ECS
EUROPEAN CYBER SECURITY ORGANISATION

Cybersecurity Awareness Calendar

CLOUD SECURITY

March 2021

Awareness Calendar

CYBERSECURITY

This calendar will feature a different topic each month to spread awareness of key aspects of cybersecurity and showcase ECSO members' and partners' solutions and services in the relevant areas to potential users.

The monthly themes for 2021 are planned as follows:

- January – Phishing
- February – Internet of Things
- March – Cloud Security
- April – Malware
- May – Ransomware
- June – Cybersecurity Skills
- July – Cyber Exercises
- August – Cybersecurity Summer School
- September – Mobile Devices & Bring Your Own Device (BYOD)
- October - Gender Diversity in Cyber
- November – Safer User Authentication & Password Hygiene
- December – Cybersecurity Trends 2022

DID YOU KNOW?

Facts & Figures about Cloud Security

- 36 % of EU enterprises used cloud computing in 2020, mostly for e-mail and storage of files. Compared with 2018, the use of cloud computing in the EU increased particularly in the manufacturing sector in 2020 (Eurostat) - source
- According to Thales, 46% of all European company data is stored in the cloud but only 54% of sensitive data in the cloud is protected by encryption - source
- A report from Accenture shows that less than 40% of companies say they are achieving the full value expected on their cloud investments - source

ECS
EUROPEAN CYBER SECURITY ORGANISATION

RESOURCES FROM ECSO MEMBERS

accenture

SECURITY AS A RESILIENCE ACCELERATOR

MORE INFO:

Secure Cloud Services

Case: Elevating Cloud Security

Podcast

The importance of Cloud Security

Now more than ever, organisations need to prioritise a "cloud first" approach to enable their companies to transform with agility at scale. But, as its name suggests, every new instance of public cloud has the potential to brew up a security storm. The default settings for a new cloud instance are unlikely to satisfy even the basic security requirements of any business operation. While cloud offers new opportunities to modernise services and transform operations, less than 40% of companies say they are achieving the full value expected on their cloud investments. Security and compliance risk remains the greatest barrier to cloud adoption. Combined with the difficulties in proactively addressing the complexity of secure configuration and a shortage of skills, these challenges can be major roadblocks to a cloud-first journey. Security is often seen as the biggest inhibitor to a cloud-first journey—but in reality, it can be its greatest accelerator. Accenture developed a multi cloud security strategy and accompanies that with some global assets like ACP, the governance platform that secures clients multi-cloud environments. Other Cloud capabilities range over these four pillars: knowledge of security posture, automating native security, proactive compliance, deploying security monitoring and response.

TIPS ON CLOUD SECURITY FOR SME'S

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

In recent times, there has been a proliferation of cloud providers (Cloud Computing), providers who have the responsibility to manage the customer's IT infrastructure, integrate applications and develop new capabilities and functionality. This increase in supply, responds, of course, to a parallel increase in demand: more and more individuals and legal entities, as well as entrepreneurs, freelancers and micro or small enterprises, are storing their documents and files in the virtual space, which is known as how to "migrate to the cloud". You have surely all heard of it or use Google Enterprise or Dropbox; these are just two of the most popular cross-platform cloud file hosting services, but there are many more.

The #Negocibersegur campaign for companies of the Cybersecurity Agency of Catalonia has written an article to help raise awareness of the dangers of having poorly configured security cloud services and simple tips on how to avoid exposure.

By @ciberseguracat #ECSO #CyberAwareness #digitalsiprotegits

CHECK OUT THE INFOGRAPHIC

In Catalan

BRING THE LAYER OF TRUST IN THE CLOUD

While the major cloud service providers are experts at ensuring the security of their cloud, security inside the cloud is largely the responsibility of the customer. The native security controls of cloud providers are useful, but they have their limits. That is why, the question enterprises need to be asking is not 'is the cloud secure?', but rather 'am I using the cloud securely?'.

A new mindset: cybersecurity goes hybrid

In today's hybrid, multi-cloud environment, organizations should integrate all their security controls into one overall security posture. Only with a robust approach to cybersecurity, protecting data that is shared across both public and private clouds, can the benefits of cloud be maximized. Atos has built a secure hybrid cloud platform for these complex new ecosystems, adding an additional layer of cloud native security controls that can be managed as a single pane-of-glass covering both cloud computing and legacy environments.

Learn more about:

What Atos can do for you

Balancing trust with agility in GCP (video)

Building trust in hybrid cloud (white paper)

NETWORK FUNCTION VIRTUALISATION AND SECURITY

ERICSSON

Cloud computing is playing an important role in the evolution of mobile network services. It offers the benefits of using **Network Function Virtualisation (NFV)** to deploy network services implemented in software on top of the cloud infrastructure. NFV benefits from the agility and scalability of cloud, as well as its security, to enable the delivery of secure mobile network services. In this blog, we outline how NFV opens up for secure and efficient monitoring and compliance verification in 5G networks.

UNANSWERED QUESTIONS ON MIGRATION TO CLOUD

One of the unanswered questions in migrating workload to cloud is if this will make the service more or less secure. There are cloud supporters suggesting that standardisations and optimisations in security controls would make the service more secure, others are concerned that losing control and ownership will inevitably imply an increase in risks. Definitively all would agree that when migrating workloads in cloud the security needs to be taken in consideration. Understanding what security controls will be required is a key element to guarantee a smooth and successful migration. In this context, one of the biggest challenges is the migration of security policies. In fact, often security policies for services on premise are depending on physical segmentation and of course migrating in cloud those references will be lost. Decoupling the relations between policies and physical segmentation is a significant enabler and facilitator in the migration. The good news is that we have a consolidated best practice called micro-segmentation to address the needs of applying workload and process-level controls depending on business needs to communicate with each other and no more on physical elements. This is going to offer more flexibility and granularity in the definition of security policies. Therefore, with micro-segmentation it is more effective the detection and prevention of lateral movements within data centres, but also a definitive enabler itself to the migration to the cloud.

Exprivia provides a large catalogue of services (in Italian) that can help you in managing your approach to cybersecurity

HUAWEI CLOUD SECURITY PROTECTION FRAMEWORK

In early 2017, Huawei formally established its Cloud Business Unit ("Cloud BU"), raising the curtain on a new era for Huawei Cloud. A comprehensive set of highly effective cloud security strategies and practices has emerged through integrating leading cloud security concepts from across the industry and established security best practices. Huawei Cloud recently released the Huawei Cloud Security White Paper, marking three years since the release of the previous version, entitled Huawei Cloud Service Security Technology White Paper. It shares Huawei Cloud's extensive cloud security experience with our users and the industry at large, so as to help us all better understand and learn from each other, while jointly promoting the openness and progress of both the cloud industry and cloud security industry. In those three short years, the cloud security market has undergone continuous dramatic changes and we are pleased to propose our insights on important topics such as Shared Responsibility Model, Security Compliance and Privacy protection, Organisation and Personnel, Infrastructure, Tenant services or operational security.

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

RESOURCES AND CHECKLISTS FOR USING CLOUD SERVICES WITH CYBERSECURITY

Cloud services offer deployment, standards and pay-per-use features that make them affordable and adaptable also for SMEs, and make them essential for their digital transformation. However, when using cloud services, SMEs have to adapt their security requirements for the protection of their data and business transactions. The privacy of their customers, the security of cloud storage, the frequency of audits and access controls are some of the aspects to consider. On the Spanish National Cybersecurity Institute's (INCIBE) website SMEs can find a Guide "Cloud computing: an approach guide for the businessman" (in Spanish) which offers measures to establish Cloud service contracts that guarantee the security of their business. In addition, this March a new section is being published, TemáTICas Cloud (in Spanish), which provides information on the different cloud services, the cybersecurity issues SMEs should consider, such as risks and threats, and measures to be taken to avoid incidents.

WHAT IS OUR CYBER SECURE CLOUD?

A complete framework for the immediate adoption of the Cloud to concretely support organisations on their path towards a sustainable digital transformation under the cyber resilience paradigm thanks to an effective protection against cyber threats. In partnership with Aruba, the largest Italian Cloud provider, with our Cyber Secure Cloud we aim at raising awareness and implementing the Italian and European guidelines for the adoption of a “secure by design” Cloud (according to a “Cloud First” approach) in compliance with the principle of digital data sovereignty and with the Italian (National Cyber Security Perimeter) and European regulations for both cyber security and privacy matters.
As Day-1 members of the GAIA-X project we bring our concrete contribution and our expertise for the development of the European cloud ecosystem and governance for processing sensitive data of European citizens.

More information can be found here.

NASK

SECURITY, RELIABILITY AND TRUST IN CLOUD DIGITAL SERVICE CHAINS

In the era of massive business digitalisation, transition to the cloud has become a standard procedure for businesses making. However, it is important to ensure that modern cloud-based business models are not at greater risk than on-premise ICT environments. Evolving such business models are progressively reshaping the scope and structure of the cloud services provided by third parties, with tight integration with the cloud. Several market forces are already driving towards the creation of multi-domain and complex business service chain in clouds, which bring more agility in security and privacy concerns. NASK, through participation in the H2020 GUARD project, collaborates with leading EU cybersecurity players in developing an innovative, open and extensible cloud-based platform for advanced assurance and protection of trustworthy and reliable business chains spanning multiple cloud administrative domains and infrastructures. Intelligent Net Anomaly Detectors and Signature-based Attack Detectors developed by NASK as the components of the GUARD platform can be successfully implemented in local cloud clusters and edge-like infrastructures (such as LoRa networks) as well as the multi-cluster cloud integrated environment.

Detailed information is available on the GUARD website

OMNES INVESTS IN SEKOIA - INTELLIGENCE-DRIVEN SAAS SIEM

Last year, Omnes led the €10M investment in Sekoia.io, a next generation SIEM and threat intelligence platform. This investment is be mainly devoted to accelerating the marketing of the platform for its European public and private companies and to strengthening its R&D teams.

Check out Sekoia's article on Cloud Security: HERE

YOUR TOP 3 CLOUD SECURITY CHALLENGES

1. Insufficient identity, authorisation & access management, insecure interfaces & APIs
2. Data privacy & data breaches in off-site storage. What about the protection of information, such as trade secrets, personal data or intellectual property?
3. System weaknesses and hackable user accounts

Highly sensitive data = higher requirements for secure data exchange

- You need extra security for secure data exchange because you do not want to rely solely on third-party providers & their security mechanisms. You want to retain control over your data. When exchanging and storing files, you depend on maximum security.
- You need a solution that enables globally deployed teams to work together on sensitive projects. It must be compatible with all common file sharing, cloud solutions (e.g. Magenta Cloud, Google Drive) & file formats. It should enable secure data exchange to different security zones.

We at Rohde & Schwarz Cybersecurity strongly recommend that you take responsibility for cloud security again, because data leaks and data breaches are also possible in the cloud! Our recommendation is a paradigm shift from perimeter security to data-centric security. The control of your data should be in your hands and consist of a mix of identity management and encryption. When migrating to the cloud, protect your data regardless of external IT infrastructure. State-of-the-art encryption guarantees that data remains unreadable for unauthorised persons. More information can be found here.

ASSESSMENT, CONSULTING AND OPERATION OF THE SECURITY OF YOUR CLOUD ENVIRONMENTS

Certified professionals in the main public cloud providers observing security operators, compliance & risk consultants, Security auditors & hackers, security integrators & IoT security experts, work towards:

- Enabling digital transformation by adopting securely Cloud technologies
- Enablin teleworking by ensuring secure cloud collaboration environments

Read more about S21Sec's Cybersecurity in Cloud & Transformation Programmes here

SECUSTACK MAKES DIGITAL SOVEREIGNTY IN THE CLOUD A REALITY

Security, trustworthiness and transparency are essential for cloud computing.

To ensure that the step into the cloud will not result in digital dependency, SecuStack by Secunet allows you to retain full control over your processed and stored data. SecuStack is a cloud operating system which enables simple and secure provision of resources for the operation of cloud applications using “Infrastructure as a Service” (IaaS). Transparently integrated cryptographic mechanisms now ensure consistent and secure transfer, storage and processing of data as well as networking of resources in a cloud environment. SecuStack thus enables various sectors and institutions, which were as yet unable or unwilling to use cloud computing due to strict security regulations or lack of trust, to get started with it. Digital sovereignty in the cloud has become a reality with SecuStack.

More information can be found here.

SECURITY MADEIN.LU

circl.lu cases.lu c-3.lu

CLOUD SECURITY: WISHFUL THINKING OR REALITY?

The eternal dilemma: where is our data more secure, on our machine or ‘somewhere’ in the cloud?

A new article from SECURITYMADEIN.LU attempts to answer what threats may affect our data in the cloud, which the most common threats are, and what trends can be expected in 2021.

Read the article HERE

STORMSHIELD

COMBINING CYBERSECURITY AND EUROPEAN SOVEREIGNTY

Moving to the cloud is a choice of simplicity and agility but could represent a loss of control unless independent and sovereign cybersecurity solutions are used. To address this stake, Stormshield Elastic Virtual Appliance provides unified threat protection for Cloud assets with a 100% European technology. More information HERE.

sweepatic SECURITY

MOVE TO THE CLOUD: KEEP TRACK OF YOUR INTERNET-FACING ASSETS

With digital transformation and the move to the cloud at full speed, organisations struggle to keep track of their online assets and their exposure. The Sweepatic Platform automatically maps, monitors and manages your attack surface for you.

Our innovative cloud platform delivers attack surface management to our customers and partners, proactively protecting them from cyberattacks. Our solution produces high impact insights and easy-to remediate findings to improve your organisation's cyber resilience.

For more information, check out Sweepatic's website HERE

THALES
Building a future we can all trust

CLOUD SECURITY IS MULTI-CLOUD SECURITY. DEPEND ON A 3RD-PARTY VENDOR

Shared Responsibility Models for Cloud Security published by AWS, Microsoft Azure and other cloud providers state that cloud users are ultimately responsible for the security of data they store in the cloud. Meanwhile, various studies reveal that nearly all large organisations consume multiple clouds. 451 Research indicates that cloud users mature in the cloud journey depend on third parties to aggregate security controls across clouds. Read about how the CipherTrust Data Security Platform from Thales helps deliver multicloud data security and secure, centralised key management.

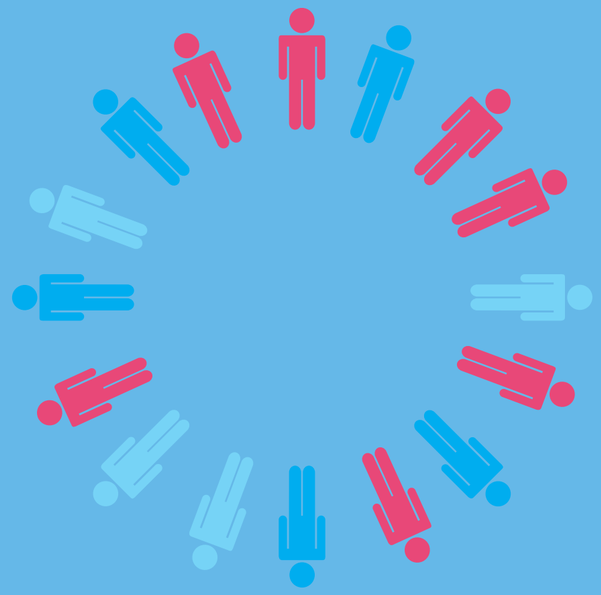
utimaco®

Drive your digital transformation

ROOT OF TRUST PLATFORM FOR A SECURE CLOUD

Organisations are embracing the cloud as the key enabler as they go through the journey of digital transformation and the COVID pandemic is further accelerating this mandate. The use of digital certificates for cloud applications and user authentication is growing rapidly. A big challenge is the diversity and heterogeneity of related data security infrastructures, leading to high cost of ownership and susceptibility to errors. Just like integrated as on-premises solutions, cloud based HSMs need to be able to protect data across the hybrid cloud, from the local datacenter to any third-party cloud. It is vital that the operating company - the 'data controller' (regardless of whether it is a financial institution or an automotive manufacturer) maintains ownership of the keys, to avoid a vendor lock-in with a cloud operator but also to prevent access to unencrypted data by third parties. Cloud technology allows both organisations and individuals to be more efficient. It enables faster, easier, and more cost-effective computing, all within a secure and customisable environment.

Read our latest Whitepaper "Building Trust in the Cloud" to learn more about HMS based cloud security, the next generation of HSMs and how they enable you to secure your keys in the cloud.



RESOURCES FROM THE COMMUNITY

AWARE7
full service awareness agency

WHY DOES IT ALWAYS RAIN ON ME - PENTESTING IN THE CLOUD

Protecting Information in the cloud is a major challenge for businesses. AWARE7 helps you to uncover risks using cloud penetration test methods and strategies. We will not leave you out in the rain. More information HERE.

SKYFLOK, NEXT GENERATION MULTI-CLOUD SHARING & STORAGE

Chocolate Cloud

SkyFlok
YOUR CLIENTS' DATA DESERVES ITS PRIVACY

SkyFlok is a (Privacy-By-Design) File Storage and Secure Sharing service that simplifies the process to go to the cloud. SkyFlok protects your data by spreading it across multiple cloud providers and cities of your choice. WEBSITE.

HOW CONFIDENTIAL COMPUTING CAN ENABLE SECURE USE OF THE PUBLIC CLOUD

Confidential computing enables organisations to migrate extremely sensitive data to the cloud which has been difficult before due to privacy, security, and regulatory concerns around securing workloads in the cloud. Check out more HERE.

DEPLOY SECURED CLOUD INFRASTRUCTURE WITH PROXMOX AND DYNFI

Discover how to secure of your Proxmox Cloud based infrastructure in this 15 page White Paper sponsored by DynFi. Deploy highly scalable secured cloud infra with Proxmox and let DynFi team secure it. The paper is available in EN and FR.

esatus® AG
Enforcing Information Security

HOW TO GUARANTEE CLOUD SECURITY WITH MAXIMUM TRUST AND NO COMPLEXITY?

Click here to see what our Self Sovereign Identity technology #SSI has to offer: secure authentication, full interoperability and easy integration. For a deeper dive into #SSI, check out this White Paper (in German).

CLOUD SECURITY AND CLOUD COMPLIANCE: PESA FOR MORE TRUST IN DIGITAL PROCESSES

procilon GROUP

pESA security cloud services meet high security demands and contribute to integrity and authenticity. Integrate our trust elements such as eIDAS-compliant signatures, encryption, and secure file exchange into your cloud app. More information can be found HERE.

THANK YOU!

for your time

Cybersecurity Awareness Calendar is an initiative launched by:
European Cyber Security Organisation (ECSO)
29, rue Ducale
1000 - Brussels

http:// www.ecs-org.eu

secretariat@ecs-org.eu

/company/ecso-cyber-security/

@ecso_eu