European Commission

HITTING THE REFRESH BUTTON ON CYBERSECURITY RULES

NIS2: PROPOSAL FOR A DIRECTIVE ON MEASURES FOR HIGH COMMON LEVEL OF CYBERSECURITY ACROSS THE UNION

16 December 2020
#SecurityUnion #DigitalEU

The first EU-wide law on cybersecurity, the NIS Directive, came into force in 2016 and helped achieve a higher and more even level of security of network and information systems across the EU. In view of the unprecedented digitalisation in the last years, the time has come to refresh it.

How?

Greater capabilities

NIS

EU Member States improve their cybersecurity capabilities.

NIS 2

More stringent supervision measures and enforcement are introduced.

A list of administrative sanctions, including fines for breach of the cybersecurity risk management and reporting obligations is established.

Cooperation

Increased EU-level cooperation.

Establishment of European Cyber crises liaison organisation network (EU- CyCLONe) to support coordinated management of large scale cybersecurity incidents and crises at EU level

Increased information sharing and cooperation between Member State authorities with enhanced role of the Cooperation Group.

Coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU is established.

Cybersecurity risk management

Operators of Essential Services (OES) and Digital Service Providers (DSP) have to adopt risk management practices and notify significant incidents to their national authorities.

Strengthened security requirements with a list of focused measures including incident response and crisis management, vulnerability handling and disclosure, policies and procedures to assess the effectiveness of cybersecurity risk management measures, basic computer hygiene practices and cybersecurity training, the effective use of cryptography, and human resource security, access control policies and asset management.

Cybersecurity of supply chain for key information and communication technologies will be strengthened.

Accountability of the company management for compliance with cybersecurity risk-management measures.

Streamlined incident reporting obligations with more precise provisions on the reporting process, content and timeline.

SECTORS COVERED BY THE NIS DIRECTIVE

NIS

- HEALTHCARE
- TRANSPORT
- BANKING AND FINANCIAL MARKET INFRASTRUCTURE
- DIGITAL INFRASTRUCTURE
- WATER SUPPLY
- ENERGY
- DIGITAL SERVICE PROVIDERS

NIS 2

Expanded scope to include more sectors and services as either essential or important entities.

- PROVIDERS OF PUBLIC ELECTRONIC COMMUNICATIONS NETWORKS OR SERVICES
- DIGITAL SERVICES SUCH AS SOCIAL NETWORKING SERVICES PLATFORMS AND DATA CENTRE SERVICES
- WASTE WATER AND WASTE MANAGEMENT
- SPACE
- MANUFACTURING OF CERTAIN CRITICAL PRODUCTS (SUCH AS PHARMACEUTICALS, MEDICAL DEVICES, CHEMICALS)
- POSTAL AND COURIER SERVICES
- FOOD
- PUBLIC ADMINISTRATION

© European Union, 2020
Reuse is authorised provided the source is acknowledged. The reuse policy of European Commission documents is regulated by Decision 2011/833/EU (OJ L 330, 14.12.2011, p. 39). For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders. All images © Getty Images Plus / iStock / DigitalVision Vectors

Publications Office of the European Union

PDF ISBN 978-92-76-27602-9 doi: 10.2759/0630 KK-02-20-102-EN-N
BOOK ISBN 978-92-76-27603-6 doi:10.2759/7745526 KK-02-20-102-EN-C

Updated 2022-05-11