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 2023	n. 4/ 2023	Aprile 2023

Alla scoperta dell'intelligenza artificiale ChatGPT

Negli ultimi tempi si è parlato molto dell'utilizzo di applicativi basati sull'intelligenza artificiale; tra questi il più famoso è ChatGPT. La piattaforma è basata su un modello di linguaggio naturale sviluppato da OpenAI, una delle più grandi e prestigiose organizzazioni di ricerca nel campo dell'intelligenza artificiale.
Il nome della piattaforma, ChatGPT, è l'acronimo di "Chat Generative Pre-trained Transformer", a significare, appunto, la sua funzione principale: generare conversazioni intelligenti con gli utenti.
Il modello di ChatGPT è stato sviluppato utilizzando un tipo di rete neurale chiamato "Transformers", il quale è stato introdotto per la prima volta da Google nel 2017. Questa rete neurale è stata progettata per gestire sequenze di dati di lunghezza variabile, come parole e frasi, e può essere addestrata su grandi quantità di testo per generare testo coerente e comprensibile.
ChatGPT è stato addestrato su una vasta quantità di testo proveniente da fonti come Wikipedia, libri, articoli, notizie e altro ancora. Ciò significa che il modello ha una conoscenza molto vasta e diversificata, consentendogli di fornire risposte accurate e pertinenti su una vasta gamma di argomenti. Un'altra peculiarità di ChatGPT è l'apprendimento continuo durante le conversazioni con gli utenti, migliorando costantemente la sua capacità di comprendere il linguaggio naturale e fornire risposte pertinenti. La piattaforma è stata utilizzata in molti contesti diversi, come ad esempio per fornire supporto ai clienti, per creare chatbot per il servizio clienti, per fornire informazioni su prodotti e servizi e molto altro ancora.
Uno degli aspetti più interessanti di ChatGPT è la sua capacità di generare testo in modo creativo. Ad esempio, è stato utilizzato per generare testo poetico, racconti brevi e persino musica. Ciò dimostra la sua flessibilità e la sua capacità di apprendere e adattarsi a diversi contesti; tuttavia, come qualsiasi altra tecnologia, ChatGPT solleva anche alcune preoccupazioni. Ad esempio, alcune persone temono che la tecnologia possa essere utilizzata per generare contenuti falsi o fuorvianti, altri si preoccupano che ChatGPT possa essere utilizzato per sostituire lavori che richiedono l'interazione umana, come quelli nel settore dei servizi clienti e altri ancora pongono l'attenzione sulla privacy.
Proprio a tal proposito recentemente il Garante per la Privacy ha predisposto un provvedimento con effetto immediato per limitare provvisoriamente il trattamento dei dati degli utenti italiani nei confronti di OpenAI. Nel provvedimento, in sintesi, il Garante ha rilevato una serie di violazioni riguardanti gli artt. 5, 6, 8, 13 e 25 del GDPR, ma, soprattutto, l'assenza di una spiegazione volta a rispondere all'esigenza della società statunitense di raccogliere dati personali al fine di migliorare il servizio.
Nel dettaglio, ciò che contesta il Garante riguarda la mancanza di un'appropriata informativa che motivi la raccolta e la conservazione massiva di dati personali. Inoltre, il servizio non prevede un filtro per la verifica dell'età dell'utente, pertanto, l'IA può generare risposte dai contenuti non adatti a un pubblico di età inferiore a 13 anni.

Ad oggi, il Garante per la Privacy risulta la prima autorità al mondo a contestare il modus operandi della società OpenAI; questa iniziativa ha aperto un dibattito all'interno dell'Unione Europea e, pertanto, a fine aprile tutte le autorità in ambito privacy del Vecchio Continenti si riuniranno per discutere la questione. In attesa delle istituzioni, è importante osservare il comportamento della startup statunitense per comprendere le modalità con quali deciderà di affrontare la tematica.

Gianluca Cipriani Ha conseguito la laurea in "Scienze Politiche" presso l'Università degli Studi "Roma Tre" e si è specializzato in "Relazioni Internazionali" presso l'Università degli Studi "Roma Tre" con un percorso incentrato sulla strategia militare e sicurezza internazionale. Dopo anni di esperienza come analista di geopolitica, attualmente svolge attività di consulenza in materia di cybersecurity.

Andrea Agostino Fumagalli Laureato in "Giurisprudenza" presso l'Università degli Studi di Milano con tesi in Informatica Giuridica Avanzata, ha maturato diverse esperienze lavorative nell'ambito legale e di compliance, occupandosi di sicurezza delle informazioni. Attualmente svolge attività di consulenza in materia di cybersecurity.

ATTIVITA' DELL'ASSOCIAZIONE

ATTIVITA' DI EDUCATION

Sono riprese le attività di formazione per soci e simpatizzanti che si svolgeranno nell'anno 2023.

L'accordo con IsacaRoma consente ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Stiamo valutando le modalità di svolgimento di altri eventi possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, come avrete notato, abbiamo ripreso le visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

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

RINNOVO ASSOCIATIVO ANNO 2023

Il 31 dicembre 2022 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La partecipazione associativa inalterata da anni, pari ad euro 40, con delibera del Consiglio Direttivo del 19.9.2022 è stata aumentata di una modesta quota pari ad euro 10 per l'aumento generale dei costi di gestione.
La nuova quota per il rinnovo individuale è quindi adesso 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 2023".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2023. 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.**

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*

NEWS E AVVENIMENTI

Cos'è la solastalgia (e in che modo il cambiamento climatico sta compromettendo la nostra salute mentale)
Le modificazioni del territorio possono indurre la popolazione a sviluppare un profondo senso di perdita e distacco dall'ambiente conosciuto che va sotto il nome di solastalgia.
Il termine è nuovo, ma sta divenendo di uso comune e nel rapporto dell'Organizzazione Mondiale della Sanità è stato introdotto tra gli effetti psicologici del cambiamento climatico. La parola **solastalgia** indica la perdita del conforto del proprio territorio, della riconoscibilità della propria "casa" naturale, quando ci si rende conto che sta inevitabilmente cambiando e che non è più la stessa, né lo sarà mai più.
***GQ** - Marco Perisse –– 20 luglio 2021*

Fire Safety of Buildings and Energy Performance - The position adopted by the European Parliament's Committee on Industry, Research and Energy (ITRE) on the revision of the Energy Performance of Buildings Directive (EPBD) after long and difficult negotiations is welcomed by Euralarm: "The compromise amendments contain significant changes and Euralarm especially welcomes recommendations to better address fire safety of buildings", they say from the Association.
Changes in fire safety and security requirements are required

In fact, better performing buildings also means safer and more secure buildings. Every year, EU countries experience major fires in residential, commercial, and industrial buildings, taking lives of thousands of European citizens and creating considerable environmental damage. "This can be avoided with the deployment of integrated fire safety and security technologie", they add.
Better performing buildings implies new technologies, such as Battery Energy Storage Systems, that can increase fire risk. "Therefore, significant changes in fire safety and security requirements are required. They must be carefully evaluated by qualified people and companies", they underline.
Euralarm on Fire Safety of Buildings and Energy Performance
"Beyond the recommendations proposed by the ITRE Committee, we call on EU decision makers and Member States to create incentives for all renovated buildings to be fitted with the latest technologies in terms of fire safety and security.
The European Parliament will vote on the draft position during the 13-16 March plenary meeting, sealing the EP position for the following trialogue negotiations.
Euralarm has full confidence in the European political institutions to take the right decisions which will strengthen the cohesion of the European Union, revive our economy, and ensure for all citizens a sustainable future, be it in terms of environment, energy, use of natural resources as well as safety and security ", they end.
https://www.snewsonline.com/en/fire-safety-buildings-energy-performance/
SNews *–Editorial Staff - 14 March 2023*

Prefettura Trapani: più videosorveglianza per sicurezza territorio - La prefettura di Trapani ha valutato positivamente alcuni progetti per la realizzazione di sistemi di videosorveglianza presentati dai comuni di Marsala, Valderice, Paceco, Calatafimi Segesta, Campobello di Mazara, Salaparuta e dell'Unione dei comuni Elimo Ericini.
"I progetti – sottolineano dal Ministero dell'Interno – concorreranno alla procedura per l'assegnazione di specifici finanziamenti con fondi statali indetta dal Ministero stesso, in collaborazione con il Ministero dell'Economia e delle Finanze. Verranno inviati ai competenti uffici del ministero dell'Interno che valuteranno la loro finanziabilità mediante un'apposita commissione. Quest'ultima stilerà una graduatoria nazionale tra quelli presentati e verranno finanziati fino a concorrenza della disponibilità delle risorse finanziarie fissate in 36 milioni di euro per l'anno 2022".
Il prefetto Filippina Cocuzza ha espresso la sua soddisfazione nei confronti dei comuni che si sono attivati allo scopo di potenziare il sistema di controllo del territorio anche per prevenire e contrastare fenomeni di criminalità diffusa e predatoria. (continua…)
https://www.snewsonline.com/prefettura-trapani-videosorveglianza-sicurezza-territorio/
SNews *– Redazione, 16 Marzo 2023*

Cos'è il sistema SARI? - Già da qualche anno è in funzione un sistema automatico di riconoscimento facciale, del quale poco si sa e sul quale molti esperti, compresa l'autorità Garante per la protezione dei dati personali, hanno avanzato perplessità. Di che si tratta?
Il sistema SARI (sistema automatico di riconoscimento immagini) è stato attivato in Italia nel 2018. In realtà, non ci troviamo davanti ad un solo applicativo, ma a due ben diversi applicativi, contrassegnati dai codici: ***SARI Enterprise*** e ***SARI Real Time***.
Il primo sistema è stato attivato dalla metà del 2018, in Italia, e viene utilizzato per attività di contrasto al terrorismo e identificazione di soggetti sospetti.

Si tratta di un sistema di riconoscimento facciale, sviluppato da un'azienda privata, che permette di confrontare le immagini riprese dai sistemi di videosorveglianza con immagini contenute nella ormai famosa banca data AFIS (automatic fingerprint identification system). Questa banca dati, per la prima volta messa a punto degli Stati Uniti, permette di effettuare il confronto automatico fra un'impronta digitale, acquisita ad esempio sulla scena di un crimine, e l'archivio delle impronte digitali già memorizzate presso le forze di polizia.
Credo che nessun lettore, che abbia visto qualche episodio della serie televisiva CSI, non sia già a conoscenza di questo archivio.
Quando viene costruita la scheda delle impronte digitali di un soggetto, si inseriscono anche le fotografie del soggetto stesso, se disponibili.
Queste fotografie, in particolare, sono conservate nel casellario centrale d'identità della polizia criminale, con sede all'Eur, quasi dirimpetto al grattacielo dell'Eni. Non sono disponibili dati accurati sul numero di schede già archiviate, ma si parla di numeri compresi fra 10 e 15 milioni di immagini.
La differenza fondamentale fra i due sistemi SARI sopraelencati sta nel fatto che SARI Enterprise, che è nato per primo, è stato già sottoposto ad un'analisi da parte della Garante per la protezione dei dati personali, per verificare il rispetto di tale applicativo, nei confronti delle disposizioni del GDPR.
In pratica, il sistema SARI Enterprise allevia il carico di lavoro dell'operatore, senza introdurre operazioni supplementari, potenzialmente in grado di violare le disposizioni in materia di dati personali.
Ben diversa invece la situazione del secondo applicativo: SARI Real Time.
Quest'ultimo è stato sottoposto ad un'attenta valutazione da parte dell'autorità Garante per la protezione dei dati personali, che ha avanzato numerose perplessità, ben evidenziate nel documento seguente:
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9575877
In questo caso, l'applicativo effettua un confronto in tempo reale fra immagini, catturate da impianti di videosorveglianza, e l'archivio dati del ministero degli interni.
È proprio questo applicativo che ha permesso, analizzando le immagini, che gli impianti videosorveglianza dalla stazione Termini avevano catturato, con riferimento all'aggressore della turista israeliana, di reperire una corrispondenza, che ha portato alla diffusione della fotografia del sospetto e al suo successivo arresto alla stazione centrale di Milano. (continua…)
https://www.puntosicuro.it/security-C-125/cos-il-sistema-sari-AR-23158/
PuntoSicuro *- Adalberto Biasiotti, 22/03/2023*

Come la biometria può ridurre le code ai varchi di sicurezza aeroportuali - La ripresa del traffico aereo ha messo in difficoltà i servizi di terra che non dispongono di sufficiente personale per effettuare rapidamente i controlli di sicurezza. L'utilizzo di tecnologie biometriche può offrire una soluzione soddisfacente?
Nel giugno del 2022, i passeggeri impiegavano circa quattro ore per attraversare i varchi di sicurezza dell'aeroporto di Düsseldorf. All'aeroporto di Amsterdam la situazione era ancora più drammatica, perché le code uscivano dall'area di accoglienza aeroportuale e i passeggeri venivano protetti da strutture a gazebo, che si estendevano per centinaia di metri.
Gli aeroporti di Heathrow e Gatwick hanno addirittura richiesto alle compagnie aeree di ridurre il numero di voli, perché si dichiaravano incapaci di gestire il normale flusso dei viaggiatori.
A fronte di questa situazione drammatica, sembra che solo sistemi biometrici, che controllano il passeggero dal checkin fino all'imbarco, possano dare una risposta soddisfacente. Non per nulla, il 73% dei passeggeri, recentemente intervistati, ha dichiarato di non aver alcuna remora all'utilizzo dei propri

dati biometrici, a condizione che questo utilizzo possa ridurre in maniera significativa le attese agli imbarchi.
Vediamo come le tecnologie oggi disponibili possono essere usate per rendere più gradevole il viaggio, senza nulla sacrificare alla sicurezza dei controlli.
Se il passaporto non dispone già di informazioni biometriche, esistono oggi delle attrezzature al check in, in cui viene catturata una immagine del volto del passeggero e viene confrontata in tempo reale con la fotografia presente sul documento di identità. La stessa attrezzatura può essere utilizzata anche l'accesso alle aree di consegna dei bagagli, per la spedizione a destino. Il confronto tra il volto catturato da una telecamera e la fotografia sul documento identità permette una gestione rapida e sicura dei bagagli.
Il passeggero a questo punto deve attraversare i controlli di sicurezza, con rivelatori di metalli e apparato radiogeno, laddove non è richiesta l'esibizione di un documento identità. Tuttavia, qualora i rivelatori segnalino situazioni sospette, le guardie addette al controllo possono effettuare accertamenti approfonditi e acquisire i dati del passeggero.
Infine, il passeggero deve presentarsi al punto di imbarco, dove ancora una volta viene controllata la sua identità, con la tecnica già prima illustrata. Numerosi esperimenti, effettuati a cura della Transport Security Adminstration, negli Stati Uniti, hanno dimostrato come il livello di efficienza ed efficacia del controllo, effettuato tramite apparecchiature biometriche automatiche, sia nettamente migliore, rispetto al controllo visivo, che ancora oggi rappresenta la forma dominante di controllo ai punti di imbarco.
Al proposito, è comunque necessario sottolineare come l'acquisizione dei dati biometrici deve avvenire in un contesto di elevatissima sicurezza, non solo per rispondere alle indicazioni del regolamento generale europeo per la protezione dei dati, ma anche per rassicurare il passeggero che i suoi dati personali verranno utilizzati esclusivamente ai fini di accelerare i transiti attraverso i varchi di sicurezza (continua…).
https://www.puntosicuro.it/security-C-125/come-la-biometria-puo-ridurre-le-code-ai-varchi-di-sicurezza-aeroportuali-AR-23183/
PuntoSicuro *- Adalberto Biasiotti, 24/03/2023*

Digitalizzazione delle linee guida ponti: nasce il BMS INBEE - Lo sviluppo di BMS (Bridge Management System) consente di ordinare le infrastrutture, di archiviare le informazioni ad esse relative e di elaborarle. INBEE è la piattaforma open e gratuita, con App Mobile, che agevola la valutazione di ponti e viadotti e permette una gestione smart del patrimonio.
Verrà creata anche una banca dati digitale di tutti i ponti e viadotti italiani
Le "Linee Guida per la classificazione e gestione del rischio, la valutazione della sicurezza ed il monitoraggio dei ponti esistenti" impongono la graduale transizione verso una gestione digitale del ciclo di vita delle infrastrutture.
In più punti, infatti, le Linee Guida impongono "l'adozione progressiva di modelli informativi dell'infrastruttura, ovvero l'insieme di contenitori di informazione strutturata e non strutturata […] che consentono una gestione efficace e trasparente del cespite attraverso l'utilizzo di ambienti di condivisione dati e piattaforme interoperabili dei dati" anche al fine di creare "progressivamente una banca dati digitale aperta di tutti i ponti e viadotti, da rendere disponibile ai competenti uffici del Ministero delle infrastrutture e dei Trasporti" (Linee Guida, §1.6 - MODELLI INFORMATIVI).
Il processo di digitalizzazione del patrimonio infrastrutturale italiano, oggi in atto, si snoda attraverso una scelta graduale di modelli informativi da parte di tutti gli Enti Gestori. Un esempio sono i BMS (Bridge Management System), che rivestono un ruolo fondamentale, in quanto sono software che

permettono di creare un inventario delle opere, di archiviare in modo accurato grandi quantità di dati e la loro istantanea elaborazione, con lo scopo di ottenere degli indicatori che possano supportare l'Ente Gestore nelle decisioni che riguardano le strategie per la sorveglianza delle infrastrutture.
(*continua*).
https://www.ingenio-web.it/articoli/digitalizzazione-delle-linee-guida-ponti-nasce-il-bms-inbee/
Ingenio *- INBEE SRL- 24/3/2023*

Intelligenza artificiale, deciso impatto sull'economia mondiale

L'aumento della produttività del lavoro, legato all'adozione dell'**intelligenza artificiale**, porterà da qui ai prossimi 10 anni, secondo Goldman Sachs, a un aumento del Pil globale annuo del 7%. Secondo questa Agenzia questo risultato sarà la conseguenza dei risparmi sul costo del lavoro, la possibilità di creare nuovi sbocchi occupazionali e l'aumento della produttività per i lavoratori. Le uniche incertezze, sempre secondo questo studio, sono quelle che sono legate alle tempistiche per arrivare al perfezionamento dello scenario.
https://www.esg360.it/report-analisi-e-ricerche/intelligenza-artificiale-impatto-da-7-trilioni-di-dollari-sulleconomia-mondiale/
ESG 360 *– Report – 30 marzo 2023*

Come Cina e Russia provano a sfidare il dominio del dollaro

La Russia e la Cina stanno suscitando nuovi timori a Washington. Ciò è conseguenza soprattutto delle loro esibizioni di unitarietà operativa.
In particolare, durante la recente visita di Xi Jinping a Mosca, Vladimir Putin si è impegnato ad adottare il renminbi, al posto del dollaro, per i pagamenti tra la Russia e i Paesi dell'Asia, dell'Africa e dell'America Latina.
Ciò è dovuto principalmente alle loro ostentazioni di unità diplomatica, amministrate in modo scenografico, intorno e non solo all'Ucraina.
Ma è anche una questione di soldi: durante la visita di Xi Jinping a Mosca la scorsa settimana, Vladimir Putin si è impegnato ad adottare il renminbi per "i pagamenti tra la Russia e i Paesi dell'Asia, dell'Africa e dell'America Latina", nel tentativo di sostituire il dollaro.
Questo avviene mentre Mosca sta già utilizzando sempre più il renminbi per i suoi crescenti scambi commerciali con la Cina e lo sta adottando nelle sue riserve della banca centrale, per ridurre la sua esposizione agli asset "tossici" americani.
https://www.startmag.it/mondo/cina-russia-contrasto-dollaro/?ct=t(RSS_EMAIL_CAMPAIGN)
Start Magazine *– Redazione - 1° aprile 2023*

The FDA's Medical Device Cybersecurity Overhaul Has Real Teeth, Experts Say

The physical and cyber safety issues surrounding medical devices like IV pumps is finally being meaningfully addressed by a new policy taking effect this week.
The Food and Drug Administration (FDA) this week put into effect fresh guidance concerning the cybersecurity of medical devices — long a concerning area of risk for healthcare organizations and patients alike. The policy is one in a long line of attempts by the FDA to put some guardrails around the susceptibility of things like insulin pumps and heart monitors to hacking, and experts say that this time, the FDA's move might actually make a difference.

Effective immediately, medical device manufacturers are advised to submit "a plan to monitor, identify, and address, as appropriate, in a reasonable time, postmarket cybersecurity vulnerabilities, and exploits."
Manufacturers are also asked to "design, develop, and maintain processes and procedures to provide a reasonable assurance that the device and related systems are cybersecure." This includes making patches available "on a reasonably justified regular cycle," and for newfound critical vulnerabilities, "as soon as possible out of cycle."
And finally, the FDA is asking that new devices come prepared with a software bill of materials (SBOM).
For some, FDA guidance may evoke memories of prior actions that failed to improve cybersecurity in this critical area in any real way. But experts say this long road has finally reached a real, genuine inflection point. Starting now, new medical devices that don't meet these standards will be blocked from the market.
"It's actually been a process that's taken place over approximately the last 10 years," says Cybellum CMO David Leichner. "And it came to fruition two days ago."

Medical Devices in Cyber-Crisis

Medical device security has been an alarmingly lagging area for cybersecurity for a very long time, and there's a laundry list of reasons why. Healthcare facilities often use legacy IT and have flat networks that aren't segmented, for instance — even as medical devices for patients are increasingly connected. And security by design isn't common. (continua…)
https://www.darkreading.com/cloud/the-fda-medical-device-cybersecurity-overhaul-real-teeth
DARKREADING - *Nate Nelson- March 31, 2023*

CISA has added nine flaws to its Known Exploited Vulnerabilities catalog, including bugs exploited by commercial spyware on mobile devices.

U.S. Cybersecurity and Infrastructure Security Agency (CISA) has added nine new vulnerabilities to its Known Exploited Vulnerabilities Catalog.
Five of the issues added by CISA to its catalog are part of the exploits used by surveillance vendors to target mobile devices with their commercial spyware:

- CVE-2021-30900 – Apple iOS, iPadOS, and macOS Out-of-Bounds Write Vulnerability.
- CVE-2022-38181 – Arm Mali GPU Kernel Driver Use-After-Free Vulnerability
- CVE-2023-0266 – Linux Kernel Use-After-Free Vulnerability
- CVE-2022-3038 – Google Chrome Use-After-Free Vulnerability
- CVE-2022-22706 – Arm Mali GPU Kernel Driver Unspecified Vulnerability

The decision to add the flaws to the catalog is the response of the agency to a **recent report** published by Google's Threat Analysis Group (TAG) that shared details about two distinct campaigns which used several zero-day exploits against Android, iOS and Chrome. The experts pointed out that both campaigns were limited and highly targeted. The threat actors behind the attacks used both zero-day and n-day exploits in their exploits.
The exploits were used to install commercial spyware and malicious apps on targets' devices. (continua…)
https://securityaffairs.com/144315/breaking-news/cisa-known-exploited-vulnerabilities-catalog-spyware-bugs.html
Securityaffairs*- Pierluigi Paganini- April 1, 2023*

Pizzetti, ChatGpt: senza diritti siamo nudi davanti all'intelligenza artificiale - In ChatGpt di OpenAI manca una adeguata informazione che renda agevole agli interessati far valere i loro diritti, a cominciare da un uso consapevole e responsabile della chat. Ma così non possiamo tutelare le nostre identità e relazioni, che sono sempre più basati sui dati. Il provvedimento del Garante anticipa un'epoca

In data 30 marzo 2023 il Presidente della Autorità italiana garante dei dati personali, avvalendosi dei **poteri d'urgenza** previsti dall'art.5.comma 8 del Regolamento 1/200058 e di quanto disposto dall'art.58 par. 2, lettera f) del **GDPR**, ha adottato un provvedimento di urgenza nei confronti della società OpenAi quale società sviluppatrice e gestrice di **ChatGPT**, col quale ha disposto con effetto immediato la limitazione provvisoria del trattamento di dati di utenti italiani.

Indice degli argomenti

I motivi di un provvedimento d'urgenza, ancora da ratificare

Il provvedimento è conseguente all'allarme scattato in seguito alla pubblicazione di dati sensibili degli utenti avvenuto a causa di un bug contenuto in una libreria open source usata da OpenAi per il servizio di **ChatGPT**.

Il provvedimento, che dovrà essere ratificato dal Collegio nella prima seduta utile, sembra basarsi su due motivi diversi:

- il primo riguarda la assenza di una adeguata informativa sui trattamenti dei dati personali degli interessati, come dimostrerebbe il fatto che le informazioni fornite da ChatGPT "non sempre corrispondono al dato reale";
- il secondo attiene invece al fatto che nel sistema CHARGPT manca la previsione di "qualsivoglia verifica dell'età degli utenti dei servizi forniti da ChatGPT" malgrado che i termini di uso del servizio specifichino che esso "è riservato a soggetti che abbiano compiuto almeno 13 anni".

In base a questi due motivi, il primo dei quali solo affermato ma non chiaramente motivato stante la urgenza del provvedimento che non ha consentito, si direbbe, una istruttoria adeguata, il Presidente del Garante, avvalendosi appunto dei suoi poteri di urgenza, ha imposto "la limitazione dei trattamenti dei dati personali degli interessati stabiliti sul territorio italiano". (continua…)

https://www.agendadigitale.eu/sicurezza/privacy/pizzetti-chatgpt-senza-diritti-siamo-nudi-davanti-allintelligenza-artificiale/

***Agenda Digitale**- Franco Pizzetti-03 Apr 2023*

L'IA generativa farà bene a professionisti e pmi? Entusiasti contro cauti - L'IA generativa ha portato la tecnologia direttamente nelle mani di privati e piccole imprese, che la usano per automatizzare compiti faticosi o per velocizzare i processi creativi. Tuttavia, gli esperti mettono in guardia sull'uso di queste tecnologie, consigliando di utilizzarle solo per supportare chi è già esperto

L'avvento dell'intelligenza artificiale (IA) generativa ha rivoluzionato il modo in cui le persone lavorano in diversi settori, dal CEO al programmatore. Da quando OpenAI ha rilasciato **ChatGPT** nel novembre del 2021, molti hanno sperimentato la nuova tecnologia per accelerare i compiti o evitare di rimanere indietro rispetto alla concorrenza.

Indice degli argomenti

L'IA generativa nelle "mani" di privati e piccole imprese: gli sviluppi

Uno dei primi a adottare questa nuova tecnologia è stato **Jeff Maggioncalda**, CEO dell'azienda di formazione online **Coursera** Inc., che ha deciso di testare ChatGPT per vedere se potesse risparmiare tempo. Ha iniziato ad utilizzare il chatbot per scrivere lettere e **note aziendali**, e ha chiesto alla sua assistente esecutiva di fare lo stesso per le risposte alle e-mail in arrivo. Lei suggerisce a ChatGPT come pensa che Maggioncalda risponderebbe, e lui modifica le risposte generate prima di inviarle. "Trascorro molto più tempo a pensare e molto meno tempo a scrivere", ha dichiarato Maggioncalda. "Non voglio essere l'unico a non usarlo, perché chi lo usa avrà molti vantaggi". (continua…)

https://www.agendadigitale.eu/industry-4-0/lia-generativa-nella-mani-di-privati-e-piccole-imprese-entusiasti-contro-cauti/

Agenda Digitale- *Maurizio Stochino - 04 Apr 2023*

Almost Half of Former Employees Say Their Passwords Still Work

It's not hacking if organizations fail to terminate password access after employees leave.

An alarming number of organizations are not properly offboarding employees when they leave, especially in regard to passwords.

In a March PasswordManager.com survey of 1,000 U.S. workers who had access to company passwords at their previous jobs, 47% admitted to using them after leaving the company.

Security teams should be terminating access to all employee accounts, such as email, cloud applications, and internal tools, after employees leave. For accounts or services where multiple employees share passwords, those passwords should be rotated to ensure that the former employees no longer have access.

According to the survey, 58% of respondents indicated they were still able to use their former company's passwords after they left. One in three respondents said they had been using the passwords for upwards of two years, which is a distressingly long time for organizations not to be aware of who is accessing those accounts and services.

"Ideally the company creates standard operating procedures or consistent schedules of updating passwords based on criticality," says Daniel Farber Huang, head of privacy and cybersecurity at PasswordManager.com. (continua…)

https://www.darkreading.com/edge-threat-monitor/almost-half-of-former-employees-say-their-passwords-still-work

Dark Reading *- Dark Reading Staff - April 07, 2023*

Israeli Irrigation Water Controllers & Postal Service Breached

Israel's National Cyber Defense is warning of increased cyberattacks by anti-Israel groups during the month of Ramadan.

On April 5, the Israel Post fell victim to a cyberattack, forcing the mail service to shut down some services. Just two days later, farmers missed scheduled irrigation times when water controllers in the Jordan Valley were hijacked with displays that read, "You Have been hacked, Down with Israel *(sic)*."

These recent cyberattacks are part of a predictable wave of increased, malicious cyber activity that Israeli organizations have come to expect during the month of Ramadan, according to the Israel National Cyber Directorate, which recently issued a warning about a spike in anti-Israel hacktivist activity.
"Each year during this period, attacks such as website defacement, distribution of phishing messages, social media hacking, DDoS attacks, intrusion into company websites, and information leaks are observed — alongside publications boasting cyberattacks that did not necessarily take place," the INCD warning said. "Additional, common attacks are on website storage and building companies, in an attempt to create a wider attack that will increase awareness. It is estimated that similar attempts will take place this year as well, using simple means and exploiting common weaknesses in the cyber sphere."(continua…)
https://www.darkreading.com/ics-ot/israeli-irrigation-water-controllers-postal-service-breached
Dark Reading *- Dark Reading Staff - April 11, 2023*

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.

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

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 Andrea Agostino Fumagalli *ai quali potete inviare suggerimenti e quesiti scrivendo a: segreteria@infrastrutturecritiche.it*