ECS
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity Awareness Calendar 2024

March

Ransomware

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

Defending Against Ransomware Attacks

A ransomware is a type of malware that encrypts data on devices or networks, requiring a payment to restore access. Exprivia, through its cybersecurity experts and its Security Operation Center, addresses such threats with timely action. It analyses the attack, isolates infected systems and tries to restore the data. In addition, it is able to subject a forensic analysis of the security incident, implements advanced security measures, and provides training to raise awareness of the threats. Prevention is prioritised, involving the design of advanced defenses, updates regular updates and employee training. Exprivia plays a key role, thanks to its Threat Intelligence, it analyses cyber attacks on a daily basis involving its customers and others.

Read more HERE.

Reduce Your Risk of Ransomware with Essential Cyber Hygiene!

GLOBAL CYBER ALLIANCE

Cyber hygiene is essential in the fight against ransomware according to recent analysis conducted by Tidal Cyber and the Global Cyber Alliance.

You can read the report here and access the free tools and resources contained within any of the GCA Cybersecurity Toolkits here (pick your community for the toolkit most relevant for you!)

Best Practices for Managing Ransomware Risk

ISC2

ISC2 ensures its members and the cybersecurity community have access to insights and best practices for mitigating ransomware risk, including the following FREE webinars:

Ransomware, Ransom-war and Ran-some-where
Insight into how the criminal organisations behind ransomware operate and a primer on how to defend yourself against their attacks

The Reason Why Ransomware is Really HEATing Up
Cybercriminals are taking advantage of users who are spending most of their day accessing work resources in a browser that also accesses unmanaged sites.

Ransomware Resilience: Build a Holistic Data Protection Strategy
Backup strategies. Protect your data properly, and even if the bad guys break into your systems, you stand a chance of avoiding disruption AND paying a ransom.

Ransomware Crisis Simulation with You in Control
Walk through a live simulation of a ransomware attack, highlighting the critical decisions you will have to make as you investigate, and eradicate, the attack.

Ransomware

KOVRR
Cyber Decisions. Financially Quantified.

In the first half of 2023, the Services Industry was the most common target of ransomware attackers, accounting for 42% of all attacks. However, the ever-growing costs of this malicious event affect global organizations market-wide, making it critical for CISOs to take a more proactive, data-driven approach to its mitigation.

Kovrr's on-demand cyber risk quantification (CRQ) solution accounts for an organization's specific cybersecurity program, producing an accurate, custom assessment of its potential to suffer from a ransomware attack, along with financial ramifications. Armed with these financial forecasts, CISOs can pursue cost-effective action initiatives that significantly reduce the likelihood of experiencing a ransomware event.

Moreover, by leveraging Kovrr's CRQ, CISOs can easily communicate this risk with key stakeholders, ensuring a tangible understanding of the value of said initiatives and thus obtain the necessary resources. To better understand your organization's financial exposure due to ransomware, get your free report.

ECS
EUROPEAN CYBER SECURITY ORGANISATION

Resources from the Community

Prioritising Cybersecurity: Beyond Ransomware Ransoms and Patching Predicaments in 2024

hackuity

When companies are having to budget in advance for ransoms, we're missing the mark as an industry. Statistically ransomware attacks exploit the low-hanging fruit of unpatched vulnerabilities we've known about for years. But can we really blame understaffed, underfunded cybersecurity organiations? CISOs and their teams require insights beyond general CVSS scores to know which CVEs to tackle – which ransomware threats most impact their specific attack surface. In 2024, there's no effective remediation without prioritisation.
Find out more HERE.

The Role of SOCs in Today's Landscape of Sophisticated Threats

HWG Sababa

Whether in-house or outsourced, a well-equipped SOC is an indispensable tool for responding to sophisticated cyber threats, including ransomware. Its continuous monitoring, threat intelligence integration, and proactive response mechanisms create a holistic defence against the evolving and complex landscape of ransomware threats, safeguarding organiational assets and ensuring business continuity.
Learn more HERE.

Ransomware: Survival Guide

Ransomware is a major concern for companies worldwide, with IDC reporting that a third of them have been affected. Gartner highlights that 95% of these attacks could have been prevented. Gaining basic knowledge about ransomware is the first step to avoid its damage. itrainsec's flagship course in Spanish, 'RANSOMWARE: GUÍA DE SUPERVIVENCIA,' led by top cybersecurity experts, is the best way to equip companies and individuals with essential skills and practical techniques for ransomware protection.
Find out more HERE.

PRODAFT assisting in disrupting the infrastructures of LOCKBIT, one of the most prominent ransomware gangs

A joint law enforcement operation dubbed “Operation Cronos” has disrupted one of the most notorious RaaS cybercrime syndicates: LOCKBIT. We at PRODAFT are proud to announce that our extensive research and insights helped the NCA, FBI, EUROPOL and other partners of OpCronos better comprehend and disrupt this large criminal enterprise. Our investigations identified over 28 LOCKBIT affiliates (and ties to FIN7, Wizard Spider or EvilCorp) and uncovered all decryption keys for their ongoing campaigns.
Find out 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