information Packages for Small and Medium Sized Enterprises (SMEs)
7. Algorithms, Key Sizes and Parameters Report – 2013
8. Cloud security guide for SMEs
9. Actionable information for security incidents response
10. Security Framework for Governmental Clouds

ENISA's Cyber-Threat overview 2015

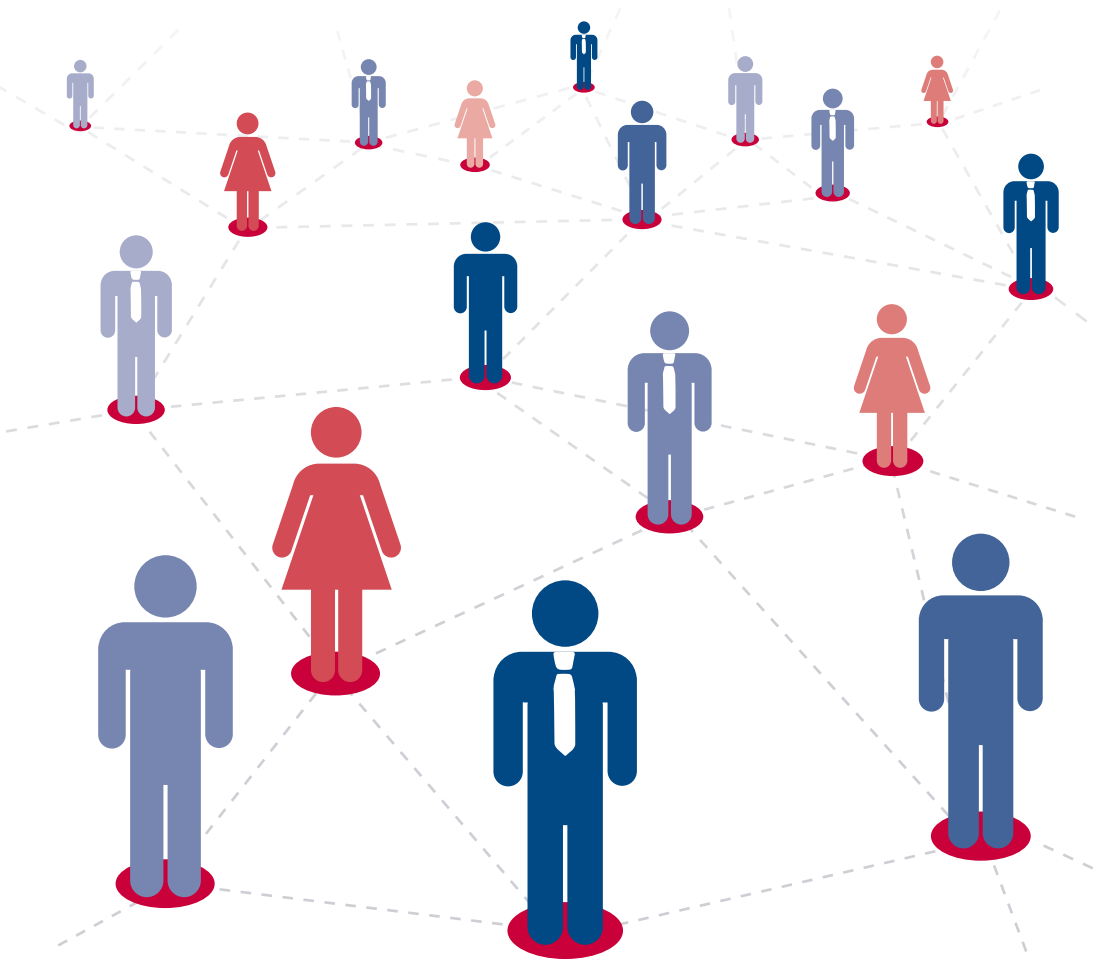
(continued from page 1)

The figure below summarizes the top 15 cyber-threats and threat trends in comparison to the threat landscape of 2014.

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

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

ENISA IS LOOKING FOR NEW COLLEAGUES



Contract agents

PROCUREMENT SUPPORT OFFICER

Closing Date: 2016-03-14

HUMAN RESOURCES OFFICER

Closing Date: 2016-03-14

Seconded National Experts

SECONDED NATIONAL EXPERTS

Closing Date: 2016-06-30

ENISA is looking for Seconded National Experts in the field of Network and Information Security (NIS) that will be requested to support the Agency's Core Operations Department in the areas such as:

- Computer Security Incident Response community (CERTs, aka CSIRTs)
- Other operational communities (e.g. EU FI-ISAC)
- CSIRT-LEA2 cooperation on fight against cybercrime

Trainees

TRAINEESHIP NOTICE - UPDATED

Closing Date: 2016-12-31

Applications for traineeships at ENISA are accepted in the following areas:

1 Network Information Security (NIS) in the following areas:

- Security technologies
- Security & resilience of communications networks
- Critical Information Infrastructure
- NIS standardisation & regulation
- Electronic Identity & authentication technologies
- Information Security Statistics
- Economics of NIS

2 Administration and Support in the following areas:

- General Administration
- Financial Administration, Human Resources
- Internal Audit
- Legal
- Information Technology (IT)

More information available here: https://www.enisa.europa.eu/recruitment/vacancies

CALENDAR OF EVENTS

MARCH
APRIL
MAY

ENISA IS ORGANISING, HAS RECEIVED INVITATIONS, OR PLANS TO PARTICIPATE:
(This list in tentative and last minute changes may occur.)

1 March	Athens, GREECE	**Smart cities conference**
2 March	Brussels, BELGIUM	**ENISA MB Ad Hoc Group meeting**
2 March	Kaiserslautern, GERMANY	**Safety Meets Security conference**
8-9 March	London, UK	**The cyber security show**
9-10 March	Budapest HUNGARY	**18th Art. 13a expert group meeting**
15 March	Brussels, BELGIUM	**C-ITS Platform WG5 Security Workshop**
16 March	Brussels, BELGIUM	**Breakfast debate with the MEPs, organised by ENISA**
16 March	Brussels, BELGIUM	**Workshop on certification of ICT products in Europe organised by ENISA**
16-17 March	Heidelberg, GERMANY	**Troopers 2016**
18 March	Brussels, BELGIUM	**EC Conference Building Trust in Cloud Services – Certification and Beyond**
22 March	Brussels, BELGIUM	**Industry event, organised by ENISA**
5 April	Athens, GREECE	**ENISA PSG meeting**
5-6 April	The Hague, THE NETHERLANDS	**International NCSC One Conference**
6-7 April	Prague, CZECH REPUBLIC	**6th Annual Cyber Security Summit**
18 April	Brussels, BELGIUM	**C-ITS Platform WG5 Security Workshop**
19 April	Brussels, BELGIUM	**ePrivacy Directive Revision Workshop with National Authorities**
18-19 May	Brussels, BELGIUM	**7th Internet of Things European Summit, Brussels**
26-28 April	London, UK	**ICS Cyber Security Conference**
27-28 April	Brussels, BELGIUM	**European FI-ISAC meeting**

CALENDAR OF EVENTS

MARCH
APRIL
MAY

ENISA IS ORGANISING, HAS RECEIVED INVITATIONS, OR PLANS TO PARTICIPATE:
(This list in tentative and last minute changes may occur.)

10-11 May	Riga, LATVIA	**ENISA annual CSIRT workshop (including EU CSIRT network meeting)**
12 May	Brussels, BELGIUM	**ePrivacy Directive Revision Workshop with industry**
24-25 May	Dublin, IRELAND	**Secure Cloud (co-organisation with CSA and Frauhofer FOKUS)**
25 May	Brussels, BELGIUM	**2nd eIDAS Forum**
1-3 June	Frankfurt, GERMANY	**2nd global Cyber Security For Financial Sector**
8 June	Athens, GREECE	**ENISA EB meeting**
9 June	Athens, GREECE	**ENISA MB Extraordinary meeting**
13-17 June	Seoul, SOUTH KOREA	**FIRST annual conference (global Forum for Incident Response and Security Teams)**
15-16 June	Athens, GREECE	**CE2016 Final Planning Conference**
15-16 June	Munich, GERMANY	**CODE conference (session on eHealth)**
16-17 June	Switzerland	**SIGS Technology Summit**
20-23 June	Vienna, AUSTRIA	**Fundamental Rights Forum**

Securing Europe's Information Society