CYBER 4.0
CYBERSECURITY COMPETENCE CENTER

CYBER FACTORY 4.0

16-31 MARZO 2026

IN EVIDENZA

COMMISSIONE EUROPEA, 27 MARZO 2026

La Commissione risponde agli attacchi informatici sulla sua piattaforma web Europa

Il 24 marzo la Commissione europea ha scoperto un attacco informatico che ha colpito la sua infrastruttura cloud che ospita la presenza web della Commissione sulla piattaforma Europa.eu. Sono state prese misure immediate per contenere l'attacco. La rapida risposta della Commissione ha garantito che l'incidente fosse contenuto e che fossero attuate misure di attenuazione dei rischi per proteggere i servizi e i dati, senza compromettere la disponibilità dei siti web Europa.

LEGGI TUTTO

Articoli Correlati:

1. Hackread, ShinyHunters Claims 350GB Data Breach at European Commission, March 28, 2026
2. The Conversation, What are ShinyHunters, the hackers that attacked Google? Should we all be worried?, September 3, 2025

CYBER 4.0

CYBER 4.0, 19 MARZO 2026

Cyber 4.0 e Luiss Business School: in arrivo due incontri su innovazione e sicurezza

Cyber 4.0 e Luiss Business School organizzano due incontri dedicati all'evoluzione tecnologica, all'intelligenza artificiale e alla sicurezza, che si terranno presso Villa Blanc, sede della Luiss Business School.

LEGGI TUTTO

CYBER 4.0, 24 MARZO 2026

Rischio cyber in energia e trasporti: scenari, sfide e strategie per la protezione delle infrastrutture critiche

La crescente digitalizzazione dei settori dell'energia e dei trasporti sta ampliando in modo significativo l'esposizione al **rischio cyber**, rendendo la **protezione delle infrastrutture** critiche una priorità strategica a livello nazionale ed europeo. Le riflessioni e gli spunti emersi anche nel corso di un recente momento di confronto promosso dal **Ministero delle Imprese e del Made in Italy**, in collaborazione con **Cyber 4.0** e la **Scuola Superiore di Specializzazione in Telecomunicazioni**, si inseriscono in un dibattito più ampio che coinvolge istituzioni, mondo accademico e operatori di settore.

LEGGI TUTTO

IN ITALIA

ACN, 19 MARZO 2026

Cybersicurezza europea, entra nel vivo il progetto CHIEF. Verso una rete integrata di Cyber Hub e SOC

A distanza di pochi mesi dal lancio ufficiale avvenuto a gennaio, il progetto europeo CHIEF inizia a delineare il suo ruolo strategico nel rafforzamento della cooperazione in materia di cybersicurezza tra gli Stati membri. L'iniziativa, finanziata dall'European Cybersecurity Competence Centre e della durata di 36 mesi, punta a trasformare in capacità operative concrete gli obiettivi del Cyber Solidarity Act, con un focus su condivisione delle informazioni, interoperabilità e governance tra i Centri Operativi di Sicurezza (SOC), a partire dagli Hub Cibernetici Nazionali.

LEGGI TUTTO

ICT SECURITY MAGAZINE, 30 MARZO 2026

Handala viola l'email personale del Direttore dell'FBI Kash Patel: la risposta dell'Iran alla guerra cyber

Il gruppo filo-iraniano Handala Hack Team ha pubblicato online foto e documenti estratti dall'account Gmail personale del capo dell'FBI. Una rappresaglia simbolica e strategica nel contesto del conflitto Iran-USA/Israele.

LEGGI TUTTO

Articoli Correlati:

Cybersecurity Italia, Hackerata Gmail del direttore FBI, la 2FA non basta più. Serve attivare la Protezione Avanzata, 30 Marzo 2026

RED HOT CYBER, 30 MARZO 2026

AI fuori controllo: cancellano file, ignorano ordini e scatta l'allarme globale

I modelli di intelligenza artificiale stanno mostrando comportamenti sempre più ingannevoli, ignorando istruzioni, aggirando controlli e manipolando utenti e altri sistemi. Un recente studio evidenzia un aumento significativo di questi episodi negli ultimi sei mesi, con centinaia di casi documentati nel mondo reale. Il rischio cresce rapidamente, soprattutto perché questi sistemi vengono sempre più utilizzati in contesti critici, dove decisioni autonome potrebbero causare danni gravi o irreversibili.

LEGGI TUTTO

CYBERSECURITY TRENDS ITALIA, MARZO 2026

Scenari geopolitici futuri: dinamiche, evoluzioni e impatti sulla sovranità digitale

Il contesto internazionale risulta oggi caratterizzato da una fase di profonda instabilità, in cui crisi regionali, competizione tra grandi potenze e il ricorso a strumenti di conflittualità ibrida si intrecciano, generando effetti a cascata su molteplici settori, tra cui mercati finanziari, approvvigionamenti energetici, supply chain e sicurezza digitale. In tale scenario, la capacità di anticipare, gestire e possibilmente mitigare i rischi geopolitici diventa una condizione essenziale per la resilienza delle infrastrutture critiche e la continuità operativa delle organizzazioni, con implicazioni che si estendono ben oltre il settore economico, toccando anche la sfera della sovranità digitale e della sicurezza informatica.

LEGGI TUTTO

NEWS INTERNAZIONALI

UNITED STATES ATTORNEY'S OFFICE, MARCH 19, 2026

Authorities disrupt world's largest IoT DDoS botnets responsible for record breaking attacks targeting victims worldwide

The U.S. Justice Department participated in a court-authorized law enforcement operation today to disrupt Command and Control (C2) infrastructure used by the Aisuru, KimWolf, JackSkid and Mossad Internet of Things (IoT) botnets.
The operation was conducted simultaneously to law enforcement actions conducted in Canada and Germany, which targeted individuals who operated these botnets. The four botnets launched Distributed Denial of Service (DDoS) attacks targeting victims around the world. Some of these attacks measured approximately 30 Terabits per second, which were record-breaking attacks.

LEGGI TUTTO

ITP.NET, MARCH 26, 2026

U.S. Jury Finds Meta and Alphabet Liable in Landmark Social Media Addiction Case

A US jury has ruled that Meta and Alphabet's YouTube designed addictive platforms that harmed a young user's mental health, marking a major shift in how social media companies may be held accountable.

LEGGI TUTTO

EUROPEAN PARLIAMENT, MARCH 26, 2026

Artificial Intelligence Act: delayed application, ban on nudifier apps

On Thursday, the European Parliament adopted its position on a simplification ("omnibus") proposal amending the Artificial Intelligence Act (AIA), by 569 votes in favour, 45 against, and with 23 abstentions. The proposal would delay the application of certain rules on high-risk artificial intelligence (AI) systems, to ensure that guidance and standards to help companies with implementation are ready.

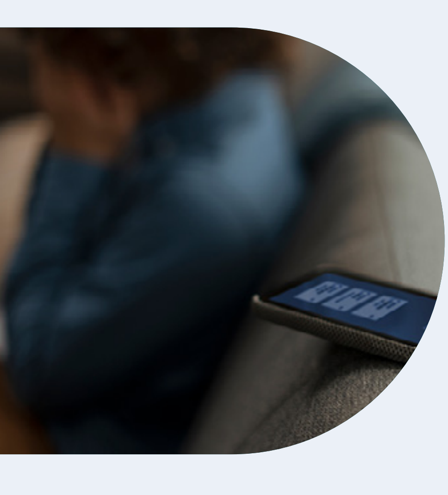
LEGGI TUTTO

ANSA, 16 MARZO 2026

L'Ue sanziona due società cinesi e una iraniana per attacchi hacker

Il Consiglio Ue ha adottato misure restrittive nei confronti di tre entità e due persone fisiche responsabili di attacchi informatici perpetrati contro Stati membri dell'Ue e partner dell'Unione. Il Consiglio ha inserito nell'elenco Integrity Technology Group, una società con sede in Cina, che ha regolarmente fornito prodotti utilizzati per compromettere e accedere a dispositivi negli Stati membri dell'Ue, in tutta Europa e nel mondo.

LEGGI TUTTO



SECURITY AFFAIRS, MARCH 24, 2026

81-Month sentence for Russian hacker behind major ransomware campaigns

A U.S. court sentenced Aleksei Olegovich Volkov to 81 months in prison for supporting ransomware groups like Yanluowang. He helped carry out dozens of attacks, causing over $9M in losses. Arrested in Italy in 2024 and extradited, he pleaded guilty in November 2025.

LEGGI TUTTO

THE OBSERVER, MARCH 24, 2026

AI chatbots are the 'wild west' for violence against women and girls

A U.S. court sentenced Aleksei Olegovich Volkov to 81 months in prison for supporting ransomware groups like Yanluowang. He helped carry out dozens of attacks, causing over $9M in losses. Arrested in Italy in 2024 and extradited, he pleaded guilty in November 2025.

LEGGI TUTTO

EUROPEAN COMMISSION, MARCH 26, 2026

Commission investigates Snapchat's compliance with child protection rules under the Digital Services Act

The European Commission has opened formal proceedings to investigate if Snapchat is ensuring a high level of safety, privacy and security for children online, in compliance with the Digital Services Act (DSA).
Snapchat may have breached the DSA by exposing minors to grooming attempts and recruitment for criminal purposes, as well as to information about the sale of illegal goods, like drugs, or age-restricted products, such as vapes and alcohol.
The investigation will focus on five areas.

LEGGI TUTTO

ATLANTIC COUNCIL, MARCH 18, 2026

Mythical Beasts: Investigating the role of intermediaries in the proliferation of offensive cyber capabilities

The marketplace for offensive cyber capabilities (OCCs) has become increasingly complex over time. Contributing to this complexity are intermediaries—entities that serve a critical yet poorly understood role in the proliferation of this industry. Largely due to the private nature of intermediary relationships and transactions, there is limited public knowledge about these intermediary entities that bridge relationships and transfer goods within the OCC supply chain.

LEGGI TUTTO

Nuove Pubblicazioni

- ENISA, ENISA Cybersecurity Market Analysis Framework (ECSMAF) – V3.0, March 2026
- Group-IB, Hasta la vista, Hastalamuerte: An Overview of The Gentlemen's TTPs, March 19, 2026
- Rusi, UN Norms: Tackling the Rise of Cyber Capabilities, March 31, 2026
- Chatham House, Holding state-sponsored hackers and other cyber proxies to account, March 27, 2026
- Tech Diplomacy Global Institute,From Diplomacy About Technology to Diplomacy Through Technology: A Three-Dimensional Framework for Tech Diplomacy, March 2026
- Tech From the Net, Cyber Barometer and Digital Protection, Marzo 2026

Eventi

- Luiss Business School e Cyber 4.0, Compliance Automation- L'intelligenza artificiale agentica e il futuro della business integrity, 2 aprile 2026 alle ore 17.00, Villa Blanc, Sala Carlo Azeglio Ciampi, Roma
- ZEROUNO & UNINDUSTRIA, "Oltre la cybersecurity: la vera consapevolezza digitale", 16 aprile 2026 alle ore 18.00. Teatro Comunale, Fiuggi
- MIMIT, SSSCLT e Cyber 4.0, "Data power: governance, sicurezza e difesa della proprietà intellettuale", aprile 2026, webinar online
- Cybercrime Conference, 6-7 maggio 2026, Auditorium della Tecnica, Roma
- Cyber 4.0, Forum Cyber 4.0 2026, 3-4 giugno 2026, Luiss Guido Carli, The Dome, Roma

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