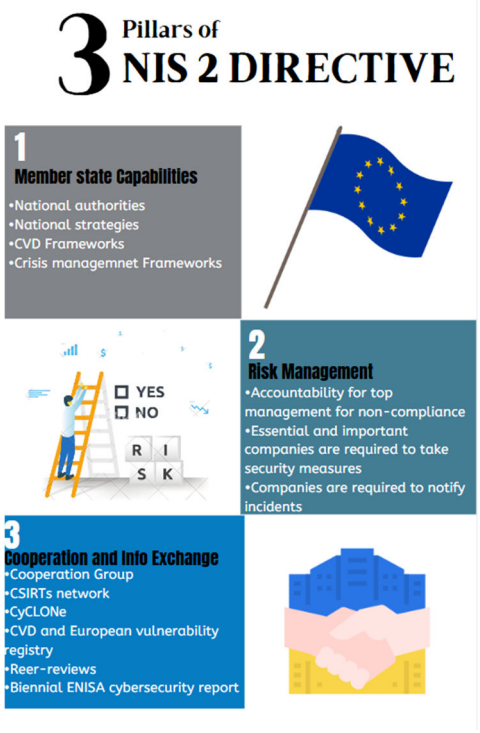
ERMIS

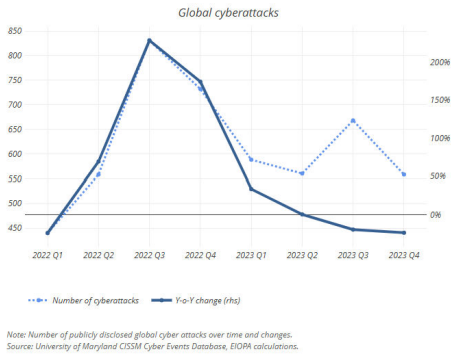
Newsletter

November 2024 - Issue No2

In this Issue



On Sept 18th, the Ministry of Digital Governance presented the NIS2 Directive to our consortium partners! Below are some key insights on new cybersecurity regulations and the future of digital security in the EU were shared.



Note: Number of publicly disclosed global cyber attacks over time and changes.
Source: University of Maryland CISSM Cyber Events Database, EIOPA calculations.

The NIS 2 Directive enters our lives

It is several years since October has been pronounced as the chosen month dedicated to Cyber Security. This year, however, there is a solid cause and a distinguished circumstance for this: October the 18th was the set day for Member States to transpose the Directive 2022/2555 (Directive on measures for high common level of cybersecurity across the Union - NIS2) into their national law and apply necessary measures to be compliant to the provisioned cybersecurity rules, including supervisory and enforcement measures. In recent months, the entire cyber security ecosystem is engaged in an unprecedented race to ensure timely and effective preparedness. This article attempts a brief overview of the upcoming landscape.

Of all the European Acts and laws, the NIS2 is the most iconic one. Its main objective is to achieve a high common level of cybersecurity across the European Union. To ensure this, the NIS2 is based on three pillars: Firstly, Member States have to deploy national capabilities. This includes the development of a national cyber security strategy, the appointment of national competent authorities to oversee its implementation along with a package of more comprehensive monitoring measures and administrative fines in case of non- compliance the establishment of a national cyber security incident response team to assist entities with incident response, the implementation of a national vulnerability disclosure policy and the deployment of a cyber crisis management framework.

Secondly, the NIS2 highlights international cooperation using well established or emerging schemes and mechanisms such as the NIS Cooperation Group, the CSIRTs Network, the Cyber Crisis Liaison Organization Network, the shared EU Vulnerability Database, a cross-border entities' Registry and the annual EU cybersecurity status Report. The abovementioned collaboration covers mainly the areas of strategic information exchange and cross-border incident response on both technical and operational level. Third, the entities within the scope of NIS2 must ensure responsibility of their management bodies when it comes to cybersecurity practices and law compliance. Management bodies approve the adequacy of the cybersecurity risk-management measures taken by the entity, supervise their implementation and subsequently are accountable for non-compliance. In this context, they follow relevant trainings and offer their employees trainings on a regular basis. Moreover, the compliance of specific requirements includes detailed risk-management measures, such as the accomplishment of cyber risk assessments, the mitigation of risks through appropriate security measures and the maintenance of specific time constraints for incident reporting. Specifically, in case of a significant cyber incident, the NIS2 provisions the entity with twenty-four hours to issue an early warning, seventy-two hours for the incident notification and one month for the final report.

There is a wide feeling among the cybersecurity stakeholders that in this case the European Union has done well, especially considering the multidisciplinary and multilevel nature of cybersecurity and the need for organized posture in each one of these levels. It remains to be seen how the new member of European legislation will take its first steps...

By Georgios Kittes, MDG

Cyber Solutions and Security Services Trends

Notes: Data shown is using current exchange rates and reflects market impacts of the Russia-Ukraine war.

Most recent update: Jun 2024

Source: Statista Market Insights

The revenue from cyber solutions and security services has been steadily increasing and is projected to grow significantly in the coming years, as reflected in the recent *Statista Market Insights, Jun24*. In 2016, the combined revenue of these services was $83.32 billion, with significant growth in both cyber solutions and security services over the years. By 2024, the total revenue is expected to reach $202.99 billion, with projections showing further increases to $255.70 billion by 2028 and $271.90 billion by 2030. This growth highlights the escalating demand for cybersecurity services, likely driven by the rise in global cyber threats and the increased focus on digital resilience in response to geopolitical factors. As cyber threats continue to evolve, the market for cyber solutions and security services is set to expand, underscoring the critical role these services play in safeguarding digital infrastructures worldwide.

By Mary Tasouli, INS

(Data source: Statista Market Insights, Cybersecurity: market data & analysis, Jun24)

Static and dynamic cyber insurance policies

As the cyber insurance market continues to mature, collaboration between insurers, technology providers and policyholders will be vital. The rapid pace of technological change means that static annual policy renewals may soon become obsolete and be replaced by innovative dynamic, data-driven risk transfer insurance solutions that adapt in real-time to a changing threat landscape. Ermis's innovation is about a market platform that offers cybersecurity assurance and insurance as a service.

This platform supports the adoption of cybersecurity and market-ready insurance solutions by integrating risk assessment, security certification and policy management tools. ERMIS aims to offer both static and dynamic cyber insurance processes. The inclusion of mechanisms for dynamic risk assessment and security certification, which provide real-time information on organisations cyber systems' risk exposure.

By Dimitra Smyrli, INS

1st Plenary Meeting

The 1st plenary meeting took place in Nicosia, Cyprus on September 26-27th, 2024. We brought together all participating companies to review progress and align key project goals. We had discussions centred on the progress of all Work Packages (WPs) and planning the next steps.

Contact

Project Coordinator: Zelus, General inquiries: info@dep-ermis.eu

ERMIS

http://dep-ermis.eu/

#DEP-ERMIS

DEP-ERMIS

ECCC

Disclaimer

The project received funding under Grant Agreement No 101128013, and is supported by the European Cybersecurity Competence Centre.

The project is supported by the Ministry of Digital Governance of Hellenic Republic and the National Cybersecurity Authority and is aligned with the Hellenic Cyber Security Strategy.

Zelus Sphynx Insuretics Nodalpoint karavias underwriting agency ΕΛΛΗΝΙΚΗ ΔΗΜΟΚΡΑΤΙΑ Υπουργείο Ψηφιακής Διακυβέρνησης