Incident Response in Europe, post-NIS Directive

ENISA, the European Union Agency for Cybersecurity releases ‘EU Member States Incident Response Development Status Report’, a analysis of current operational Incident Response (IR) set-up within the NIS Directive sectors.

Published on November 27, 2019



Copyright: Shutterstock

Tagged with

* [NIS Directive](https://www.enisa.europa.eu/search?Subject%3Alist=NIS%20Directive)
* [ENISA](https://www.enisa.europa.eu/search?Subject%3Alist=ENISA)
* [Incident Response](https://www.enisa.europa.eu/search?Subject%3Alist=Incident%20Response)
* [CSIRTs](https://www.enisa.europa.eu/search?Subject%3Alist=CSIRTs)

**The NIS Directive and Incident Response**

The EU’s NIS Directive (Directive on security of network and information systems) was the first piece of EU-wide cybersecurity legislation. It aims to achieve a high common level of network and information system security across the EU’s critical infrastructure by bolstering capacities, cooperation and risk management practices across the Member States (MSs). The NISD covers the following sectors; energy, transport, banking, financial market infrastructures, the health sector, drinking water supply and distribution and digital infrastructure.

The protection of an organisation's information by developing and implementing an incident response process (e.g. plans, defined roles, training, communications, management oversight) is vital in order to quickly discover an attack and effectively contain the damage, eradicate the attacker's presence, and restore the integrity of the network and systems

Following the recent transposition of the Directive into Member States legislation, this study aims to analyse the current operational Incident Response (IR) set-up within NISD sectors and identify the recent changes.

**State of Play of NISD sectoral Incident Response**

The ENISA '[EU Member States Incident Response Development Status Report](https://www.enisa.europa.eu/publications/eu-ms-incident-response-development-status-report/)' provides a deeper insight into NISD sectoral Incident Response capabilities, procedures, processes and tools to identify the trends and possible gaps and overlaps.

The study was done by involving CSIRTs network members (National, governmental and sectoral CSIRTs) to understand their perspective (as one of the main actors involved) of operational Incident Response (IR) set-up within the NISD sectors.

Additionally, an informal expert group was formed in order to have input from specialists in different sectors.

**Key Findings**

The main findings of the study include:

* Organisational culture has an influence on IR set-up within NISD sectors.
* Concludes that NISD main impact from the perspective of IR was to clarify actors’ roles and responsibilities within the IR organisation.
* Looks at services specific to their sectors’ needs that sectoral CSIRTs provide, in particular a more in-depth knowledge of the threat and actor landscape, better-adapted tools, solutions and operational expertise.
* Sectoral cooperation and information-exchange initiatives, their visibility and efficiency.
* Sectoral level training as key to fostering and enhancing preparedness.

**Incident Response Capabilities in Europe**

Incident Response Capabilities (IRC) within the NISD sectors is a growing concern to tackle potential incidents, which could have a major impact on European societies and citizens.

ENISA’s Executive Director, Juhan Lepassaar, stated:

 “*The input from national and sectoral CSIRTs as well as the expert group, allowed us to take stock of the current landscape of incident response within the NIS sectors and the findings are essential for establishing or developing sector specific incident response capabilities.”*

**Target Audience**

This study provides recommendations for Member States and particularly for national and/or governmental CSIRTs and operators of essential services (OES) in the seven sectors identified in the NISD. However, the main objective of the study is for ENISA to gain a better understanding of and draw conclusions about the current status and the recent changes in the European Incident Response landscape.