Warsaw, July 25, 2024

On behalf Member Polish Computer Society I have a honor submit the following comments regarding draft of

Commission Implementing Regulation for laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures

Team members:

Elżbieta Andrukiewicz

Paweł Jasionowski

Rafał Kołodziejczyk

Marek Ujejski marek_u@onet.pl

No	Page	Row	Comments	Proposal	Justification
1.		General	The Regulation imposes the approach to risks related to network and information security which is flawed: it discusses in detail only one risk factor (severity of consequences)	The whole approach should be reconsidered to include second risk factor i.e. likelihood of incident occurrence, not only incident severity. One possible option is to convert the content of Annexes into Regulation itself and current content of the Regulation into the	In NIS2 Directive, art. 21 (1) second subparagraph it reads: "*the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed.* ***When assessing the proportionality of those measures****, due account shall be taken of the degree of the entity's exposure to risks, the entity's size and the* ***likelihood of occurrence of incidents*** *and* ***their severity****, including their societal and economic impact*." Likelihood of incidents is assessed based on many factors

				Annex related to risk assessment methods.	i.e. motivation, means and opportunities, according to well-known methodology called CTI (Cyberthreat Intelligence). Clear overrepresentation of the consequence factor could lead into a false impression that risk is measured by consequences and their severity only.
2.		General	Many quantitative parameters are given as criteria to qualify the incident as significant one	Provide justifications for all quantitative parameters used in the Regulation (should be defined in the Preamble)	For several ICT services unavailability parameters are more stringent than '1o second' 'one hour', 5%, 1 million, etc.
3.		Art 3(3)	"Planned consequences of maintenance operations carried out by or on behalf of the relevant entities shall not be considered to be significant incidents."	Remove it	Usually, the maintenance outage is planned, and such activity is a part of normal operation. Consequence is defined as the result of unwanted and unplanned incident. Therefore, 'planned consequences' seems to contradict each other.
4.	9	Art 3.1 (a)	Proposed threshold of 100000 EUR for financial loss does not take under consideration significant differences in purchased of services among European Union Members.	Consider to delete constant amount and keep only percentage value of 5% as drafted.	The result of unifying the threshold to constant amount led to the different probability of reaching the same threshold in different European Union countries and can be considered as unequal treatment of different service providers.
5.	9	Art 3.1 (b)	The incident has caused or is capable to causing considerable reputational damage to the relevant entity	Clarify the "considerable reputational damage" (lack of definition)	Considerable reputational damage can be interpreted differently by a different entity. Legal definition of this term would provide the basis for the understanding of the reporting obligation.
6.		Art 4	"they have occurred at least twice within 6 months" – such criterion could not fit into all types of significant incidents	Change to: "they have occurred twice or more times within defined time period"	For some types of services (e.g. DNS) one can imagine that significant incidents could happen more frequently than twice a year.

7.		Art 8 b)	"the customer service level agreement for one or more of the data centre services of one or more of the data centres operated by the provider is not met for a duration of more than one hour"	Change to (..) "is not met for a duration longer than critical value set up in the SLA"	For high-availability systems (Tier 3/4) one hour is far beyond the SLA critical parameter. It's depended on contract signed with customer
8.		Art 8 e)	"physical access to one or more of the data centres operated by the provider is compromised." – this criterion is not sufficient, one could enter first gate in a multizone Data Center not even touching sensitive data or critical infrastructure	Change to "physical access to one or more of the data centres operated by the provider resulted in loss of confidentiality, integrity or availability of sensitive data"	To indicate that unauthorized physical access is not the incident, but it could lead to the (significant) incident.
9.		Art 10 c)	"the availability of one or more of the managed or managed security services of a provider that **has no customer service level agreement in place** is impacted by the incident;" – is not understandable. Why the case of 'not having the SLA in place' is a criterion for significant incident?	clarify or remove it	One can understand the provision that ANY, even minor incident is qualified as significant only because the customer does not have the SLA
10.		Art 14 d)	"physical access to one or more of the areas where network and information systems are located and to which access is restricted to trusted personnel of the trust	Change to "physical access to one or more of the areas information systems are located resulted in loss of confidentiality, integrity or availability of sensitive	To indicate that unauthorized physical access is not the incident, but it could lead to the (significant) incident and to unify the provision with Art 8 e).

			service provider, or the protection of such physical access, is compromised; - the same question as for art 8 e)	data;”	