CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

Newsletter N. 19
1-15 Febbraio 2023

FACT.ZERO

La strategia del MIMIT e il potenziamento di Cyber 4.0

Leonardo Querzoni, Presidente Cyber 4.0 - 4 Febbraio 2023

La firma del Ministro Urso sul Decreto per il potenziamento dei centri per il trasferimento tecnologico era una notizia che aspettavamo da tempo e che conferma la strategicità dei Competence Center nel disegno di potenziamento e sviluppo industriale del Sistema Paese. L'azione di Cyber 4.0 viene ad essere significativamente rafforzata come interfaccia con il mondo industriale, e in particolare le PMI, sulle questioni di cybersecurity, sia in termini di capacità di erogare servizi che di rafforzare le infrastrutture di test-before-invest. Il Centro peraltro è doppiamente impattato, dal momento che - altra notizia molto rilevante di questo periodo - è anche coordinatore di un Polo Europeo di Innovazione Digitale (European Digital Innovation Hub), che ha ricevuto il Seal of Excellence dalla Commissione Europea, e la cui azione riceverà supporto sempre sotto la stessa linea di budget PNRR. Cyber 4.0 sarà pertanto un vero e proprio perno anche nell'implementazione della Strategia Nazionale di Cybersecurity,.

IN EVIDENZA

350 milioni per i Centri di trasferimento tecnologico

Ministero delle Imprese e del Made in Italy - 17 Febbraio 23

Il ministro delle Imprese e del Made in Italy, Adolfo Urso, ha firmato il decreto ministeriale che finanzia con 350 milioni i centri di trasferimento tecnologico nel nostro Paese. La misura, prevista dal PNRR alla missione 4, serve al potenziamento e all'estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria così da incoraggiare l'erogazione alle imprese, nonché alle pubbliche amministrazioni, di servizi tecnologici avanzati e innovativi focalizzati su tecnologie e specializzazioni produttive di eccellenza.

Il provvedimento stanzia la somma complessiva di **350 milioni** di euro. In particolare, 113,4 milioni di euro sono destinati al rifinanziamento degli 8 centri di competenza ad alta specializzazione; 33,6 milioni di euro sono per il cofinanziamento dei 13 Poli europei di innovazione digitale (EDIH) selezionati a valle della gara europea Digital Europe; infine una quota pari a circa 114,5 milioni di euro è destinata a finanziare i 24 Poli europei di innovazione digitale che hanno ricevuto il "Seal of Excellence" dalla Commissione Europea.

Vedi altro

Articoli Correlati:

Cyber 4.0, Il Ministro Urso firma il decreto per il potenziamento dei Centri di Trasferimento Tecnologico, 17 Febbraio 23
Innovation Post, PNRR, firmato il decreto che assegna 350 milioni alle strutture dedicate al trasferimento tecnologico, 17 Febbraio 23

Cyber security, il polo europeo di innovazione digitale Nest riceve il Seal of Excellence della Commissione UE

Innovation Post - 14 Febbraio 23

Favorire l'innovazione nella cybersecurity a livello nazionale e regionale, dalla pubblica amministrazione, all'industria automotive, dall'aerospaziale alla sanità: è questo l'obiettivo di NEST – Network for European Security and Trust, progetto per un nuovo Polo Europeo di Innovazione Digitale (EDIH) con capofila il Centro di competenza nazionale Cyber 4.0 di Roma, con una proposta che ha ottenuto il "Seal of Excellence" della Commissione Europea.

Lo European Digital Innovation Hub NEST è stato concepito come punto di aggregazione in cui convergeranno soluzioni di cybersecurity (settore ad alta specializzazione di Cyber 4.0) e iniziative di capacity building rivolte alle Pmi e alle Pa del Centro Italia (Lazio, Umbria e Abruzzo).

Vedi altro

Articoli Correlati:

Cyber 4.0, NEST riceve il "Seal of Excellence" della Commissione UE, 14 Febbraio 23

Corsi e master, quanto è importante una cultura cyber diffusa

Cybersecurity 360 - 15 Febbraio 23

Un percorso formativo di tipo esperienziale invece è dato dall'iniziativa CyberX – Mind4Future sviluppata dal centro Cyber 4.0, competence Center di Cybersecurity del MISE, in collaborazione con Leonardo e presentata a Roma il 19 Gennaio. L'iniziativa ha raccolto 518 iscritti che proveranno a vincere una delle 10 borse di studio messe a disposizione. La formazione avanzata riguarda: crittografia, sicurezza delle reti di calcolatori, analisi del codice binario, sicurezza dei sistemi e delle reti.

Vedi altro

La Cybersecurity in Italia e le nuove sfide tecnologiche

Ministero delle Imprese e del Made in Italy - 20 Febbraio 23

Ciclo di seminari online - Lo scenario cyber, in ambito nazionale ed internazionale, sta diventando sempre più complesso e caratterizzato da minacce informatiche sempre più pericolose e tecniche di attacco sempre più evolute. Cittadini, Imprese e Pubbliche Amministrazioni subiscono danni a volte molto onerosi che incidono, oltre che sulla sfera personale, sulla funzionalità e sulla operatività delle organizzazioni, con impatto sui servizi forniti, talvolta nell'ambito di attività essenziali per il Paese.

Vedi altro

Le PMI italiane pronte ad investire 470 milioni di euro sulla sicurezza informatica nel 2023. I dati di Confesercenti

Cybersecurity Italia - 17 Febbraio 23

Secondo un sondaggio condotto da SWG per Confesercenti, il 52% delle PMI tra i 10 e i 50 dipendenti prevede di destinare risorse a questo fine nell'anno in corso, con una spesa media di 4.800 euro per impresa per un totale di oltre 470milioni.

Vedi altro

Sustained Activity by Threat Actors

ENISA - 15 February 23

The European Union Agency for Cybersecurity (ENISA) and the CERT of the EU institutions, bodies and agencies (CERT-EU) jointly published a report to alert on sustained activity by particular threat actors. The malicious cyber activities of the presented threat actors pose a significant and ongoing threat to the European Union. [...] ENISA and CERT-EU strongly encourage all public and private sector organisations in the EU to apply the recommendations listed in the current joint publication "Sustained Activity by specific Threat Actors."

Vedi altro

La strategia nazionale sulla cybersicurezza: dalla pubblica amministrazione alle start up

Il Sole 24 Ore - 9 Febbraio 23

Si tratta di circa 2 miliardi di euro che il governo ha deciso di investire per programmi, bandi e fondi in molte direzioni, da qui al 2037. Da una parte, il mega progetto serve a sostenere programmi di adeguamento alle esigenze della sicurezza delle pubbliche amministrazioni. Dall'altro, si investe in start up e progetti innovativi che si occupano di scienza dei dati, intelligenza artificiale, robotica, internet delle cose, blockchain, computazione quantistica e crittografia [....].

Per quanto riguarda in particolare le start up, l'ACN potrà erogare finanziamenti a fondo perduto direttamente alle aziende innovative, sostenerne la comunicazione, selezionare le candidature e sviluppare collaborazioni utili.

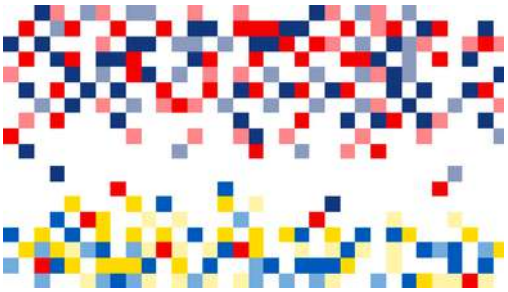
Vedi altro

Coordinated Vulnerability Disclosure: Towards a Common EU Approach

ENISA - 16 February 23

The new report of the European Union Agency for Cybersecurity (ENISA) explores how to develop harmonised national vulnerability programmes and initiatives in the EU.

Vedi altro



Fog of war: how the Ukraine conflict transformed the cyber threat landscape

Google Threat Analysis Group - 16 February 2023

First, Russian government-backed attackers have engaged in an aggressive, multi-pronged effort to gain a decisive wartime advantage in cyberspace, often with mixed results. […] Second, Moscow has leveraged the full spectrum of information operations — from overt state-backed media to covert platforms and accounts — to shape public perception of the war. […]
Finally, the invasion has triggered a notable shift in the Eastern European cybercriminal ecosystem that will likely have long term implications for both coordination between criminal groups and the scale of cybercrime worldwide.

Vedi altro

Pro-Russia hacker group Killnet targets NATO websites with DDoS attacks

Security Affairs - 13 February 23

Pro-Russia hacker group Killnet launched a Distributed Denial of Service (DDoS) attack on NATO sites, including the NATO Special Operations Headquarters (NSHQ) website. […] According to The Telegraph, the website of Nato Special Operations Headquarters remained unreachable for a couple of hours.

Vedi altro

Cloud: pubblicato il decreto per la transizione di infrastrutture e servizi digitali

ACN – 8 Febbraio 23

L'Agenzia per la Cybersicurezza Nazionale ha pubblicato oggi il decreto direttoriale che determina tempi e modi per la transizione delle infrastrutture e servizi digitali gestiti dalle Pubbliche Amministrazioni o dalle Società a controllo pubblico al nuovo quadro regolatorio relativo alla valutazione e verifica di rispondenza ai requisiti di qualità e sicurezza.

Vedi altro

An email attack can end up costing you over $1 million

Helpnet Security - 10 February 23

75% of the organizations had fallen victim to at least one successful email attack in the last 12 months, with those affected facing average potential costs of more than $1 million for their most expensive attack. […] Email-based attacks can be the initial access point for a wide range of cyberthreats, including ransomware, information stealers, spyware, crypto mining, other malware, and more.

Vedi altro

Nove consigli per il Safer Internet Day

ACN - 7 Febbraio 23

- Imposta una password lunga e complessa. Se la ricordi senza sforzo non è una buona password. Meglio ancora è usare l'autenticazione a più fattori (2MFA) per accedere ai servizi sensibili. Esistono dei modi per risalire alle password di default dei router, ricorda di cambiarle! Infine, non usare la stessa password per più servizi. Useresti mai la stessa chiave per accendere la macchina, aprire il portone di casa o la cassetta di sicurezza in banca?
- Ricorda di aggiornare il tuo sistema operativo. È un'operazione che richiede poco tempo, rende più sicuro il tuo dispositivo e ne ottimizza le prestazioni. Nessun apparato deve essere "lasciato indietro" perché come in ogni catena la forza è uguale a quella del suo anello più debole. E installa un antivirus.
- Fai sempre una copia di backup dei tuoi dati più importanti e tienilo in una memoria elettronica (penna USB o HD) staccata dalla rete.
- Controlla se il sito web a cui ti connetti ha la Https. Se ce l'ha, la comunicazione è più sicura.
- Non rispondere a e-mail di persone sconosciute e non aprire link e allegati inattesi. Verifica sempre prima, potrebbe trattarsi di phishing. La vostra banca dati vi manda una nuova App? Un amico vi chiede di inviargli il codice? Ricontattateli utilizzando i contatti abituali (l'assistenza, il numero telefonico), senza fretta!<.li>
- Minimizza il tipo e la quantità di dati che cedi volontariamente per accedere a qualsiasi servizio online.
- Pulisci i dati di navigazione e i cookie dal tuo browser quando hai finito.
- In vacanza, in albergo, in viaggio, evita di usare wi-fi pubblici non sicuri. Se puoi usa una Virtual Private Network (Vpn) affidabile.
- Non lasciare il tuo dispositivo incustodito in spiaggia, al bar, a una festa con gli amici.

Vedi altro

NUOVE PUBBLICAZIONI

ICT Security Magazine, Quaderni di Cyber Intelligence #3 - Cyber Warfare, 17 Febbraio 2023

Hackmageddon, January 2023 CyberAttacks Statistics, 10 February 2023

Coinnect, Ransomware Intelligence Global Report 2023, 9 Febbraio 2023

PROSSIMI EVENTI

ENISA/ ECCC webinar on good practices for strengthening SME capacities on cybersecurity, presentation by Cyber 4.0, 20 February 2023

A&T - Automation & Testing 2023, Best practice di successo e prospettive future: servizi e attività dei Centri di Competenza nazionali per l'evoluzione delle PMI Italiane e dei rispettivi modelli di business, 23 Febbraio 2023, Torino

DIH Lombardia - Confindustria Mantova , Minacce Rischi, Prevenzione: la Sicurezza informatica nelle Imprese, Seminario di Cybersecurity, 24 Febbraio 2023, Confindustria Mantova

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