CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

Newsletter N. 22
15-31 Marzo 2023

FACT.ZERO

Primo Forum Cyber 4.0: 6 e 7 Giugno 2023

Leonardo Querzoni, Presidente Cyber 4.0 - 7 Aprile 2023

CYBER 4.0 si prepara alla prima edizione del suo Forum! Il 6 e 7 Giugno prossimi incontreremo le istituzioni, il mondo della ricerca e le imprese per discutere di come il nostro paese sta affrontando le emergenze della cybersecurity, quanto si è fatto e quanto ancora possiamo fare, e soprattutto come CYBER 4.0 sta contribuendo a tutto questo. L'appuntamento è presso l'Aula Magna della Sapienza Università di Roma, una location di prestigio per un evento che vedrà la partecipazione dei principali attori che agiscono in questo settore: dalle istituzioni italiane a quelle europee, dal mondo accademico a quello delle imprese, con un particolare accento sulla realtà di CYBER 4.0 e dei suoi soci. SAVE THE DATE!

IN EVIDENZA

Cyber security, cambio di mentalità e governance integrata fondamentali per aumentare la sicurezza

Innovation Post - 7 Aprile 23

"Un cambio di mentalità, che consideri finalmente la cybersecurity un asset strategico e imprescindibile per le aziende. E una governance integrata, perché la cyber-sicurezza è un aspetto che riguarda e comprende tutte le aree e le attività di un'impresa". […]Sono molti i fenomeni cyber cui sono soggette le imprese e, spesso, anche i loro clienti, come frodi informatiche, furto di dati, blocco dei dispositivi, errori umani legati alla mancanza di consapevolezza dell'uso sicuro di dispositivi elettronici, internet, e-mail, social network.

Vedi altro

Cyber Security, rischi e opportunità per chi opera nel settore dell'Energia

Innovation Post - 31 Marzo 23

[…] Secondo Matteo Lucchetti, direttore del Competence Center Cyber 4.0, che ha partecipato all'incontro, "nel settore energia l'aumento dei casi di ransomware andati a segno si inserisce in un quadro in cui l'integrazione delle tecnologie operative (OT) con i sistemi IT ha da tempo sottolineato la necessità indifferibile di gestire la cybersecurity come fattore abilitante che deve sostanziare le strategie del business aziendale".

Vedi altro

Diagnose your SME's Cybersecurity and Scan for Recommendations

ENISA - March 28, 23

Standing as a major driver for innovation and growth in the EU and as key actors of our economy, SMEs are constantly facing cybersecurity challenges. This is why it is essential to support them in addressing these challenges and in identifying improvements. The cybersecurity maturity assessment tool designed by ENISA supports those small and medium-size businesses who seek to understand their current cybersecurity maturity level. Thanks to this tool, they will be able to define the risks they face. They will also be given a remediation plan to mitigate them and improve their maturity.

Vedi altro

Articoli Correlati:
Cybersec Italia, PMI e cybersecurity, ENISA rilascia un tool per 'testare' la sicurezza delle piccole e medie imprese

Sicurezza e tecnologia, imprese e istituzioni a confronto all'Aquila nella seconda tappa del Roadshow di Ministero delle Imprese e Invitalia organizzata dal Comune

Comune L'Aquila – 28 Marzo 23

[...] Durante la mattinata sono state presentate le principali opportunità messe in campo dal Ministero per le imprese, gli incentivi e servizi di accompagnamento di Invitalia a supporto delle startup, con un focus specifico sul tema cyber security, anche grazie alla partecipazione del Competence Center Cyber 4.0 che ha offerto un momento di formazione mirata.

Vedi altro

Accordo di collaborazione tra SOCINT e Cyber 4.0

Cyber 4.0 – 7 Aprile 23

Cyber 4.0 ha sottoscritto un accordo di collaborazione con SOCINT, la Società Italiana di Intelligence, e in particolare con la sua Commissione Cyber Threat Intelligence & Cyberwarfare. SOCINT e Cyber 4.0 avviano così una collaborazione tecnico-scientifica in tema di cybersecurity e cyber intelligence, allo scopo di promuovere la cultura della cybersecurity attraverso la redazione di articoli, report e policy brief, e l'organizzazione o la partecipazione congiunta ad eventi specializzati del settore.

Vedi altro

Articoli Correlati:
Socint, Accordo di collaborazione con Cyber 4.0

Codice Appalti: cybersicurezza tra i criteri premianti

Edilportale - 4 Aprile 23

L'articolo 108 del Codice Appalti prevede che, nelle attività di approvvigionamento di beni e servizi informatici, le stazioni appaltanti, nella valutazione dell'elemento qualitativo ai fini dell'individuazione del miglior rapporto qualità prezzo per l'aggiudicazione, tengano sempre in considerazione gli elementi di cybersicurezza. Il riferimento alla cybersicurezza è presente anche nell'Allegato I.9, contenente i "Metodi e strumenti di gestione informativa digitale delle costruzioni". L'Allegato stabilisce che le stazioni appaltanti possono definire requisiti e soluzioni tecnologiche che costituiscono criteri premianti nella valutazione delle offerte. Tra le soluzioni che possono ottenere un punteggio aggiuntivo ci sono quelle per facilitare la gestione dell'ambiente di condivisione dei dati nell'ambito della cyber security.

Vedi altro

Thierry Breton: "Ci vogliono in media 190 giorni per rilevare un attacco cyber sofisticato. Presto un Cyber Solidarity Act a livello Ue"

Cybersecurity Italia – 7 Aprile 23

"Oggi ci vogliono in media 190 giorni per rilevare un attacco cyber sofisticato. Dobbiamo ridurre drasticamente questo tempo a poche ore. A tal fine, tra poche settimane, la Commissione proporrà un Cyber Solidarity Act per istituire un'infrastruttura europea di centri operativi di sicurezza (Soc) che scansioneranno la rete utilizzando tecnologie di intelligenza artificiale e individueranno i segnali deboli degli attacchi. Questa infrastruttura comune europea di rilevamento avanzato costituirà un vero e proprio scudo informatico europeo e sarà una sorta di 'cupola di protezione europea'. Sarà, per così dire, il nostro Cyber Galileo. Ma oltre ai Soc, dobbiamo anche rafforzare la sicurezza e la resilienza delle nostre infrastrutture critiche. A tal fine, stiamo allestendo, in collaborazione con gli Stati membri, scenari di attacco e test di penetrazione". Lo ha detto Thierry Breton, commissario per il Mercato interno, intervenendo a Lille al Forum internazionale sulla sicurezza informatica.

Vedi altro

Intelligenza artificiale: il Garante blocca ChatGPT. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori

GPDP – 31 Marzo 23

Stop a ChatGPT finché non rispetterà la disciplina privacy. Il Garante per la protezione dei dati personali ha disposto, con effetto immediato, la limitazione provvisoria del trattamento dei dati degli utenti italiani nei confronti di OpenAI, la società statunitense che ha sviluppato e gestisce la piattaforma. L'Autorità ha contestualmente aperto un'istruttoria.

Vedi altro

Articoli Correlati:

Gpdp, ChatGPT: OpenAI collabora con il Garante privacy con impegni per tutelare gli utenti italiani

Global woman Magazine, Mira Murati: The Albanian Woman Who Developed ChatGPT

Online market selling stolen account credentials to criminals worldwide taken down in multi-country effort dubbed Operation Cookie Monster

Eurojust– April 5, 23

Genesis Market has been taken down in an operation involving judicial and law enforcement authorities in the United States, nine European Union countries, Australia, Canada and the United Kingdom. Genesis Market was a criminal marketplace accessible on the dark web and clear web that sold packages of account access credentials – including usernames and passwords for email, bank accounts, and social media.

Vedi altro

German Police Raid DDoS-Friendly Host 'FlyHosting'

Krebs On Security – March 31, 2023

Authorities in Germany this week seized Internet servers that powered FlyHosting, a dark web offering that catered to cybercriminals operating DDoS-for-hire services, KrebsOnSecurity has learned. FlyHosting first advertised on cybercrime forums in November 2022, saying it was a Germany-based hosting firm that was open for business to anyone looking for a reliable place to host malware, botnet controllers, or DDoS-for-hire infrastructure.

Vedi altro

'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics

The Guardian – March 30, 2023

Documents leaked by whistleblower angry over Ukraine war. Private Moscow consultancy bolstering Russian cyberwarfare. Tools support hacking operations and attacks on infrastructure. Documents linked to notorious Russian hacking group Sandworm. Russian program aims to control internet and spread disinformation.

Vedi altro

Customers still can't access My Cloud data after Western Digital hack fallout

Apple Insider – April 6, 2023

A hacker breached Western Digital and stole data, and in response, the company has shut down a wide swathe of its services which is preventing users from accessing their My Cloud files. On April 3, Western Digital disclosed that it had a security incident on March 26. It is still unknown who was responsible for the breach or if it was a ransomware attack. However, some of Western Digital's data was stolen in the incident. The company is trying to determine how much data was affected and if it included information from customers.

Vedi altro

Articoli Correlati:

Red Hot Cyber, Western Digital Subisce un Enorme Attacco Informatico, I servizi Cloud sono completamente paralizzati

Tesla Model 3 Hacked in Less Than 2 Minutes at Pwn2Own Contest

Dark Reading– March 24, 2023

Researchers from France-based pen-testing firm Synacktiv demonstrated two separate exploits against the Tesla Model 3 this week at the Pwn2Own hacking contest in Vancouver. The attacks gave them deep access into subsystems controlling the vehicle's safety and other components. One of the exploits involved executing what is known as a time-of-check-to-time-of-use (TOCTTOU) attack on Tesla's Gateway energy management system. They showed how they could then — among other things — open the front trunk or door of a Tesla Model 3 while the car was in motion.

Vedi altro

NUOVE PUBBLICAZIONI

Stanford, Measuring trends in Artificial Intelligence, 2023

FBI, Internet Crime Complaint Center Report 2022

Europol, ChatGPT - the impact of Large Language Models on Law Enforcement, March 28, 23

ENISA, Cybersecurity Market Analysis Framework (ECSMAF) -V2.0, March 27, 23

PROSSIMI EVENTI

Cyber 4.0, Roadshow Cyber 4.0 Marche, 13 Aprile 2023, Pesaro

Cyber 4.0 - Leonardo, Evento premiazione CyberX - Mind4Future, 18 Aprile, Roma

Cyber 4.0 - Ict Security Magazine - SOCINT, Cybercrime Conference, 11-12 Maggio, Roma

Cyber 4.0 - Forum Cyber 4.0, 6-7 Giugno, Roma, Aula Magna La Sapienza Università di Roma

Cyber FACTory 4.0 è una newsletter con cadenza bisettimanale.
Le notizie sono selezionate per attinenza alle attuali aree di interesse di Cyber 4.0 e non rappresentano posizioni ufficiali del Centro di Competenza.
Ricevi questo contenuto in quanto hai preso parte alle attività del Centro.
Per ulteriori informazioni, contributi, iscrizioni o rimozioni da questa lista di distribuzione, contattare: **comunicazione@cyber40.it**

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER