



In partenza l'Accademia Cybersicurezza Lazio

Leonardo Querzoni, Presidente Cyber 4.0 - 1 Settembre 22

Passata la breve pausa estiva, in questi giorni stanno partendo numerose attività che vedono impegnato CYBER 4.0. Mi piace in particolare sottolineare per questo numero, il lancio da parte della Regione Lazio dei bandi legati all'Accademia Cybersicurezza Lazio. La stretta collaborazione che nei mesi passati ha messo allo stesso tavolo i nostri esperti, insieme al personale della Regione, del Ministero dell'Istruzione e dell'Agenzia per la Cybersicurezza Nazionale, permette oggi di avviare un programma di formazione ambizioso che mira a formare, nei prossimi anni, il personale che garantirà la sicurezza delle realtà economiche e governative del Lazio.

IN EVIDENZA



La formazione come leva strategica di cyber resilienza: le sfide da affrontare e le iniziative in corso

Cyber 4.0 - 16 Agosto 22

Si è svolto Mercoledì 27 Luglio il quarto ed ultimo incontro del ciclo di webinar che Cyber 4.0, in collaborazione con ACN, ha dedicato ad approfondire alcuni aspetti di rilievo della Strategia Nazionale di Cybersecurity. Il seminario è stato focalizzato sulla formazione quale fattore abilitante per il raggiungimento degli obiettivi della Strategia, che lo vede oggetto di ben 12 "Misure" presenti nel Piano di Implementazione.

[Vedi altro](#)

**European
Cybersecurity
in Context**
A Policy-Oriented
Comparative Analysis

The normative landscape in security and resilience: the future of Critical Infrastructure and Essential Service in the EU

Cyber 4.0 - 1 Settembre 22

Pubblicato nel volume "European Cybersecurity in Context" l'articolo scritto dalla nostra responsabile formazione ed orientamento Martina Castiglioni in collaborazione con Alessandro Lazari.

[Vedi altro](#)



Online il Bando per docenti/studenti Accademia Cybersicurezza Lazio

Regione Lazio - 22 Agosto 22

E' disponibile online il Bando per l'ammissione di allievi/e al percorso formativo "Cybersecurity Technician" presso l'Accademia Cybersicurezza Lazio, e l'Avviso per la manifestazione di interesse per l'istituzione di un Albo per incarichi di docenza presso l'Accademia di Cybersicurezza Lazio e le relative domande di partecipazione/adesione.

[Vedi altro](#)



L'ACN come autorità di certificazione cyber: cosa cambia col nuovo quadro normativo

Cybersecurity 360 - 29 Agosto 22

Con la pubblicazione in Gazzetta Ufficiale del D.lgs. 123, l'Agenzia per la Cybersicurezza Nazionale è stata designata come Autorità nazionale di certificazione della cybersicurezza. Ecco le novità del decreto e cosa cambia con il nuovo quadro normativo.

[Vedi altro](#)

Correlati:

[DECRETO LEGISLATIVO 3 agosto 2022, n. 123](#)



CVCN, come accreditare i laboratori di prova con le misure minime di sicurezza

Cybersec Italia - 22 Agosto 22

Approvati dall'ACN i requisiti e le misure minime di sicurezza fisica e tecnica per l'accREDITAMENTO dei laboratori di prova (LAP) del Centro di Valutazione e Certificazione Nazionale (CVCN).

[Vedi altro](#)



Publicato l'Avviso n. 4/2022 per il potenziamento delle capacità di analisi e scrutinio software nella PA Centrale

ACN - 5 Settembre 22

Obiettivo dell'avviso finanziato dall'investimento 1.5 del PNRR sulla Cybersecurity è quello di continuare il percorso di rafforzamento delle capacità cyber della PA, in particolare per il potenziamento delle capacità di analisi e scrutinio software.

[Vedi altro](#)

NEWS



Web 3.0: ecco le vulnerabilità specifiche e come mitigarle

Cybersecurity 360 - 23 Agosto 22

Ecco una panoramica della tecnologia che sta alla base del Web 3.0 e degli attacchi più noti, come i bug degli smart contract, il cryptojacking, il rug pulling e l'ice phishing.

[Vedi altro](#)



Attacco al sito Gse, tutti i dati sensibili in mano agli hacker secondo l'intelligence

Start Magazine - 1 Settembre 22

Attacco informatico al Gse: i servizi hanno "appurato che gli hacker hanno superato le fragili barriere di sicurezza esistenti e per diverse ore hanno potuto fare man bassa di ogni genere di dati sensibili" segnalano fonti di Intelligence.

[Vedi altro](#)

Articoli correlati:

[Repubblica, Sull'attacco al Gse le impronte degli hacker russi, 30 Agosto 22](#)

[Reuters, Ransomware group BlackCat behind Italy's GSE hacking, researchers say, September 2, 22](#)



Cybercrime, anche Eni nel mirino degli hacker: si alza la soglia d'allarme

CorCom - 1 Settembre 22

Rilevati accessi non autorizzati alla rete aziendale. Le conseguenze sarebbero di lieve entità, ma si tratta del secondo attacco in pochi giorni al comparto, dopo l'offensiva sferrata nei confronti del Gestore dei servizi energetici.

[Vedi altro](#)

Articoli correlati:

[The Record, Greek gas operator refuses to negotiate with ransomware group after attack, August 22, 22](#)



Relazione Copasir e l'infowarfare russa. Mario Caligiuri "Stiamo vivendo una fase di disinformazione permanente"

Cybersec Italia - 23 Agosto 22

La relazione annuale del Comitato mette in luce i tentativi di condizionamento da parte di Mosca, evidenziando i rischi per il Paese, in vista delle prossime elezioni del 25 settembre. L'analisi del prof. Mario Caligiuri, presidente della Società Italiana di Intelligence e direttore del Master in Intelligence dell'Università della Calabria.

[Vedi altro](#)



Attacco cyber all'Asl Torino: "Prelievi a mezzo servizio, referti scritti a mano e sospese visite per le patenti speciali"

Cybersecurity Italia - 24 Agosto 22

Dall'attacco informatico di venerdì 19 agosto, l'ASL Città di Torino non ha ancora ripreso completamente a fornire tutti i servizi ai cittadini. Al lavoro task force di 14 tecnici dell'Asl e da Csirt Italia dell'ACN. Ecco tutti i disagi.

[Vedi altro](#)



Attacco cyber al comune di Gorizia: "Sembra un Film, ma è un messaggio reale"

Red Hot Cyber - 1 Settembre 22

La vicenda del Comune di Gorizia i cui servizi sono stati paralizzati da un attacco ransomware è stata descritta dallo stesso sindaco in un messaggio sulla pagina Facebook Comune di Gorizia – Newscome una "incredibile vicenda".

All'interno del comunicato la cittadinanza è stata informata dell'attacco subito e scoperto dopo il "blackout informatico che aveva colpito l'ente nella notte fra domenica e lunedì" e del ripristino di "alcuni servizi".

[Vedi altro](#)



Ransomware Group Claims Access to SCADA in Confusing UK Water Company Hack

Security Week - August 16, 22

A ransomware group has hit at least one water company in the United Kingdom, but there is some confusion over whose systems were actually breached.

The Cl0p ransomware group has claimed on its Tor-based leak website that it has breached the systems of Thames Water, which advertises itself as the UK's largest water and wastewater company, serving 15 million people.

[Vedi altro](#)



France hospital Center Hospitalier Sud Francilien suffered ransomware attack

Security Affairs - August 24, 22

The Center Hospitalier Sud Francilien (CHSF), a hospital southeast of Paris, has suffered a ransomware attack over the weekend. The attack disrupted the emergency services and surgeries and forced the hospital to refer patients to other structures.

[Vedi altro](#)



LockBit ransomware gang gets aggressive with triple-extortion tactic

Bleeping Computer - August 28, 22

LockBit ransomware gang announced that it is improving defenses against distributed denial-of-service (DDoS) attacks and working to take the operation to triple extortion level. The gang has recently suffered a DDoS attack, allegedly on behalf of digital security giant Entrust, that prevented access to data published on its corporate leaks site.

[Vedi altro](#)



NATO Probes Hackers Selling Data from Top Missile Firm MBDA

Hackread - August 29, 22

A cybercrime gang is selling classified data apparently stolen from European firm MBDA Missile Systems. For your information, MBDA is a European company that produces missiles and other weapons. It was formed in 2001 from a merger of French, Italian, and British companies. MBDA is the world's second-largest missile maker after Boeing.

[Vedi altro](#)



Misconfigured Meta Pixel exposed healthcare data of 1.3M patients

Bleeping Computer - August 22, 22

U.S. healthcare provider Novant Health has disclosed a data breach impacting 1,362,296 individuals who have had their sensitive information mistakenly collected by the Meta Pixel ad tracking script.

Meta Pixel (formerly Facebook Pixel) is a JavaScript tracking script that Facebook advertisers can add to their site to track advertising performance.

[Vedi altro](#)



Lloyd's to end insurance coverage for state cyber attacks

Computer Weekly - August 22, 22

Lloyd's of London has instructed its members to exclude nation state cyber attacks from insurance policies beginning in 2023, saying they pose unacceptable levels of risk

[Vedi altro](#)

NUOVE PUBBLICAZIONI

[Threat post, Ransomware Attacks are on the Rise, August 26, 2022](#)

[Global Cyber Alliance, Ransomware Task Force Releases Blueprint for Ransomware Defense, August 4, 2022](#)

[MIT Technology Review, Hackers linked to China have been targeting human rights groups for years, August 16 2022](#)

[CISA, Preparing Critical Infrastructure for Post-Quantum Cryptography, August 2022](#)

PROSSIMI EVENTI

[Capitolo di Roma AFCEA International, Arsenale Cyber: la nuova realtà nei conflitti ibridi, 13 Settembre 2022, Roma](#)

[GFCE, Global Annual Meeting 2022, September 13-15 2022, The Hague Netherlands](#)

[ENISA, European Cybersecurity Challenge 2022, September 13-16, 2022 Vienna](#)

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

