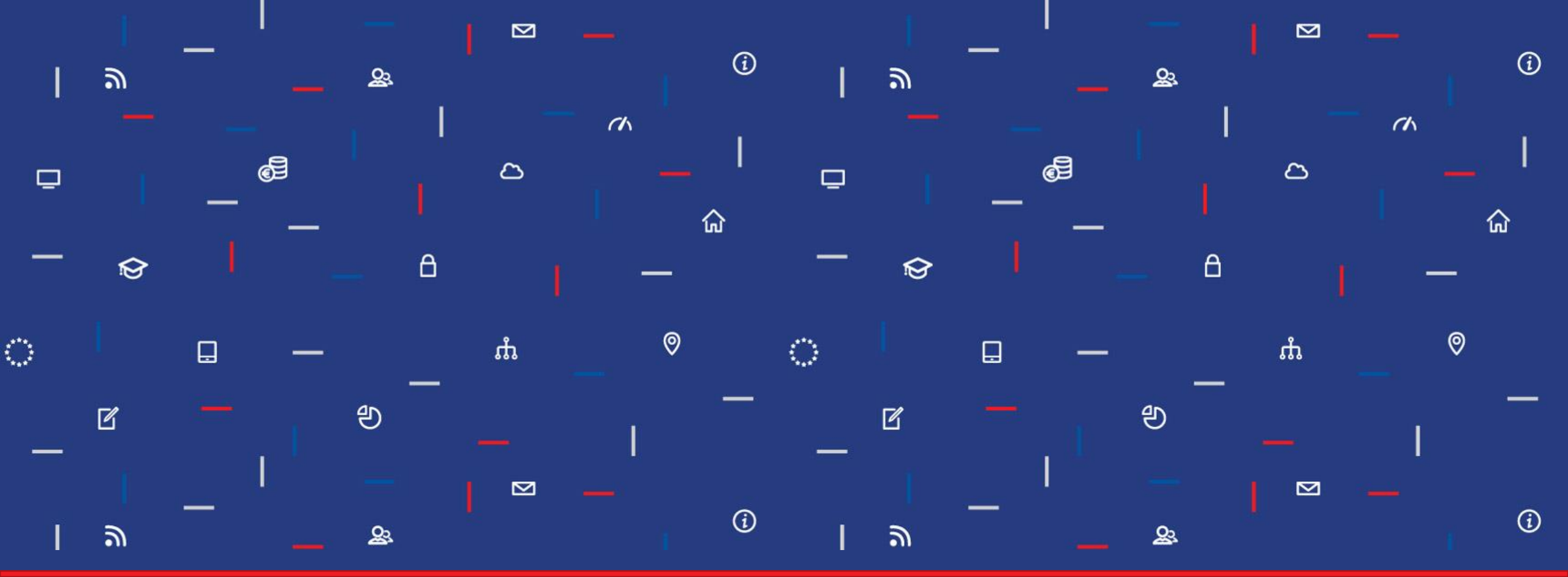

ÚRAD PODPREDSEDU VLÁDY SR
PRE INVESTÍCIE
A INFORMATIZÁCIU

Cyber security in the EU

Marek Canecky

Global Forum, 8 November 2019, Angers

Cybersecurity landscape in the EU

- Cybersecurity incidents are increasing at an alarming pace and could disrupt the supply of essential services we take for granted such as water, healthcare, electricity, financial or mobile services.
- Threats can have different origins including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes.
- Increasing dependence on digital technologies has made cybersecurity a critical issue requiring swift and coordinated action at EU level.

Cybersecurity landscape in the EU

- Since the first EU Cybersecurity Strategy of 2013, the EU has built solid regulatory and policy foundations and invested considerably in this area.
- The cybersecurity market is currently one of the fastest growing markets in the ICT sector with huge economic opportunities.
- Key legislative tools that strengthen the EU's cybersecurity industry and reinforce trust of citizens and businesses in the digital world: NIS Directive and Cybersecurity Act.

Network and Information Security Directive

- The NIS Directive has been the first piece of EU-wide legislation on cybersecurity (since 2016).
- Includes a number of requirements around cybersecurity incident response and the implementation of technical security measures based on risk.
- The requirements are designed to improve cross-border cooperation in information and network security and foster a culture of risk management.

Network and Information Security Directive

- It has created a network of Computer Security Incident Response Teams (CSIRTs) in each Member State that carry out a range of tasks, including monitoring national security incidents, disseminating early warnings, alerts, and announcements about cybersecurity.
- Each Member State is required to implement a national cybersecurity strategy.
- Digital Service Providers must implement a range of risk management measures both technical and operational.

EU Cybersecurity Act

- Since 27 June 2019, the EU Cybersecurity Act has established an EU-wide cybersecurity certification framework for digital products, services and processes.
- Companies doing business in the EU will benefit from having to certify their ICT products, processes and services only once and see their certificates recognised across the European Union.

EU Cybersecurity Act

- The use of certification schemes will be voluntary unless EU legislation prescribes an EU certificate as a mandatory.
- Certified conformity assessment bodies or conformity self-assessment.
- Three priority areas for certification: 1. IoT; 2. critical or high-risk applications; 3. security products, networks, systems and services (e.g. cloud services, 5G).

EU funding of cybersecurity

- Horizon Europe Programme (digital including cyber is one of the key priorities)
- Digital Europe Programme (2 bln. EUR earmarked for cyber)
- Connecting Europe Facility (3 bln. EUR earmarked for gigabit connectivity)
- Invest EU (digital including cyber is one of the key priorities)

What is expected in the future

- 2020 - Regulation on the European cybersecurity competence centre and network: the proposal aims to help the EU retain and develop the cybersecurity technological and industrial capacities necessary to increase the competitiveness of its cybersecurity industry and secure its digital single market.
- 2021 - Revision of the NIS Directive in view of the implementation practice and new technological developments
- ??? - Joint Cyber Unit announced by the new president of the European Commission

Thank you!

Štefánikova 15, 811 05 Bratislava
www.vicepremier.gov.sk