Press release

Act together to counter cyber attacks, urges Civil Liberties Committee

Committees Committee on Civil Liberties, Justice and Home Affairs 06-06-2013 - 11:21]

Cyber criminals would face tougher EU-wide penalties, under a draft directive agreed by MEPs, Council and Commission negotiators last year and endorsed by the Civil Liberties Committee on Thursday. The new rules also aim to facilitate prevention and to boost police and judicial cooperation in this field. The deadline for replies to urgent requests for help will be eight hours.

Cyber attacks can strike anywhere. A cyber criminal may be in the Netherlands, his command-and-control centre in Germany, the compromised computers in Ukraine, and the attack directed at a bank in the UK.

"Cyber crime knows no borders. This directive introduces much-needed common rules for criminal law penalties, and also aims to facilitate joint measures to prevent attacks and foster information exchange among competent authorities", said rapporteur Monika Hohlmeier (EPP, DE).

Stricter penalties

The text would require member states to set their maximum terms of imprisonment at not less than two years for the crimes of: illegally accessing or interfering with information systems, illegally interfering with data, illegally intercepting communications or intentionally producing and selling tools used to commit these offences.

It also introduces new "aggravating circumstances" in order to counter the growing threat and occurrence of large-scale attacks against information systems more effectively. "Minor" cases are excluded, but it is up to each member state to determine what constitutes a "minor" case.

Attacks on critical infrastructure

The maximum term of imprisonment for attacks against "critical infrastructure", such as power plants, transport networks and government networks, would have to be at least five years. The same applies if an attack is committed by a criminal organisation or if it causes serious damage.

"Botnets"

The draft directive would also introduce a penalty of at least three years' imprisonment for using "botnets", i.e. establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber attacks.

Eight-hour deadline for urgent requests

Member states would be required to respond quickly to urgent requests for help in the event of cyber attacks, so as to render police cooperation more effective. They will have to make better use of the existing 24/7 network of contact points to respond to urgent requests within eight hours.

Press Service
Directorate for the Media
Director - Spokesperson : Jaume DUCH GUILLOT
Reference No:20130603IPR11005
Press switchboard number (32-2) 28 33000

Liability of legal persons

Legal persons, such as firms, would be liable for offences committed for their benefit (e.g. for hiring a hacker to get access to a competitor's database). Penalties could include exclusion from entitlement to public benefits or closure of establishments.

Next steps

The compromise text is to be voted by the full House in July and be formally adopted by the Council shortly thereafter. The new directive on cybercrime builds on rules that have been in force since 2005. The UK and Ireland have decided to take part in the application of this directive, but Denmark will not be bound by it.

Committee vote: 36 votes in favour, 8 against, 0 abstentions

In the chair: Juan Fernando López Aguilar (S&D, ES)

Contact

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