Cybersecurity best practices

Speech by ENISA's Executive Director, Prof. Dr. Udo Helmbrecht – Deutor Cybersecurity best practice conference

12TH DECEMBER 2018

Deutor Cybersecurity best practice conference

Good morning and thank you for the invitation to speak to you today.

It is always a pleasure to speak in front of such a diverse audience. I am pleased to see that experts from industry, the public sector, academia and defence are gathered here today.

This conference is a great example of the growing realisation that cybersecurity is a shared responsibility. Cybersecurity concerns all citizens and touches all domains.

I am happy to cross paths with Stefanie Frey, who is an expert on ENISA's Permanent Stakeholders' Group. Stephanie is the co-editor of the book we are here to discuss tonight, "*Cybersecurity Best Practices*".

The book is an example of a joint effort between the private and public sector, and also includes input from academia and the cyber defence sector. The book *"Cybersecurity Best Practices"* is an impressive collection of articles from researchers and cybersecurity experts about the challenges that they face in their daily work, the risks and opportunities of cyber, and the resulting best practices that can be identified.

A few years ago, the words "cyber" and "cyber incidents" were largely unknown to the wider public. Now cyber incidents are a part of our everyday lives.

The terms **cybersecurity, cyber warfare, cyber espionage, cyber terrorism and cyber defence** are increasingly referred to in daily conversation by citizens, politicians, and media alike. Some concepts that have emerged as prominent in the last few years include fake news, cyber ethics, cyber diplomacy and digital sovereignty.

The ENISA Threat Landscape Report of 2017 highlighted **the growth in traditional cyber challenges,** where we have witnessed the increased complexity of cyber incidents, the monetisation of cybercrime such as through the increasing use of ransomware, as well as cyber espionage, advanced persistent threats and attacks on critical infrastructure.

Are we prepared to address the challenges arising from increasing and emerging threats and the new hybrid threat landscape in cyber space?

To name a few, we are witnessing the development and deployment of new technologies such **as Robotics and Artificial Intelligence.** From a technical perspective, we have new technologies changing the cyber landscape.

The Internet of Things/ Internet of people is now being deployed with an estimated **20 Billion devices** expected to be operational by 2020. Industry 4.0, Robotics, Artificial Intelligence, **Quantum Computing,** and Blockchain technologies are emerging as **disruptive technologies** and are beginning to affect our daily lives.

These technologies mark the beginning of a **significant societal impact**.

Europe and its digital single market need **to be ready to adapt and reap the benefits of these technologies in a safe and secure cyber environment.** Traditional approaches to security will have to be adapted in order to cope with these new challenges.

Research indicates that the EU cybersecurity market is **growing more slowly** than the cybersecurity markets of other regions.

In 2016, the EU cybersecurity market was estimated at €20.1bn and compared favourably with the cybersecurity market of other global regions. The Compound Annual Growth Rate (CAGR) of the EU market however is 6%, whereas the average growth rate is around 8%.

We are seeing an **increase in the monetisation of cybercrime, crime as a service and targeted attacks.** Targeted attacks, like ransomware, are now listed as top cyber threats in the ENISA Threat Landscape report of 2017.

Recent data breaches (Mariott/Quora.com) and cyber incidents such as ransomware, and the scale of these events, are now a matter of public debate. The more we look at this issue, the more we realise that there is more to be done to adapt to the continuously changing landscape of threats and challenges in cyber space.

Cooperation and exchange of information

In the majority of the EU Member States, **private companies own critical infrastructure and some critical services are provided by the private sector**.

Consequently, a high degree of communication and cooperation between the private and public sectors is necessary.

For this reason**, public-private partnership (PPPs), information sharing and analysis centres (ISACs) and cybersecurity exercises can be effective tools** to assist in managing cyber threats.

ENISA's efforts in this area include offering incentives and actual recommendations on how to set up and run PPPs and ISACs. Moreover, ENISA organises **cybersecurity exercises every two years. ENISA's flagship cybersecurity exercise, "Cyber Europe",** has simulated **large-scale cybersecurity incidents.**

Furthermore, in 2016, the European Union adopted the **NIS Directive**. It is the first piece of EU legislation specifically aimed at improving and promoting cybersecurity at Union level and throughout the EU Member States. The Directive focuses primarily on the protection of Critical Information Infrastructures and national essential services.

Among other measures, the NIS Directive requires the EU Member States **to adopt and implement national strategies** on the security of network and information systems. ENISA has acquired extensive knowledge on this topic and has provided an article in the book presented today.

But we do not stop here.

Securing network and information systems in the European Union is essential to keep the online economy running and to ensure the prosperity of our society.

Under this prism, on September of 2017 the Commission adopted a cybersecurity package. The package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response.

One of the main **elements is the Cybersecurity Act Proposal, which includes provisions on a European Cybersecurity Certification Framework**.

The proposed cybersecurity certification framework, which is currently with the co-legislators will aim to provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures. This will be based on an agreement at EU level for the evaluation of the security properties of a specific ICT-based product, service or process.

The certification framework will ensure that **ICT products, services and processes that have been certified in accordance with such a scheme comply with specified cybersecurity requirements.** The resulting certificate will be recognized in all Member States, making it easier for businesses to trade across borders and for purchasers to understand the security features of the product or service.

It is evident that businesses across the EU will **benefit** from the provisions of the Cybersecurity act and the proposed certification framework in particular.

Firstly, new markets will open up for industry.

Secondly, the harmonised **EU wide certification framework** will inherently promote the cross-border flow and exchange of secure ICT products and services. Businesses will be able to work with more homogeneous systems and should therefore require less resources in dealing with diverse compliance schemes.

Thirdly, the level of consumer **trust** will increase the confidence in EU products, services and processes.

Currently, **the landscape** of security certification of ICT products and services **in the EU is quite sparse**. This proposal should greatly increase the level of certification across Europe.

The role of ENISA

Throughout 2018, ENISA has worked alongside the European Commission and Member State authorities to assist in **planning a course of action for the transition to the new EU framework known as Cybersecurity Act.**

Furthermore **ENISA has engaged** with the industry (e.g. manufacturers, health care, IoT) and conformity assessment bodies alike to document their priorities and promote the merits of the framework.

ENISA has **also further developed its relationship** with the standardisation organisations in the EU (CEN and ETSI) and internationally (IEC) in an effort to provide a solid basis of cooperation that is likely to support the development of the certification schemes.

Closing Remarks

The EU has an opportunity to become **a global leader.**

By putting cybersecurity at the forefront of our efforts, the EU has the potential to set the scene and serve as the yardstick for other markets to compare against by **leveraging the collective experience and expertise** of the Member States and European industry.

ENISA, **since 2004**, acts as a centre of expertise dedicated to enhancing network and information security in the Union and supporting capacity building of Members States.

Ladies and gentlemen.

Ideas for **initial schemes** have already been suggested by the different stakeholders and the Agency is prepared to define a timeline with the Commission and the European Cybersecurity Certification Group (ECCG).

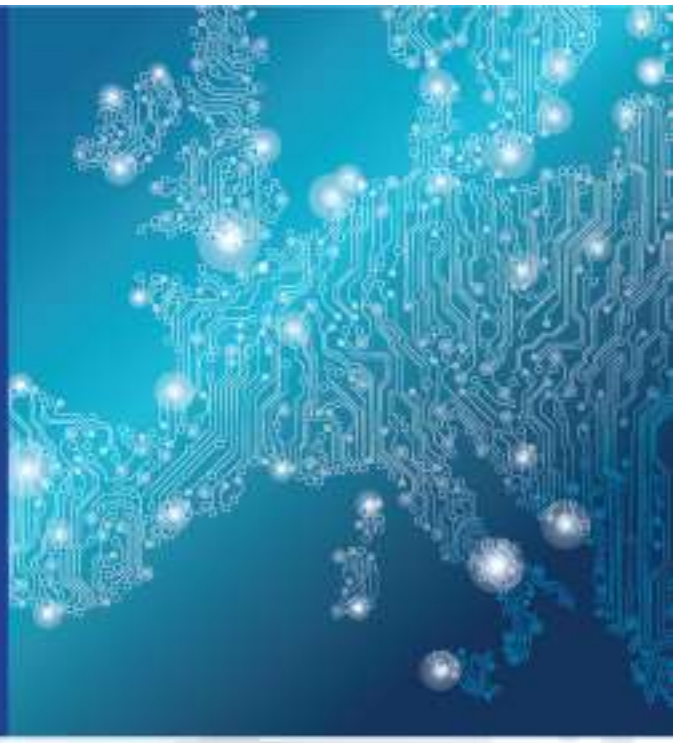
Over the past year, **ENISA has been working with all its stakeholder communities** to prepare them for contributing to the first schemes and we believe that the majority of these communities are also up-to-speed and ready to contribute.

The Agency has put together a **recruitment plan** to enable us to grow the certification activity in a consistent manner and is proactively recruiting for reserve lists so as to **have additional skill sets in house at the earliest moment.**

In conclusion, we have established the momentum in our stakeholder communities that is necessary to ensure an efficient start-up of this activity and are looking forward to a positive outcome from the political process in order to start.

I believe that acting together we will make Europe a better place.

Thank you for your attention.



ENISA

European Union Agency for Network
and Information Security
1 Vasilissis Sofias
Marousi 151 24, Attiki, Greece

Heraklion Office

Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

1 Vasilissis Sofias Str, Maroussi 151 24, Attiki, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu