European Union Agency
for Cybersecurity

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

BRIEFING: IRISH EU AFFAIRS COMMITTEE

1. BACKGROUND

5 minutes to make opening remarks “The EU Cybersecurity Strategy (resumed)” followed by 5 mins opening remarks by Mr Ossian Smyth, Minister of State at the Department of Public Expenditure and Reform.

2. OPENING REMARKS

Incidents

- For the year 2020, ENISA received a total of 949 reports about cybersecurity incidents with significant impact including **742 from the critical sectors under the NIS Directive**. In 2019, 432 cyber incidents within critical sectors were reported to have a significant impact. This represents a **72% increase** of reported NIS incidents (with significant impact) between 2019 and 2020.
- In the health sector it was a 47% increase of significant cyber incidents from 2019 to 2020. A total of 262, up from 122 in 2019.

Irish HSE Ransomware attack

- The Irish HSE Attack is one such a cyberattack that had a very significant impact.
- It was a national level incident that could happen in a similar way in other MS, it represents a real case study of how to manage a crisis, and what are the issues at stake in an incident of such magnitude
- It was an example from which lessons either learnt for the management of large-scale incidents and crisis, at national or at EU level, can be extracted, hence the EU Agency for Cybersecurity created a lessons learnt document that was shared amongst other national incident response teams across the EU.

Resilience and the NISD

- In the area of European legislation the **EU policy/regulatory response** has come in the form of the NISD, which among other things aims at increasing collaboration between EU Member States and the public and private sectors, establishes EU-wide cooperation and cyber-resilience mechanisms.
- As the first piece of EU-wide cybersecurity legislation, the NISD has had an important impact

- 70 or so entities in Ireland were designated OES
- The differences in reporting across Member States poses a challenge to understanding the true number of cyber incidents and attacks in the EU.
- Although the directive is bearing its first fruit; we have also noted gaps such as the incident reporting that have appeared since the directive was negotiated.
- This is important to streamline this so that when a cyber incident takes place across borders then the entity would not need to report this separately and with different criteria in all 27 MS.
- The current NIS2 proposal aims to further strengthen the resilience of key services, expand the scope of the sectors it covers, consolidate vital information on vulnerabilities and engage more with the private sector. It has just received a unique cross-party consensus in the European Parliament and will be a key milestone for the EU Member States to adopt in early 2022. Irish support for a strengthened NIS2 package remains a key piece of the puzzle in getting this through.