Digital Single Market

Cybersecurity

Securing network and information systems in the EU is essential to keep the online economy running and to ensure prosperity. The European Union works on a number of fronts to ensure cybersecurity in Europe, from raising the capabilities of the Member States to implementing the international cooperation on cybersecurity and cybercrime.

EU Strategies

The cybersecurity strategy for the European Union [1] and the European Agenda on security [2] provide the overall strategic framework for the EU initiatives on cybersecurity and cybercrime. The Digital Single Market Strategy also recognises the importance of trust and security. By completing the Digital Single Market [3], the EU could boost its economy by almost €415 billion per year and create hundreds of thousands of new jobs. But for new connected technologies and services to take off Europeans need trust and confidence.

Tackling cybersecurity challenges together is one of the three emerging challenges identified in the

mid-term review [4]. The actions to be implemented are:

- by September 2017, the Commission will review the EU Cybersecurity Strategy and the mandate of the European Union Agency for Network and Information Security (ENISA), to align it to the new EU-wide framework on cybersecurity.
- to propose additional measures on cybersecurity standards, certification and labelling to make connected objects more cyber secure.

For more details, read the Communication [5].

What are the key objectives of the Commission in the field of cybersecurity?

1. Increasing cybersecurity capabilities and cooperation

The aim is to bring cybersecurity capabilities at the same level of development in all the EU Member States and ensure that exchanges of information and cooperation are efficient, including at cross-border level. In this area, the Directive on security of network and information systems [6] (the NIS Directive) is the main instrument supporting Europe's cyber resilience.

1. Making the EU a strong player in cybersecurity

Europe needs to be more ambitious in nurturing its competitive advantage in the field of cybersecurity to ensure that European citizens, enterprises (including SMEs), public administrations have access to the latest digital security technology, which is interoperable, competitive, trustworthy and respects fundamental rights including the right to privacy. This should also help take advantage of the booming global cybersecurity market. To achieve this Europe needs to overcome the current cybersecurity market fragmentation and foster European cybersecurity industry. The Commission is working towards strengthening industrial capabilities [7] in Europe.

1. Mainstreaming cybersecurity in EU policies

The objective is to embed cybersecurity in the future EU policy initiatives from the start, in particular with regard to new technologies and emerging sectors such as connected cars, smart grids and the Internet of Things (IoT).

Engaging with Stakeholders

The public-private network and information security NIS Platform was set up under the EU Cybersecurity Strategy in June 2013, with the aim of identifying good practices that organisations, across the value chain, can follow in order to tackle cybersecurity risks. A special focus of the Platform is to help SMEs tackle such risks.

The progress of work and guidance [8] produced by the Platform can be followed on the NIS Platform portal [8].

ENISA and CERT-EU

These activities on network and information security are supported by the European Network and Information Security Agency [9], as well as by the Computer Emergency Response Team for the EU institutions (CERT-EU [10]).

International Activities

The EU is active in an EU-US Working Group on Cybersecurity and Cybercrime, as well as in other multilateral fora, such as the Organisation for Economic Co-operation and Development (OECD) [11], the United Nations General Assembly (UNGA) [12], the International Telecommunication Union (ITU) [13], the Organisation for Security and Co-operation in Europe (OSCE) [14], the World Summit on the Information Society (WSIS) [15] and the Internet Governance Forum (IGF) [16]. Strengthened network and information security will also help better deter cybercrime. The European Cybercrime Centre [17] is established within Europol and should act as the focal point for the fight against cybercrime in the EU.

Team responsible

DG CONNECT [18]

Published:
Thursday, 7 February, 2013
Last update:
Thursday, 11 May, 2017

Links
[1] http://ec.europa.eu/digital-single-market/news-redirect/9596
[2] http://europa.eu/rapid/press-release_IP-15-4865_en.htm
[3] https://ec.europa.eu/digital-single-market/en/digital-single-market
[4] https://ec.europa.eu/digital-single-market/news-redirect/58102
[5] http://ec.europa.eu/newsroom/document.cfm?doc_id=44527
[6] http://ec.europa.eu/digital-single-market/en/nis-directive
[7] https://ec.europa.eu/digital-single-market/en/cybersecurity-industry
[8] https://resilience.enisa.europa.eu/nis-platform/shared-documents
[9] http://www.enisa.europa.eu/
[10] http://cert.europa.eu/cert/plainedition/en/cert_about.html
[11] http://www.oecd.org/
[12] http://www.un.org/en/ga/
[13] http://www.itu.int/en/Pages/default.aspx
[14] http://www.osce.org/
[15] http://www.itu.int/wsis/index.html
[16] http://www.intgovforum.org/cms/
[17] https://www.europol.europa.eu/ec3
[18] https://ec.europa.eu/info/departments/communications-networks-content-and-technology_en