Council of the
European Union

Brussels, 31 May 2017
(OR. en)

9621/17

TELECOM 138
CYBER 86
COPEN 183
JAI 557
ENFOPOL 280

NOTE

From:	General Secretariat of the Council
To:	Council
Subject:	Cybersecurity - Information from the Commission

The recent *WannaCry* cyberattack where a wave of ransomware attacks impacted organizations and citizens across the globe was the first time where Member States exchanged information on cybersecurity incident within the mechanism for operational cooperation under the NIS Directive[1], the so-called Computer Security Incident Response Teams network[2]. This is yet another real-life example that proves how important cooperation in the area of cybersecurity is.

1 Directive (EU) 2016/1148 of the European Parliament and the Council concerning measures for a high common level of security of network and information systems, OJ L 194, 19.7.2016, p. 1.

2 CSIRTs network.

The impact of this global cyberattack was mitigated due to the actions taken by an individual researcher but it was still widely recognised as being unprecedented in scale. More importantly, the *WannaCry* attack provides a clear indication of the kinds of threats with which we are increasingly likely to be faced in today's highly connected and globalised society. Therefore it is important for Member States to grasp and make full use of the opportunities given by the cooperation mechanisms under the NIS Directive and ensure effective and timely transposition process. As a result of the transposition, identified operators of essential services in key economic sectors such as health and transport will have to comply with the legal requirements of the directive. In particular, the operators will need to take appropriate security measures and ensure resilience of their networks. Such security measures that include the timely updating of IT systems could for example mitigate the risks impacting the operator's systems against attacks such as the *WannaCry*.

In the context of the public response to the *WannaCry* attack, Europol (via its European Cybercrime Centre [EC3]) created a dedicated information page[3] and disseminated flyers and awareness materials via Europol social media channels. The information materials were also published on EC3's Secure Platform for Accredited Cybercrime Experts (SPACE), hosted on Europol's Platform for Experts (EPE). The NoMoreRansom page which was updated with tailored consumer advice[4] experienced a huge peak in visits between 12 and 16 May that showed the effectiveness of the measures.

Conclusions drawn from the attack include the need for CSIRTs, law enforcement authorities and the private sector to work together and the need for law enforcement authorities to have right tools to investigate these types of crimes and to prosecute criminals.

---

3 https://www.europol.europa.eu/wannacry-ransomware

4 available at: https://www.nomoreransom.org/prevention-advice.html

The current EU policy response to cyber threats is guided by the 2013 Cybersecurity Strategy. While a number of actions of this Strategy remain relevant, the threat landscape has evolved drastically. New threats include new actors and motives for cyber-attacks, cybercrime is on the rise; the 2013 Strategy does not address the Internet of Things whereas we expect tens of billions of devices to be connected to the internet by 2020. Therefore we need to consider how to further improve the EU's resilience, response capacity and cooperation in this field.

This is why the Digital Single Market mid-term Review[5] announced that the Commission, together with the High Representative will review the EU Cybersecurity Strategy in September. The Commission is also looking into the revision of the European Network and Information Security Agency (ENISA)'s mandate subject to the results of the ongoing evaluation exercise, as well as at establishing a certification framework for cybersecurity products.

The review of the Strategy is a common effort and a close cooperation with Member States is needed. Member States have been already consulted through a high-level Roundtable with VP Ansip (25 April) and detailed discussions in the Horizontal Working Party on Cybersecurity (22 March and 12 May) where further meetings are planned. The Commission also welcomes any additional input from Member States.

Furthermore ongoing efforts are made by the Commission in order to address the need throughout the EU to adapt our reaction to the reality of fast-evolving sophisticated cyberattacks and deliver concrete results, notably through stronger public-private partnerships and allowing for better access to electronic evidence for criminal investigations. The Commission is committed to improving criminal justice in cyberspace by addressing barriers to cross-border access to electronic evidence and on the role of encryption in criminal investigations.

---

[5] COM(2017) 228.