CISPE.cloud

9 October, 2017

CISPE Response
to the draft implementing Regulation on security and notification obligations for Digital Service

CISPE (Cloud Infrastructure Service Providers in Europe) welcomes the opportunity to provide feedback on the draft Commission Implementing Regulation that concerns the security and notification obligations of so-called "digital service providers" (DSPs) which will help implement the Network and Information Security (NIS) Directive.

CISPE supports the objectives of the NIS Directive and would like to reiterate the importance of an implementation that is true to its intended outcome, especially regarding the definition of substantial impact, which triggers the obligation for DSPs to notify an incident. It is crucial that the implementing Regulation reflect the "light-touch approach" agreed by Council and the European Parliament in this regard.

This "light touch" approach is of the upmost importance for medium European companies to allow them to comply with the implementing Regulation without stifling their development. We are concerned that costly and complex systems to implement could change the structure of the European Cloud market, and in particular the Infrastructure as a Service (IaaS) market, which is mainly made by SMEs.

1. DSP obligations should not be stricter than those for Operators of Essential Services

We are concerned that with proposed Regulation DSPs' obligations could become stricter than those of Operators of Essential Services (OES). Given the *non-essential* nature of the DSPs services and operations as specified in the Recital 49 of the NIS Directive, the degree of economic and societal risks for an incident affecting OESs (e.g. banking sector) would be expected to be substantially higher than for an incident involving a DSP (e.g. cloud computing service provider, marketplace and search engines).

2. A definition of substantial impact that is proportionate and fit for purpose

The "light-touch approach" is also reflected in the definition of a substantial incident in the NIS Directive. The threshold for triggering an incident report for a DSP is markedly higher than for an OES. It is determined by more parameters, most of which focus on service availability, ensuring that only substantial incidents are notified. In this regard, CISPE would like to raise your attention to the following provisions:

2.1 The service provided by a digital service provider was unavailable for more than 5 000 000 user hours whereby the term user hour refers to the number of affected users for a duration of sixty minutes (Art. 4a)

CISPE proposes to exclude the unavailability of the service for voluntary maintenance purposes.

2.2 The incident has resulted in a loss of integrity, authenticity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via a network and information system of the digital service provider affecting more than 100 000 users in the Union (Art. 4b)

CISPE understands the term "user" should apply to "paying customer in a contractual agreement" (e.g. the first layer of customers, excluding end-users). CISPE would like to clarify the definition of the term "user" and whether 100 000 users is an appropriate number depending on that definition. Additionally, the definition of the timeframe of this requirement should clarify if it applies to 1 incident or cumulative incidents.

CISPE proposes to the term, "user" is applied to "paying customer in a contractual agreement". CISPE also asks to define timeframe and if it is applied to one incident.

2.3 The incident has created a risk for the public safety (Art. 4c)

The term "public safety" has not been defined at EU level which leaves room for Member States' interpretation. The risk is that a broad interpretation of the term "public safety" can undermine the entire "light touch approach" for DSPs.

It is difficult to see how DSPs activities can create a risk for public safety. If the service is not available, customers will still have the option to use another service. Additionally, cloud service providers will not be able to determine this aspect since only the end user using the service would have that insight.

CISPE proposes to remove this provision from the Regulation since we believe it is not fit for purpose.

2.4 The incident has affected the provision of the services in two or more Member States (Art. 4e)

As DSPs approach the EU single market as a common market it would be disproportionate to order incident reporting whenever it affects two or more countries, which is often the case. Cross border trade is the modus operandi of DSPs operating within the Digital Single Market. Therefore, this provision will classify every incident as having a substantial impact. Moreover, DSPs will have stricter obligations than OES which goes against the aims of the Directive and the light-touch approach granted for DSPs.

Alternatively, we encourage the Commission to support a more flexible wording such as 'In case the incident met one of the above criteria, the DSP will communicate the affected Member States'.

3. DSPs obligations and limited resources of medium companies

Some of the provisions seem to be very difficult if not impossible for medium companies to implement as they are both too costly and would require radical disruption in how they currently operate. In particular:

- Recital 7 which refers to segregation of networks and systems
- Disaster recovery capabilities referred in Art. 2.3b

CISPE is concerned that new obligations are not fit for medium companies and would change the structure of the European cloud market which is mainly made of them.

CISPE proposal is to delete those provisions or to exclude medium companies from their scope.

4. A requirement to report vulnerabilities that is balanced

According to the implementing regulation, DSPs are required to develop processes and procedures on reporting vulnerabilities and identified weaknesses in information systems. Vulnerabilities are possible impacts that may or may not materialize over the course of years. There are many instances in which a vulnerability has no impact on an information system and can be easily remediated. DSPs should not be required to report on every conceivable vulnerability.

We suggest removing this provision from Art. 2.2 b since it could be unduly burdensome for companies and has little value for competent authorities.

We trust that CISPE suggestions will be taken into consideration to ensure that the implementation of the "light-touch approach" as envisaged in the NIS Directive. CISPE is happy to constructively engage with all stakeholders involved in the implementation of this crucial piece of EU cybersecurity legislation.

***