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

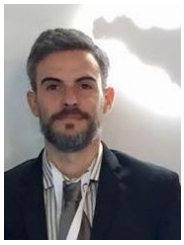
Newsletter

ANNO 2024 | **n. 08/ 2024** | **settembre 2024**

L'importanza dei cavi sottomarini nella connessione globale

I cavi sottomarini rappresentano l'infrastruttura essenziale che sostiene l'economia digitale globale, garantendo la trasmissione di dati, voce e immagini tra continenti attraverso migliaia di chilometri sotto gli oceani. Sebbene spesso invisibili, questi cavi sono il fulcro del nostro mondo iperconnesso.
Oggi, circa il 99% del traffico dati internazionale passa attraverso cavi sottomarini. Senza questa rete, le comunicazioni tra Paesi e continenti sarebbero drasticamente ridotte o estremamente lente. Essi consentono alle persone di navigare su Internet, fare videoconferenze e accedere a servizi cloud, in modo quasi istantaneo, contribuendo a mantenere l'infrastruttura delle telecomunicazioni stabile e sicura.
Rispetto alle alternative come i satelliti, i cavi sottomarini offrono velocità superiori e maggiore affidabilità. Le fibre ottiche utilizzate all'interno dei cavi trasportano enormi quantità di dati in tempi rapidissimi, rendendo possibili connessioni veloci tra continenti. Inoltre, i cavi sottomarini sono meno vulnerabili a interruzioni atmosferiche, offrendo una connessione più stabile rispetto ai satelliti.
Dal punto di vista economico, i cavi sottomarini sono fondamentali per il commercio globale. Consentono a imprese, governi e individui di scambiarsi informazioni e condurre transazioni finanziarie in tempo reale. Il settore bancario, i mercati azionari e le piattaforme di e-commerce dipendono interamente da questa rete per funzionare in modo efficace e sicuro.
Nonostante la loro importanza, i cavi sottomarini sono soggetti a sfide continue, tra cui danni causati da fenomeni naturali, attività umane come la pesca o l'ancoraggio di navi, e preoccupazioni legate alla sicurezza informatica. La protezione di questi cavi è diventata una priorità per governi e aziende private, che investono sempre di più in tecnologie per monitorare e prevenire eventuali danni o attacchi.
Non di meno, questi cavi, che collegano Paesi e continenti, sono spesso al centro di tensioni tra le maggiori potenze mondiali. Il controllo delle rotte dei cavi e l'accesso ai dati trasportati sono considerati strategici. Alcuni governi vedono la protezione e il monitoraggio di queste infrastrutture come una questione di sicurezza nazionale. Per quanto concerne l'aspetto geopolitico e cibernetico, l'espansione della Cina nel settore delle telecomunicazioni e il controllo di diverse infrastrutture critiche, compresi i cavi sottomarini, ha sollevato dubbi tra i Paesi occidentali, che temono l'uso dei cavi come strumento di sorveglianza o di pressione economica e politica. Analogamente la Federazione Russa vede i cavi sottomarini come infrastrutture strategiche sia per le proprie esigenze di comunicazione che come potenziali obiettivi militari e politici. Gli Stati Uniti e altri Paesi occidentali hanno espresso preoccupazioni per il crescente interesse della Russia nelle operazioni sottomarine in prossimità dei cavi. In particolare, le attività della Marina russa, comprese le missioni condotte da sottomarini specializzati, hanno sollevato timori riguardo a possibili sabotaggi o spionaggio delle comunicazioni trasmesse da questi cavi.
In un mondo sempre più interconnesso, i cavi sottomarini rappresentano l'infrastruttura invisibile che sostiene la nostra vita digitale quotidiana. Il loro ruolo è cruciale per garantire la continuità delle

comunicazioni globali, sostenendo il commercio e l'innovazione. Tuttavia, la loro crescente rilevanza li rende anche un terreno di competizione geopolitica e una potenziale vulnerabilità strategica. La protezione di questa rete globale è essenziale per garantire un futuro sicuro e connesso.



Gianluca Cipriani

Laureato in Relazioni Internazionali all'Università degli Studi "Roma Tre" e Master in Protezione Strategica del Sistema Paese alla SIOI di Roma. Attualmente lavora come Senior Consultant presso Hermes Bay SrL su Enterprise Risk Management, Cyber Security e Cyber Governance.

ATTIVITA' DELL'ASSOCIAZIONE

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.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

Analisi big data: come sfruttarla per ottenere un vantaggio competitivo - L'**analisi dei big data** sta assumendo un ruolo sempre più centrale, consentendo alle organizzazioni di crescere grazie a funzionalità come l'analisi in tempo reale e il miglioramento del processo decisionale. Ne consegue che, investire in una strategia efficace per la gestione dei dati permette di mantenere un vantaggio competitivo nel mercato.
I vantaggi offerti dai big data si sono moltiplicati a fronte della trasformazione digitale e della diffusione di tecnologie, quali il cloud computing, l'Internet of Things (IoT) e l'intelligenza artificiale.
Di fatto, **una solida strategia per la gestione dei dati è indispensabile per le organizzazioni che vogliono mantenere un vantaggio competitivo** e sfruttare al massimo il potenziale dei big data. Inoltre, l'analisi dei dati è ormai integrata in vari settori e dipartimenti, oltre a svolgere un ruolo cruciale nelle iniziative di sostenibilità, come il monitoraggio delle emissioni e degli agenti inquinanti, contribuendo così alla lotta contro il cambiamento climatico.
Indice degli argomenti

Importanza e vantaggi dell'analisi dei big dati
I big data offrono vantaggi significativi attraverso l'analisi avanzata che permette previsioni precise, ottimizzazione dei processi, miglioramento delle performance aziendali e personalizzazione dell'esperienza del cliente. Ecco i principali vantaggi che offrono:

- **Decisioni strategiche –** I big data offrono una comprensione dettagliata che guida decisioni più informate e strategiche, consentendo alle organizzazioni di individuare opportunità di crescita, migliorare l'efficienza operativa e ridurre i rischi. I
- **Vantaggio competitivo –** Le organizzazioni, sfruttando efficacemente i big data, ottengono un vantaggio competitivo significativo. Inoltre, esse possono identificare nuove opportunità di business, sviluppare prodotti e servizi innovativi e anticipare le esigenze dei clienti, conquistando così una posizione di leadership nel mercato.
- **Efficienza operativa –** L'analisi dei big data permette alle organizzazioni di ottimizzare le operazioni aziendali, identificando colli di bottiglia, riducendo gli sprechi e automatizzando le attività. Ciò consente di ottenere un risparmio sui costi e una maggiore produttività, liberando risorse per investire in altre aree strategiche. *(continua…)*

https://www.agendadigitale.eu/infrastrutture/analisi-big-data-come-sfruttarla-per-ottenere-un-vantaggio-competitivo/?utm_campaign=agenda_nl_base_20240713&utm_source=agenda_nl_base_20240713&utm_medium=email&sfdcid=0030O00002LXHlXQAX
AGENDA DIGITALE *-Federica Maria Rita Livelli - 8 lug 2024*

L'Ue nella corsa globale dei microchip: finanziamenti e progetti strategici - L'Unione Europea ha annunciato un investimento di 325 milioni di euro per la ricerca e l'innovazione nei semiconduttori, nell'ambito del Chips Act. Il programma mira a rafforzare l'ecosistema dei semiconduttori europeo, affrontando carenze di approvvigionamento e migliorando l'autonomia digitale. Progetti in Germania e Italia sottolineano l'importanza strategica del settore

Il 4 luglio il **Chips Joint Undertaking** ha annunciato **un investimento da 325 milioni di euro** per le iniziative di ricerca e innovazione sui **semiconduttori** nel campo della fotonica, dei centri di competenza e di una piattaforma di progettazione di semiconduttori basata sul cloud, nell'ambito dell'iniziativa "**Chips for Europe**" prevista dal "**Chips Act**", ossia il Regolamento n. 2023/781 per l'istituzione di un quadro di misure per il rafforzamento dell'ecosistema dei semiconduttori.

Indice degli argomenti

Iniziative principali del Chips Joint Undertaking

Il programma Chips Joint Undertaking era stato inaugurato il 30 novembre 2023 dalla Commissione europea per l'implementazione dell'iniziativa Chips for Europe al fine di **affrontare la carenza di semiconduttori e migliorare l'autonomia digitale dell'Europa,** attraverso la ricerca, lo sviluppo e l'innovazione con un significativo finanziamento dell'UE di circa 11 miliardi di euro.

Ricerca e innovazione nel campo dei semiconduttori e della fotonica

Nel Chips JU, dunque, sono state individuate **tre aree di intervento**. La prima concerne le iniziative di ricerca e innovazione nel campo dei semiconduttori e della fotonica: **la nuova serie di bandi sosterrà l'industria europea dei semiconduttori** istituendo una linea pilota per i circuiti integrati fotonici. Questi semiconduttori utilizzano la luce per elaborare e trasmettere informazioni a velocità più elevate, consumando meno energia. In un futuro non troppo lontano, ciò sarà particolarmente importante per la prossima generazione di computer ad alte prestazioni, comunicazioni ad alta velocità e centri dati. (*continua…)*

https://www.agendadigitale.eu/mercati-digitali/lue-nella-corsa-globale-dei-microchip-finanziamenti-e-progetti-strategici/?utm_campaign=agenda_nl_base_20240713&utm_source=agenda_nl_base_20240713&utm_medium=email&sfdcid=0030O00002LXHlXQAX

AGENDA DIGITALE - *Luisa Franchina, Corrado Fulgenzi - 9 lug 2024*

Microsoft says massive Azure outage was caused by DDoS attack - Microsoft confirmed today that a nine-hour outage on Tuesday, which took down and disrupted multiple Microsoft 365 and Azure services worldwide, was triggered by a distributed denial-of-service (DDoS) attack.

Redmond says the outage impacted Microsoft Entra, some Microsoft 365 and Microsoft Purview services (including Intune, Power BI, and Power Platform), as well as Azure App Services, Application Insights, Azure IoT Central, Azure Log Search Alerts, Azure Policy, and the Azure portal.

The company confirmed in a mitigation statement published today that the root cause behind yesterday's outage was a DDoS attack, although it has yet to link it to a specific threat actor.

"While the initial trigger event was a Distributed Denial-of-Service (DDoS) attack, which activated our DDoS protection mechanisms, initial investigations suggest that an error in the implementation of our defenses amplified the impact of the attack rather than mitigating it," Microsoft said.

"Once the nature of the usage spike was understood, we implemented networking configuration changes to support our DDoS protection efforts, and performed failovers to alternate networking paths to provide relief."

BleepingComputer also contacted Microsoft on Tuesday regarding rumors that a DDoS attack was behind the outage, but we have yet to receive a reply.

The confirmation comes after the company said while mitigating the outage incident that it was caused by an "unexpected usage spike" that "resulted in Azure Front Door (AFD) and Azure Content Delivery Network (CDN) components performing below acceptable thresholds, leading to intermittent errors, timeout, and latency spikes."

Redmond says it plans to release a Preliminary Post-Incident Review (PIR) within 72 hours and a Final Post-Incident Review within the next two weeks with additional details and lessons learned from this week's outage.

In June 2023, Microsoft also confirmed that a threat actor known as Anonymous Sudan (aka Storm-1359), believed to have Russian links, took down its Azure, Outlook, and OneDrive web portals in Layer 7 DDoS attacks. *(continua…)*

https://www.bleepingcomputer.com/news/microsoft/microsoft-says-massive-azure-outage-was-caused-by-ddos-attack/

Bleepingcomputer - *Sergiu Gatlan - July 31, 2024*

Solar Power Installations Worldwide Open to Cloud API Bugs - The weaknesses gave attackers an avenue to take over millions of photovoltaic devices connected to Solarman and Deye's cloud-hosted management systems.
A recent analysis of two widely used technologies in residential and commercial solar power installations revealed multiple vulnerabilities in their cloud APIs, which, if exploited, would potentially have allowed an attacker to take down parts of any connected power grid.
Researchers at Bitdefender discovered the issues on Solarman, one of the world's largest platforms for managing solar power systems, and on Deye Cloud for managing inverters from China's Ningbo Deye Inverter Technology. Both have since addressed the issues that Bitdefender reported to them.
An inverter is a device that coverts the direct current (DC) electricity produced by solar panels into alternating current (AC) electricity, the standard form used in homes and the electrical grid. They can also monitor and report on the solar system's performance.
"In grid-tied solar power systems, the inverter synchronizes the phase and frequency of the AC output with the grid," Bitdefender said in a report. The goal is to ensure that solar-generated energy is compatible with the grid and can be safely exported to it. Because differences in phase and voltage can crash the grid, "power distributors and governments see any deliberate attempts to bypass these grid safety measures as a threat to national security," Bitdefender noted.
Solarman's platform allows residential and commercial users of Deye and other inverter brands to remotely monitor the devices in real-time. Multiple vendors of other photovoltaic (PV) equipment also use the Solarman platform to connect users with their respective products, over the cloud. Among other things, Solarman offers a data logger that gathers metrics such as the total power output from a solar installation, as well as its voltage and current.
"This management feature improves system performance, enhances reliability, and supports informed decision-making," Bitdefender noted. Some 2.5 million photovoltaic installations are currently connected to the Solarman platform, from more than 190 countries. Together they produce over 195 gigawatts of power in total — or roughly 20% of total solar electric production globally. (continua…)
https://www.darkreading.com/ics-ot-security/solar-power-installations-worldwide-open-to-cloud-api-bugs
DARKREADING- *Jai Vijayan, - August 9, 2024*

10 elementi di sicurezza informatica potenziata dall'AI per i CISO - Quali sono i 10 elementi di sicurezza informatica potenziata dall'AI che i CISO dovrebbero considerare? Secondo la MIT Technology Review, il principale vantaggio tangibile dell'IA segnalato finora dai managers aziendali, è il miglioramento della sicurezza e della gestione dei rischi. Attualmente, quasi il 70% delle aziende afferma di non poter rispondere efficacemente alle minacce informatiche senza l'utilizzo di strumenti di sicurezza potenziati dall'Intelligenza Artificiale. Ad evidenziarlo è Check Point, che sottolinea: "Nonostante, però, le opportunità di sicurezza informatica basate sull'IA siano decisamente valide e apprezzabili, il sensazionalismo continua a oscurare il modo con cui questi strumenti possono realmente far progredire le iniziative di sicurezza".
I 10 elementi di sicurezza informatica potenziata dall'AI per i CISO
Ecco quindi i 10 principali elementi secondo Check Point che i CISO devono tenere in considerazione per gestire la sicurezza informatica nell'era dell'Intelligenza Artificiale *(continua).*
https://www.snewsonline.com/10-elementi-sicurezza-informatica-potenziata-ai-ciso/
S News – *Redazione, 26/08/2024*

Le insidie del ransomware e come gestirlo secondo la legge - È una delle minacce digitali più temute, sia per il livello di danno economico reputazionale e tecnico che può causare e sia perché se non si affronta correttamente in modo preventivo c'è il serio "rischio di ricaduta nel baratro". Ecco perché conoscere gli strumenti giuridici e le normative a tema diventa decisivo

Si scrive **ransomware** e si legge guaio perché il **malware** che blocca l'operatività dietro la richiesta di riscatto è spesso utilizzato dai criminali informatici per fare cassa.

Nonostante le raccomandazioni e diverse possibili azioni preventive suggerite dagli esperti di sicurezza informatica e nonostante guide e community dedicate al tema, le vittime non accennano a diminuire e quando cala la percentuale di attacco, sembra sempre sia solo per una minore attività dei criminali.

Sovvertire questa dinamica sta a ciascuno di noi nel suo quotidiano lavorativo e personale, avendo contezza della minaccia e di come prevenirla.

Un'utile guida di mezzi tecnici preventivi e post attacco è stata recentemente resa disponibile, ma accanto a tali misure per scongiurare un attacco e un danno da ransomware è necessario conoscere anche la disciplina giuridica su questo tema, sia quella nazionale che internazionale per capire misure di contrasto e diritti legali della vittima.

Ci aiuta in questo excursus la professoressa **Annita Larissa Sciacovelli,** professoressa di diritto internazionale, specialista in sicurezza informatica presso l'Università di Bari e membro dell'Advisory Group (AG) dell'Agenzia europea per la sicurezza informatica (ENISA).

Indice degli argomenti

Il ransomware e le sue criticità

Qualsiasi attacco informatico apporta danneggiamenti sul fronte economico per gli effetti sull'operatività standard, ma è forse il danno reputazionale quello maggiormente temuto.

Sciacovelli ricorda a questo proposito come il ransomware sia un attacco complesso sia dal punto di vista tecnico sia da quello giuridico e che "per gli analisti di **Chainanalysis il 2023 è stato l'anno neri nei pagamenti di riscatti**, proprio perché, come dicono in USA, ci vogliono 20 anni per costruire una reputazione e pochi minuti per un attacco informatico che la rovini".

Che il ransomware sia temuto è noto a molti e la docente ricorda "gli attacchi **WannaCry** e **NotPetya** del 2016 e 2017" come esempi noti e dolorosi per molte vittime e in alcuni casi anche capaci di incidere sulla sicurezza nazionale. "Ad esempio, nel 2022 il Costa Rica ha dichiarato lo stato di emergenza nazionale per il blocco quasi totale degli enti governativi ad opera del gruppo filorusso Conti".

Ma una delle maggiori difficoltà risiede nella identificazione e corretta attribuzione degli attacchi da parte del gruppo criminale e dello Stato mandante. (continua…)

https://www.cybersecurity360.it/outlook/le-leggi-del-ransomware-e-il-ransomware-secondo-la-legge/

Cybersecurity360 *- Alessia Valentini - 4 set 2024*

Le frodi informatiche afferenti a pagamenti elettronici sono in costante aumento - L'uso degli applicativi di intelligenza artificiale generativi non ha fatto che accrescere, in maniera esponenziale, le frodi informatiche, che inducono le vittime ad effettuare pagamenti elettronici.
Un recente studio del Federal Bureau of Investigations, negli Stati Uniti, ha messo in evidenza come le frodi, basate su messaggi di posta elettronica od altre comunicazioni, che inducono il destinatario ad effettuare pagamenti elettronici, sono in costante aumento. Queste frodi informatiche creano delle perdite finanziarie significative e rappresentano un crescente problema negli Stati Uniti, ma anche in altri paesi del mondo.
Ci si domanda come le istituzioni finanziarie, come le banche e gli applicativi di pagamenti elettronici, possano dare un contributo per prevenire, individuare e rimediare a queste frodi elettroniche.
Le istituzioni finanziarie, in particolare, possono aiutare i propri clienti ad evitare queste frodi, grazie a programmi di educazione dei consumatori l'addestramento del personale.
Ad oggi, tuttavia, le istituzioni finanziarie non sono obbligate a rimborsare i propri enti, che hanno subito perdite per queste frodi, in quanto i pagamenti fraudolenti sono stati effettuati rispettando tutte le clausole di legittimità.
Queste frodi informatiche possono assumere varie forme, ma in genere i criminali informatici giocano sugli aspetti emotivi delle vittime, per indurle ad inviare del denaro. Secondo uno studio del Servizio Segreto negli Stati Uniti, l'uso di applicativi di intelligenza artificiale generativa permette di creare dei contenuti estremamente realistici, in termini di voci e di immagini, in modo da rendere assai difficile l'identificazione di queste frodi. *(continua…)*
https://www.puntosicuro.it/sicurezza-informatica-C-90/le-frodi-informatiche-afferenti-a-pagamenti-elettronici-sono-in-costante-aumento-AR-24610/
Punto Sicuro *– Adalberto Biasiotti , 06/09/2024*

Russia-linked GRU Unit 29155 targeted critical infrastructure globally - The United States and its allies state that Russia-linked threat actors operating under the GRU are behind global critical infrastructure attacks**.**
The FBI, CISA, and NSA linked threat actors from Russia's GRU Unit 29155 to global cyber operations since at least 2020. These operations include espionage, sabotage, and reputational damage. The United States and its allies state that GRU is behind global critical infrastructure attacks.
Starting January 13, 2022, the group employed the WhisperGate wiper in attacks against Ukrainian organizations. The government expert pointed out that Unit 29155 operates independently from other GRU-affiliated groups like Unit 26165 and Unit 74455.
Russia's GRU Unit 29155 is also responsible for attempted coups, influence operations, and assassination attempts across Europe. Since 2020, the unit has expanded into offensive cyber operations aimed at espionage, reputational harm, and data destruction.
The FBI, NSA, and CISA assess that Russia's GRU Unit 29155 is responsible for various activities such as attempted coups, sabotage, influence operations, and assassination attempts across Europe. Since 2020, the unit has expanded into offensive cyber operations aimed at espionage, reputational harm, and data destruction. The FBI believes the unit's cyber actors are junior GRU officers gaining experience under senior leadership. They also rely on non-GRU actors, including cybercriminals, to carry out their operations.
"FBI assesses the Unit 29155 cyber actors to be junior active-duty GRU officers under the direction of experienced Unit 29155 leadership. These individuals appear to be gaining cyber experience and

enhancing their technical skills through conducting cyber operations and intrusions." reads the joint advisory. (continua)
https://securityaffairs.com/168095/cyber-warfare-2/russia-gru-unit-29155-critical-infrastructure.html
SECURITY AFFAIRS -*Pierluigi Paganini -September 06, 2024*

Ondata cyber. Allarme multinazionale sugli hacker russi - Nuove accuse provenienti da istituzioni euroatlantiche puntano il dito contro la Russia per quel che riguarda le attività cibernetiche. I cui bersagli vanno dall'Ucraina agli Stati Uniti
Un gruppo di hacker russi avrebbe condotto azioni di sabotaggio, spionaggio e "danno alla reputazione" contro ben ventisei Paesi appartenenti all'Alleanza Atlantica, compresi gli Stati Uniti, cercando così di interrompere, o quantomeno di inficiare, gli sforzi transatlantici di sostegno all'Ucraina.
A lanciare l'allarme sono state la National Security Agency (Nsa), il Fbi, la Cybersecurity and Infrastructure Security Agency (Cisa) e altri partner internazionali tra cui agenzie ucraine, lettoni, tedesche e ceche. In particolare, questa compagine di enti ha individuato come responsabile indiretto di questi attacchi l'unità Unità 29155 afferente al 161° Centro di addestramento per specialisti dello Stato Maggiore russo.
Oltre a utilizzare il malware WhisperGate per colpire i sistemi ucraini, il gruppo avrebbe anche condotto "campagne informatiche distruttive, scansioni di infrastrutture ed esfiltrazioni di dati, con l'obiettivo primario, dall'inizio del 2022, di interrompere gli aiuti all'Ucraina", si legge nel report pubblicato lo scorso giovedì 5 settembre.
Dave Luber, direttore della sicurezza informatica dell'Nsa, ha avvertito le aziende americane delle capacità dell'Unità 29155 e le ha esortate a prendere le opportune precauzioni per proteggersi dal rischio di diventare vittime del gruppo. "È importante che le organizzazioni utilizzino queste informazioni e prendano provvedimenti immediati per proteggere i dati e mitigare i danni causati da questi attori informatici malintenzionati", ha dichiarato Luber in un comunicato stampa. (continua…)
https://formiche.net/2024/09/ondata-cyber-hacker-russi-nato/#content
FORMICHE *-Lorenzo Piccioli -07/09/2024*

Crisi climatica: i piani anti-alluvione per Lower Manhattan - New York City più di altre città soffre gli effetti della crisi climatica. Dall'uragano Sandy del 2012 in poi ha saputo però reagire e mettere in campo studi e progetti importanti, chiamando a lavorare i migliori studi di progettazione internazionale. E da poco sono iniziati i lavori di messa in sicurezza e di riqualificazione del waterfront sud (prima parte).
New York City, come molte altre città del mondo, sta affrontando la difficile realtà del cambiamento climatico e dei suoi pesanti impatti sull'ambiente urbano. La "città che non dorme mai" è considerata infatti una delle metropoli più vulnerabili, sottoposta a tempeste intense, precipitazioni estreme e all'innalzamento del livello delle acque del mare. Gli uragani Sandy (2012) e Ida (2021) sono stati i casi più eclatanti della fragilità climatica della Grande Mela.
Il 22 ottobre del 2012, quasi un quinto della città andò sott'acqua, colpita dalla forza di Sandy: alla fine si contarono 44 vittime, danni per 19 miliardi di dollari, migliaia di edifici rimasero allagati e più di 20mila attività dovettero chiudere.
Nei dodici anni che ci separano da quei giorni drammatici, a New York vi è stata una mobilitazione senza precedenti, sia degli enti locali, federali e governativi sia da parte della popolazione newyorkese sotto

la spinta dell'organizzazione Rebuild by Design: sono state avanzate proposte, avviate iniziative, messi a punto progetti, recuperati fondi, attivati confronti con gli abitanti delle zone più colpite.
Dagli studi si è poi passati ai progetti e ora si è finalmente arrivati alle prime realizzazioni, per mettere in sicurezza una delle zone più densamente popolate al mondo. In questo primo articolo raccontiamo i masterplan e i primi progetti; nel successivo il loro avanzamento e alcune prime realizzazioni.
(continua…)
https://www.ingenio-web.it/articoli/crisi-climatica-i-piani-anti-alluvione-per-lower-manhattan/
Ingenio *– Pietro Mezzi, 09.09.2024*

Cyber nella PA, così i nuovi fondi da 347 milioni rafforzano le amministrazioni più a rischio
ACN, ministeri della Difesa e dell'Università, dipartimento del Tesoro del Mef e poi Campania, Veneto, Sardegna e altre PA che hanno presentato progetti per migliorare la propria sicurezza informatica: a loro andranno i fondi stanziati dal Governo per l'attuazione della Strategia nazionale cyber. Il punto
Il 4 settembre 2024 è stato **pubblicato in Gazzetta Ufficiale** il Decreto del Presidente del Consiglio dei ministri 8 luglio 2024 per l'**assegnazione alla Pubblica Amministrazione** delle risorse contenute nel **Fondo per l'attuazione della Strategia nazionale di cybersicurezza** e nel **Fondo per la gestione della cybersicurezza** per un totale di **347,6 milioni di euro per il triennio 2023-2026**.
Questi fondi erano stati **istituiti** nello stato di previsione del Ministero dell'economia e finanze (MEF) con la Legge di Bilancio n.197/2022, articolo 1, comma 899, lettere a) e b).
Le dotazioni previste per il Fondo per l'attuazione della Strategia nazionale di cybersicurezza erano di 70 milioni di euro per il 2023, di 90 milioni di euro per il 2024, di 110 milioni di euro per il 2025 e di 150 milioni di euro dal 2026 fino al 2037; mentre, per il Fondo per la gestione della cybersicurezza era stato previsa una dotazione di 10 milioni di euro per il 2023, di 50 milioni di euro per il 2024 e di 70 milioni di euro annui a partire dal 2025.
Indice degli argomenti
- **Fondi cyber per la PA: come sono ripartiti**
- **Le risorse per le PA a maggior rischio cyber**
- **Obiettivo: migliorare la sicurezza cyber del Paese**

Fondi cyber per la PA: come sono ripartiti
Con il DPCM 8 luglio 2024 sono stati prelevati dal Fondo per l'attuazione della strategia nazionale di cybersicurezza 37,8 milioni di euro per il 2024: una gran parte sono stati assegnati al MEF, a cui sono stati stanziati 7,66 milioni di euro per il Dipartimento del Tesoro e 3,55 milioni di euro per il Dipartimento dell'Amministrazione generale, del Personale e dei Servizi, seguono l'Agenzia per la Cybersicurezza Nazionale (ACN) con 4,35 milioni di euro, l'Istituzione nazionale Assicurazione Infortuni sul Lavoro con 2,11 milioni di euro e le Regioni Campania e Sardegna con 2 milioni a testa.
Confrontando il totale assegnato, 37,8 milioni di euro, con le previsioni di stanziamento per il 2024, 90 milioni di euro, si nota una differenza importante, la quale però non tiene conto dei 44,5 milioni di euro residui dell'ACN dal 2023, facendo salire ipoteticamente la cifra a 84,3 milioni di euro.
La regia della Strategia nazionale di cybersicurezza, si ricorda, è in capo all'ACN che ne cura l'indirizzo, il coordinamento e il monitoraggio del piano attuativo, come stabilito dall'articolo 3 del DPCM 8 luglio 2024, dunque, supervisiona anche la programmazione delle risorse ricevute dalle PA. (continua..)
https://www.cybersecurity360.it/cybersecurity-nazionale/cyber-nella-pa-cosi-i-nuovi-fondi-da-347-milioni-rafforzano-le-amministrazioni-piu-a-rischio/
Cybersecurity360 - *Luisa Franchina, Corrado Fulgenzi -11 set 2024*

Arrivati i modelli o1 e o1-mini OpenAI di intelligenza artificiale disegnati per "ragionare" - Una prova per cogliere la portata di questo passo avanti e le implicazioni

I **modelli o1 e o1-mini di OpenAI** sono i primi **di intelligenza artificiale disegnati per "ragionare".** Adesso è il momento di comprendere cosa farci e le implicazioni per tutti noi.

Cominciamo da una **prova** approfondita di questi modelli a lungo attesi – da tempo si parlava di un progetto OpenAi nome in codice era *Strawberry*.

Il modello è disponibile per ora in anteprima agli utenti del servizio plus di **ChatGpt**.

Coding with OpenAI o1

Indice degli argomenti

O1 e o1-mini ragionano? Un esempio

Cosa vuol dire che questi nuovi modelli "ragionano"? Prima di cercare di capire i contenuti dell'annuncio proviamo a capire cosa vuol dire che il modello pensi ponendo un semplice problema e osservando come si comporta o1. **Poniamo il seguente problema al modello O1:**

"Siamo a cena in 13 ma sono 2 famiglie solo con un figlio e una mamma e una figlia e il resto sono coppie senza figli. Non volendo far pagare i figli se il conto totale è 1300 euro quanto deve spendere ciascuna famiglia?"

La risposta ha richiesto 28 secondi, e durante l'elaborazione l'interfaccia mostra i passi intermedi del ragionamento come mostrato nella seguente figura (in cui non sono riportati tutti) (continua..):

https://www.agendadigitale.eu/industry-4-0/openai-01-e-01-mini-ora-lai-ragiona-vediamo-come/

AGENDADIGITALE - *Antonio Cisternino - 16 set 2024*

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

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/*

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 *ai quali potete inviare suggerimenti e quesiti scrivendo 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

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.