CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

1-15 FEBBRAIO 2024

IN EVIDENZA

CYBERSECURITY ITALIA, 10 FEBBRAIO 2024

Lucchetti (Cyber 4.0): "Ecco come eroghiamo 15 milioni del PNRR per la cybersicurezza anche di PMI"

La videointervista di Luigi Garofalo a Matteo Lucchetti, Direttore Operativo di Cyber 4.0, il Centro di Competenza nazionale sulla cybersecurity promosso e co-finanziato dal Ministero delle Imprese e del Made in Italy, in occasione del workshop "Strumenti per migliorare la cyber posture delle Pmi" organizzato dall'Academy dell'Università Campus Bio-Medico di Roma, nell'ambito della Facoltà di Ingegneria, con il quale l'ateneo ha dato simbolicamente il via alla prima edizione del Master di I livello in cybersecurity management.

CYBER 4.0

AVVENIRE, 4 FEBBRAIO 2024

Un ciclo di seminari nelle scuole

Partito il progetto "A scuola connessi: navighiamo in sicurezza". Si tratta di un ciclo di seminari dedicati al cyberbullismo per diffondere la cultura della sicurezza tra insegnanti, studenti e personale scolastico. Si legge in una notizia pubblicata mercoledì scorso nel sito della Regione Lazio (www.regione.lazio.it). La finalità è quella informare sui possibili rischi connessi all'utilizzo dei dispositivi digitali e della navigazione sul web. Il progetto è organizzato secondo una serie di incontri gratuiti che si svolgeranno fino a maggio e destinato alle scuole secondarie del Lazio. "L'iniziativa è stata introdotta dalla Regione, in collaborazione con l'Ufficio Scolastico Regionale del Lazio del ministero dell'istruzione e del Merito e Cyber 4.0 Centro di competenza nazionale ad alta specializzazione sulla cybersecurity.

LEGGI TUTTO

Articoli Correlati:
Cyberbullismo, al via il progetto "A scuola connessi"
Corriere di Viterbo, 1 Febbraio 2024

AIRPRESS, 1 FEBBRAIO 2024

Digitalizziamo in sicurezza

Tra gli obiettivi principali del Pnrr c'è la trasformazione digitale dell'Italia, con l'obiettivo di rendere il Paese più competitivo e resiliente. Ma migliorare il livello tecnologico e della connettività implica anche una maggiore esposizione ai rischi di attacchi informatici. La spesa italiana in cyber-security rappresenta ancora solo lo 0,1% del Pil, ultima tra i membri del G7. Diventa quindi fondamentale investire per scongiurare rischi e cogliere opportunità
In Italia.

LEGGI TUTTO

SOLE 24 ORE, 6 FEBBRAIO 2024

Pmi troppo esposte ai rischi cyber, il supporto deve arrivare dalle università

In Italia, le piccole e medie imprese rappresentano la quasi totalità delle aziende. Secondo il Report Swascan di Tinexta l'80% delle aziende italiane colpite da attacchi informatici sono piccole o medie. Nei primi 6 mesi del 2023 il numero degli attacchi andati a buon fine è cresciuto di oltre il 40% rispetto allo stesso periodo del 2022, con un tasso di incremento che in Italia è stato quattro volte superiore a quello globale.

LEGGI TUTTO

Articoli Correlati:
Cybersecurity, 'Pmi sempre più esposte e a rischio chiusura'
Ansa, 8 Febbraio 2024

IN ITALIA

CYBERSECURITY ITALIA, 13 FEBBRAIO 2024

PA, ecco come sarà rafforzata la postura cyber. Le 3 linee di azioni fino al 2026

L'Agenzia per l'Italia Digitale ha pubblicato il Piano triennale per l'informatica nella Pa 2024-2026, il documento di programmazione strategica per la Pubblica amministrazione, esito di un'approfondita di concertazione tra amministrazioni e soggetti istituzionali. Al suo interno, le PA e le imprese interessate troveranno tutte le informazioni e le azioni da mettere in campo per concorrere allo sviluppo della maturità digitale del Paese nel prossimo triennio.

LEGGI TUTTO

ACN, 10 FEBBRAIO 2024

L'ACN ripristina i sistemi ospedalieri colpiti da un attacco informatico in Basilicata

Dopo 12 giorni di intenso lavoro, la squadra di pronto intervento dell'Agenzia per la cybersicurezza nazionale è riuscita a ripristinare tutti i dati e i servizi essenziali degli ospedali lucani bloccati dall'attacco informatico delle scorse settimane. La squadra dell'articolazione operativa dell'Agenzia, il Computer Security Incident Response Team, Csirt - Italia, una volta giunta sul posto ha potuto fin da subito definire con i responsabili regionali le priorità e pianificare una complessa operazione di ripristino dei servizi, a seguito di una approfondita analisi dell'incidente che è servita a identificare l'estensione temporale e spaziale della compromissione.

LEGGI TUTTO

ACN, 13 FEBBRAIO 2024

La cybersecurity requisito fondamentale per lo sviluppo dell'IA

Il Vice Capo di Gabinetto di ACN, Marcello Albergoni, ha partecipato all'incontro "Governare l'Intelligenza Artificiale" della Camera di Commercio di Roma. L'incontro, promosso lo scorso 8 febbraio dalla Camera di Commercio di Roma, è stato organizzato da Maker Faire Rome - The European Edition nell'ambito del progetto PID - Punto Impresa Digitale, ha approfondito i vari aspetti del Regolamento europeo sull'intelligenza artificiale (AI Act). All'incontro hanno partecipato anche le Autorità per la protezione dei dati personali, per le garanzie nelle comunicazioni, della concorrenza e del mercato, nonché AgID e il relatore per l'Europarlamento della proposta di regolamento europeo sull'intelligenza artificiale (AI Act).

LEGGI TUTTO

POLIZIA POSTALE, 13 FEBBRAIO 2024

Attenzione alle false comunicazioni da parte di piattaforme di streaming

Attenzione alle false comunicazioni ricevute tramite e-mail che ti informano dell'imminente scadenza dell'abbonamento ai servizi di streaming di film e serie tv. Il messaggio replica la grafica e i loghi della piattaforma di streaming e richiede di inserire i dati della carta di credito per rinnovare l'abbonamento in scadenza. Si tratta di una truffa che permette ai cyber-criminali di carpire i dati della carta di credito della vittima al fine di eseguire addebiti illeciti sul conto corrente. Le piattaforme che offrono servizi online non chiedono mai di inserire dati personali e bancari tramite e-mail o SMS.

LEGGI TUTTO

NEWS INTERNAZIONALI

POLITICO, FEBRUARY 2, 2024

EU Parliament cyber chief to step down amid election hacking fears

The European Parliament's chief cybersecurity official will leave his post early, just months before the June elections, amid criticism that the assembly is struggling to cope with increasing cyberthreats.

LEGGI TUTTO

Articoli Correlati:
Global Malicious Activity Targeting Elections Is Skyrocketing
Ansa, 8 Febbraio 2024

GLOBAL INITIATIVE, FEBRUARY 15, 2024

A dream deferred or a near miss?

After two years of negotiations, state representatives gathered in New York from 29 January to 9 February 2024 for the concluding session of the Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (or a 'cybercrime convention').

LEGGI TUTTO

ENISA, FEBRUARY 6, 2024

Joint Statement on Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities

The European Commission, ENISA, the EU Agency for Cybersecurity, CERT-EU, Europol and the network of the EU national computer security incident response teams (CSIRTs network), have been closely following the active exploitation of vulnerabilities in the Ivanti Connect Secure and Ivanti Policy Secure Gateway products, commercial virtual private network (VPN) solutions previously known as Pulse Connect Secure.

LEGGI TUTTO

EUROPOL, FEBRUARY 12, 2024

International cybercrime malware service targeting thousands of unsuspecting consumers dismantled

An international operation has resulted in the seizure of several internet domains that were used by cybercriminals to sell malware. Through use of this malware, cybercriminals could secretly access and connect to victims' computers for malicious purposes. The operation was led by the FBI and supported by Europol and the Joint Cybercrime Action Taskforce (J-CAT).

LEGGI TUTTO

INTERPOL, FEBRUARY 1 2024

INTERPOL-led operation targets growing cyber threats

SINGAPORE – Some 1,300 suspicious IP addresses or URLs have been identified as part of a global INTERPOL operation targeting phishing, malware and ransomware attacks.
Operation Synergia, which ran from September to November 2023, was launched in response to the clear growth, escalation and professionalisation of transnational cybercrime and the need for coordinated action against new cyber threats.

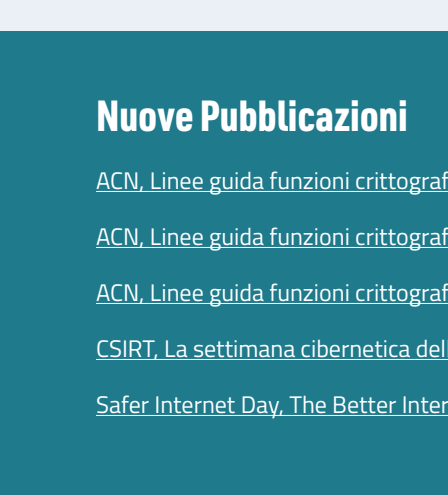
LEGGI TUTTO

CYBERSECURITY ITALIA, 12 FEBBRAIO 2024

Cyber criminali interrompono le trasmissioni tv degli Emirati Arabi con un finto TG: il giornalista è un deepfake

Secondo gli analisti di Microsoft, il collettivo iraniano Cotton Sandstorm ha diffuso video creati con l'AI anche nel Regno Unito e in Canada. L'intento: disinformare e influenzare l'opinione pubblica sulla guerra in Medio Oriente.

LEGGI TUTTO



SECURITY AFFAIRS, FEBRUARY 12, 2024

9 Possible ways hackers can use public wi-fi to steal your sensitive data

We've all used public Wi-Fi: it's convenient, saves our data, and speeds up browsing. But while we enjoy its benefits, hackers do too. Here, we'll explore how cybercriminals exploit public Wi-Fi to access your private data and possibly steal your identity. Plus, we'll discuss ways to protect yourself when using public Wi-Fi, even when you have no other option.

LEGGI TUTTO

Nuove Pubblicazioni

ACN, Linee guida funzioni crittografiche, Funzioni di Hash, Dicembre 2023

ACN, Linee guida funzioni crittografiche Codici di Autenticazione di Messaggi (MAC)

ACN, Linee guida funzioni crittografiche Conservazione delle Password

CSIRT, La settimana cibernetica dell'11 Febbraio 2024

Safer Internet Day, The Better Internet for Kids annual report 2023

Prossimi Eventi

I-Com, La sfida della cibersicurezza per un'Italia sempre più digitale. Politiche, competenze, regole, 15 Febbraio, Roma, Sala Matteotti, Camera dei Deputati, ore 9:50

EU CyberNet, EU-LAC Digital Alliance Dialogue on Cybersecurity, 14-16 February, Santo Domingo

ECCC Info Day, 22 February, Bucharest, Romania

CTE Cagliari, Smart Cities & Buildings e Cybersecurity, 28 Febbraio ore 10:00

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