DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Press release

European Parliament adopts new legislative rules to strengthen the cyber resilience of the European Union as a whole – NIS2 and DORA

Bucharest, 11 November 2022

On 10 November 2022, the European Parliament adopted new rules to strengthen cyber resilience across the European Union (EU).

In order respond to the growing threats posed by digitalisation and the intensification of cyber-attacks, the European Commission has put forward a proposal to replace the Network and Information Security (NIS) Directive, and thereby strengthen security requirements, address supply chain security, streamline reporting obligations and introduce more stringent enforcement measures, including harmonised sanctions across the EU.

Thus, Parliament adopted the "NIS2" Directive, which imposes stricter cybersecurity rules on EU Member States for risk management, reporting and information exchange. Requirements address, among others, incident response, supply chain security, encryption and vulnerability disclosure.

More entities and sectors will need to act to protect themselves. Key sectors such as energy, transport, banking, health, digital infrastructure, public administration and space will be covered by the new security provisions.

The new norms imposed by the NIS2 Directive will also protect important sectors such as postal services, waste management, chemicals, food, medical devices, electronics, machinery, motor vehicles and digital suppliers. All medium-sized and large companies in certain sectors would be subject to legislation.

Consequently, the NIS2 Directive applies to all economic entities that reach or exceed the standards for medium-sized enterprises. The Romanian National Cybersecurity Directorate (NCSD), a specialised body of the central public administration that is responsible for the cybersecurity of the national civil cyberspace, component of national security, as the competent authority at national level for the security of network and information systems, has already started the process of setting legislative priorities and will lead the implementation of the NIS2 Directive at national level.

The NCSD will also consider the inclusion of micro and small enterprises that meet specific criteria indicating a key role in the list of operators of essential/important services. Essential/important entities may already be required to certify certain IT &C products, services and processes based on European cybersecurity certification schemes, adopted in accordance with Article 49 of Regulation (EU) 2019/881.

The NIS2 Directive proposes a new approach for important actors, essential entities and important entities, i.e. the economic sectors, 11 essential sectors and 7 important sectors.

Essential Entities

• 11 sectors: Energy, Transport, Banking, Financial Market, Health, Drinking Water, Waste Water, Digital Infrastructure, Public Administration, IT&C Service Management (B2B) and Space.

• 9 subsectors: Electricity, Central heating and cooling, Oil, Gas, Hydrogen, Air transport, Rail transport, Water transport and Road transport.

Important Entities

• 7 sectors: Post mail; Courier, Waste Management, Manufacture, Production and Distribution of Chemicals, Food, Manufacture, Digital Suppliers and Research.

• 6 subsectors: Medical devices, Computers, electronic and optical products, Electrical equipment, Machinery and equipment n.e.c. (not elsewhere classified), Motor vehicles, trailers and semi-trailers, Transport equipment.

The NIS2 Directive also addresses new methods for the ongoing trainings of employees in the field of cybersecurity, the use of encryption, the use of multi-factor authentication solutions and the introduction of secure voice, video and text communications.

In addition to the NIS2 Directive, the European Parliament has adopted the **Digital Operational Resilience Act** (DORA), which will harmonise and strengthen digital operational resilience requirements for the EU financial services sector. The bill sets out requirements for protection against attacks, detection, limitation, restauration and recovery from Information and Communication Technology (ICT) incidents. These requirements will be associated with digital reporting and testing capabilities.

The new DORA rules will apply to banks, payment providers, e-money providers, investment firms, crypto-asset service providers, and third-party ICT service providers that are regulated at EU level.

According to Frances Fitzgerald, member of the European Parliament, "*Financial institutions and companies, including crypto space, hold highly sensitive customer information and it is vital that EU-wide digital security measures are implemented to overcome the threat that exists. We need to implement stronger safeguards for our citizens. We don't want anyone's personal financial information to be hacked*".

In Romania, NCSD, the competent authority at national level for the security of networks and information systems, together with the National Bank of Romania and the Financial Supervisory Authority, will identify the best conditions required to ensure the cybersecurity of the networks and information systems, specific to the banking sector and financial market infrastructure.

Press contact: Mihai Rotariu | mihai.rotariu@dnsc.ro | 0740 066 866