CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

Newsletter N. 7
1-15 Agosto 2022

FACT.ZERO

Cyber 4.0 lancia lo Sportello Resilienza Cyber

Leonardo Querzoni, Presidente Cyber 4.0 - 16 Agosto 22

Nonostante la tradizionale atmosfera estiva che caratterizza la nostra penisola in agosto, la cybersecurity non conosce pause. Questo mese CYBER 4.0 lancia uno sportello dedicato alle PA che intendono approfittare del bando aperto dall'ACN. Di carattere diverso la notizia sulla vulnerabilità trovata in uno degli algoritmi (SIKE) per post-quantum cryptography al vaglio del NIST per garantire la confidenzialità dei dati negli anni a venire: la strada da percorrere è ancora lunga.

IN EVIDENZA

Sportello Resilienza Cyber: il Centro di Competenza a supporto delle PA

Cyber 4.0 - 10 Agosto 22

Nell'ambito dell'investimento 1.5 "Cybersecurity" previsto dal PNRR, l'Agenzia di Cybersecurity Nazionale ha pubblicato di recente l'avviso 3/2022, che prevede il finanziamento di interventi di potenziamento della resilienza cyber della Pubblica Amministrazione, con focus specifico su Regioni, Province autonome e Città metropolitane, per un valore complessivo di 45 milioni.

Vedi altro

Pubblicato l'Avviso n. 3/2022 per il potenziamento della resilienza cyber per la PA Locale

ACN - 2 Agosto 22

Un nuovo avviso, pubblicato sul sito Italia Domani, prevede il finaziamento per un valore di 45 milioni di interventi di potenziamento della resilienza cyber destinati alle Regioni, Province Autonome e Città Metropolitane.

Vedi altro

Cybersecurity, Consip aggiudica il primo lotto della gara "Sicurezza da remoto"

Corcom - 4 Agosto 22

Consip spa, la centrale acquisti della pubblica amministrazione italiana, ha stipulato oggi il contratto relativo al lotto 1 della gara per i "servizi di sicurezza da remoto", con gli aggiudicatari Accenture e Tim. Lo riferisce la stessa Consip con un comunicato stampa.

Vedi altro

Cybersecurity, EU funds and Russia. An interview with Italy's cyber czar

Decode 39 - August 5, 22

Our interview with the director of the National Cybersecurity Agency one year after its birth. From the cloud to foreign direct investments, Italy has raised its cyber defences and allies (as well as enemies) have noticed. Russian hackers? The campaign is not over.

Vedi altro

Come funziona il nuovo potere offensivo del governo nel settore cyber

Formiche - 12 Agosto 22

Anche l'Italia si dota di uno strumento normativo che consente di condurre operazioni offensive su suolo straniero anche in assenza di uno stato di guerra formalmente dichiarato. La nuova normalità degli assetti internazionali impone anche all'Italia di accelerare l'adozione di quadro normativo completo. L'analisi di Andrea Monti, professore incaricato di Digital Law dell'università di Chieti-Pescara.

Vedi altro

Italian Elections, Reflections on Digital Vote and Cyber Vulnerabilities

Cybersec Italia - August 10, 22

The Italian elections come in a very sensitive time in Europe, and thus may attract rivals to harm our democratic process, manipulate results, and influence our people through trolls especially on social media. We must put all the efforts needed to monitor and mitigate these risks. We will need to raise public awareness to make sure we are less exposed to information manipulation and fake news injected by external powers.

Vedi altro

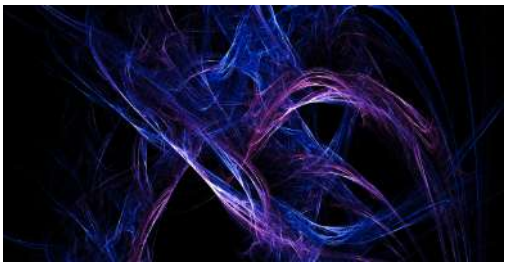
Dominio aerospaziale, il nuovo ruolo dell'Intelligence: come cambiano gli scenari

Cybersecurity 360 - 13 Agosto 22

Il Copasir ha pubblicato la "Relazione annuale sul dominio aerospaziale quale nuova frontiera della competizione geopolitica". Tra gli obiettivi, il potenziamento delle strutture di governance per l'interesse nazionale.

Vedi altro

NEWS



Luxembourg energy companies struggling with alleged ransomware attack, data breach

The Record - August 1, 22

Two companies based in Luxembourg are grappling with an alleged ransomware attack that began last week, the latest in a string of incidents involving European energy companies. Encevo Group said its Luxembourg entities Creos – an energy network operator – and the supplier Enovos were "victims of a cyberattack on the night of July 22."

Vedi altro

Cyberattack on Albanian government suggests new Iranian aggression

Ars Technica - August 5, 22

In mid-July, a cyberattack on the Albanian government knocked out state websites and public services for hours. With Russia's war raging in Ukraine, the Kremlin might seem like the likeliest suspect. But research published on Thursday by the threat intelligence firm Mandiant attributes the attack to Iran. And while Tehran's espionage operations and digital meddling have shown up all over the world, Mandiant researchers say that a disruptive attack from Iran on a NATO member is a noteworthy escalation

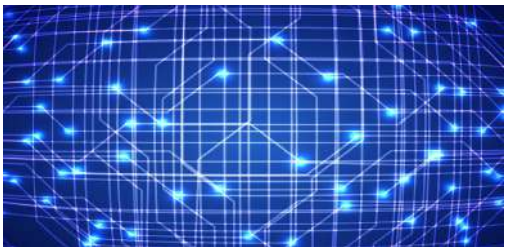
Vedi altro

Russian hackers target Finland parliament's website

Cybernews - August 10, 22

The website of the Finnish parliament went down for several hours yesterday after a distributed denial-of-service (DDoS) attack launched by Russian threat actors. "A denial-of-service attack is directed against the Parliament's external websites. […] The Parliament takes steps to limit the attack together with service providers and the Cybersecurity Center," the Finnish parliament said in a statement.

Vedi altro

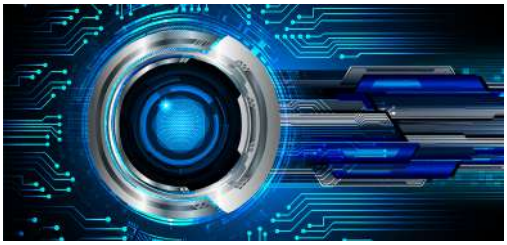


Post-quantum crypto cracked in an hour with one core of an ancient Xeon

The Register - August 3, 22

One of the four encryption algorithms America's National Institute of Standards and Technology (NIST) considered as likely to resist decryption by quantum computers has had holes kicked in it by researchers using a single core of a regular Intel Xeon CPU, released in 2013.

Vedi altro



FIRST Releases Traffic Light Protocol Version 2.0 with important updates

First- August 5, 22

The Forum of Incident Response and Security Team (FIRST) has updated the globally renowned Traffic Light Protocol (TLP) for the cybersecurity industry - a vital system used by organizations all around the world to share sensitive information. The new version of the TLP results from a thorough consultation with over 50 security industry experts over three years with the goals to standardize, unify and modernize the content and language and provide improved supporting materials.

Vedi altro

How to find out if you are involved in a data breach -- and what to do next

ZD Net - August 8, 22

Think you've been involved in a data breach? This guide will help you find out where and when, and it lists the steps you should take next.

Data breaches are security incidents we now hear about every day. They strike every industry, every sector, every county; victim organizations can be everything from small, independent businesses to Fortune 500 companies.

Vedi altro

#YourAccountYourCrime: Global campaign exposes use of money mules

INTERPOL - August 10, 22

INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC) is launching a global awareness campaign today in order to highlight the massive use of money mules in facilitating the movement of criminal proceeds. Money mules are people recruited by criminals, often unwittingly, to transfer funds on their behalf and launder their illicit profits.

Vedi altro

NUOVE PUBBLICAZIONI

GFCE, Developing Cyber Security as a Profession, August 8, 2022

Helpnet Security, Cyberattacks on healthcare organizations negatively impact patient care, August 8, 2022

The Horizon Results Booster, Cyber Ranges for a Resilient Europe, August 2022

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