New EU directive against cyberattacks on information systems

The EU Directive on attacks against information systems (2013/40/EU) came into force on 3 September 2013. This Directive aims to harmonise European criminal laws that cover large-scale cyberattacks. The Directive requires the implementation of tougher criminal sanctions and the strengthening of cybercrime laws.

This information is available in English only.

The Directive replaces the existing Council Framework Decision (2005/222/JBZ). The main crimes defined in the Directive include illegal access to information systems, illegal system and data interference and illegal interception. With this Directive, member states are required to introduce more and tougher criminal sanctions, and to strengthen their anti-cybercrime laws for such crimes to the extent they are not considered “minor”. These crimes should at least be subject to sanctions of a maximum penalty ranging from two to five years imprisonment, depending on the severity of the offence. Legal persons should also be punishable, e.g. through fines and other measures.

Member states are also required to introduce criminal sanctions for the distribution of tools to commit such crimes. This provision is currently targeted at, inter alia, software used for the creation of botnets. With botnets, a cybercriminal can establish remote control over a multitude of computers by infecting it with malicious software. After infection, criminals can use the botnet without computer users’ knowledge or consent and launch a large-scale cyberattack through their respective computers. In view of the continuous development in hardware and software, the Directive does not regulate botnets specifically, but rather criminalises the distribution of all tools that have such purpose.

Another goal of this Directive is to improve the cooperation between member states and the competent European Union agencies, such as the European Cybercrime Centre, Europol, Eurojust and the European Network and Information Security Agency. In October 2013, the Dutch National Coordinator of Counter-Terrorism and Security announced that the Netherlands and Germany intend to collaborate more on the prevention of cyberattacks.

The impact of the Directive is likely to be limited in the Netherlands, as the offences mentioned above are already criminalised under Dutch law. However, the implementation of similar criminal provisions throughout the EU and the enhanced cooperation between authorities are anticipated to make fighting cybercrime easier and more effective.

Member states have until 4 September 2015 to comply with all the Directive’s provisions.