The European Commission presents its new cybersecurity strategy

In September 2017, the European Commission (EC) issued new proposals to scale up the European Union's (EU) Cybersecurity structures and to build greater resilience and strategic autonomy in this area. Cybersecurity has a special resonance, under the Estonian EU presidency, after the country experienced what has now been widely recognised as the world's first cyber war. The cyber threat landscape has changed since the 2007 Estonian cyberattacks: cybersecurity is not an isolated topic anymore, understood by a handful of experts only.

Besides the legislative agenda, large scale cyberattacks such as WannaCry and NotPetya have brought cyber risks into the public eye. Recent figures confirm the trend it has been reported that as many as 80% of European companies have experienced at least one cybersecurity incident in the past year. Internet users across Europe experience more than 4,000 ransomware attacks every day. As our daily lives and our economies rely more and more on digital technologies, it is critical to ensure that our devices and networks are protected and are better equipped to deter cyberattacks.

By reviewing the 2013 existing 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. This article aims to give an overview of the main propositions put forward by the EC.

The EU Cybersecurity package in a nutshell

The Commission proposes three pillars for action: resilience, deterrence and defence. In short, the EC puts an emphasis on building greater strategic autonomy, and wishes to boost capabilities in terms of technology and skills, along with the building of a strong single market in the area of cybersecurity.

<u>Building Greater Resilience</u>

The EC first insists on the full implementation of the Network and Information Systems (NIS) Directive by Member States as an essential pre-requisite for cyber-resilience. The NIS Directive is the first piece of EU-wide legislation on cybersecurity and its transposition deadline is coming up in May 2018. For example, the Directive asks Digital Service Providers to notify authorities of any incident having a substantial impact on the provision of service.

Within the new strategy and building on the NIS Directive, the EC aims firstly, to improve the EU's cyber resilience by promoting cyber hygiene, with a shared belief that cybersecurity is a common societal challenge. The EC asks that Member States now include cybersecurity as part of academic and vocational training curricula. It also recommends the spread of cybersecurity information campaigns to get the message across. Additionally, the creation of a one-stop-shop, as pushed forward by the EC, would enable users to signal cyberattacks, provide assistance or simply inform upstream and advise users.

In addition, to reduce the skills shortage and maintain a strategic autonomy, the EC proposes to set up an EU Cybersecurity Research and Competence Centre including initiatives such as apprenticeship schemes in cybersecurity for SMEs, building on national initiatives. At the industry sector level, the EC argues in favour of a 'security by design' approach, in other words, devices designed from the ground

up to be secure. Another action to increase consumers' trust in digital products will be the set-up of a European-wide certification framework. Such a label, as announced by the EC, would inform and reassure purchasers. This certification framework would be controlled by an empowered European agency, the ENISA (European Union Agency for Network and Information Security), as part of the so called 'Cybersecurity Act'. Moreover, the new mandate given to ENISA would also include a strong advisory role on EU policy implementation and would act as a Cybersecurity crisis management centre assisting Member State Computer Security Incident Response Teams (CSIRTs).

Enabling a robust deterrence to Cyberattacks

Deterrence means discouraging cyber criminals and attackers to take action through instilling doubt or fear of consequences. A more effective law enforcement response is a way of dissuading cybercrime, with the help of enhanced cyber forensics. Deterrence is also about technological practices.

As such, the Commission encourages the uptake of the new IPv6 (Internet Protocol version 6) as it provides the clear benefit of assigning to users a unique IP address for identification purposes and location definition. If this practice was widespread, it would facilitate online investigations and help identify malicious actors faster.

The Commission is also currently considering the role of encryption in criminal investigations in order to improve forensics standards and collect e-evidences. Another cybercrime activity feared by many users is the spread of fraudulent use of credit card details. To boost deterrence in this area, the Commission is presenting a Directive on the combatting of fraud and counterfeiting of non-cash means of payment.

A global vision for a cybersecurity strategy and defence cooperation

As the digital world knows no border, the EC will prioritise cross-border information-sharing in Europe and beyond, as well as the promotion of a strengthened international cooperation to facilitate prevention and deterrence of cyberattacks. The EC wishes to build and maintain alliances with third countries in order to promote global cyber-stability. Conversely, through a 'Cyber Diplomacy Toolbox' within the Framework of the Common Foreign and Security Policy instruments, the EU has stated it was ready to respond with a range of measures, including sanctions, if State and non-State actors were to threaten the integrity of the European cyberspace. Regarding cooperation on cyber defence, the EC would also like to see a strengthened EU-NATO cooperation, through training and exercises along with interoperability of cybersecurity standards.

The European Commission has expressed the wish to have this new cybersecurity strategy adopted by the end of its mandate, in 2019.

Orange and cybersecurity

Orange Business Services operates managed security services in 160 countries and territories, working 24/7/365. We have 1000 experts, working together with our six Security Operation Centres (SOCs) around the world, constituting one of the largest repositories of security expertise. We manage security for over 600 multinational companies and their 400,000 distant users.
In addition, we have R&D labs and an industry-leading centre focusing on 'cyber epidemiology' and 'signal intelligence'.

Find out more:: http://www.orange-business.com/en/security