ENISA today and in the future

Who are we

ENISA is an European Agency, which is a centre of expertise for cyber security in Europe. The Agency operates under EU Regulation 526/2013 of the European Parliament and the Council of the 21 of May 2013. The mandate of the Agency runs until the 19 of June 2020. Pursuant to a decision of the European Council, the Agency is located in Greece with its seat in Heraklion and an operational office in Athens. The Agency has around 70 staff members and an annual budget of around 10 million Euro. The Agency currently has the operational department located in Athens and is assisted by administrative staff located in Heraklion, as defined in the Regulation. The Agency is supported by a Management Board made up of representatives of the European Commission and all 28 Member States who pursuant to the Regulation define the direction of the operation of the Agency. [1]

What do we do at a policy level

In the pursuit of an open, safe and secure cyberspace, ENISA supports the EU and the Member States in enhancing and strengthening their capability and preparedness to prevent, detect and respond to network and information security problems and incidents. ENISA also supports the development of the European Union (EU) policy and law on matters relating to network and information security (NIS).

How do we work

ENISA's greatest strength is the strong ties it has developed with its stakeholder communities. The Agency works closely together with members of both the public and private sector, to deliver advice and solutions that are based on solid operational experience. This approach is inherently scalable as it leverages the capabilities that have already been developed in the different Member States. It also results in stronger buy-in by all concerned and builds trust. As an example, the pan-European Cyber Security Exercises clearly illustrate the benefits of such an approach. Whereas in 2010, there was only a table top exercise and no crisis management procedures at the EU level for dealing with a cyber-events. Now in 2014, these standard operational procedures not only exist but are being tested via a sophisticated exercise involving the operational communities of all Member States.

[1] The contents of this document are drawn from a speech given by the Executive Director of ENISA Professor Dr. Udo Helmbrecht to the Industry Research and Energy Committee (ITRE) of the European Parliament on the 2nd September 2014 in Brussels.

Why is our work important

Information and communication technologies (ICT) are the backbone of every modern society. An open, safe and secure cyberspace is key to, on the one hand, supporting our core values set down in the EU Charter of fundamental rights such as privacy, freedom of expression and, on the other hand, the smooth running of our economies within the European single market. However, the ICT technologies and business opportunities in cyberspace also present opportunities for crime and misuse[2].

In today's world, cybersecurity is essential to the operation of our critical network information systems. Banking, telecommunications, energy and water management, health care and production industry are all dependent on global communications networks including the internet. The internet of things, where every electronic device will be uniquely accessible over the internet, is approaching quickly. This will allow for the remote control of our heating, lighting and security systems in our homes. More advanced applications of this technology will allow the medical device that one is wearing to continuously monitor their health e.g. a heart pacemaker can send data to the hospital alerting them of possible health problems before one is even aware of it. E-banking, e-health, e-commerce, e- education, e-*everything* 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 Smart living, the Smart Home and the Smart Cities of the future.

Some of ENISA's contributions to date

For an open, safe and secure cyberspace, ENISA has brought together the majority of the stakeholders in the EU in order to mitigate the risks associated with cyber security.

This work has involved supporting:

- Policy development by identifying evolving cyber threats, risks and challenges and by supporting the development of national cyber security strategies.
- Capacity building across all Member States involving governments and key private sector stakeholders.
- Public sector and private sector institutions in the secure adoption of evolving technologies, such as Cloud Computing and the use of mobile devices.
- Cooperation between key cyber stakeholders by way of the delivery of crisis cooperation exercises at both the operational and strategic levels.
- Cooperation and capacity building between the law enforcement community and national computer emergency response teams (CERT) across the EU.

[2] Recently the German newspaper Süddeutsche Zeitung reported an increase in damages only for Germany arising from cybercrime from 37 M€ in 2008 to 42M€ in 2012 and in increase in reported cybercrime cases from 37.900 in 2008 to 63.595 cases in 2012.

- Areas, where strong approaches to network and information security can improve data protection and privacy across the EU.
- Statutory reporting of significant security breaches and losses of integrity in public electronic communications networks pursuant to Article 13a of the Framework Directive of the Telecom Package agreed in 2009.
- The Member States, pursuant to Art. 14 of the ENISA Regulation. Examples of this assistance include CERT training, assistance with organising national exercises for Member States, advice to the European Commission on technical implementation measures, guidance on implementation aspects of privacy and data protection and input into the work programmes of other EU agencies.

Challenges for the future

The only constant in the cybersecurity area is rapid change.

It is expected that there will be over 3 billion internet users in early 2015[3]. Any individual one of these connections is capable of attacking a banking system to extract funds unlawfully, attacking a critical infrastructure that controls energy, water or industrial processes or assuming the electronic identity of another individual. All this is possible from any internet connection in the world.

By 2030, it is expected that there will be 50 billion devices[4] connected to the internet. Each device has a purpose and function and will need to be protected from unauthorised access or control by cyber criminals.

To facilitate an open, safe and secure cyberspace ENISA addresses these challenges, provides solutions and knowledge that support investment and the deployment of electronic services in the EU internal market. Some of these investments will have an impact for the next few decades.

Focusing below are two cyber security areas that are key to European citizens and the economies of the Member States and which will need the ongoing strategic attention of ENISA. These are *cloud computing* and the control of one of our critical infrastructure: the *energy networks*.

Cloud computing is changing the way we do business in the electronic world. Already in 2009 ENISA published its report entitled "Cloud Computing Risk Assessment"[5]. The computer world is going through a rapid change where electronic storage and electronic processing power are shifting from customer controlled infrastructure to large data processing centres in the so called *cloud*. This leads to new scalable business models with new services. Professionally managed cloud computing centres significantly increase the IT-security level, especially for small and medium companies (SMEs) and consumers. Cloud providers operating globally are outside the control of end users and these processing centres are effectively a single point of

[3] Internet Society Global Internet report 2014
[4] Ericsson Group
[5] http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

attack. Furthermore, such centres can potentially be located anywhere, which leads to challenging questions regarding legal jurisdiction and supervision.

New cyber threats are emerging from the asymmetry in the electronic processing power of the cloud operators and the end user devices. This asymmetry arises where the end user devices often based on mobile technology are used to upload and control applications in the cloud. Given their size and flexibility, these devices may be vulnerable to unauthorised remote control or become victims of malware. Where these vulnerable applications are compromised, it is possible that other cloud services, hosted on the same platform, can become victims. As Europe moves towards the increasing use of the cloud, including e-health, e-commerce and related services, the cloud data centres, the end user devices that drive the applications and the underlying network infrastructure become a high risk target.

ENISA has invested a lot in analysing cloud risks and by way of example has recommended security service level agreements, certification and audit schemes. Given that Europe has some of the highest data protection and privacy standards in the world, the challenge will be on Europe to lead on protecting businesses and citizens using the cloud model. All the evidence suggests that the cloud business model is here to stay and that ENISA has a critical role in analysing the ongoing threat landscape, advising on solutions and responses to cyber-attacks. ENISA is driving the European cloud security strategy by supporting the drivery and adoption of appropriate security standards.

The second area is the upcoming *intelligent energy infrastructure, the Smart Grid*, which is used for the control and distribution of electricity. It is estimated that over $400 billion will be invested by energy utilities in Smart Grid technology by 2030[6]. While citizens with e.g. solar panels on their roofs producing electricity and consumers begin to enter into the micro-generation electricity market, the ambition is to have a smarter, two way, more cost efficient and more robust grid. New sensors and control devices will be installed across these grids and every home and electricity termination location will have a small computer unit – the smart meter - that will provide remote on/ off control, pricing information and possible control of customer generated electricity into the grid network. All of these sensors and domestic units will be driven by software and linked by communications technology back to control rooms.

Experience has shown that there is no perfect piece of software. We are all aware of the need for software upgrades or patches to remove vulnerabilities to cyber-attack. For example, if a large number of smart meter on/off control switches are switched quickly and remotely by a cyber-criminal, the serving transformer infrastructure could be rendered inoperable. At another level the privacy details of the use of electricity could be compromised.

There are two aspects to this project that make it particularly challenging. The first is the selection and deployment of Smart Grid technology which is expected to last for decades.

[6] Pike Research Group

The second aspect is that Smart Grid technology only uses small levels of data. Therefore software upgrades to address new vulnerabilities will not be easily possible.

The impact of these investment decisions across Europe should not be underestimated.

Utility operators across Europe are now trialling, testing and scoping their technology options for Smart Grids. New skill sets are required, involving the merging of the traditional transmissions engineering, software development and cyber security expertise.

From a technical and strategic perspective there is much work to be done in the area of network and information security (NIS), the most relevant ones are:

1. New challenges in the production sector: *Industry 4.0* - The first industrial revolution was driven by the steam engine. The second was driven by mass production in factories that produced for example the FORD automobiles. The third was driven by automation and artificial intelligence in the form of robots. The fourth revolution *industry 4.0* will be about interconnection, mobile and software applications with the internet and internet security being the common link. This revolution will bring intelligent data collection and will involve processing of many aspects of our work and personal lives. All of this presupposes that the cyberspace functions correctly and delivers what it is intended to do.
2. The advent of Big Data brings with it a host of new opportunities for identifying and analysing patterns of behaviour that have so far escaped attention. However, Big Data also introduces a number of security concerns, which can give rise to difficulty. Difficulty of maintaining privacy, particularly for results of data analysis, which are not predictable in advance.
3. Mobile computing remains a key security challenge for the next decade as new devices appear on the market at an ever increasing rate. These devises are usually not equipped with an adequate security in their early (and sometimes later) models. In order to use mobile computing securely in modern business environments, the EU must ensure that software and hardware development processes are modified to deliver devices that are 'secure by design' and not simply secured after the event on a case by case basis.
4. The Internet of Things is a term that refers to a situation in which objects of all kinds (household equipment, portable technology, business devices, industrial systems, etc.) are able to communicate with each other autonomously over the internet. An example of the power of such an architecture would be a situation in which the heating, lighting and security of our homes could be monitored and controlled. It is clear that such a network needs to be extremely secure if the EU is to avoid serious disruptions to daily life. There are however serious issues of scalability and cost associated with securing such infrastructure.
5. Data protection and privacy is becoming increasingly important and the emphasis will be put on implementation rather than legal frameworks. ENISA is ideally placed to assist Member States and the private sector in defining and rolling out cost-effective approaches to dealing with this issue.

6. We have seen many examples of data bases across the EU and further afield where the identity details including bank account details of many people have been compromised. We have also seen in May 2014, the European Court of Justice adjudicate that in certain circumstances the individual has the right to have information about them removed from the results of an internet search. This is commonly known as "the right to be forgotten". The area of data privacy and data protection is moving from a legal and principle based debate to an implementation phase where better coordination across all Member states will be required. ENISA has started to play a role in this area and is working with the relevant EU bodies and the Data Protection Authorities, e.g. the Article29 Working Party, in each Member State to address a more standardised approach across the EU in this area.
7. The internal market for security products and services in the EU is not balanced. The market is dominated by US companies and functions on a "supply push" principle rather than a "demand pull" principle. ENISA has an important role in working with industry in the EU to define and disseminate approaches to NIS by EU industry for EU industry and EU customers.
8. Given the level of commitment to research and development by the EU in the Horizon 2020 (H2020) project, ENISA has an important role in helping to ensure that H2020 projects are aligned with key NIS policy objectives that will contribute to the development of the EU market for NIS products and services. In addition, ENISA will continue to work closely with the research community and with industry to improve the rate at which good research ideas are translated into commercial services and products.
9. One of the most challenging aspects of cyber security is that it is often addressed during the final stage of the design and/or the implementation of technology projects. ENISA is addressing this gap by promoting "security by design", where the cyber security of software and hardware products are considered at the very beginning of projects. To this effect ENISA recognises and is committed to the importance of encouraging standardisation and certification activities with industry. ENISA has already signed memoranda of understanding with the European Telecommunications Standards Institute (ETSI) and the European Committees for Standardisation and Electro Technical Standardisation CEN/CENELEC.
10. There are many stakeholders that play a key role in helping ENISA to deliver and maintain an open safe and secure cyber space in Europe. ENISA is building relationships with all the key stakeholders. These relationships are being built in a spirit of trust and cooperation. All of this takes time. ENISA is working closely with Europol, (an MOU was signed between ENISA and Europol in July 2014), CERT EU, the European Commission, national regulatory authorities in electronic communications and data protection authorities, industry and the standardisation bodies mentioned above.

Vision statement and strategy objectives for moving forward

ENISA's vision is *to secure and enable Europe's information society* and to use its unique competencies to help to drive the NIS landscape in Europe. The Agency will deliver its vision by supporting the Member States and European legislative processes in securing Europe's information society, thereby contributing to economic growth in Europe's internal market.

This vision is supported by the following four strategic objectives[7]:

1. To develop and maintain a high level of expertise of the EU actors taking into account evolutions in NIS.
2. To assist the Member States and the European Commission in enhancing capacity building throughout the EU.
3. To assist the Member States and the European Commission in developing and implementing the policies necessary to meet the legal and regulatory requirements of NIS.
4. To enhance cooperation both between the Member States of the EU and between related NIS communities.

ENISA's will use its unique competencies to help to drive the cyber landscape in Europe, and work with the relevant stakeholders to promote the delivery of the best investment decisions from a cybersecurity perspective.

Concluding Remarks

ENISA, as a centre of expertise in cyber security for Europe, is uniquely positioned to address these challenges.

The Agency's Mission is essentially to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union.

September 2014

[7] These Objectives are the basis for ENISA's WorkProgramme 2016 and multi-annual programming.