European Parliament

Press release

First-ever EU-wide cyber-security rules backed by Internal Market Committee

[14-01-2016 - 10:05]

Firms supplying essential services, e.g. for energy, transport, banking and health, or digital ones, such as search engines and cloud computing, will have to take action to improve their ability to withstand cyber-attacks under new rules approved by Internal Market MEPs on Thursday. These rules, informally agreed by MEPs and Council negotiators on 7 December, were approved by 34 votes to 2. They now need to be endorsed by the Council and the full Parliament.

The new directive for a high common level of security of network and information systems (NIS) across the Union aims to end the current fragmentation of 28 national cybersecurity systems, by listing sectors in which critical service companies will have to ensure that they are robust enough to resist cyber-attacks. These will also be required to report serious security breaches to national authorities.

"Parliament has pushed hard for a harmonised identification of critical operators in energy, transport, health or banking fields, which will have to fulfil security measures and notify significant cyber incidents. Member states will also have to cooperate more on cybersecurity – which is even more important in light of the current security situation in Europe", said rapporteur Andreas Schwab (EPP, DE), after a deal was reached last month on the NIS directive.

EU countries to list “essential service” firms

EU member states will have to identify concrete "operators of essential services" in these fields, using set criteria: whether the service is critical for society and the economy, whether it depends on network and information systems and whether an incident could have significant disruptive effects on service provision or public safety.

Some digital service providers, such as online marketplaces (e.g. eBay, Amazon), search engines (e.g. Google) and clouds, will also have to take measures to ensure the safety of their infrastructure and will have to report major incidents to national authorities. Micro and small digital companies will be excluded from the scope of the directive.

EU-wide cooperation mechanisms

To ensure a high level of security across the EU and to build trust and confidence among EU member states, the draft rules provide for a strategic "cooperation group" to exchange information and best practices, draw up guidelines and assist member states in cybersecurity capacity-building. Each EU country will be required to adopt a national NIS strategy.

Each EU member state 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 also play a key role in implementing the directive, particularly in relation to cooperation.

The need to respect data protection rules is reiterated throughout the text.

Next steps

The draft NIS directive will now be checked by lawyer-linguists before being endorsed by both Council and the full Parliament. It will then 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.

Note to editors

Information systems, essential networks and services, such as online banking, electricity grids or airport control, can be affected by security incidents caused by human mistakes, technical failures or malicious attacks. These incidents result in annual losses of €260 - €340 billion, ENISA estimates. The EU currently has no common approach on cyber-security and reporting.

In the chair: Vicky Ford (ECR, UK)

Further information

- Internal Market and Consumer Protection Committee: http://www.europarl.europa.eu/committees/en/imco/home.html
- NIS directive informal consolidated version after Coreper approval of 18.12.2015: http://data.consilium.europa.eu/doc/document/ST-15229-2015-REV-2/en/pdf
- Interview with rapporteur Andreas Schwab (EPP, DE): "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
- Special Eurobarometer on cybersecurity : http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf?utm_source=webcomm&utm_medium=email&utm_campaign=ep_media_network
- Procedure file: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2013/0027(COD)&l=en
- Profile of rapporteur Andreas Schwab (EPP, DE): http://www.europarl.europa.eu/meps/en/28223/ANDREAS_SCHWAB_home.html

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