Agreement reached on the Network and Information Security (NIS) Directive

Boosting Cybersecurity in the European Union

Petra Hazenberg
Partner
EU Institutions & Agencies
Industry Leader
Deloitte

Stéphane Hurtaud
Partner
Governance, Risk & Compliance
Deloitte

Alexander Cespedes Arkush
Manager
Governance, Risk & Compliance
Deloitte

What is Cybersecurity in the EU about?

Cybersecurity refers to the safeguards and actions to protect the cyber domain from threats. These cyber threats in question may harm interdependent networks and information infrastructure. Cybersecurity preserves the availability and integrity of the networks and infrastructure, as well as the confidentiality of its information.

Network and Information Security (NIS) is the ability of a network or an information system to resist accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of data and the related services.

The main problem as identified by the Impact Assessment[1] on Cybersecurity performed by the European Commission is that there is insufficient protection against NIS threats and disruptions across the EU. However, securing network and information systems in the EU is key to ensure prosperity and to support the online economy.

What is the Cybersecurity Strategy of the EU?

The current framework on cybersecurity, stemming from the Digital Agenda for Europe, is contained in the Cybersecurity Strategy for the EU. Its aim is to ensure a secure and trustworthy digital environment, while promoting and protecting fundamental rights and EU core values. It outlines the EU's vision in the domain of cybersecurity, clarifying roles and responsibilities, and specifying required actions to promote online security and citizens' rights.

The vision presented in the Cybersecurity Strategy is articulated in five priorities; one of which is about achieving cyber resilience.

Reduce cyber-crime

Achieve cyber resilience

Develop cyber defence

Develop industrial and technologival resrouces

Establish EU international cyberspace policy

To boost cyber resilience, both the public and private sector should develop capabilities and cooperate effectively. For this reason, the Commission has proposed a directive aiming to ensure a high common level of NIS across Member States (MS).

What will the NIS Directive change?

The NIS Directive aims to achieve a high common level of security of networks and information systems within the EU. The European Council reached an informal agreement with the Parliament on 7 December 2015, and the agreed final compromise text was approved on 18 December 2015. The NIS Directive aims to achieve the following:

01/ Increase the cybersecurity capabilities in the Member States

02/ Enhance cooperation on cybersecurity among the Member States

03/ Ensure a high level of risk management practices in key sectors

[1] *Impact Assessment - SWD(2013)32 final - 7/2/2013*

[2] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace - JOIN(2013) 1 final - 7/2/2013*

How will Member States increase their cybersecurity capabilities?

MSs will be required to adopt a national NIS strategy, defining the strategic objectives and appropriate policy and regulatory measures in relation to cybersecurity and coverage of essential sectors. This will include setting up a governance framework with roles and responsibilities of the governmental bodies and relevant actors; the identification of measures on preparedness, response, and recovery, as well as cooperation between the public and private sectors.

MSs will also be required to designate a National Competent Authority (NCA) for the implementation and enforcement of the NIS Directive. These NCAs will cooperate with the national law enforcement authorities and national data protection authorities. In addition, each MS will have to designate a national Single Point of Contact (SPoC) that will ensure cross-border cooperation between other MS authorities.

Each MS will have to designate one or more Computer Security Incident Response Teams (CSIRTs) responsible for handling incidents and risks in the relevant sectors. Tasks of the CSIRTs will include responding to cybersecurity incidents, providing risk analyses, and situational awareness.

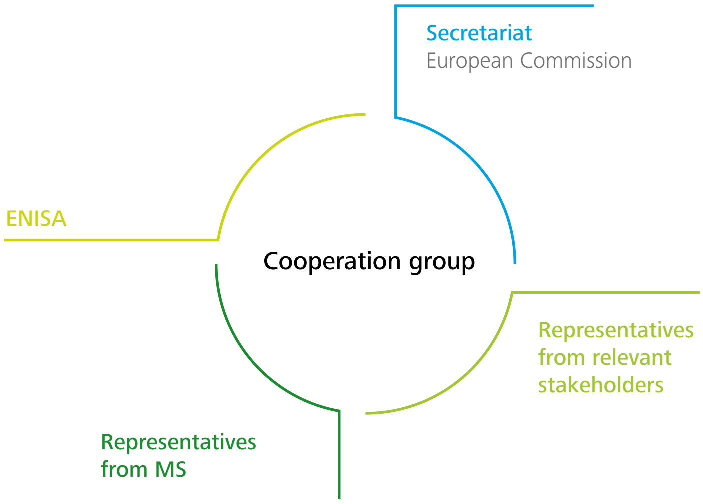
How will cooperation between Member States be fostered?

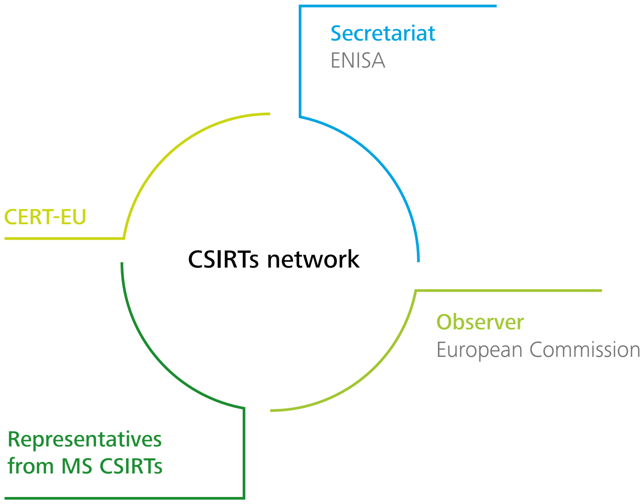
The NIS Directive will set up a strategic cooperation group to draw up strategic guidelines for the activities of the CSIRTs network and discuss the capabilities and preparedness of MSs, among other tasks.

This group will be mainly composed of representatives from the MSs, the Commission, and the European Union Agency for Network and Information Security (ENISA). The Commission will provide the secretariat for this group.

In addition, a network of CSIRTs will be assigned multiple tasks at an operational level, including supporting MSs in addressing cross-border incidents, exchanging best practices on the exchange of information related to incident notification, and assisting MSs in building capacity in NIS.

This network will be composed of representatives of the MSs' CSIRTs and CERT-EU, while the Commission will participate as an observer. ENISA will provide the secretariat for the CSIRTs Network and will be encouraged to maintain a website with general information on major NIS incidents occurring across the Union.





How will EU Institutions, Agencies and Bodies benefit from more cooperation in the EU?

According to one of the recitals of the NIS Directive, the Cooperation Group should, where appropriate, cooperate with relevant EU Institutions, Bodies, and Agencies, to exchange know-how and best practices and to provide advice on NIS. In addition, both CERT-EU and ENISA will, by participating in the CSIRTs Network, further build their expertise regarding NIS capacity development, well-functioning practices as well as information concerning critical weaknesses that should be addressed. According to its 2016 Work Program , ENISA intends to provice such expertise to EU Institutions, Agencies and Bodies, in cooperation with CERT-EU.

How will a high level of risk management practices in key sectors be ensured?

Both Operator of Essential Services (OoES) and Digital Service Providers (DSPs) will have to ensure the security of their networks and systems to promote a culture of risk management and ensure that serious incidents are reported to NCAs or CSIRTs. These would primarily include private networks and systems for which security is managed either by internal IT staff or by outsourced staff.

In this context, NCAs will have the power to require both OoES and DSPs to provide information needed to assess the security of their networks and information systems, including documented security policies.

Conclusion

The Cybersecurity Strategy of the EU is the first comprehensive policy document in the area of NIS of which the main action is the proposed NIS Directive. After more than two years of negotiation, the agreed final compromise text was approved by the EU Member States (MS) on 18 December 2015. This means that the EU is now closer than ever to boosting its overall level of cybersecurity not only for MS and organizations in key sectors but also for EU Institutions, Agencies and Bodies.

What is next?

To conclude the procedure, the NIS Directive must still be approved by the European Parliament at a second reading. Therefore, it is expected to enter into force in August 2016. After the Directive has entered into force, MSs will have 21 months to transpose the Directive into national law. After this period, they will have another six months to identify the essential services operators established in their territory which are to be covered by the directive. However, the Cooperation Group and the CSIRTs Network will be established when the Directive will be published in the Official Journal of the EU.

[3] *https://www.enisa.europa.eu/publications/programmes-reports/enisa-work-programme-2016*

[4] *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union - Examination of the final compromise text in view to agreement 2013/0027 (COD)*