Implementing the EU's NIS Directive in Romania

Back to Technology Law Committee publications

Alina Popescu
MPR Partners, Maravela, Popescu & Roman, Bucharest
alina.popescu@mprpartners.com

Flavia Stefura
MPR Partners, Maravela, Popescu & Roman, Bucharest
flavia.stefura@mprpartners.com

Background

Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the European Union (the 'NIS Directive') was adopted on 6 July 2016.

The Directive aims at achieving a high common standard of network and information security across Member States, in the context of the ever increasing importance of networks and information systems to European economies.

EU Member States had until 9 May 2018, to adopt legislative acts for the transposition of the Directive. Romania published Law 362/2018 concerning the assurance of a high common level of security of networks and information systems (the 'NIS Law') transposing the NIS Directive on 9 January 2019.

Romania has designated the Romanian Computer Incidence Response Team (CERT-RO) as the national authority charged with supervising network and information systems security. CERT-RO also acts as a single point of contact to ensure cooperation with the

national authorities in other Member States, as well as national response team to security incident ('national CSIRT').

Romania’s ongoing legislative process in implementing the NIS Directive

Romania published secondary legislation for the implementation of the NIS Law, namely:

• a Government Decision amending the legislation regarding the setting up of the CERT-RO;

• three Orders of the Minister of Communications and Information Society regarding: (a) identification of operators of essential services (OESs) and digital service providers (DSPs), (b) the organising and functioning of the registry of OESs, and (c) the methodology for establishing the disruptive effect of incidents over networks and information systems; as well as;

• guidelines for the identification of OESs and DSPs, as well as for preparing the self-evaluation documentation as regards minimum security measures.

However, the legislative process is not yet completed, as more secondary legislation still needs to be enacted. According to the NIS Law, the Romanian Government further needs to adopt government decisions on:

• the list of essential services;

• threshold values for establishing the disruptive effect of incidents over networks and information systems, as well as the inter-sector criteria and the sector-specific criteria for assessing disruptive effects of incidents;

• technical norms for establishing the impact of incidents over networks and information systems over each category of OESs and DSPs; and

• the membership, attributions and organisation of the inter-institutional working group determining the threshold values needed to assess the significant disruptive effect of incidents at the level of computer networks and systems of the OESs.

The Ministry of Communications and Information Society also needs to adopt orders for establishing requirements, rules and regulations regarding:

• teams for response to information security incidents (CSIRTs) and related services;

• the minimum network and information systems security requirements;

• security auditors; and

• control of the fulfilment of the security obligations by OESs and DSPs.

According to the NIS Directive, Member States must develop national strategies on the security of network and information systems. Romania has yet to develop such a strategy, even though the NIS Law provides that the strategy would have to be adopted within six months of the new law entering into force.

CERT-RO is tasked with elaborating:

• common guidelines and practices for administering risks and incidents;

• guidelines for minimum security measures for OESs and DSPs;

• forms for notifying security incidents and details on the documentation that needs to be provided;

• lists of the European and international standards and specifications used in security auditing;

• the themes and subjects for auditor specialisation and forming of CSIRT teams; and

• norms for establishing the attributions of the personnel empowered with the supervising the observance of the NIS Law.

The lack of having the NIS legal framework in place and fully functional creates difficulties for the subjects of the NIS Law, namely the OESs or DSPs.

OESs can be service providers active in the following sectors: energy (ie, electricity, oil and gas); transport (ie, air transport, rail transport, water transport and road transport); banking, financial market infrastructures; health (ie, health care settings, including hospitals and private clinics); drinking water supply; and distribution and digital infrastructures (ie internet exchange points, domain name systems service providers and top-level domain name registries).

DSPs, namely service providers of online market places, online search engines and cloud computing, are also subject to the NIS Law.

OESs and DSPs have specific obligations with respect to applying appropriate security measures and notifying security incidents to the national competent authorities.

OESs and DPSs must notify CERT-RO in order to be registered in national registries. In order to do that, a company must determine whether it qualifies as OES or DSP by carrying out an identification process.

Determining whether an undertaking is an OES

An undertaking with economic activity in at least one of the NIS sectors must first conclude a self-assessment of whether it qualifies as an OES. The process involves three stages: (1) identifying essential services; (2) notifying CERT-RO about being an OES; and (3) evaluation by CERT-RO and registration in the registry of OESs.

Identification of the essential services also involves three stages: (1) cataloguing the importance of the service; (2) identifying whether the service uses networks or information systems; and (3) establishing the disturbance effect of an incident.

Cataloguing the importance of the service

A service is deemed essential if it: (1) is essential for the maintenance of critical societal and/or economic activities; (2) the provision of that service depends on network and information systems; and (3) an incident would have significant disruptive effects on the provision of that service.

As mentioned above, the Romanian government has still to draw up a list of essential services, which should be updated every two years. Currently, such a list is in the form of a draft government decision that has not yet been approved.

If the service provided by the undertaking is on the government list, then the evaluation process continues. If that service is not on the list, the undertaking will conduct an internal assessment of the service's importance, and continue or stop the evaluation according to its findings.

Identifying the modalities of providing the service

If the services provided by the undertaking are dependent on networks and information systems, the assessment proceeds to the next step. If not, then such services are not essential and the undertaking is not an OES.

Establishing the degree of disruptive effects of incidents on the provision of that service

The final step in the identification process will be evaluated by taking into consideration inter-sector and sector-specific criteria.

The undertaking will take into consideration the following inter-sector criteria, which are not cumulative:

- (1) the number of users relying on the service provided by the entity concerned;
- (2) the dependency of other essential sectors on the service provided by that undertaking;
- (3) the impact that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
- (4) the market share of that undertaking;
- (5) the geographic spread with regard to the area that could be affected by an incident;
- (6) the importance of the undertaking for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.

The inter-sector and sector-specific criteria are currently set out in the methodology approved by Order of the Minister of Communications and Information Society no 601/2019. The undertaking will first analyse the inter-sector thresholds. To the extent the inter-sector analysis is inconclusive, a specific-sector analysis will be performed. In case an effect or risk of disturbance is noticed in this stage, the service is deemed essential and the undertaking notifies CERT-RO for it to be registered in the OES registry. CERT-RO will then make its own evaluation of whether the undertaking is an OES and, if the status is confirmed, registers the undertaking in the OES registry.

Determining whether an undertaking is a DSP

An undertaking may register a DSP following a self-evaluation process. If the undertaking provides services of an online market place, of an online search engine or a cloud computing service, then the undertaking is a DSP. To the extent the undertaking is a small or medium company, it will not be qualified as a DSP.

After the self-assessment phase, the DSP notifies CERT-RO of its finding and CERT-RO performs its own evaluation. After registration, CERT-RO monitors and controls the application of all obligations for OSEs and DSPs.

Turnover-based fines

OESs and DSPs must implement minimum security measures regarding network and information systems, meant to prevent or minimise the impact of incidents that hinder the continuity of essential services and digital services. Such incidents must be reported to CERT-RO.

Failures of OESs and DSPs to comply with their legal obligations regarding network and information systems security constitute administrative offences, sanctioned by fines ranging between RON3,000 (approximately €625) to RON50,000 (€10,400). If the turnover of the OES or DSP in the year preceding the offence is greater than RON2m (approximately €416,650), the fines range between 0.5 per cent and two per cent of that turnover. For repeated offences, fines may increase to five per cent of the turnover.

What to expect

As mentioned above, several normative acts have still be adopted by the Romanian authorities. Although the NIS Law provides that OESs are required to identify themselves and notify CERT-RO, the fact that the legal framework is not fully adopted makes this obligation unenforceable. However, certain OESs have already performed the self-assessment on a voluntary basis, and they are now registered with CERT-RO. Consequently, the undertakings which have already registered must pay attention to observing the obligations in forthcoming legislation.

Unlike OESs, DSPs can already identify themselves to CERT-RO. However, even in their case, part of the relevant requirements must still be defined by the forthcoming legisla-

tion, such as, for example, the minimum security measures to be implemented by DSPs, which need to be established by CERT-RO.

Considering all of the above, OSEs and DSPs should keep up-to-date with legislative developments and liaise with CERT-RO for guidance in applying the law. Given the potential high fines for non-compliance, it is important to start the compliance process as early as possible. It is reasonably expected that fines will be applied as soon as the secondary legislation has been finalised.