AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2024 | **n. 04/ 2024** | **aprile 2024**

Giganti del tech in corsa: la nuova era dello sviluppo in intelligenza artificiale

L'era della superintelligenza artificiale potrebbe essere più vicina di quanto si pensi. Le principali aziende del settore tecnologico stanno compiendo passi da gigante verso lo sviluppo di sistemi di intelligenza artificiale in grado non solo di eguagliare, ma addirittura di superare le capacità cognitive umane. È in atto una competizione per conseguire ciò che viene denominato dai ricercatori "intelligenza artificiale generale" (AGI), ovvero un livello di cognizione artificiale paragonabile, se non superiore, a quella del pensiero umano.
In prima linea in questa sfida troviamo tech company come OpenAI, Meta, Google, Anthropic e Cohere. Queste aziende stanno lavorando intensamente per sviluppare nuovi modelli di linguaggio evoluti rispetto agli attuali sistemi di IA generativa che eccellono nel generare testi, immagini e codice. L'obiettivo è consentire a questi sistemi non solo di generare output, ma anche di ragionare, pianificare e conservare informazioni nel tempo. (https://www.ft.com/content/78834fd4-c4d1-4bab-bc40-a64ad9d65e0d)

Al fine di favorire tale sviluppo, Microsoft e OpenAI hanno avviato un'ambiziosa collaborazione volta alla costruzione di un mega data center dal valore di oltre 100 miliardi di dollari che soddisferà l'enorme fabbisogno di potenza di calcolo necessario per sostenere la rapida ascesa e la crescente domanda di sistemi di IA generativa. Questa nuova frontiera dell'intelligenza artificiale richiede infatti capacità computazionali enormemente superiori rispetto ai tradizionali carichi di lavoro, rendendo indispensabili investimenti massicci in infrastrutture all'avanguardia. I piani prevedono lo sviluppo di un supercomputer denominato "Stargate", il cui lancio è atteso per il 2028. Questo sistema, che troverà sede in un'apposita struttura negli Stati Uniti, è stato concepito per superare nettamente in potenza di calcolo numerosi altri supercomputer di ultimissima generazione attualmente in fase di realizzazione in diverse parti del mondo. (https://www.reuters.com/technology/microsoft-openai-planning-100-billion-data-center-project-information-reports-2024-03-29/)

Le prossime versioni dei modelli linguistici di OpenAI e Meta, rispettivamente GPT-5 e Llama 3, mostreranno progressi significativi in queste direzioni secondo quanto affermato dai vertici aziendali. Le IA saranno in grado di fornire assistenza avanzata in campi diversificati, dalla medicina alla ricerca scientifica, dalla produzione industriale all'educazione. Nell'ambito medico, potranno analizzare dati clinici in modo approfondito, contribuendo a diagnosi più accurate e terapie personalizzate. Nella ricerca scientifica, assisteranno gli scienziati nell'analisi di vasti insiemi di dati, individuando patterns e insights difficili da rilevare per l'occhio umano. Nel settore manifatturiero, ottimizzeranno i processi produttivi riducendo sprechi e costi. Nell'educazione, forniranno strumenti di apprendimento adattivi e personalizzati per ogni studente. Queste sono solo alcune delle potenziali applicazioni che dimostreranno come l'intelligenza artificiale possa affiancarsi all'intelligenza umana, aprendo nuovi orizzonti di conoscenza e innovazione in molteplici settori.

Il raggiungimento di queste abilità è cruciale per compiere progressi verso l'AGI, poiché consentirebbe agli assistenti virtuali di completare sequenze di task correlati, prevedere le conseguenze delle proprie azioni e costruire modelli mentali del mondo circostante. Attualmente, i sistemi di IA producono output parola dopo parola senza una vera capacità di pensiero e pianificazione, commettendo ancora errori banali dovuti alla mancanza di ragionamento.
Anche l'imprenditore Elon Musk, fondatore di realtà come Tesla, SpaceX e Neuralink, si è recentemente espresso in merito, azzardando una previsione ancor più ardita. Musk sostiene che potremmo vedere l'emergere di un'intelligenza artificiale che supera le capacità di qualsiasi essere umano in ogni singolo compito specifico entro la fine del 2024. Una previsione che stringe ulteriormente i tempi rispetto a quanto affermato in passato dallo stesso Musk, che nel 2023 aveva ipotizzato l'arrivo della super IA entro il 2029. L'imprenditore ha però avvertito che potenziali carenze di chip e di forniture energetiche potrebbero rallentare questo processo.
(https://www.theguardian.com/technology/2024/apr/09/elon-musk-predicts-superhuman-ai-will-be-smarter-than-people-next-year)

Mentre le aziende tecnologiche accelerano la corsa verso sistemi sempre più sofisticati e "intelligenti", crescono anche i timori per le implicazioni etiche e di sicurezza di questa tecnologia. Una delle principali sfide è quella di garantire che un'eventuale IA super intelligente venga programmata con valori e obiettivi perfettamente allineati a quelli umani. La prospettiva di un sistema con capacità cognitive sovraumane ma mosso da fini e principi diversi dai nostri potrebbe portare a conseguenze indesiderate o addirittura pericolose per l'umanità stessa. Allo stesso modo, è fondamentale prevenire che i modelli di IA altamente avanzati ereditino pregiudizi e discriminazioni presenti nei dati di addestramento. Un'intelligenza artificiale superiore, ma condizionata da bias etnici, di genere o di altro tipo, potrebbe amplificare e perpetuare queste forme di discriminazione su scala globale. La privacy e la sorveglianza di massa, inoltre, rappresentano un'ulteriore minaccia. Sistemi di IA estremamente evoluti potrebbero diventare strumenti di controllo e violazione della sfera privata senza precedenti, se utilizzati a fini di monitoraggio indiscriminato delle attività umane. In conclusione, mentre la prospettiva dell'AGI apre nuove opportunità, è necessario affrontare con attenzione le complesse implicazioni etiche e sociali correlate, al fine di sviluppare questa tecnologia in modo responsabile e allineato ai valori e ai diritti umani fondamentali.

Marco Raul Massoni
Laureato in "Scienze della Politica" presso l'Università degli Studi di Macerata. Ha conseguito un master in Protezione Strategica del Sistema Paese: Cyber Intelligence, Big Data e Sicurezza delle Infrastrutture Critiche presso la Società Italiana per l'Organizzazione Internazionale (SIOI). Attualmente svolge attività di consulenza in materia di cybersecurity

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2024

Il 31 dicembre 2023 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare con sollecitudine l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2024".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2024. Dopo questa data, si decade dalla qualifica di socio e sarà necessario procedere ad una nuova iscrizione versando anche il contributo per le spese di segreteria.**
La nostra segreteria è a disposizione, per informazioni, alla mail segreteria@infrastrutturecritiche.it.

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.
La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

VISITA GUIDATA
AL CORPO NAZIONALE DEI VIGILI DEL FUOCO

Lunedì 8 aprile si è svolta la prevista visita al Centro Studi ed Esperienze (CSE) del Corpo Nazionale dei Vigili del Fuoco situato in Roma, largo Santa Barbara.
All'arrivo, i soci AIIC - guidati dal vicepresidente Silvano Bari - sono stati accolti dal Direttore Centrale Prevenzione e Sicurezza Tecnica, ing. Eros Mannino, che ha spiegato l'organizzazione ed i compiti della Direzione. Successivamente l'ing. Massimo Nazareno Bonfatti, Direttore del Centro Studi ed Esperienze, ha illustrato le attività svolte nell'ambito del Centro: è stato possibile visitare il Laboratorio Merceologico, dove si verificano le tute e gli abbigliamenti speciali usati in caso di emergenza, il Laboratorio di Reazione al Fuoco ed il Forno Sperimentale, dove si sottopongono a prove di tenuta, di reazione e di resistenza al fuoco e al calore i materiali più vari e in modo da fornire indicazioni in merito al loro utilizzo nella realtà delle costruzioni civili e industriali del Paese. La mattinata si è conclusa con la visita al Nucleo Investigativo Antincendio.

Ricordiamo che anche le visite previste nel prossimo futuro saranno riservate ai soli soci AIIC in regola con il pagamento delle quote sociali. I signori non-soci che volessero partecipare, possono iscriversi all'Associazione AIIC usufruendo di una quota di associazione minima (euro 50 anno + 10 una tantum). Le modalità per l'iscrizione si trovano sul sito www.infrastrutturecritiche.it o si possono richiedere inviando una mail a segreteria@infrastrutturecritiche.it

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

NEWS E AVVENIMENTI

Convegno "Sfida e Futuro delle Comunità Energetiche" - Torino 23 Aprile (14-19), in presenza e a distanza.

Il Convegno è stato inserito nell'ambito degli eventi della Planet Week organizzati dal Ministero dell'Ambiente e della Sicurezza Energetica in anticipazione dell'incontro dei ministri del G7 a Venaria Reale a fine Aprile.

La partecipazione è gratuita. Bisogna solo registrarsi, per ricevere poi il link per il collegamento.

Con il decreto ministeriale Mase 414 del 23/01/2024 si è concluso il lungo e travagliato iter normativo sulle Comunità Energetiche e sull'Autoconsumo Diffuso.

Siamo di fronte a una grande opportunità per il Paese, che va adeguatamente conosciuta e fruttata.

La normativa è molto complessa. I dubbi e le perplessità sono diffusi e rilevanti. È facile commettere errori di valutazione. C'è molta incertezza non soltanto sugli aspetti economici ma anche su importanti aspetti legali e fiscali.

Obiettivo del Convegno è illustrare lo stato dell'arte, i vantaggi possibili, gli errori rischiosi, le prospettive prevedibili, insieme a una panoramica di quanto sin qui realizzato e in corso di realizzazione.

Tutto ciò si inserisce in un contesto della transizione energetica che si arricchisce in continuazione di nuovi approcci, grazie ai progressi nell'intelligenza artificiale, nel cloud computing e in IoT (Internet of Things). I sistemi energetici (elettrico, termico, idrico) diventano sempre più complicati e con sempre più numerosi protagonisti attivi.

Le situazioni reali possono essere diversissime e richiedono nuove interazioni fra rete e utenti.

I sistemi elettrici 4.0 si basano su novi paradigmi, per certi aspetti con effetti rivoluzionari sull'articolazione dell'infrastruttura elettrica. Accanto agli aspetti statici riguardanti i flussi di energia, c'è un mondo ancora inesplorato dei servizi dinamici, che costituiscono una parte molto importante del mercato elettrico del futuro.

Sotto questo aspetto il Convegno rappresenta un'occasione unica per approfondire ed aggiornarsi su un tema che può rappresentare un punto di svolta per la situazione energetica del Paese, con nuove interessanti prospettive per i professionisti e nuove opportunità di risparmio per i cittadini e per il mondo economico-industriale.

Per i professionisti i vari Ordini e Collegi prevedono il riconoscimento di crediti formativi per l'aggiornamento.

Iscrizione: per partecipare occorre iscriversi (a scelta) a uno dei seguenti link:
https://www.foit.it/corsi/dettaglievento/2696/-/convegno-sfida-e-futuro-delle-comunita-energetiche
https://docs.google.com/forms/d/e/1FAIpQLSf-OBllhQCp6hEqynqZRvDoWK784BrdHxkz_Tk996pxLTi1Cg/viewform?usp=sf_link

Sete digitale. L'amministrazione Biden mette in allerta di possibili attacchi alle infrastrutture idriche statunitensi - L'amministrazione Biden mette in guardia dal rischio di attacchi informatici alle forniture idriche, citando le minacce persistenti da parte di hacker legati ai governi di Iran e Cina.
Attacchi alle infrastrutture idriche statunitensi
In una lettera ai governatori pubblicata il 19 marzo, l'amministratore dell'EPA Michael Regan e il consigliere per la sicurezza nazionale Jake Sullivan hanno espresso preoccupazione per il fatto che attacchi informatici mirati potrebbero interrompere la funzione vitale di fornire acqua potabile pulita e sicura e causare danni finanziari significativi alle comunità colpite dalla chiusura.
È stato chiarito che gli hacker affiliati al Corpo delle Guardie rivoluzionarie islamiche iraniane hanno recentemente attaccato i sistemi di acqua potabile degli Stati Uniti, mentre il gruppo Volt Typhoon, sponsorizzato dalla Cina, ha compromesso la tecnologia informatica delle forniture di acqua potabile e altri sistemi di infrastrutture critiche.
La lettera afferma che i dipartimenti e le agenzie federali valutano con un alto grado di fiducia le azioni degli attori del Volt Typhoon come preparazione per una possibile interruzione delle operazioni delle infrastrutture critiche in caso di tensioni geopolitiche e/o conflitti militari.
Sistemi altamente vulnerabili
L'approvvigionamento idrico statunitense è una parte particolarmente vulnerabile delle infrastrutture del paese a causa degli scarsi controlli, dei finanziamenti e del personale insufficienti. L'Environmental Protection Agency è la principale agenzia federale responsabile di garantire la resilienza del settore idrico nazionale a tutte le minacce e i rischi, compresi gli attacchi informatici. *(continua…)*
https://www.redhotcyber.com/post/sete-digitale-lamministrazione-biden-mette-in-allerta-di-possibili-attacchi-alle-infrastrutture-idriche-statunitensi/
Red Hot Cyber *– Redazione RHC – 20 Marzo 2024*

Gli Hacker Cinesi di APT31 Attaccano le Infrastrutture Critiche degli USA e del Regno Unito. 10 Milioni di dollari per informazioni! - Secondo le autorità statunitensi e britanniche, gli hacker cinesi APT31, presumibilmente associati al Ministero della Sicurezza di Stato cinese (MSS), hanno attaccato reti di computer, e-mail e archivi cloud di agenzie governative, aziende e individui, comprese infrastrutture critiche statunitensi, aziende statunitensi, politici e loro partiti politici.
Nello specifico, il Regno Unito ha dichiarato che APT31 ha tentato di hackerare le e-mail dei parlamentari britannici nel 2021. Inoltre, le autorità britanniche ritengono che gli agenti cinesi abbiano avuto accesso ai dati della Commissione elettorale britannica tra il 2021 e il 2022 rubando e-mail e dati dal registro degli elettori.
Gli Stati Uniti hanno accusato sette presunti membri dell'APT31. Washington ha anche annunciato una ricompensa fino a 10 milioni di dollari per informazioni che portino all'arresto dei sospettati.
Secondo l'accusa, gli hacker hanno condotto campagne su larga scala in tutto il mondo dal 2010, spiando reti e account di interesse di Pechino. Le vittime degli attacchi sono stati giornalisti, attivisti per i diritti umani, esperti di politica estera, accademici, dipendenti di aziende informatiche, imprese di telecomunicazioni, aziende manifatturiere e commerciali, istituti finanziari, agenzie di consulenza, studi legali, istituti di ricerca, nonché funzionari governativi e politici che ha criticato il governo cinese. *(continua…)*
https://www.redhotcyber.com/post/gli-hacker-cinesi-di-apt31-attaccano-le-infrastrutture-critiche-degli-usa-e-del-regno-unito-10-milioni-di-dollari-per-informazioni/
Red Hot Cyber *– Redazione RHC – 26 Marzo 2024*

US TREASURY DEP ANNOUNCED SANCTIONS AGAINST MEMBERS OF CHINA-LINKED APT31

The US Treasury Department announced sanctions on two APT31 Chinese hackers linked to attacks against organizations in the US critical infrastructure sector**.**

The US government announced sanctions against a pair of Chinese hackers (Zhao Guangzong and Ni Gaobin), alleged members of the China-linked APT31 group, who are responsible for "malicious cyber operations targeting U.S. entities that operate within U.S. critical infrastructure sectors."

The U.S. Treasury Department has sanctioned a tech company based in Wuhan, the Wuhan Xiaoruizhi Science and Technology Company, Limited (Wuhan XRZ), used by the Chinese Ministry of State Security (MSS) as a front in attacks against organizations in the U.S. critical infrastructure sector.

"Today, the Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned ***Wuhan Xiaoruizhi Science and Technology Company, Limited*** *(****Wuhan XRZ****), a Wuhan, China-based Ministry of State Security (MSS) front company that has served as cover for multiple malicious cyber operations. OFAC is also designating* ***Zhao Guangzong*** *and* ***Ni Gaobin****, two Chinese nationals affiliated with Wuhan XRZ, for their roles in malicious cyber operations targeting U.S. entities that operate within U.S. critical infrastructure sectors, directly endangering U.S. national security." reads the press release published by the U.S. Treasury Department. "This action is part of a collaborative effort with the U.S. Department of Justice, Federal Bureau of Investigation (FBI), Department of State, and the United Kingdom Foreign, Commonwealth & Development Office (FCDO)." (continua..)*

https://securityaffairs.com/161064/apt/us-treasury-dep-sanctions-apt31.html

SecurityAffairs *- Pierluigi Paganini -March 26, 2024Topics*

La progettazione di ponti: l'influenza del contesto nella scelta di schemi strutturali, materiali e tipologie - L'articolo individua alcuni degli aspetti più rilevanti da tenere in considerazione nella concezione e progettazione di un ponte, affrontando unitamente gli aspetti strutturali, di progetto, ambientali e di inserimento nel contesto. Vengono inoltre presentati tre casi studio di strutture di piccola, media e grande luce, nei quali i principi suesposti sono applicati a dei casi pratici.

La qualità di un ponte non dipende solo dal suo valore implicito o dal suo utilizzo. Il valore di un ponte va ben oltre il suo uso pratico, essendo un elemento con capacità di diventare "paesaggio".

Questa consapevolezza si sta estendendo negli ultimi anni a tutto il sistema infrastrutturale, considerando la viabilità e le sue pertinenze come un'occasione architettonica per modificare e contemporaneamente valorizzare l'ambiente circostante.

Pertanto, avere a che fare con i ponti non significa solo concepire strutture importanti, necessarie per la nostra vita nelle comunità in quanto connessione tra luoghi.

Progettare e costruire ponti significa relazionarsi con la nostra cultura e la nostra identità.

(continua…).

https://www.ingenio-web.it/articoli/la-progettazione-di-ponti-l-influenza-del-contesto-nella-scelta-di-schemi-strutturali-materiali-e-tipologie/

Ingenio *- Enzo Siviero | Alberto Zanchettin - 29/03/2024*

UN Peace Operations Under Fire From State-Sponsored Hackers

The international body isn't doing enough to protect details on dissidents and activists gathered by peacekeeping operations, particularly across Central Africa.

United Nations peacekeeping missions, especially in Africa, are at a growing risk of compromise by sophisticated nation-state-sponsored threat actors, and they need to adopt basic cybersecurity infrastructure best practices and tools to defend them, according to new research.

The consequences of failing to do so could be deadly, according to a paper from the International Peace Institute.
These peacekeeping missions are gathering substantial amounts of sensitive data, including the identities and locations of activists, dissidents, and others, which makes them a desirable target for governments across the world, as well as loosely associated actors, like the mercenaryWagner Group.
At particular risk are UN missions in central Africa, due to increasingly fraught geopolitics across the region, according to the brief's author, Dirk Druet, an adjunct professor at McGill University in Montreal.
He warns potential breaches of these UN peacekeeping missions could have deadly consequences.
"As the UN's missions in the Central African Republic, Mali, Libya, and elsewhere become increasingly caught up in geopolitical struggles, it will become more and more important for the UN to credibly demonstrate independent control of the data it gathers," Druet says. (continua…)"
https://www.darkreading.com/cyber-risk/un-peace-operations-under-fire-from-state-sponsored-hackers
Dark Reading *- Becky Bracken - March 29, 2024*

Cyberattacks Wreaking Physical Disruption on the Rise
Ransomware groups tore into manufacturing other parts of the OT sector in 2023, and a few attacks caused eight- and nine-figure damages. But worse is yet to come in 2024.
At least 68 cyberattacks last year caused physical consequences to operational technology (OT) networks at more than 500 sites worldwide in some cases causing $10 million to $100 million in damages.
Unsurprisingly, these weren't Stuxnet-like events, but the opposite.
According to a new report from industrial control system (ICS) vendor Waterfall Security Solutions, which studied real-world cyberattacks on OT organizations, most of the hackers known to be targeting the OT sector these days are hacktivists. And the majority of disruptions are not caused by such direct manipulation of OT systems but are downstream consequences of IT-based attacks, most often involving ransomware.
That doesn't mean, though, that the impacts are any less severe. Incidents involving Johnson Controls and Clorox last year ended up costing those companies around $27 million and $49 million, respectively. One cyberattack that led to the temporary suspension of operations at MKS Instruments in Massachusetts cost $200 million, and one of its suppliers California-based Applied Materials Inc. reported losing another $250 million as a result.
The number of attacks with physical consequences increased by nearly 20% last year, according to the report.
IT Attacks With OT Consequences
In the past decade and a half, only around a quarter of cyberattacks with OT consequences were caused by actually hitting the OT network, according to the report Waterfall published in collaboration with OT incident threat database ICS STRIVE.(continua…)
https://www.darkreading.com/ics-ot-security/cyberattacks-wreaking-physical-disruption-on-the-rise
Dark Reading *- Nate Nelson, - April 2, 2024*

La qualità e la quantità dell'acqua sono fondamentali per il benessere - A causa dello sfruttamento eccessivo e del cambiamento climatico, molte aree in Europa soffrono sempre più di scarsità d'acqua. Allo stesso tempo, l'inquinamento esercita un'ulteriore pressione su questa risorsa limitata.

Se volete fare il bagno in Europa, c'è una buona probabilità che la qualità dell'acqua nella località balneare prescelta sia eccellente. Inoltre, la maggior parte dei residenti europei può usufruire di acqua potabile di buona qualità direttamente dal rubinetto.
Tuttavia, l'Europa deve ridurre l'inquinamento idrico causato dai terreni agricoli e dall'industria e migliorare il trattamento delle acque reflue. Questo perché stanno emergendo nuove prove sull'impatto dei microinquinanti, delle microplastiche e della resistenza antimicrobica sulla qualità dell'acqua. Allo stesso tempo, in alcune aree, il cambiamento climatico minaccia sempre più le risorse idriche.
Esigenze concorrenti, inquinamento e cambiamento climatico
L'acqua è una parte fondamentale della natura e una risorsa essenziale per l'uomo. Oltre a berla, usiamo l'acqua per qualsiasi cosa, dalla cucina alla pulizia, alla doccia, allo sciacquone e al nuoto. Allo stesso modo, i nostri settori economici, tra cui energia, trasporti, agricoltura e produzione, dipendono tutti dall'acqua.
La concorrenza tra le richieste di acqua contribuisce all'inquinamento e può portare a uno sfruttamento eccessivo, che può incidere negativamente sulla salute umana. I problemi sanitari diretti sono spesso legati a specifici contaminanti presenti nell'acqua, come batteri, virus, metalli o pesticidi. Sebbene la maggior parte delle persone in Europa abbia un buon accesso all'acqua potabile e all'acqua di balneazione di alta qualità , nuove prove sull'inquinamento chimico e sulla scarsità d'acqua destano crescente preoccupazione.
Il cambiamento climatico sta amplificando le sfide legate alla quantità e alla qualità dell'acqua in Europa. Ad esempio, stiamo assistendo a siccità e inondazioni più frequenti e intense. Le inondazioni sono state il tipo di evento estremo legato al clima più costoso, con danni per oltre 223 miliardi di euro negli ultimi quattro decenni. Soprattutto nell'Europa meridionale, la scarsità d'acqua peggiorerà e colpirà tutti i settori.
(continua…)
https://www.puntosicuro.it/archivio-news-brevi/la-qualita-la-quantita-dell-acqua-sono-fondamentali-per-il-benessere-iNews1-2442.php?
PuntoSicuro *- Redazione - 03/04/2024*

Russia is trying to sabotage European railways, warns Prague - Russia has made "thousands" of attempts to interfere with European rail networks in a campaign to destabilise the EU and sabotage critical infrastructure, the Czech Republic's transport minister has said. Martin Kupka told the Financial Times Moscow was suspected of having made "thousands of attempts to weaken our systems" since Russian President Vladimir Putin ordered the full-scale invasion of Ukraine in February 2022.
The hacking campaign included attacks on signalling systems and on the networks of the Czech national railway operator České dráhy, Kupka said. Past attacks have put ticketing systems out of service and raised concerns about successful interference with signals causing serious accidents.
"It's definitely a difficult point…[but] I'm really very satisfied because we are able to defend all systems [from] a successful attack," Kupka said.
Russian attempts to destabilise European energy infrastructure have been well documented but interference in transport networks has been less discussed.
The EU Agency for Cybersecurity published its first report on threats to transport in March last year. It said there had been "attacks against railway companies with an increasing rate, primarily due to Russia's invasion of Ukraine".
It noted major cyber attacks by "pro-Russia hacker groups" on railway companies in Latvia, Lithuania, Romania and Estonia.

The Czech cyber security agency, NUKIB, has warned of rising cyber attacks in recent years. "One of the last year's prominent trends has been the growing interest of malicious attackers in the energy and transportation sectors," it said in a report published in July. *(continua…)*
https://www.ft.com/content/f8207823-f5e1-4caf-934d-67c648f807bf
Financial Times *- Alice Hancock – 5 Aprile 2024*

Investimenti, partnership e IA. La ricetta di Benigni (Elt) per la cyber-security
Intelligenza artificiale, partnership pubblico privato e maggiori investimenti da parte del sistema-Paese sulla sua sicurezza informatica. Ecco le priorità illustrate da Domitilla Benigni, presidente di CY4Gate e amministratore delegato e chief operating officer di Elettronica, che dovrebbero essere alla base del Ddl Cyber-sicurezza
Il tema della sicurezza informatica è fondamentale e necessario in questo momento storico, e l'obiettivo dell'architettura normativa nel quadro della cyber-security dovrà essere quello di dare una visione di lungo periodo e una strategia chiara per tutte le forze in gioco. A sottolinearlo è stata **Domitilla Benigni**, presidente di CY4Gate e amministratore delegato e chief operating officer di Elettronica nel corso della sua recente audizione informale davanti alle commissioni Affari costituzionali e Giustizia della Camera dei deputati, nell'ambito del riesame del disegno di legge sulla sicurezza informatica differenziata, il cosiddetto ddl Cyber-sicurezza, presentato dal governo.
Collaborazione pubblico-privata
Benigni è intervenuta sul tema sempre più centrale dell'intelligenza artificiale "risorsa indispensabile per la sicurezza nazionale", in particolare sull'articolo 7 contenuto nel Ddl, che interviene sulla materia delle partnership pubblico-privato e definisce il ruolo dell'Agenzia per la cybersecurity nazionale (Acn) nazionale) nella valorizzazione dell'IA. Benigni ha auspicato "un'estensione di questa collaborazione a tutti gli altri aspetti della cybersecurity dove il pubblico, in particolare l'Acn, ha un ruolo chiave di indirizzo e guida e le aziende possono esprimere capacità tecnologica ed umana".
Spingere sull'IA
I benefici di questa collaborazione, ha sottolineato ancora la manager di Elt Group, sono evidenti innanzitutto "nella capacità di gestione degli incidenti e delle crisi, laddove si auspica che siano condivisi ancora di più obiettivi quali lo sviluppo di ulteriori tecnologie e competenze per la gestione delle minacce".(continua…)
https://formiche.net/2024/04/investimenti-partnership-e-ia-la-ricetta-di-benigni-elt-per-la-cyber-security/#content
FORMICHE *- Marco Battaglia- 05/04/2024*

Intelligenza Artificiale. Ecco i dieci cardini della strategia dell'Italia
Il dipartimento per la Trasformazione digitale e l'Agenzia per l'Italia digitale hanno presentato la strategia con cui il nostro Paese si impegna a implementare, proteggere e utilizzare l'enorme evoluzione che lo sviluppo dell'intelligenza artificiale rappresenterà per il futuro collettivo dell'umanità
L'Intelligenza Artificiale (AI) offre un'ampia gamma di tecnologie che, già in un orizzonte di breve e medio periodo, potranno essere utilizzate per stimolare e accelerare lo sviluppo del nostro Paese, spiega il governo italiano nell'executive summary che accompagna della visione strategica dell'Italia su uno dei temi dominanti del momento.

L'Intelligenza Artificiale è sempre più efficace, ad esempio, nel potenziare la produttività delle imprese e l'efficacia della Pubblica Amministrazione, ottimizzando i processi, riducendo gli errori e migliorando la qualità di prodotti e servizi. Essa sta già abilitando innovativi approcci nel campo della salute e delle cure mediche, garantendo una prevenzione più capillare e attenta, diagnosi più precoci e trattamenti più efficaci. L'AI inoltre migliora l'esperienza dei cittadini nel rapporto con le istituzioni; fornisce — spiega il documento che traguarda un orizzonte temporale che va dal 2024 al 2026 — un prezioso supporto nei processi educativi e di apprendimento; è una preziosa alleata nel miglioramento della qualità della vita delle persone e della gestione sostenibile delle risorse, ottimizzando l'utilizzo di energia e materie prime; è un elemento determinante per garantire la sicurezza nazionale e la difesa del Paese.
Lo sviluppo delle tecnologie di AI ha infatti avuto, e sempre più avrà nel prossimo futuro, ritmi frenetici che apriranno a opportunità e cambiamenti da saper ben governare. Proprio in questo dinamismo si deciderà gran parte della nostra competitività: la capacità di affrontare i cambiamenti non solo come spettatori passivi di una rivoluzione epocale, bensì come attori consapevoli e attenti, capaci di utilizzare e produrre nuove soluzioni tecnologiche, concepite e sviluppate in sintonia con i nostri valori e le peculiarità del nostro sistema-Paese.
Una strategia italiana per l'Intelligenza Artificiale, orientata verso le prospettive della competitività e del benessere dei cittadini, dovrà dunque caratterizzarsi come (continua…)
https://formiche.net/2024/04/intelligenza-artificiale-ecco-i-dieci-cardini-della-strategia-dellitalia/#content
***FORMICHE** - Ferruccio Michelin - 07/04/2024*

Ddl Cybersicurezza: Intelligenza Artificiale (IA) per la protezione delle infrastrutture critiche e dei dati sensibili - Questo articolo è il terzo e ultimo di una serie dedicata all'analisi tecnico-giuridica del Disegno di Legge recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici" approvato dal Consiglio dei Ministri lo scorso 25 gennaio e attualmente in corso di esame parlamentare (qui la prima e la seconda parte).
L'Intelligenza Artificiale al servizio della cybersicurezza
Nel panorama tecnologico attuale, se da un lato le Pubbliche Amministrazioni si attrezzano adottando procedure e prassi avanzate per difendersi dagli attacchi informatici, dall'altro l'emergere dell'Intelligenza Artificiale (IA) apre nuove frontiere nella protezione delle infrastrutture critiche e dei dati sensibili.
Questo scenario è al centro dell'articolo 7 del Disegno di Legge Cybersicurezza, che introduce una visione all'avanguardia dell'uso dell'IA ponendola come pilastro nella strategia di sicurezza nazionale, con un occhio attento agli imperativi etici che devono guidarne l'impiego.
L'approccio etico all'utilizzo dell'IA diventa quindi un'estensione naturale dell'impegno delle Pubbliche Amministrazioni verso una gestione sicura e responsabile dell'ambiente digitale.
L'inclusione esplicita di un mandato per l'Agenzia per la Cybersicurezza Nazionale (ACN) di promuovere iniziative di partenariato pubblico-privato per l'impiego dell'IA nella cybersicurezza evidenzia un riconoscimento del valore che questa tecnologia può apportare in termini di efficacia operativa, nonché nella promozione di pratiche etiche contro potenziali abusi. *(continua…)*
https://www.ictsecuritymagazine.com/articoli/ddl-cybersicurezza-intelligenza-artificiale-ia-per-la-protezione-delle-infrastrutture-critiche-e-dei-dati-sensibili/
***ICT Security Magazine** - Francesco Capparelli e Maria Rosaria De Ligio – 8 Aprile 2024*

La nuova Ue non sarà un museo. Il patto per lo sviluppo tra Roma, Berlino e Parigi - "Noi non vogliamo che l'Europa da continente dello sviluppo della tecnologia, diventi un museo all'aria aperta. Per evitare questo destino e la consapevolezza della forza dei popoli e delle nazioni europee, noi dobbiamo lavorare insieme". Questa la traccia indicata dal ministro delle Imprese e del made in Italy, **Adolfo Urso**, al termine della terza riunione trilaterale sulla politica industriale europea con Francia e Germania.
https://formiche.net/2024/04/patto-fra-roma-berlino-e-parigi-nuova-ue/#content
Formiche *– Francesco De Palo – 08/04/2024*

US Environmental Protection Agency hack exposes data of 8.5 million users
The leaked database has personal information of users including name, email, phone numbers, and address.
The US federal arm tasked with environmental protection matters, the Environmental Protection Agency (EPA), is allegedly experiencing a data breach affecting over 8.5 million users.
The breach, which has reportedly exposed personal and sensitive information belonging to EPA's customers and contractors, was claimed by a hacker operating under the alias USDoD on Sunday.
"Hello Breachforums, this is your favorite TA and today I'm proud to say that I'm releasing epa.gov database of contact list. This is their entire contact of Critical Infra not only for the USA but for the entire globe "USDoD posted on the dark web.
Various reports confirm the legitimacy of USDoD's claims and have published the details of their own analysis. The EPA hasn't yet confirmed the breach.
Breached data include personal user data
An analysis of the leaked database by Hackread.com found it containing three zipped files with 500MB of data inside, all in CSV formats. The files are named: Contact (3,726,130 records), Inter_Contact (9,952,374 records), and Staff (3,325,973 records).. (continua…)
https://www.csoonline.com/article/2085541/us-environmental-protection-agency-hack-exposes-data-of-8-5-million-users.html
CSOONLINE *- Shweta Sharma - Apr 08, 2024*

Rivendicazione ransomware a Benetton, ma la vittima è Olimpias: cosa è successo
Una rivendicazione ransomware apparsa nel Dark Web proprio in questi giorni e rivolta a Benetton Group è, in realtà, riferita a un'altra azienda, di cui la multinazionale detiene quote di partecipazione, e fa seguito a un attacco di oltre un anno fa. Cerchiamo di capire cos'è successo e cosa sappiamo del rebrand di HiveLeaks
Nei giorni scorsi la **cyber gang** di **ransomware Hunters** ha pubblicato, sul proprio Data Leak Site, una rivendicazione di responsabilità su un attacco abbastanza ambizioso: **Benetton Group**, hanno titolato i criminali. Ma andando ad analizzare la vicenda, bisogna fare delle precisazioni rispetto a quanto dichiarato dagli attaccanti.
Questo è successo il 3 aprile scorso e il post riferiva di una tempistica fino al 7 aprile per la pubblicazione di tutto l'insieme dei dati esfiltrati durante l'attacco: **433 GB di informazioni interne**.
Ciò che abbiamo scoperto, non appena i criminali hanno rilasciato quanto promesso, è che il nome di Benetton Group compare solo alla lontana. **La vittima interessata sarebbe stata l'azienda Olimpias**, della quale il gruppo Benetton detiene delle quote di partecipazione, e non l'infrastruttura realmente interna a Benetton.

Indice degli argomenti

La rivendicazione a Benetton non è riferita a loro

Occorre, inoltre, fare un'altra precisazione su questo attacco ransomware. I fatti sono riferiti a gennaio 2023 quando un gruppo criminale ransomware conosciuto con il nome di Hive pare abbia preso di mira Benetton Group, con ipotesi di esfiltrazione di dati. Tuttavia, questa rivendicazione non apparirà mai sui sistemi pubblici del gruppo Hive e nello stesso anno la cyber gang subirà un'azione legale da parte delle forze dell'ordine di diversi paesi, scomparendo dalla scena cyber. (continua…)

https://www.cybersecurity360.it/news/rivendicazione-ransomware-a-benetton-ma-la-vittima-e-olimpias-cosa-e-successo/

Cybersecurity360 *- Dario Fadda - 8 apr 2024*

Cyber resilience, una road map agile per le organizzazioni

Garantire la capacità di anticipare, resistere e recuperare da eventi avversi cibernetici è fondamentale nell'era digitale. Cyber security, Information Security (InfoSec), e Risk Management giocano ruoli cruciali in questo processo

La cyber resilience è una priorità strategica per tutte le organizzazioni in un mondo sempre più digitalizzato e interconnesso, in cui la cyber security, l'Information Security (InfoSec) e il Risk Management hanno un ruolo fondamentale specifico e, al contempo, complementare nel proteggere dalle minacce cibernetiche e nel garantire la continuità operativa.

Indice degli argomenti

I ruoli di cyber security, Information Security (InfoSec) e Risk Management nella cyber resilience

Garantire la cyber resilience, ovvero la capacità di un'organizzazione di anticipare, resistere, recuperare da eventi avversi cibernetici, è fondamentale nell'era digitale. Cyber security, Information Security (InfoSec), e Risk Management giocano ruoli cruciali in questo processo, contribuendo in modo complementare a definire una strategia di cyber resilience

Cyber security – La cyber security si concentra sulla protezione dei sistemi informatici, delle reti e dei dati dagli attacchi cibernetici. Il suo obiettivo è difendere le risorse digitali da accessi non autorizzati, danneggiamenti o interruzioni causate da attacchi come malware, ransomware, phishing e altre forme di cybercrime.

Le pratiche di cyber security includono:

- Implementazione di misure tecniche come firewall, antivirus e sistemi di prevenzione delle intrusioni.
- Monitoraggio continuo delle reti e dei sistemi per rilevare e rispondere tempestivamente agli incidenti di sicurezza.
- Crittografia dei dati per proteggere le informazioni sensibili durante la trasmissione e l'archiviazione.

Information Security (InfoSec) – L'information security è un concetto che comprende la protezione di tutte le forme di informazioni, sia digitali che fisiche, da accessi non autorizzati, divulgazione, alterazione, distruzione o perdita. È doveroso ricordare che l'InfoSec si basa su tre principi fondamentali noti come CIA Triad, ovvero (continua…)
https://www.cybersecurity360.it/outlook/cyber-resilience-una-road-map-agile-per-le-organizzazioni/
Cybersecurity360 *- Federica Maria Rita Livelli - 9 apr 2024*

CHINA IS USING GENERATIVE AI TO CARRY OUT INFLUENCE OPERATIONS

China-linked threat actors are using AI to carry out influence operations aimed at fueling social disorders in the U.S. and Taiwan.

China is using generative artificial intelligence to carry out influence operations against foreign countries, including the U.S. and Taiwan, and fuel social disorders.

According to the report published by the Microsoft Threat Analysis Center (MTAC), titled *Same targets, new playbooks: East Asia threat actors employ unique methods*, China-linked threat actors are using generative artificial intelligence to create content aimed at influencing U.S. voters.

The state-sponsored activity relies on deceptive social media accounts posing provocative questions on divisive U.S. domestic issues. These operations allow for identifying the key concerns dividing American voters, possibly to gather intelligence on crucial voting demographics ahead of the U.S. presidential election.

"There has been an increased use of Chinese AI-generated content in recent months, attempting to influence and sow division in the U.S. and elsewhere on a range of topics including: the train derailment in Kentucky in November 2023, the Maui wildfires in August 2023, the disposal of Japanese nuclear wastewater, drug use in the U.S. as well as immigration policies and racial tensions in the country." states Microsoft. "There is little evidence these efforts have been successful in swaying opinion."

China's geopolitical priorities remain unchanged but it has doubled down on its targets and increased the sophistication of its influence operations (IO) attacks.

In January, experts observed a surge in the use of AI-generated content to augment IO operations by CCP-affiliated actors ahead of the Taiwanese presidential election. (continua….)
https://securityaffairs.com/161608/security/china-ai-influence-operations.html
SecurityAffairs *- Pierluigi Paganini - April 09, 2024*

Custom-made Awareness Raising to enhance Cybersecurity Culture - Advanced protection of systems and a robust cybersecurity strategy have become a priority for all kinds of organisations, as cybersecurity issues and threats have evolved to be increasingly sophisticated and pervasive. Thus, awareness raising activities and having a relevant methodology in place are a fundamental to integrating cybersecurity in the organisational culture. With a view to achieve this goal, applying game design elements in cybersecurity awareness activities can simplify familiarisation with terms and concepts through a hands-on experience and motivate employees' participation.

To test the new edition of the all-in-one toolkit, ENISA piloted the Awareness Raising in a Box (AR-in-a-BOX) with the Cypriot Digital Security Authority and the Cypriot National Coordination Centre.

AR-in-a-Box allows professionals from small and medium (SMEs) to big enterprises and public or private entities, to improve their knowledge on cybersecurity awareness techniques. This comprehensive toolkit offers a blend of theoretical frameworks and practical resources, enabling

organisations to craft tailored cybersecurity awareness programmes, including gamification of content. *(continua…)*
https://www.enisa.europa.eu/news/custom-made-awareness-raising-to-enhance-cybersecurity-culture
Enisa *– Enisa – 10 Aprile 2024*

Attacco Regione Lazio, il Garante Privacy conferma i gravi errori

Arrivano le sanzioni del Garante per i fatti cyber accaduti in pieno periodo vaccinale anti Covid, a servizio sanitario di Regione Lazio. Un attacco ransomware dagli impatti gravi e importanti per i cittadini che trovarono indisponibilità delle strutture sensibili per giorni

Nella notte tra il 31 luglio e il primo agosto del 2021, un attacco informatico scuoteva le fondamenta del sistema sanitario regionale del Lazio, causando un grave data breach che ha compromesso la sicurezza dei dati personali di milioni di assistiti.

Come pubblicato oggi dall'autorità italiana per la protezione dei dati, le conseguenze di questo attacco hanno **ora portato a una serie di sanzioni da parte del Garante,** delineando responsabilità e gravi violazioni della normativa sulla privacy.

Indice degli argomenti

L'attacco a Regione Lazio in periodo Covid

L'attacco, perpetrato attraverso l'introduzione di ransomware tramite un portatile di un dipendente della Regione Lazio, ha avuto ripercussioni devastanti: blocchi d'accesso a servizi sanitari cruciali, tra cui gestione delle prenotazioni, pagamenti, ritiro dei referti e registrazione delle vaccinazioni. Asl, aziende ospedaliere e case di cura hanno dovuto fronteggiare l'impossibilità di utilizzare sistemi informativi regionali per diverse ore, e in alcuni casi anche per mesi.

Le indagini condotte dall'autorità Garante Privacy hanno rivelato una serie di gravi violazioni da parte di LAZIOcrea, la società responsabile dei sistemi informativi regionali, e della Regione Lazio stessa. Entrambe le entità sono state ritenute colpevoli di adottare sistemi obsoleti e di non implementare adeguate misure di sicurezza per prevenire e rilevare tempestivamente violazioni dei dati personali, come definito nel provvedimento.

In particolare, LAZIOcrea è stata accusata di non aver agito prontamente per gestire l'attacco informatico e le sue conseguenze, **decidendo di spegnere tutti i sistemi senza essere in grado di determinare quelli effettivamente compromessi** o di prevenire ulteriori propagazioni del malware. Questa mancanza di azione ha aggravato notevolmente l'impatto dell'attacco, causando disagi significativi per le strutture sanitarie regionali e i loro assistiti. (continua…)
https://www.cybersecurity360.it/legal/privacy-dati-personali/attacco-regione-lazio-il-garante-privacy-conferma-gravi-errori/
Cybersecurity360 *- Dario Fadda- 10 apr 2024*

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link
http://www.infrastrutturecritiche.it/new/per-iscriversi/

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00182 Roma, via Urbino 31 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani Marco Raul Massoni

ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it

La NewsLetter ha lo scopo di rendere note le principali informazioni nell'ambito delle Infrastrutture Critiche e le attività dell'Associazione Italiana esperti in Infrastrutture Critiche (AIIC). Tutti i contenuti relativi alla sezione NEWS e Eventi sono pubblici on line e di proprietà dei rispettivi editori.