ECSO

EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity Awareness Calendar 2024

July

European Regulations and Compliance

Turning up Neon Lights for Awareness Nights!

ECSO aims to spread awareness of key aspects of cybersecurity and showcase ECSO Members and the cybersecurity community's solutions and services.

Introducing our 2024 topics:

January: Zero Trust
February: Quantum Computing and Cryptography
March: Ransomware
April: Cybersecurity Solutions to Secure SME Businesses
May: The Road to a Career in cyber
June: Supply Chain
July: European Regulations and Compliance
August: Generative AI
September: Internet Of Things (IOT)
October: Artificial Intelligence
November: Threat Vulnerability
December: Cloud Computing

ECS

EUROPEAN CYBER SECURITY ORGANISATION

Resources from our Members

CyberSEAS

ENGINEERING
THE DIGITAL TRANSFORMATION COMPANY

Strengthening Cybersecurity in the Energy Sector with the NIS2 Directive and CyberSEAS project initiatives

In December 2022, the EU introduced the NIS2 directive to address cybersecurity vulnerabilities caused by the digitisation of critical sectors, like energy. This directive expands on the previous one by enhancing security requirements. Its adoption by October 2024, isn't just about compliance but also presents an opportunity to bolster resilience and guarantee business continuity. One of the CyberSEAS project activities focuses on developing a unified, multi-phased cybersecurity governance model for organisations under NIS2. This includes the creation of a cybersecurity team with accountable leadership and employee participation; the development of policies including stakeholder alignment and risk management; a focus on preventive activities such as basic cyber hygiene and employee training; and last, incident response to ensure business continuity. Furthermore, in March 2024, the consortium and Women4Cyber Slovenia conducted a webinar 'Unpacking Cyber-Resilience for EPES with NIS2 (Woman's Perspective)' to exchange knowledge about NIS2 with speakers from different backgrounds sharing expertise.

Learn more HERE.

European regulations and compliance in Cybersecurity

European cybersecurity regulations are crucial for protecting data and information. The General Data Protection Regulation (GDPR) requires companies to safeguard the personal data of EU citizens and report breaches. In addition to GDPR, the Network and Information Systems Directive (NIS) mandates member states to improve the security of networks and information systems, with specific requirements for essential service operators and digital service providers. The NIS 2 Directive, approved in 2022, updates the previous directive, extending its scope to new sectors and increasing security requirements. It introduces stricter obligations for risk management and incident reporting, requiring advanced preventive measures and rapid responses to cyber threats. Compliance with these regulations is essential not only to avoid penalties but also to build customer trust and protect corporate integrity.

Our cybersecurity services meet the requirements defined in the regulations, read more HERE.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Resources from the Community

Recommendations from the ATHENA project on protecting critical infrastructure

There are digital security threats resulting from geopolitical developments that affect the critical infrastructure (CI). Mainly, targeting CI has become part of the arsenal showcasing geopolitical influence. Furthermore, attacks on CI have increased, putting their integrity and services at risk. Moreover, the trend of digitalisation in CI and the ensuing interconnectedness between IT and OT introduces new risks in this domain. The legislation, such as the NIS2 Directive, aims to address this risk, but further improvements to the Directive are required to firmly position OT in regulatory language.
Find out more HERE.

Setting the Standard: GenAI Regulation and Its Impact on Cybersecurity

hackuity

Be the industry standard that future regulators look to. Just as GDPR set the new data privacy bar more than five years ago, GenAI regulation will establish standards for decades to come. AI's a match to the current cyber wildfire, but does it deserve more blame than the kerosene we've been ignoring for more than a decade? That's what the EU's Artificial Intelligence Act and even less AI-centric regulation like DORA are seeking to remediate.
Find out more HERE.

Enhancing Cybersecurity: The Expanded Scope of NIST CSF 2.0

HWG Sababa

Cybersecurity compliance is crucial for protecting digital assets and meeting regulatory requirements. The updated NIST CSF 2.0 framework – which now extends beyond its original focus on critical infrastructure to serve businesses of all sizes and sectors – is a key resource in this effort. With significant updates such as privacy integration, supply chain focus, and enhanced risk management, the framework provides essential tools for developing comprehensive and resilient cybersecurity programs.
Learn more HERE.

Thank you for your time!

The Cybersecurity Awareness Calendar
is an initiative launched by:
European Cyber Security Organisation (ECSO)
Avenue des Arts 46
1000, Brussels

company/ecso-cyber-security

@ecso_eu

www.ecs-org.eu

secretariat@ecs-org.eu