Press release

Hacking IT systems to become a criminal offence

Committees: Committee on Civil Liberties, Justice and Home Affairs

Cyber attacks on IT systems would become a criminal offence punishable by at least two years in prison throughout the EU under a draft law backed by the Civil Liberties Committee on Tuesday. Possessing or distributing hacking software and tools would also be an offence, and companies would be liable for cyber attacks committed for their benefit.

The proposal, which would update existing EU legislation on cyber attacks, was approved with by 50 votes in favour, 1 against and 3 abstentions.

"We are dealing here with serious criminal attacks, some of which are even conducted by criminal organisations. The financial damage caused for companies, private users and the public side amounts to several billions each year" said rapporteur Monika Hohlmeier (EPP, DE). "No car manufacturer may send a car without a seatbelt into the streets. And if this happens, the company will be held liable for any damage. These rules must also apply in the virtual world" she added.

The proposal would establish harmonised penal sanctions against perpetrators of cyber attacks against an information system - for instance a network, database or website. Illegal access, interference or interception of data should be treated as a criminal offence, MEPs say.

The maximum penalty to be imposed by Member States for these offences would be at least two years' imprisonment, and at least five years where there are aggravating circumstances such as the use of a tool specifically designed to for large-scale (e.g. "botnet") attacks, or attacks cause considerable damage (e.g. by disrupting system service), financial costs or loss of financial data.

IP spoofing

Using another person's electronic identity (e.g. by "spoofing" their IP address), to commit an attack, and causing prejudice to the rightful identity owner would also be an aggravating circumstance - for which MEPs say Member States must set a maximum penalty of at least three years.

MEPs also propose tougher penalties if the attack is committed by a criminal organisation and/or if it targets critical infrastructure such as the IT systems of power plants or transport networks.

However, no criminal sanctions should apply to "minor cases", i.e. when the damage caused by the offence is insignificant.

Cyber-attack tools

The proposal also targets tools used to commit offences: the production or sale of devices such as computer programs designed for cyber-attacks, or which find a computer password by which an information system can be accessed, would constitute criminal offences.

Press Service
Directorate for the Media
Director - Spokesperson : Jaume DUCH GUILLOT
Reference No:20120326IPR41843
Press switchboard number (32-2) 28 33000

Liability of legal persons

Legal persons would be liable for offences committed for their benefit (e.g. a company would be liable for hiring a hacker to get access to a competitor's database), whether deliberately or through a lack of supervision. They would also face penalties such as exclusion for entitlement to public benefits or judicial winding-up.

To resist cross-border cyber-attacks, Member States need to ensure that their networks of national contact points are available round the clock, and can respond to urgent requests within a maximum of eight hours, says the text.

Background

Large-scale cyber-attacks took place in Estonia in 2007 and Lithuania in 2008. In March 2009, public and private sector IT systems in more than 103 countries were attacked using a "zombie" network of compromised, infected computers.

Next steps

The Rapporteur aims for a political agreement between Parliament and Council on this Directive by the summer.

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

Contact :

Baptiste CHATAIN
BXL: +32 2 28 40992
PORT: +32 498 98 1337
EMAIL: libe-press@europarl.europa.eu