EU Law Enforcement Emergency Response Protocol

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

In order to provide law enforcement authorities in the EU with a tool for immediate response to major cross-border cyber-attacks, the Council of the EU adopted an EU Law Enforcement Emergency Response Protocol. The Protocol, on which Europol reported in March 2019, is part of the EU Blue-print for Coordinated Response to Large-Scale Cross-Border Cybersecurity Incidents and Crises of September 2017. It sets out a multi-stakeholder process with seven possible core stages beginning with the early detection and identification of a major cyber-attack. The next steps include threat classification, an emergency response coordination centre, early warning notification, a law enforcement operational action plan, investigation and multi-layered analysis, and ultimately, emergency response protocol closure.

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

ISSN: 1862-6947
https://eucrim.eu

The protocol determines the procedures, roles and responsibilities of key players both within the EU and beyond. It sets out secure communication channels and 24/7 contact points for the exchange of critical information; as well as the overall coordination and de-confliction mechanism.

The scope of the protocol only covers “cyber security events of a malicious and suspected criminal nature” and does not include incidents or crises caused by a natural disaster, man-made error or system failure.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and “criministrative” law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union