Committed to Europe

The Cybersecurity Act

Background

The cyber threat landscape is rapidly evolving and cyber-attacks are on the rise. There were as many as 4000 ransomware attacks per day in 2016. Security incidents in companies rose by 38% in 2015, and 80% of companies admitted that they had experienced at least one cyber incident in 2015[1]. Cyber-attacks know no borders and no one is immune. The "Wannacry" and "Petya" attacks were a recent serious wake up call. It was estimated that a serious cyber-attack could cost the global economy more than €100 million[2].

The rapid development of the Internet of Things (IoT) and the reality of our connected world are upon us; hundreds of thousands of new IoT services will connect billions of new IoT devices over the next decade. Security is and will be critical to both the success of these services and the development of this new ecosystem. Therefore it is important that robust security measures are adopted by the whole IoT value chain. In that sense, Orange's view is that the principle of "Security by design" has to be the guiding principle and security standards must be integrated at all stages of the product lifecycle.

Awareness and knowledge are key in dealing with cyber threats, but, surprisingly, 69% of companies have no basic understanding of their exposure to cyber risks; 60% of companies have never estimated the potential financial losses from a major cyber-attack[3]; and 51% of EU citizens feel not at all or not well informed about cyber threats[4].

It is therefore not astonishing that there are calls from across industry, institutions and administrations for more action to withstand attacks in the future.

Orange welcomes the proposal to review the EU's Cybersecurity Strategy

Orange welcomes the new proposals of the European Commission (EC) to scale up the EU's Cybersecurity strategy. While sector specific provisions were already in force for the telecom industry following the entry into force of the 2009 EU Telecom Package, the initial and wider European Cybersecurity strategy was set out in 2013. The Network and Information System (NIS) Directive constituted the most significant step of this strategy towards a more harmonised European answer to cyber threats and is due to be transposed into national laws in May 2018. By reviewing the 2013 strategy, the EC demonstrates a commitment to adapt to current needs and threats, as well as an engagement to work with the industry under public-private cooperation. Amongst a variety of intiatives by the EC to build a strong cybersecurity in Europe: resilience, deterrence and defence are the cornerstones of this strategy. Hereafter we shall focus on the Cybersecurity Act put forward by the EC that essentially treats two key aspects:

- the revision of ENISA's mandate
- a EU framework for cybersecurity certification.

[1] PWC Global State of Information Security Survey 2016
[2] EC Cybersecurity Factsheet State of the Union 2017
[3] Continental European Cyber Risk Survey 2016 report
[4] EC Cybersecurity Factsheet State of the Union 2017

orange™

A new mandate for ENISA

Orange welcomes the new mandate for ENISA as proposed by the Commission. In the Cybersecurity Act, ENISA's mandate is foreseen as pre-eminently supportive in nature, to the Member States' role (Art. 3, Art. 4). Indeed, ENISA could play a key role to enhance and promote a common cybersecurity understanding among the different public and private stakeholders. ENISA, as new permanent European agency, should support the generation of situational awareness, building expertise, coordinated reactions and supporting the development of common capabilities. These capacities should not only be available to Member States but also to the private sector.

It is important to acknowledge that these tasks require a substantial development and capacity-building effort on ENISA's side along with relevant skills and expertise to ensure that ENISA can indeed deliver. To that extent, we would strongly advocate that ENISA should work very closely with experts in industry and within the Member States to achieve its objectives, notably in collaborating with security experts from national security agencies that already have a sound experience of certification matters gathered over 15 years of certifications within SOGIS-MRA (https://www.sogis.org/documents/mra/20100107-sogis-v3.pdf).

Finally, ENISA should ensure in the future that EU industry is effectively involved in its working process before a scheme is drafted and during the overall process of such definition; some adjustments to the text are suggested below.

An EU Framework for Cybersecurity Certification on a voluntary basis is welcome

Orange welcomes the principle of the EU Cybersecurity certification framework as it minimises duplication and fragmentation across Member States and will make it easier to attest that ICT products and services comply with cybersecurity requirements, while remaining on a voluntary basis.

It would enable businesses to easily trade across borders and for purchasers to understand the security features of an ICT product or service. Such a framework could evolve into a competitive advantage for EU companies. At the same time, it can also involve costs and it is important not to create market barriers for companies, such as SMEs, due to high entry costs. A level playing field with the same rules applying to all stakeholders will provide legal certainty and imply cost benefits.

However, it is important that such a framework considers the following elements:

- Clarity is required in the process described by the EC in Art. 44. In particular, the roles of the different actors, specifically, who can propose a scheme (EC, European Cybersecurity Certification Group (ECCG), Industry etc.), and, the bases on which the EC may or may not adopt an EU scheme at the end of the process.

- Orange believes that EU industry should be more actively involved in the certification process. It should be clearer that the "Permanent Stakeholders Group" referred to in Art. 20 should gather European ICT industry and European providers of electronic communication services and networks. Also, the industry through this "Permanent Stakeholders Group" should be empowered within Art. 44 to propose certification schemes to the EC, and also be consulted by ENISA and give input during the process of defining the schemes.

- Regarding the role of Member States and for the ICT products and services that will be covered by the scope of article 49, Member States should be given a stronger role than merely advisory in the definition and validation process. It would seem more justified, especially given the reality of expertise in the area at this point of time, to follow the examination procedure in Art. 5 of Regulation n°182/2011, instead of referring to its Art. 4, in Art. 55 of the draft Act.

- Concerning the assurance levels (basic, substantial and high levels) described in Art.46, Orange considers that such levels should be defined on a case by case basis per certification scheme, and not explicitly in the Cybersecurity Act. It is not possible to define them in this Act as there is no "one-fits-for-all" type of levels; it would thus be too rigid and not adapted to market realities.

- The proposed ownership of the scheme should be added to Art. 47 as an integral part of the scheme elements to be provided. The owner will have to take responsibility for the scheme's design, administration and maintenance. The owner of a scheme can be a private or a public organisation. The scheme will have to be documented so as to be accreditable by a Member State's National Accreditation Body. This Art. 47 should also request ENISA to advise EC on whether the scheme should be accredited by national accreditation bodies.

- Cybersecurity certification should be voluntary (Art. 48 (2)); this is a key feature of the EC proposal. The scope of the Act is wide and the IoT market currently only at an early stage. Having an EU certification scheme relying on a voluntary implementation process is therefore relevant to increase awareness and the level of security in the EU without automatically increasing costs for the industry, smaller players, or intervention on innovative services or products.

- The Act proposes in art. 48 (6) a three years validity period for all certification schemes. This should be deleted as such validity period should be determined on a case by case basis and function of the certification scheme in question.

- Art. 49 stipulates that once a EU scheme exists, any national scheme should cease to exist. It should be clarified that the Act does not cover specific matters in the remit of the sole Member States and national security agencies' power, as mentioned in article 4.2 of the TEU[5]. This means that this Act cannot empower the EC to adopt EU schemes on the regal domains, namely national security, defence, including sectors of activity of vital importance in the Member States.

- As stated in the Cybersecurity Act, national certification supervisory authorities should retain their role of monitoring, supervising and enforcing standards (Art. 50). Conformity assessment bodies should systematically be accredited by a national accreditation body recognized by the Member State (Art. 51 (1)) as stipulated by EU Regulation 765/2008.

Don't reinvent the wheel!

Orange supports the Commission's policy objectives to ensure cybersecurity competencies are raised throughout the EU to achieve a secure and performant DSM. It is however important when defining this new overarching Cybersecurity strategy, not to reinvent the wheel! In particular, when defining certification schemes, the EU should rely on existing national and international standards and on existing expert competencies in different Member States.

At this stage, efforts should be focused on the development of competencies and trust through existing mechanisms. Indeed, time should be allowed for all actors in the ecosystem, including industry actors and Member States to acquire adequate maturity and security levels with increased cooperation between all actors. Also, national and European public authorities should set a good example by integrating appropriate security requirements into their public procurement practices.

[5] Article 4(2) TEU states that:"[t]he Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State."

Orange Cyberdefense: a unique centre of excellence with experts and solutions dedicated to security

As a global company, we have the capability to hire and retain highly demanded skills. Our 1,200 security experts share their diverse experiences among themselves to gain a deeper understanding of the security landscape. Our global capability, with a local presence in 160 countries, ensures a dedicated and tailored service to our customers. Orange has set up a Cybersecurity Academy to enable people to become skilled experts in Cybersecurity. To ensure the security of our customer's systems and the protection of their data, Orange has created a dedicated entity that has become a benchmark for the sector: Orange Cyberdefense. Its benefits:

- 1,200 experts in matters of security,
- 60,000 security devices managed by Orange Cyberdefense,
- 1 epidemiology laboratory,
- 3 CyberSoc bringing together the best expertise in threat analysis
- 3 Computer Emergency Response Team (CERT)
- 7 Security Operation Centres (SOC) around the world,
- 3 DDoS Scrubbing Centres

For more information: www.orange.com/committedtoeurope, or follow us on Twitter: @Orange_Brussels