European Parliament

Press release

Cybersecurity: MEPs back rules to help vital services resist online threats

Plenary sessions [06-07-2016 - 13:15]

Firms supplying essential services, e.g. for energy, transport, banking and health, or digital ones, such as search engines and cloud services, will have to improve their ability to withstand cyber-attacks under the first EU-wide rules on cybersecurity, approved by MEPs on Wednesday.

Setting common cybersecurity standards and stepping up cooperation among EU countries will help firms to protect themselves, and also help prevent attacks on EU countries' interconnected infrastructure, say MEPs.

"Cybersecurity incidents very often have a cross-border element and therefore concern more than one EU member state. Fragmentary cybersecurity protection makes us all vulnerable and poses a big security risk for Europe as a whole. This directive will establish a common level of network and information security and enhance cooperation among EU member states, which will help prevent cyberattacks on Europe's important interconnected infrastructures in the future", said Parliament's rapporteur Andreas Schwab (EPP, DE).

The EU network and information security (NIS) directive "is also one of the first legislative frameworks that applies to platforms. In line with the Digital Single Market strategy, it establishes harmonised requirements for platforms and ensures that they can expect similar rules wherever they operate in the EU. This is a huge success and a big first step to establishing a comprehensive regulatory framework for platforms in the EU", he added.

EU countries to list "essential service" firms

The new EU law lays down security and reporting obligations for "operators of essential services" in sectors such as energy, transport, health, banking and drinking water supply. EU member states will have to identify entities in these fields using specific criteria, e.g. whether the service is critical for society and the economy and whether an incident would have significant disruptive effects on the provision of that service.

Some digital service providers - online marketplaces, search engines and cloud services - will also have to take measures to ensure the safety of their infrastructure and will have to report major incidents to national authorities. The security and notification requirements are, however, lighter for these providers. Micro- and small digital companies will be exempted from these requirements.

EU-wide cooperation mechanisms

The new rules provide for a strategic "cooperation group" to exchange information and assist member states in cybersecurity capacity-building. Each EU country will be required to adopt a national NIS strategy.

Member states will also have to set up a network of Computer Security Incident Response Teams (CSIRTs) to handle incidents and risks, discuss cross-border security issues and identify coordinated responses. The European Network and Information Security Agency (ENISA) will play a key role in implementing the directive, particularly in relation to cooperation. The need to respect data protection rules is reiterated throughout the

Press Service
Directorate for the Media
Director - Spokesperson : Jaume DUCH GUILLOT
Reference No:20160701IPR34481
Press switchboard number (32-2) 28 33000

directive.

Next steps

The NIS directive will soon be published in the EU Official Journal and will enter into force on the twentieth day after publication. Member states will then have 21 months to transpose the directive into their national laws and six additional months to identify operators of essential services.

Further information

- Adopted text will be available here

  : http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/en/pdf
- Video recording of debate (click on 05.07.2016)

  : http://www.europarl.europa.eu/ep-live/en/plenary/search-by-date
- Audiovisual material for media

  : http://audiovisual.europarl.europa.eu/default.aspx

Further information

- Interview with rapporteur Andreas Schwab: "Without fair protection at European level, we will be in trouble"
  : http://www.europarl.europa.eu/news/en/news-room/20160113STO09602/Cyber-security-Without-fair-protection-at-European-level-we'll-be-in-trouble
- EP Research - Publications on cybersecurity

  : http://www.europarl.europa.eu/thinktank/en/search.html?word=Cybersecurity&page=0
- Special Eurobarometer on cybersecurity, published in 2015

  : http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf?utm_source=webcomm&utm_medium=email&utm_campaign=ep_media_network
- NIS directive - text agreed by Parliament and Council

  : http://data.consilium.europa.eu/doc/document/ST-5581-2016-REV-1/en/pdf

Political groups

- News pages of the EPP group: http://bit.ly/1WuQLqB
- Press release by the S&D group: http://bit.ly/29ht2E0
- News pages of the ECR group: http://bit.ly/1Y0YFrj
- News pages of the ALDE group: http://bit.ly/1XbSQs6
- News pages of the GUE/NGL group: http://bit.ly/1UrAlM9
- News pages of the Greens/EFA group: http://bit.ly/1TV9vxr
- News pages of the EFDD group: http://bit.ly/1TUnDFU

Contact

Isabel Teixeira NADKARNI
BXL: (+32) 2 28 32198
STR: (+33) 3 881 76758
PORT: (+32) 498 98 33 36
EMAIL: imco-press@europarl.europa.eu
TWITTER: EP_SingleMarket