Committed to Europe

Orange's position on the European Commission's proposal to review the Network and Information Systems Directive (EU) 2016/1148

Executive Summary

Orange welcomes the proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS 2), as part of a wider set of existing legal instruments and upcoming initiatives aimed at increasing the resilience of public and private entities against threats.

An important novelty is that NIS 2 emphasises the risk management of the ICT supply chain, but without directly addressing obligations to ICT providers, notably software and hardware manufacturers. Supply chains have always been and are becoming even more global and complex with a multitude of parties involved, while telecommunications networks are undergoing an ever-increasing network sophistication, given the shift to 5G and to virtualised, software-based and cloud infrastructure. To ensure efficiency, it is crucial that NIS 2 targets the right players with ad-hoc cyber security liabilities.

Orange considers that the current proposal raises a number of issues that need to be addressed in the ongoing legislative process:

- NIS 2 introduces cyber security obligations on the ICT supply chain on all entities, including the telecom sector. Orange calls for directly addressing cyber security obligations to key software and hardware ICT providers as they are in a better position to analyse and mitigate their own cyber security vulnerabilities. Such hardware and software providers should be designated as essential entities themselves.
- NIS 2 introduces an obligation to notify "potential" incidents within a very short timeframe – 24 hours, with very high levels of maximum sanctions in case of non-compliance. Orange highlights that reporting "potential" (in addition to significant) incidents could cause inaccuracies and administrative overload. In addition, the 24 hours delay for significant incidents is too short and should be lengthened. Sanctions for non-compliance are excessive and should be proportionate.
- NIS 2 offers the possibility to entities established in multiple EU territories to centralise incident management and reporting under the jurisdiction of the Member State where they have their main establishment in the Union. In parallel, Orange requires to maintain the current possibility to have legal establishments in multiple EU Member States to ensure legal certainty and operational efficiency.
- The inclusion of "data centers" within the scope of the NIS 2 is based on a broad definition that creates legal uncertainty and should be reviewed.

NIS 2 should directly address key providers of hardware and software

NIS 2 Art. 18 establishes that both essential and important entities, including the telecom sector, "shall take appropriate measures" to assess and mitigate the security level of all the ICT products and services they rely on. This obligation is not feasible because telecom operators do not have the exhaustive knowledge of hardware and software conception, do not have access to the code nor to the chipsets design of all the ICT they deploy in their networks. Telecom operators conceive design and build the networks and can establish which IT support their critical applications run upon, so they can identify which IT is critical for their functioning. Hardware and software providers are the only players in a position to analyse and mitigate their own cyber security vulnerabilities.

Orange therefore calls for substantial changes to the proposed liability chain in Art. 2 and Art.18. NIS 2 should be extended in scope to include hardware and software manufacturers key for essential entities. Telecom operators should be in charge of identifying the IT system, products or services that support their critical applications. The software and hardware manufacturers of such key applications should become essential entities themselves.

In addition, Art. 21 enables Member States to require both essential and important entities to certify specific ICT products, services and processes in relation to the EU Cybersecurity Act. The Commission is in charge of adopting delegated acts specifying which categories of essential entities shall be required to obtain a certificate and under which specific European cybersecurity certification schemes. These products may be developed by an essential or important entity or procured from third parties.

Orange shares the view that certification of key ICT products/services/systems is important, but it is the vendors that should be responsible for such certification. The list of ICT products to be certified should be established according with Art. 18.1 risk assessment.

A streamlined and more meaningful incident reporting & sanctions

The proposed reporting obligations need to better define and limit what, when and to whom entities should report, only significant and tangible incidents:

- Potential incidents: NIS 2 Art. 20 would expand reporting obligations, including having in place a risk analysis procedure to identify and manage potential threats. This measure would end up drowning authorities in useless notifications that may create unnecessary uncertainty. Entities should only report significant and tangible incidents, and not “potential” incidents as it is disproportionate and not realistic.
- Delay: The 24 hours delay under which important and essential entities would have to submit an initial notification to the competent authorities or the CSIRT is too short, as a clear identification of the incident and cause could take longer. A 72h delay would be more manageable and coherent with the personal data security breach under the GDPR.
- Competent authorities: the proposal suggests that Member States can identify the competent authorities or the CSIRT to notify incidents. To avoid reporting duplications each Member State should identify a single point for reporting.
- Sanctions: NIS 2 Art. 31.1 establishes a very high level of sanctions. Level of fines should be harmonised and reduced and should also apply to ICT key providers of technologies and services that refuse to deliver patches to correct incidents in a reasonable delay.

Jurisdiction in multiple territories should be maintained

According to NIS 2 Art. 24, DNS service providers, TLD name registries, cloud computing service providers, data centre service providers and content delivery networks (CDN) providers as well as certain digital providers will be under the jurisdiction of the Member State where they have their main establishment in the Union. Orange does not oppose this provision but would maintain, in parallel, the possibility to keep legal establishments in multiple territories of the Union for those entities that operate in multiple territories but do not have a main establishment.

A more balanced approach on vulnerabilities registries

Orange supports initiatives aiming at coordinating the management of cybersecurity incidents, but questions the effectiveness of listing and giving access to vulnerabilities registries. It is important to ensure confidentiality and to clarify who would have access to the registries and for what purpose.

In addition, any disclosure and registering of vulnerabilities should only be done when a mitigation is available. If mitigation is not available, a deadline should be imposed upon the providers to ensure a mitigation is made available in a reasonable timeframe.

Finally, the NIS 2 should ensure that the existing channel of communication at national level between the national authority and the entity remains the privileged reporting channel.

Unclear definition regarding "data centre services"

NIS 2 would cover data centres, but the proposed definition of data centres services is so wide that any service relying on a data centre would be in the scope, regardless of the number of customers served and the purpose of the service provided. The application of this definition to multi-access edge computing non critical services (e.g. gaming) is a specific concern for the telecommunication sector. The definition of Data Centre services needs to be clarified to avoid legal uncertainty.

A streamlined and consistent cybersecurity framework

The NIS 2 is put forward at a time where there are several initiatives at EU and at national level with a focus on cybersecurity, whether it be the proposed Directive for the Resilience of Critical Entities, the European Electronic Communications Code, the 5G toolbox, and the draft "eIDAS" Regulation, amongst others. It is critical that the framework for all actors is streamlined and clear to avoid legal uncertainty and double layers of obligations.

For more information: https://www.orange.com/en/groupe/orange-bruxelles, or follow us on Twitter: @Orange_Brussels