CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

16-31 GENNAIO 2024

IN EVIDENZA

REGIONE LAZIO, **31 GENNAIO 2024**

Cyberbullismo, al via i seminari per diffondere la cultura della sicurezza: parte il progetto 'A scuola connessi'

[...] 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. **Saranno coinvolti circa 40 istituti scolastici, per un totale di oltre 600 studenti e 600 tra docenti e personale scolastico**. Condurranno l'evento esperti e docenti nel campo della cybersicurezza.

LEGGI TUTTO

Articoli Correlati:

Cyberbullismo, al via i seminari per diffondere la cultura della sicurezza: parte il progetto 'A scuola connessi'
Cyber 4.0, 30 Gennaio 2024

CYBER 4.0

AGENPARL, **19 GENNAIO 2024**

Cybersecurity, Lucchetti (Cyber 4.0): "Transizione digitale sicura, competenze, formazione, promozione dell'innovazione"

L'Agenparl ha intervistato Matteo Lucchetti, Direttore operativo del Competence Center nazionale sulla cyber security CYBER 4.0, promosso dal Ministero dello Sviluppo Economico.

LEGGI TUTTO

LIBERO, **23 GENNAIO 2024**

Con Cyber 4.0 l'Italia al top della sicurezza digitale

Si chiama Cyber 4.0 ed è il Centro di Competenza nazionale ad alta specializzazione per la cybersecurity, uno degli otto centri istituiti e cofinanziati dal Ministero delle Imprese e del Made in Italy (Mise) nel contesto delle azioni Industria 4.0, Transizione 4.0 e Pnrr. L'obiettivo dell'innovativo centro è quello di elevare il livello di competenza di imprese e Pubblica Amministrazione (Pa) in tema di sicurezza digitale, grazie a soluzioni concrete, strategiche e sostenibili basate su conoscenze, tecnologie innovative e servizi abilitanti sviluppati con le competenze del proprio network, che valorizzino le eccellenze italiane nel contesto Ue ed internazionale.

LEGGI TUTTO

IN ITALIA

FORMICHE, **24 GENNAIO 2024**

Cyber rivoluzione. Tutto sul disegno di legge

Il Ddl cyber, arrivato oggi in pre Consiglio dei ministri in vista della riunione di domani, è una mezza rivoluzione in materia di sicurezza informatica, soprattutto per la Pubblica amministrazione.
Il disegno di legge prevede, tra le varie cose, il coinvolgimento della magistratura in caso di cyber-attacchi (articolo 7). È previsto, inoltre, l'obbligo di notifica degli incidenti per le pubbliche amministrazioni centrali, le regioni e le province autonome di Trento e Bolzano, i comuni con una popolazione superiore ai 100.000 abitanti e i comuni capoluoghi di regione, le società di trasporto pubblico urbano con bacino di utenza non inferiore ai 100.000 abitanti e le aziende sanitarie locali (articolo 8). Gli stessi attori sono chiamati a dotarsi di un referente per la cybersicurezza (articolo 13). Si tratterebbe di un allargamento delle logiche del Perimetro di sicurezza nazionale cibernetica ad alcuni ambiti della pubblica amministrazione.

LEGGI TUTTO

CYBERSECURITY ITALIA, **30 GENNAIO 2024**

Attacco ransomware contro i sistemi informatici della Regione Basilicata. ACN invia pool operativo

Sferrato un attacco ransomware, con richiesta di riscatto, che sta creando criticità all'interno del sistema sanitario regionale. L'Agenzia per la cybersicurezza nazionale ha inviato un proprio pool operativo per supportare l'amministrazione.

LEGGI TUTTO

ACN, **25 GENNAIO 2024**

PNRR: pubblicata la graduatoria finale dell'Avviso n.7 per le PA centrali

L'Agenzia per la Cybersicurezza Nazionale (ACN), con l'Avviso finanziato dall'Investimento 1.5 del PNRR sulla Cybersecurity, intende promuovere l'erogazione di interventi volti ad irrobustire le infrastrutture e i servizi digitali del Sistema Paese nonché a migliorare le competenze specialistiche necessarie a garantire adeguati livelli di cyber resilienza.

LEGGI TUTTO

RED HOT CYBER, **31 GENNAIO 2024**

Il ransomware cala al minimo storico. -29% nel quarto trimestre 2023. Ma attenzione ai divieti

Secondo la società di sicurezza informatica Coveware, il numero di vittime che hanno pagato il riscatto è sceso al minimo storico. Si parla del 29% nell'ultimo trimestre del 2023. La tendenza è diventata evidente già a metà del 2021, quando il tasso di pagamento è sceso al 46% (dopo l'85% all'inizio del 2019). Secondo i ricercatori, le ragioni di questo calo sono molteplici: tra queste vi è la maggiore prontezza delle organizzazioni agli attacchi.

LEGGI TUTTO

CYBERSECURITY ITALIA, **17 GENNAIO 2024**

L'allarme di Piero Cipollone (BCE): "Gli attacchi informatici sono un rischio sistemico per la stabilità del sistema finanziario europeo"

Il componente del Comitato esecutivo della Banca Centrale Europea, Piero Cipollone, ha lanciato l'allarme durante il suo intervento in apertura dello Euro Cyber Resilience Board (ECRB), gruppo pan europeo di osservazione sui mercati.

LEGGI TUTTO

INDUSTRIA ITALIANA, **16 GENNAIO 2024**

2024: l'anno nero delle pmi! Fabio Arpe spiega perché

Nel 2024 molte pmi potrebbero andare in crisi. Una crisi irreversibile per effetto di una politica dei tassi scellerata e del sovraindebitamento accumulato nell'era Covid: «ripagare le rate con il costo del denaro attuale è insostenibile per le aziende con un'ebitda inferiore al 5% e bassa patrimonializzazione», dice a Industria Italiana Fabio Arpe banchiere di lungo corso, la cui storia nel mondo della finanza inizia nel gruppo Imi alla fine degli anni Ottanta.

LEGGI TUTTO

NEWS INTERNAZIONALI

ENISA, **JANUARY 31, 2024**

An EU Prime! EU adopts first Cybersecurity Certification Scheme

The European Commission adopted the implementing regulation concerning the EU cybersecurity certification scheme on Common Criteria (EUCC). The outcome is fully in line with the candidate cybersecurity certification scheme on EUCC that ENISA drafted in response to a request issued by the European Commission. In drafting the candidate scheme, ENISA was supported by an Ad-hoc working group (AHWG) composed by area experts from across the industry and EU Member States National Cybersecurity Certification Authorities (NCCAs).

LEGGI TUTTO

INTERPOL, **JANUARY 18, 2024**

Grooming, radicalization and cyber-attacks: INTERPOL warns of 'Metacrime'

A comprehensive analysis of the Metaverse's key challenges, threats and harms from a law enforcement perspective is outlined in a new INTERPOL White Paper published today. Contributing towards a secure-by-design Metaverse, the document identifies current and potential Metacrimes, such as grooming, radicalization and cyber-physical attacks against critical infrastructure, as well as theft of 3D virtual/cultural property, trespassing in private virtual spaces, and robbery from an avatar.

LEGGI TUTTO

NATO, **JANUARY 17, 2024**

NATO releases first ever quantum strategy

Quantum technologies are getting closer to revolutionizing the world of innovation and can be game-changers for security, including modern warfare. Ensuring that the Alliance is "quantum-ready" is the aim of NATO's first-ever quantum strategy that was approved by NATO Foreign Ministers on 28 November. On Wednesday (17 January 2024), NATO released a summary of the strategy.

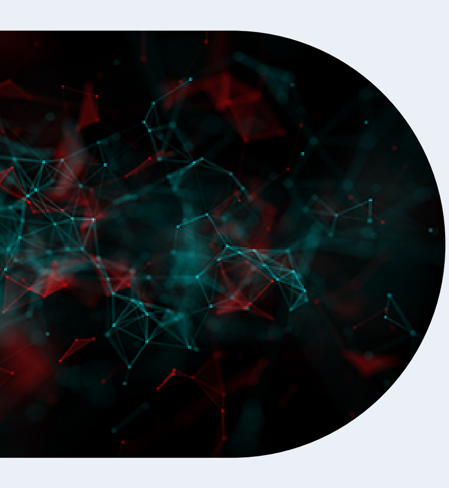
LEGGI TUTTO

BGR, **JANUARY 24, 2024**

26 billion private records leaked in 'mother of all breaches'

Somehow, one of the largest data breaches in recent memory has already been trumped. This week, the Cybernews research team and SecurityDiscovery.com owner Bob Dyachenko worked together to uncover a data breach containing 12 terabytes of information spread across 26 billion records. They claim the leak is possibly the biggest ever discovered, with user data from popular sites such as Tencent, Weibo, MySpace, Twitter, and LinkedIn.

LEGGI TUTTO



SECURITY AFFAIRS, **JANUARY 30, 2024**

Hundreds of network operators' credentials found circulating in dark web

Resecurity conducted a thorough scan of the Dark Web and identified over 1,572 compromised customers of RIPE, Asia-Pacific Network Information Centre (APNIC), the African Network Information Centre (AFRINIC), and the Latin America and Caribbean Network Information Center (LACNIC), resulting from infostealer infections.

LEGGI TUTTO

DATA BREACH TODAY, **JANUARY 24, 2024**

North Korean Hackers Using AI in Advanced Cyberattacks

South Korea's intelligence agency reported Wednesday that North Korean hackers are using generative AI technology to conduct sophisticated cyberattacks and identify hacking targets.
An official from the National Intelligence Service said the agency is monitoring North Korea's use of generative AI in cyberwarfare efforts.

LEGGI TUTTO

KREBS ON SECURITY, JANUARY 25, 2024

Using Google Search to Find Software Can Be Risky

Google continues to struggle with cybercriminals running malicious ads on its search platform to trick people into downloading booby-trapped copies of popular free software applications. The malicious ads, which appear above organic search results and often precede links to legitimate sources of the same software, can make searching for software on Google a dicey affair.

LEGGI TUTTO

Nuove Pubblicazioni

New NCCoE Guide Helps Major Industries Observe Incoming Data While Using Latest Internet Security Protocol, Nist, January 30, 2024

World Economic Forum, Reflections on Davos 2024: The state of cybersecurity, January 25, 2024

Countering Online Terrorist Propaganda Europol, January 16, 2024

Prossimi Eventi

Casa delle Tecnologie Emergenti, TECNOLOGIE EMERGENTI: SFIDE ED OPPORTUNITA' PER LE IMPRESE
Cagliari, Mediateca del Mediterraneo, via Mameli 164B, 5 Febbraio ore 15.00

UniCampus, Strumenti per migliorare la cyber posture delle PMI -Giornata inaugurale I edizioneMaster in Cyber Security Management
6 Febbraio ore 15:00 - Sala conferenze PRABB, Università Campus Bio-Medico di Roma

ACL, LE PROFESSIONI DELLA CYBERSECURITY: FABBISOGNI, PROFILI, COMPETENZE, TRENDS
La programmazione formativa a supporto delle esigenze delle aziende, 7 Febbraio ore 15:30

EU CyberNet, EU-LAC Digital Alliance Dialogue on Cybersecurity, 14-16 February, Santo Domingo, 9:00 AM

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

Fiera A&T, AIA Guard - soluzione end-to-end per la cybersecurity progettata contro gli Artificial Intelligence Attacks
Torino, 14 Febbraio ore 15:00

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