CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

Newsletter N. 9
1-15 Settembre 2022

FACT.ZERO

La formazione come arma migliore contro i cybercriminali

Leonardo Querzoni, Presidente Cyber 4.0 - 22 Settembre 22

Bentornati al nostro consueto appuntamento con la newsletter di Cyber 4.0. In questo inizio di settembre cattura certamente l'attenzione la notizia che l'Italia sia stato il paese europeo maggiormente colpiti da malware nella prima metà del 2022. Le "gang" Lockbit e Conti (per citare le maggiori) hanno visto un enorme incremento delle loro attività, spesso a danno delle nostre pubbliche amministrazioni o imprese. Per contrastare questo tipo di minaccia, oltre alle dotazioni tecnologiche, è indispensabile che il personale sia addestrato per riconoscere i vettori di attacco tipici di questi attori, permettendo di anticipare e bloccare gli attacchi sul nascere. La formazione, tra le missioni fondamentali di CYBER 4.0, rimane oggi la nostra migliore arma contro i cybercriminali.

IN EVIDENZA

State of the Union: EU Cyber Resilience Act - Questions & Answers

European Commission - September, 15, 22

The Cyber Resilience Act is a first ever EU-wide legislation of its kind: it introduces common cybersecurity rules for manufacturers and developers of products with digital elements, covering both hardware and software. It will ensure that wired and wireless products that are connected to the internet and software placed on the EU market are more secure and that manufacturers remain responsible for cybersecurity throughout a product's life cycle.

Vedi altro

Italia prima in Europa per attacchi ransomware

Ansa, 14 Settembre 22

L'Italia è il Paese europeo più colpito dai ransomware nel primo semestre del 2022. Secondo "Defending the Expanding Attack Surface", l'ultimo report dell'azienda di sicurezza informatica Trend Micro, sulle minacce della prima parte dell'anno, i ransomware hanno visto un vero boom in Italia, primo Paese in Europa, con il 3,56% del totale.

Vedi altro

Cybersicurezza, strutture energetiche italiane sotto attacco

Milano Finanza - 2 Settembre 22

Dopo gli attacchi a Gse e Eni si riunisce il Nucleo per la cybersicurezza. Italia tra i paesi più colpiti. Nel mirino ci sono le principali aziende del settore energia ma anche la catena di distribuzione dei prodotti o servizi connesse.

Vedi altro

Correlati:
Cybersecurity Italia, Energia, Terzo attacco: un'altra vittima il gruppo Canarbino

Servono corsi obbligatori di cybersecurity per chi ricopre cariche pubbliche

Repubblica - 15 Settembre 22

Il profilo Twitter del ministero della Transizione ecologica è stato hackerato. Non è la prima volta che succede ad un ministro in Italia o nel mondo. Capita. Non tutti i giorni, ma capita. E va aggiunto che questi episodi dimostrano una certa vulnerabilità informatica di un ministero chiave in questa fase di crisi del prezzo del gas.

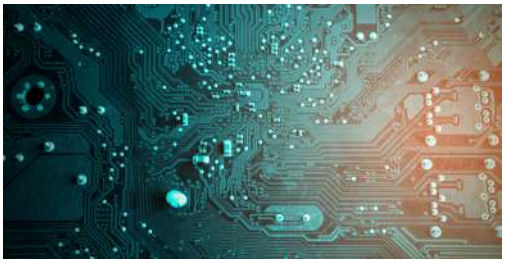
Vedi altro

Una legge europea per la cybersecurity dei prodotti tecnologici

Wired - 15 Settembre 22

La Commissione europea ha presentato una proposta relativa a una nuova legge sulla cybersecurity per proteggere i consumatori e le imprese da prodotti con caratteristiche di sicurezza informatiche inadeguate. La legge è stata annunciata dalla presidente della Commissione Ursula von der Leyen durante il discorso sullo stato dell'unione del 2021 e si basa sulla strategia dell'Unione europea per la cybersecurity presentata nel 2020.

Vedi altro

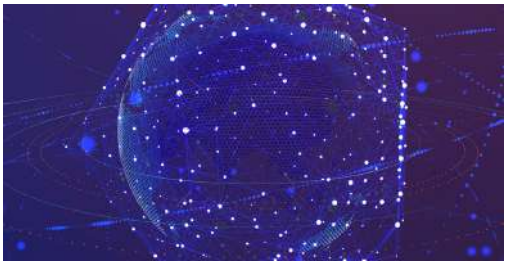


The Artificial Intelligence and Cybersecurity Nexus: Taking Stock of the European Union's Approach

Carnegie Europe - September, 15, 22

The EU's AI-cybersecurity ecosystem remains highly fragmented. To realize its technological leadership ambitions, the bloc must connect the dots between its myriad initiatives, processes, and stakeholders.

Vedi altro



Finanza, poche donne nei settori fintech e cybersecurity

Italia Oggi - 15 Settembre 22

Nei settori più emergenti dell'economia italiana e mondiali, cioè cybersecurity e fintech, "le donne sono praticamente assenti". Lo denuncia Claudia Segre, presidente di Global Thinking Foundation, non-profit nata nel 2016 per diffondere l'alfabetizzazione finanziaria e digitale come strumento di empowerment per raggiungere l'indipendenza economica e, quindi, lo sviluppo sociale.

Vedi altro

Hackers Heavily Use Minecraft Game to Lure Players into Installing Malware

Cybersecurity News - September 7, 22

Cybercriminals use Minecraft to lure unsuspecting players into installing malware on their computers, as it is the most frequently abused game title by them.
Kaspersky Labs, which is known for its cybersecurity expertise, have compiled some data between July 2021 and July 2022 that shows some important statistics related to the spread of malicious files via the abuse of game brands.

Vedi altro

Another European nation hit by hackers, Montenegro grapples with ongoing ransomware attack

Cyberscoop - September 2, 22

Multiple Montenegrin government websites remained inaccessible Friday, a week after government officials there said the country's "critical state infrastructure" had been targeted with an "unprecedented" cyberattacks.

Vedi altro

Albania severs diplomatic ties with Iran over cyber-attack

BBC News - September 7, 22

Albania has severed diplomatic ties with Iran and ordered Iranian embassy staff to leave, accusing it of orchestrating a major cyber-attack.
Prime Minister Edi Rama said a probe had found "incontrovertible evidence" that Iran "hired four groups to mount the attack on Albania" on 15 July.
The hackers tried to paralyse public services, delete and steal government data, and incite chaos, he added.

Vedi altro

Classified NATO documents stolen from Portugal, now sold on darkweb

Bleeping Computer - September 8, 22

The Armed Forces General Staff agency of Portugal (EMGFA) has suffered a cyberattack that allegedly allowed the theft of classified NATO documents, which are now sold on the dark web.

EMGFA is the government agency responsible for the control, planning, and operations of the armed forces of Portugal.

Vedi altro

How Fake GPS Coordinates Are Leading to Lawlessness on the High Seas

The New York Times - September 3, 22

A technology enabling the transmission of fake locations to carry out murky or even illegal business operations could have profound implications for the enforcement of international law.

Vedi altro

GPS jammers are being used to hijack trucks and down drones: How to stop them

ZD Net - September 16, 22

Satellite navigation and tracking via GPS has become a critical link in the world's rapidly growing logistics and freight carrying ecosystem. Companies use GPS to track trucks and keep them on time and their cargo secure.

Vedi altro

Hacktivist Group GhostSec Compromises 55 Berghof PLCs Across Israel

The Hacker News - September 12, 22

A hacktivist collective called GhostSec has claimed credit for compromising as many as 55 Berghof programmable logic controllers (PLCs) used by Israeli organizations as part of a "Free Palestine" campaign.

Industrial cybersecurity firm OTORIO, which dug deeper into the incident, said the breach was made possible owing to the fact that the PLCs were accessible through the Internet and were secured by trivially guessable credentials.

Vedi altro

GHIDRA- Free Software Reverse Engineering Framework By NSA

Hackersonlineclub - September 6, 22

GHIDRA is a Software Free Reverse Engineering (SRE) Framework released by The National Security Agency (NSA). In support of NSA's Cybersecurity mission, Ghidra was built to solve scaling and teaming problems on complex SRE efforts, and to provide a customizable and extensible SRE research platform. NSA has applied Ghidra SRE capabilities to a variety of problems that involve analyzing malicious code and generating deep insights for SRE analysts who seek a better understanding of potential vulnerabilities in networks and systems.

Vedi altro

Researcher demonstrates biometric data theft from smart lock with droplock hack

Biometric Update - September 5, 22

Biometric smart locks used in internet of things deployments can be hacked through their wireless connectivity capabilities, according to a new paper from a researcher with James Cook University in Singapore.

Vedi altro

NUOVE PUBBLICAZIONI

ENISA, Be aware, be prepared - Cybersecurity tips for SMEs, 1/3

ENISA, Be aware, be prepared - Cybersecurity tips for SMEs, 2/3

ENISA, Be aware, be prepared - Cybersecurity tips for SMEs, 3/3

Cisa, **Alert (AA22-249A), September 6, 2022**

PROSSIMI EVENTI

European Council, Interinstitutional kick-off event, September 27, Online Event

Cybersecurity for Europe, What can Member States expect from their cybersecurity communities?, September 15, 2022, Brussels

Stati Generali Mondo Lavoro Italia, 27-29 Settembre, Torino

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