



## Continuano le attività di Luglio

*Leonardo Querzoni, Presidente Cyber 4.0 - 18 Luglio 22*

Proseguono in questi giorni i seminari del ciclo "La strategia Nazionale di Cybersecurity: impatto e prospettive". Quattro webinar che affrontano, attraverso le testimonianze di grandi esperti del settore, il tema dell'impatto che la neonata strategia nazionale avrà nel prossimo futuro. Non perdetevi i prossimi appuntamenti!

## IN EVIDENZA



### Formazione come leva strategica di cyber resilienza

*Cyber 4.0 - 20 Luglio 22*

Prossimo webinar mercoledì 27 alle ore 16.00 con un approfondimento sul tema della formazione in materia di cybersecurity. Ambito di intervento prioritario della Strategia Nazionale di Cybersecurity, il ruolo della formazione va oltre quello di upskilling, reskilling e/ o creazione di nuove competenze, ma diventa vera e propria leva di cyber resilience e gestione del rischio per un numero crescente di organizzazioni.

[Vedi altro](#)



### Sanità digitale: il futuro passa per la cybersecurity

*Cyber 4.0 - 18 Luglio 22*

Si è svolto Mercoledì 13 Luglio il secondo appuntamento del ciclo di webinar che Cyber 4.0, in collaborazione con ACN, sta dedicando ad approfondire alcuni degli aspetti di rilievo della Strategia Nazionale di Cybersecurity.

[Vedi altro](#)



### Certificazioni di sicurezza: uno scenario in forte evoluzione

*Cyber 4.0 - 8 Luglio 22*

Mercoledì 6 Luglio il primo appuntamento del ciclo di webinar che Cyber 4.0, in collaborazione con ACN, sta dedicando ad approfondire alcuni degli aspetti di rilievo della Strategia Nazionale di Cybersecurity.

[Vedi altro](#)



## Centro di Valutazione e Certificazione Nazionale (CVCN)

ACN - 16 Luglio, 22

Con l'ultimo regolamento, adottato con Dpcm del 18 maggio 2022, n. 92 pubblicato in G.U. il 15 luglio 2022, è completato il quadro normativo del Perimetro di Sicurezza Nazionale Cibernetica. Grazie a quest'ultimo tassello, si è compiuto un importante passo per raggiungere gli obiettivi contenuti nella Strategia Nazionale di Cybersicurezza, volto ad innalzare il livello di sicurezza della supply chain di infrastrutture da cui dipende l'erogazione dei servizi essenziali dello Stato.

[Vedi altro](#)



## Cybersecurity e innovazione: le leve strategiche della trasformazione digitale

Cyber 4.0 - 18 Luglio 22

Importante occasione di scambio e confronto lunedì 18 Luglio per l'evento organizzato da Innovation Manager Hub in collaborazione con CYBER 4.0.

Tema dell'incontro è stato "Cybersecurity e Innovazione: le leve strategiche della trasformazione digitale".

Manager di grandi aziende hanno condiviso le loro esperienze, mettendo in luce lo status della digital transformation e con essa della cybersecurity in Italia.

[Vedi altro](#)

## NEWS



## Formazione 4.0, potenziato il credito d'imposta per le imprese

MISE - 8 Luglio 22

Per garantire un sistema efficace di attività formative 4.0 e sviluppare nuove competenze digitali tra i lavoratori è riconosciuto alle imprese un credito d'imposta potenziato fino al 70% per le piccole e al 50% per le medie, nel caso in cui questi servizi siano eseguiti da soggetti certificati dal Ministero dello Sviluppo economico. I Competence Center saranno tra i soggetti accreditati.

[Vedi altro](#)

### Articoli correlati:

[BI-REX, Credito d'imposta Formazione 4.0: i Competence Center tra i soggetti accreditati, 13 Luglio 22](#)



## Prima seduta del Comitato Tecnico-Scientifico dell'Agenzia per la Cybersicurezza Nazionale (ACN)

ACN - 6 Luglio 22

Si è svolta la prima riunione del Comitato tecnico-scientifico dell'Agenzia per la Cybersicurezza Nazionale alla presenza del Sottosegretario Franco Gabrielli - Autorità delegata per la sicurezza della Repubblica.

[Vedi altro](#)



## How to map the Cybersecurity Threat Landscape? Follow the ENISA 6-step Methodology

ENISA - July 6, 22

The cybersecurity threat landscape methodology developed by the European Union Agency for Cybersecurity (ENISA) aims at promoting consistent and transparent threat intelligence sharing across the European Union.

[Vedi altro](#)



## Hackers are targeting industrial systems with malware

*Ars Technica - July 15, 22*

From the what-could-possibly-go-wrong files comes this: People hawking password-cracking software are targeting the hardware used in industrial-control facilities with malicious code that makes their systems part of a botnet, a researcher reported.

[Vedi altro](#)

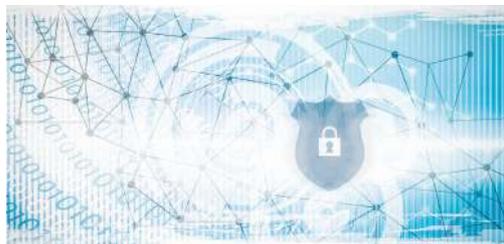


## Infrastrutture critiche, come l'attacco al Colonial Pipeline ha cambiato il mercato assicurativo

*Cybersec Italia- 12 Luglio 22*

Le crescenti preoccupazioni per gli attacchi informatici alle infrastrutture critiche, aggravate dalla guerra in Ucraina, stanno riaccendendo i dubbi sulle reali capacità delle grandi compagnie assicurative di coprire i rischi di un attacco che potrebbe avere conseguenze catastrofiche.

[Vedi altro](#)



## Sanità, in Italia il 41% dei leader indica come priorità assoluta la cybersecurity

*Cybersecurity Italia - 14 Luglio, 22*

Il 41% dei leader della sanità indica come priorità assoluta la cybersecurity e la privacy dei dati. Una preoccupazione legittima secondo gli ultimi dati appena registrati. L'Italia è il Paese più colpito in Europa e il sesto al mondo con una percentuale di attacchi informatici subiti del 4,44%.

[Vedi altro](#)



## Formazione, conclusa la prima Summer School per la Pa. Brunetta: "Senza la cybersecurity mettiamo a rischio la nostra prosperità economica"

*Cybersecurity Italia - 15 Luglio, 22*

Si è conclusa la prima Summer School sulla Cybersicurezza rivolta ai vertici delle amministrazioni pubbliche centrali, un'iniziativa promossa dall'Agenzia per la Cybersicurezza nazionale, dalla SNA e dal Dipartimento della Funzione Pubblica, con la collaborazione del Dipartimento per le Informazioni e la Sicurezza, del Dipartimento per la Trasformazione Digitale, del Ministero della Difesa, della Polizia Postale e della Cyber & Security Academy di Leonardo.

[Vedi altro](#)



## La cybersecurity al servizio del Paese. Intervista a Galtieri (Cy4Gate)

*Formiche - 6 Luglio, 22*

Dalle opportunità poste dal Pnrr al Centro di valutazione e certificazione nazionale, dalla sicurezza della nostra Pa alla costruzione di una autonomia strategica nazionale nel campo delle tecnologie proprietarie e del know-how, quanto è cyber-resiliente il nostro Paese e quali sono i prossimi passi da compiere? L'intervista di Airpress ad Emanuele Galtieri, amministratore delegato di Cy4Gate.

[Vedi altro](#)



## 10,000 organisations targeted by phishing attack that bypasses multi-factor authentication

*Tripwire - July 14, 22*

Microsoft has shared details of a widespread phishing campaign that not only attempted to steal the passwords of targeted organisations, but was also capable of circumventing multi-factor authentication (MFA) defences.

[Vedi altro](#)

### Articoli correlati:

[Threat Post, Large-Scale Phishing Campaign Bypasses MFA, July 13, 22](#)



## Ransomware Group Conti Reaches 40 Successful Attacks in a Single Month

KnowBe4 - July 14, 22

In less than 2 years, the most successful ransomware group to date has reached new levels of campaign and individual attack effectiveness, targeting over 160 industries worldwide.

[Vedi altro](#)

## NUOVE PUBBLICAZIONI

[Betanews, Disaster Recovery Planning: A successful framework for strategy and execution, July 14, 22](#)

[Microsoft, From cookie theft to BEC: Attackers use AiTM phishing sites as entry point to further financial fraud, July 12, 2022](#)

[Hackmageddon, Q2 2022 Cyber Attacks Statistics, July 14, 22](#)

[Threat Post, A Guide to Surviving a Ransomware Attack, June 30, 2022](#)

## PROSSIMI EVENTI

[Cyber 4.0, Webinar Information sharing pubblico-privato, 20 Luglio, 2022](#)

[Cyber 4.0, Webinar Formazione come leva strategica di cyber resilienza, 27 Luglio, 2022](#)

[IEEE Word Congress on Computational Intelligence, Le competenze dell'AI per il trasferimento tecnologico e l'innovazione, Padova, 21 Luglio, 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](mailto:comunicazione@cyber40.it)

