European Union Agency for Network and Information Security

EU Cybersecurity Cooperation:
ENISA - 10 years of securing Europe's cyber future

EU Cybersecurity Cooperation: ENISA -10 years of securing Europe's cyber future

Contact
For contacting ENISA please use the following details:
e-mail: info@enisa.europa.eu
website: www.enisa.europa.eu

Print ISBN 978-92-9204-093-2, doi:10.2824/32805
Pdf ISBN 978-92-9204-094-9, doi:10.2824/32858

Printed in Belgium

Printed on elemental chlorine-free bleached paper (ECF)

I would like to welcome you to the High Level Event 2014 organised by ENISA. This Event brings together key figures in policy, government, industry and users' organisations with a view to exchange information and ideas on network and information security. The High Level Event seeks to be a strategic foresight forum to share and validate views on policies and strategies that are likely to render our activities and societies safer and more secure in the face of harm posed by cyber-threats.

This year marks the first ten years of ENISA. Since 2004 the Agency has managed to draw the attention of policy makers and the industry alike to the need to prepare in the face of cyber-threats and work together to bring about better results. ENISA is but a wheel in the grand policy machinery put together by the EU to tackle cyber-threats. ENISA's contribution has been its unique ability to bring together the various actors and facilitate the exchange of information through informed opinion. ENISA has greatly assisted its stakeholders to be better informed and appreciate the value in working together towards a more cyber-secure environment. This is no mean achievement and we are proud to celebrate it this year in the Agency's tenth anniversary.

ENISA Executive Director,
Prof. Udo Helmbrecht

Introduction

The European Union Agency for Network and Information Security (ENISA) has been set up for the purpose of contributing to the goals of ensuring a high level of network and information security within the European Union and developing a culture of network and information security for the benefit of citizens, consumers, enterprises and public administration. To meet its policy goals ENISA supports its stakeholders, being EU institutions and Bodies and the EU Member States in various ways for the purpose of preparing to meet the challenges posed by the cyber-security threats.

What does ENISA currently do?

The primary activity of ENISA is to provide input on its various tasks by exercising its technical capability to study and analyse complex issues on network and information security. The way ENISA works is by bringing together stakeholders, to provide a discussion forum for the exchange of practices and the shaping of policies. Key areas of current activity for ENISA include but are not limited to the ones briefly outlined in this paper.

A pro-active analysis of the **threat landscape** aims at giving advance notice to stakeholders on what's lurking ahead. Painting the cyber-threat landscape and

keeping up with the dynamics behind it requires an on-going analysis of cyber-incidents reported.

Cybersecurity experts rely on this information to assess risks to various systems and develop cybersecurity strategies and policies to defend them. Working with the first line of defence has been a priority for ENISA as it has been supporting **CERT cooperation** in the EU Member States since the very beginning. ENISA has contributed to the multiplication and further development of the capabilities of CERTs to meet public sector needs, rendering in the process, government information more secure. ENISA has extended its support to the EU CERT that serves EU Institutions and Bodies. To bring about policy outcomes in CERT cooperation, ENISA relies on a mix of trainings, exchange of good practice, advisories, and conferences. Additionally ENISA supports the closer collaboration of CERTs with law enforcement bodies.

Cyber crisis cooperation and cyber-exercises in the EU have been a major activity for ENISA in an effort to support the development of strong relationships among the EU Institutions, EU Members States themselves and beyond, in the EFTA Member States and with trans-Atlantic partners. ENISA has concretely supported such organisations as the Eurocontrol air traffic control Agency, with a large-scale cyber incidents' scenario. ENISA's series of international conferences on cyber crisis cooperation and exercises offers a key knowledge sharing platform to international cyber security experts and decision makers. The EU-Standard Operating Procedures to which ENISA has contributed, provide guidance on how to manage major cyber incidents before they escalate to a crisis. The pan-European exercises organised by ENISA are **Cyber Atlantic** and **Cyber Europe**.

Identifying the main issues of concern regarding the **security of smart grids** in support of national, pan-European and international initiatives has evolved in ENISA in close cooperation and consultations with stakeholders. Recommendations issued, focus on smart grid security and measures. ENISA also contributes to the Smart Grids Task Force and reports progress to the EG2 ad hoc group on security measures of smart grids.

In an evolving landscape, I**ndustrial Control Systems and SCADA** have been put under the spotlight by ENISA. Recommendations made, aim at achieving an appropriate level of preparedness with respect to ex-post incident analysis, improved learning capability and patch management deployment. As no harmonized and commonly accepted schemes for the certification of Cyber security skills of ICS-SCADA experts in Europe are available, ENISA seeks to provide guidance on these schemes.

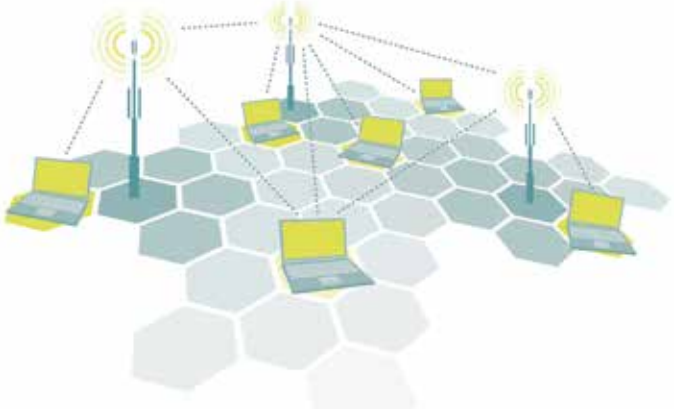
The recommendations of ENISA on **cloud computing** have impacted the way users carry out their risk assessments before turning to Cloud-based services. ENISA has further provided guidance for governmental clouds and made available practical assistance to public bodies thereto. Additionally ENISA supports the European Commission to implement its EU cloud strategy and it participates in select industry fora (Cloud Certification SIG, Cloud SLA etc.).

ENISA advocates that the **security and resilience of European Internet Infrastructure and Critical Information Infrastructures** calls for EU Member States to cooperate in cross border interdependencies while at the same time enhance the resilience of infrastructure within their borders. The EU Members States should get to the point where they develop an insight of the current infrastructure, the critical infrastructure interdependencies and have a baseline for future development. The technical and organizational aspects of these interdependencies along with good practices have been analysed and reported upon by ENISA.

Mobile communication networks and services such as roaming could be used nationally to mitigate large mobile network outages. ENISA has provided Na-

tional Regulatory Authorities in the EU Member States with a portfolio of options that have been appropriately rated for suitability for security and resilience.

Supply chain integrity in ICT is of interest to the public and private sectors alike. ENISA has identified what supply chain integrity means in the ICT context and it has proposed measures to improve assurance in supply chain integrity.



In support of **Smart Cities**, ENISA focuses on the cyber security of the information infrastructure taking a holistic approach. Smart Cities underline the collaboration among organisational stakeholders and citizens. ENISA has reported on good practices and common threats. Additionally ENISA has analysed intelligent transport systems with a view to evaluate the current status of cyber security by public transport operators across the EU.

In support of the new EU framework on **electronic identification and trust services** ENISA has drafted guidelines on maintaining appropriate security level for trust services providers. ENISA has also discussed the principles and concepts of managing risks applicable to trust services providers by defining and controlling threats and vulnerabilities and by proposing suitable technical and organisational means to handle security risks faced by trust services providers.

ENISA has tracked the development of **standards** for products and services in network and information security and it closely cooperates with standardisation bodies including ISO, ETSI, ITU, CEN and CENELEC. ENISA has also facilitated the cooperation among all relevant sector actors (SDOs, EU organisations, Industry), in order to address shortcomings of standards in network and information security.

To foster the resilience of the networks and information systems which underpin the services provided by market operators and public administrations in Europe, ENISA supports a NIS Public-Private Platform. The **NIS Public-Private Platform** will help implement the measures set out in the regulatory framework (e.g. NIS Directive) and ensure convergent and harmonised application across the board.

The support of ENISA for **network and information security in Finance**, aim at the outsourced assets of the finance sector, the supply chain and the reporting of breaches. The security of the communication networks and services seeks to support financial institutions that have yet to come to terms with measures needed to improve their network and information security standing.

The **European Cyber Security Month** is an EU advocacy campaign that takes place in October each year. The main objective of this campaign is to promote cyber security awareness among citizens, to modify their perception of cyber threats at work and in the private sphere, and to provide updated security information through education, good practices and competitions. As an instrument of collaboration among stakeholders in network and information security, ENISA seeks to facilitate sharing good practice, and thereby increase the results for the work of network and information security communities.

In the area of **privacy and data protection** ENISA works closely with the art. 29 Working Party and select Data Protection Authorities in the EU Member States, with expert guidance on certain privacy and security issues. ENISA seeks to provide analysis of the threats and risks that new technologies may bring about for privacy and data protection and propose measures thereto.

A **network and information security driving licence** is a concrete voluntary certification programme supported by ENISA to promote enhanced skills for IT professionals. ENISA has carried out a consultation with relevant stakeholders and it aims at developing a self-evaluation scheme.

The next 10 years

As ENISA turns page, the outlook for network and information security provides mixed feedback to policy makers. While significant threats of the past (e.g. spam) appear to have subsided, new and pressing ones have reared. The regulatory framework has also provided new impetus to address requirements in the entire spectrum of telecommunications, applications such as commerce and trust services, rights such as privacy, compliance, such as data protection etc. As technology leaps to the next stage the need for dependable expert advice on network and information security is not likely to wane. Working together and sharing knowledge is the proven method of ENISA to halt threats on their track to the benefit of all stakeholders in the EU institutions, and in the public and the private sectors alike. Policy makers and industry can look up on ENISA confidently for both professional grade advice and a forum to collaborate and exchange ideas in their efforts prepare responses and prevent threats in the area of network and information security.

TP-02-14-891-EN-C

ENISA - European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13 Heraklion, Greece
Tel: +30 2814 409 710
www.enisa.europa.eu

ISBN 978-92-9204-093-2
doi:10.2824/32805