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. 10/ 2024** | **novembre 2024**

Quali sono i rischi di un sistema integrato di Intelligenza Artificiale in una struttura sanitaria?

L'implementazione di un sistema integrato di intelligenza artificiale (IA) in una struttura sanitaria offre molti benefici, ma comporta anche alcuni rischi significativi che devono essere considerati con attenzione. Tra i principali rischi vi sono quelli legati alla sicurezza dei dati, all'affidabilità dei sistemi, all'etica e all'impatto sulle relazioni medico-paziente. Analizziamo questi rischi in dettaglio.

- Sicurezza dei dati e privacy

Uno dei rischi principali riguarda la gestione dei dati "sensibili" dei pazienti. Le strutture sanitarie trattano enormi quantità di informazioni personali e cliniche che, se gestite da sistemi di IA, potrebbero diventare preda di attacchi informatici. Le violazioni dei dati possono portare a conseguenze gravi, tra cui furti di identità, uso improprio dei dati medici e compromissione della privacy dei pazienti.
Inoltre, l'integrazione tra più sistemi informatici che trattano dati di diversa natura (clinici, amministrativi e assicurativi) può aumentare il rischio di accesso non autorizzato o di perdita di informazioni critiche. Le strutture sanitarie devono implementare protocolli di sicurezza avanzati, come la crittografia, l'uso di blockchain o sistemi di autenticazione multifattoriale, per proteggere i dati da tali minacce.

- Affidabilità ed errori del sistema

Nonostante i sistemi di IA siano generalmente progettati per ridurre gli errori umani, possono comunque essere soggetti a malfunzionamenti o a errori sistemici. Gli algoritmi di IA possono basarsi su dati incompleti o non aggiornati, oppure fare inferenze errate a causa di errori e pregiudizi nei dati su cui sono stati addestrati. Questo può portare a diagnosi o raccomandazioni terapeutiche sbagliate, con conseguenze potenzialmente dannose per i pazienti.
Un rischio significativo è la cosiddetta "opacità algoritmica", dove le decisioni prese dall'IA sono difficili da interpretare anche per gli specialisti. Se un sistema di IA elabora una raccomandazione clinica senza fornire una spiegazione chiara e trasparente, può essere difficile per i medici valutare l'affidabilità del suggerimento, mettendo a rischio la salute del paziente.
Il problema della "black box", cioè l'impossibilità di "guardare dentro" il meccanismo di funzionamento del sistema, caratterizza proprio la opacità, con gradi diversi, di tutti i modelli algoritmici, in particolare dei sistemi di "deep learning".

- Discriminazioni

Gli algoritmi di IA si basano sui dati su cui vengono addestrati, e se questi dati sono influenzati da pregiudizi storici o culturali, il sistema di IA può tener conto di tali discriminazioni. Ad esempio, se un algoritmo è addestrato su dati che riflettono una disparità nel trattamento tra gruppi etnici o di genere, l'IA potrebbe suggerire trattamenti meno efficaci per determinate popolazioni.
Ciò è particolarmente preoccupante in ambito sanitario, dove decisioni scorrette e basate su pregiudizi potrebbero portare a disparità nell'accesso alle cure e nei risultati clinici. Assicurare che gli algoritmi siano equi e trasparenti è una sfida critica per ridurre questo rischio.

- Perdita del ruolo umano e impatto sul personale

L'automazione avanzata offerta dall'IA potrebbe ridurre la necessità di alcuni ruoli tradizionali all'interno delle strutture sanitarie, portando a una potenziale riduzione del personale. Questo può

causare timori tra i lavoratori e creare resistenze all'adozione della tecnologia. In particolare, c'è il rischio che la fiducia nelle capacità umane diminuisca man mano che le macchine diventano sempre più presenti nella gestione delle diagnosi e delle cure.
Inoltre, potrebbe risentirne anche il rapporto medico-paziente: l'IA, se utilizzata per decisioni diagnostiche o terapeutiche, potrebbe ridurre l'interazione umana, che invece è fondamentale per la comprensione empatica dei bisogni dei pazienti e per il sostegno psicologico durante il trattamento.

- Mancanza di standardizzazione e interoperabilità

Un altro rischio rilevante riguarda la mancanza di standardizzazione tra i vari sistemi di IA utilizzati nelle diverse strutture sanitarie. Se le piattaforme non sono interoperabili o non seguono standard comuni, l'integrazione dei dati tra diverse strutture o la condivisione di informazioni tra i vari sistemi sanitari diventa problematica. Questo potrebbe rallentare l'efficacia dei trattamenti, soprattutto in situazioni di emergenza, e creare barriere nell'adozione su larga scala della tecnologia.

- Dipendenza eccessiva dalla tecnologia

Un altro rischio riguarda l'eccessiva dipendenza dalla tecnologia. Se il personale medico si abitua a fare affidamento sui sistemi di IA per prendere decisioni cruciali, potrebbe perdere parte delle proprie capacità critiche e cliniche, riducendo l'autonomia decisionale in casi complessi: la fiducia cieca nella tecnologia può portare a un abbassamento della vigilanza, con possibili conseguenze disastrose in caso di errore tecnico o di situazioni inusuali non gestite dal sistema.

- Problemi etici

Infine, ci sono questioni etiche legate all'uso dell'IA in sanità. Chi è responsabile in caso di errore causato da un sistema di intelligenza artificiale? Se l'IA raccomanda un trattamento sbagliato, la responsabilità ricade sul medico che segue la raccomandazione, sulla struttura sanitaria che adotta il sistema, o sulla ditta che lo ha sviluppato? Questi dilemmi etici richiedono una regolamentazione chiara e rigorosa, così come l'istituzione di meccanismi per monitorare e valutare costantemente l'affidabilità e la sicurezza dei sistemi.

Conclusione

Un sistema integrato di intelligenza artificiale in una struttura sanitaria può portare grandi benefici, ma i rischi non devono essere sottovalutati. Problemi legati alla sicurezza dei dati, all'affidabilità, alle discriminazioni, alla perdita di competenze umane e alle questioni etiche devono essere affrontati con un monitoraggio attento e costante. Per mitigare questi rischi, è essenziale che i sistemi di IA siano progettati con trasparenza, siano soggetti a standard rigorosi e che il ruolo umano rimanga centrale, utilizzando l'IA come strumento di supporto piuttosto che come sostituto.

Silvano Bari
Docente di "Risk Management" presso l'Università Campus Bio-medico di Roma, è vicepresidente di AIIC

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 2025

Il 31 dicembre 2024 scadrà il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo 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 2025".
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.

Il Consiglio Direttivo di AIIC ha deciso una facilitazione per chi si iscriverà come nuovo socio: a partire dal mese di ottobre 2024, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2025.

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

Salvaguardia delle risorse idriche attraverso una gestione efficace, efficiente e sostenibile dei servizi idrici - Un'analisi approfondita sulla gestione sostenibile delle risorse idriche, con focus su strategie innovative per ridurre le perdite nella rete idrica, ottimizzare l'uso delle acque reflue e meteoriche, e migliorare l'efficienza idrica in vari settori.
L'acqua è una risorsa fondamentale per la vita, per la salute e per lo sviluppo economico insidiata dalla crisi idrica che coinvolge sempre più Paesi.
L'Italia, benché non sia tra le regioni a alto rischio, rientra comunque tra le zone sensibili: infatti, nonostante una disponibilità di acqua relativamente abbondante, sono in crescita le premesse di uno stato di elevati problemi idrici.
La distribuzione non omogena delle risorse idriche sul territorio, lo stato di degrado e di vetustà della rete idrica, le situazioni di gestione non sempre ottimale, i prelievi di acqua potabile per usi agricoli e industriali, sono alcuni dei fattori alla base della situazione di crisi idrica verso la quale sta andando l'Italia in relazione anche ai recenti cambiamenti climatici.
Queste sono alcune delle conclusioni che risaltano dal rapporto Istat presentato in occasione della Giornata mondiale dell'acqua. Questi argomenti rientrano anche tra i programmi del Piano Nazionale di Ripresa e Resilienza (PNRR).*(continua…)*
https://www.ingenio-web.it/articoli/salvaguardia-delle-risorse-idriche-attraverso-una-gestione-efficace-efficiente-e-sostenibile-dei-servizi-idrici/
Ingenio - *Vittorio Bruzzo, 17.10.2024*

Il futuro delle assicurazioni: polizze climatiche e piattaforme centrate sul cliente - La digitalizzazione sarà al centro del processo, ma serve un approccio olistico nei confronti dei consumatori. La maggiore frequenza e gravità dei disastri naturali richiede nuovi prodotti assicurativi. Gli esperti la chiamano la capacità di "vedere il rischio in modo diverso" e la identificano come uno degli assi portanti del pensiero innovativo. È un concetto che ritorna spesso quando si parla dell'evoluzione del mondo delle assicurazioni. Alla conferenza Exceedance di maggio in Canada, uno dei più grandi raduni di professionisti del settore, il tema principale era proprio questo: 'See risk differently". I

mercati, le incertezze geopolitiche, l'inflazione. E poi il cambiamento climatico, gli investimenti in tecnologia e le competenze per sfruttare l'intelligenza artificiale. C'è tutto questo a scandire il presente e il futuro delle assicurazioni.

Soluzioni personalizzate

L'era dei prodotti finanziari one size fits all ("taglia unica") è destinata a finire. Le ricerche mostrano che i consumatori richiedono soluzioni altamente personalizzate che si integrino nelle loro vite. Per questo la polizza assicurativa del futuro non si limiterà a garantire soltanto risarcimenti economici, ma dovrà prevedere e rispondere alle esigenze degli utenti. La tecnologia svolge un ruolo fondamentale nell'abilitare queste soluzioni su misura. Insurtech, un termine che combina "assicurazione" e "tecnologia", sta emergendo come una forza significativa per guidare l'innovazione nel settore. Un recente report di Klecha & Co., investment bank specializzata nei settori tech, prevede che l'Insurtech 2.0 arriverà a valere in Europa 200 miliardi di euro nel 2032, cinque volte più delle dimensioni attuali. In Italia, si contano oggi 65 startup Insurtech, 34 delle quali hanno ricevuto "capitali di rischio", o venture capital, investimenti per finanziare l'avvio o la crescita di un'attività in settori ad elevato potenziale di sviluppo, innovazione e attrattiva. Queste società stanno innovando il settore attraverso l'uso dell'intelligenza artificiale, che finora è stata utilizzata principalmente per la gestione dei sinistri e nei call center, ma ha potenzialità ben più ampie.*(continua)*

https://www.puntosicuro.it/sostenibilita-C-149/il-futuro-delle-assicurazioni-polizze-climatiche-piattaforme-centrate-sul-cliente-AR-24605/

Punto Sicuro - *Redazione, 22/10/2024*

Sicurezza e resilienza dei cavi sottomarini, anche l'Italia farà la sua parte: gli scenari - L'adesione dell'Italia al Comunicato congiunto di New York rappresenta un passo significativo nel rafforzamento della posizione strategica nel contesto delle infrastrutture critiche globali, dimostrando una capacità concreta del Paese di essere protagonista nella salvaguardia delle reti di comunicazione sottomarine

Cavi sottomarini obiettivo cyber Cina e Russia

L'adesione dell'Italia al "Comunicato congiunto di New York sulla sicurezza e la resilienza dei cavi sottomarini in un mondo globalmente digitalizzato" adottato in occasione della 79° Assemblea Generale delle Nazioni Unite, al termine della Riunione Ministeriale Tecnologia e Digitale del G7, consolida la propria posizione di Paese all'avanguardia sul tema dei cavi sottomarini.

L'obiettivo dell'accordo è il raggiungimento di elevati standard di sicurezza, affidabilità, interoperabilità e resilienza delle infrastrutture dei cavi sottomarini, sempre più cruciali all'interno dei rapporti internazionali tra Stati e, in particolar modo, di vitale importanza per il dominio cibernetico: i cavi sottomarini rappresentano il 95% del traffico dati a livello globale.

Indice degli argomenti

Cavi sottomarini: il comunicato congiunto di New York

Equilibri geopolitici e cooperazione internazionale

Un'interazione tra dominio subacqueo e cibernetico

Conclusioni (*continua…)*

https://www.cybersecurity360.it/cybersecurity-nazionale/sicurezza-e-resilienza-dei-cavi-sottomarini-anche-litalia-fara-la-sua-parte-gli-scenari/

Cybersecurity360 - *Luisa Franchina, Corrado Fulgenzi - 28 ott 2024*

Banche dati, che fare quando la minaccia è interna? Scrive Costanzo

Da quando è scoppiato il caso "dossieraggio" a Milano, con collegamenti anche su Roma, si parla erroneamente di "hackeraggio". Se vogliamo realmente discutere di una "cultura della sicurezza", è necessario usare i termini corretti. In questo caso, non si tratta di hackeraggio nel senso doloso del termine. Non c'è stata alcuna penetrazione esterna da parte di hacker. Qui si parla di una tipica operazione di insider, mossa da interessi economici o finalizzata a consolidare il potere di ricatto, accompagnata da una diffusa e sempreverde infedeltà nei confronti dello Stato.

Non credo serva istituire un'ulteriore agenzia o authority. Le strutture necessarie esistono già: usiamole in modo efficace.

Come la maggior parte dei professionisti e dipendenti di aziende private e pubbliche, utilizzo ogni giorno sistemi di videoconferenza, un'abitudine accelerata dall'emergenza pandemica che ha subito evidenziato le vulnerabilità di questi sistemi, introducendo anche nuovi termini come "zoombombing". Molti applicativi dispongono già di misure di sicurezza, ma il rischio di violazione dei dati è reale, come dimostra il passaggio dei sistemi dai server centrali ai portatili collegati alle reti domestiche. Numerosi applicativi includono la crittografia, ma garantire una protezione totale della sicurezza fisica delle reti resta arduo. Anche il comportamento degli utenti, infatti, è complesso da monitorare.

È quindi fondamentale introdurre procedure per la cancellazione dei dati quando non sono più necessari, sia per questioni di riesame che per eventuali audit. E se si tratta di documenti classificati, dovrebbero essere impenetrabili dall'esterno. Ma cosa accade se chi ha accesso dall'interno decide di vendere queste informazioni? (continua…)

https://formiche.net/2024/11/dossieraggio-fattore-umano-costanzo/#content

Formiche *- Biagino Costanzo - 01/11/2024*

Can Automatic Updates for Critical Infrastructure Be Trusted?

The true measure of our cybersecurity prowess lies in our capacity to endure.

In July, the industry witnessed one of the largest technology outages in recent history, with estimates of $5.4 billion in damages. When CrowdStrike distributed a Rapid Response Content Channel Update with an exception-handling logic flaw, it opened the door for constructive conversations about automatic updates — when to use them, when not to use them, whether they make us more or less secure. It's time to reflect and ask: What is the cost of our relentless pursuit of innovation, software currency, and speed to market? How can we reprioritize to reestablish the balance in the C-I-A triad?

IT and security teams are under enormous pressure to stay ahead of threats. However, teams must not sacrifice the right checks and balances for speed. The CrowdStrike incident serves as a reminder to the industry that even the most secure and trusted systems can fail, and it's time to revisit how teams test and deploy critical updates.

The C-I-A Triad: Rebalancing Priorities

The C-I-A triad is a foundational pillar of cybersecurity, representing the Confidentiality (security), Integrity (accuracy), and Availability of technology platforms. For too long, the cybersecurity community — vendors and customers alike — have fixated on the C in this triad. However, the C-I-A triad is supposed to represent the full scope of a cybersecurity program. With the main focus on privacy and data security, the industry over emphasized security — and in doing so, added speed to the equation. Teams are now responding faster and deploying updates quicker to stay ahead of emerging threats and day-to-day attacks, but that's leading to mistakes and improper testing.

Meanwhile, the I and A were relegated to secondary status — even outsourced to other technology teams. Integrity — the accuracy, completeness, and consistency of the ecosystem and underlying data — was compromised in the name of speed. Availability also suffered as the focus shifted to rapid recovery rather than ensuring uptime and reliability, all for the sake of rapid innovation and response to perceived threats.
If the CrowdStrike event has taught us anything, it is that now is the time for both vendors and customers to recommit themselves to recognizing the integral importance of and essential need to rebalance all three pillars of the C-I-A triad. In doing so, teams can build more resilient systems. (continua…)
https://www.darkreading.com/vulnerabilities-threats/can-automatic-updates-critical-infrastructure-be-trusted
***DARK READING** -John Paul Cunningham, - November 4, 2024*

Iranian APT Group Targets IP Cameras, Extends Attacks Beyond Israel
The Iran-linked group Emennet Pasargad aims to undermine public confidence in Israel and Western nations by using hack-and-leak campaigns and disrupting government services, including elections.
An Iranian cyber-operations group, Emennet Pasargad — also known as Cotton Sandstorm — has broadened its attacks, expanding its targets beyond Israel and the United States and targeting new IT assets, such as IP cameras.
In an advisory published last week, the US departments of Justice and Treasury — along with the Israel National Cyber Directorate (INCD) — called out the change in tactics and noted that the group had provided resources and infrastructure services to Middle Eastern threat groups by operating as a legitimate company, Aria Sepehr Ayandehsazan (ASA). In addition, since the beginning of the year, Emennet Pasargad has scanned for IP cameras, targeted organizations in France and Sweden, and actively probed a variety of election sites and systems, according to the government advisory.
"Similar to the Emennet campaign that targeted the 2020 U.S. Presidential election, the FBI judges the group's recent campaigns include a mix of computer intrusion activity and exaggerated or fictitious claims of access to victim networks or stolen data to enhance the psychological effects of their operations," the advisory stated.
The latest intelligence highlights Iran's increasing use of cyber operations as a way to target its perceived enemies. In 2020 and 2022, Emennet Pasargad created disinformation campaigns to target the US presidential and midterm elections, posing as Proud Boys volunteers and sending fake videos to Republican lawmakers. The US Department of Justice indicted two Iranian nationals for the crimes, as well as for sending threats through email and attempting to hack election websites. (continua…)
https://www.darkreading.com/vulnerabilities-threats/iranian-group-targets-ip-cameras-extends-attacks-beyond-israel
***DARK READING -** Robert Lemos - November 5, 2024*

Analyzing the supply chain risks behind the top data breaches in 2024
In 2024, cyberattacks targeting critical sectors like healthcare, telecommunications, and finance escalated dramatically in the first half of 2024, exposing vulnerabilities in sensitive content communications and the digital supply chain. We evaluated the top 11 data breaches in 1H 2024 using an AI-developed algorithm named the Risk Exposure Index (score 1 to 10 from lowest to highest risk), and found that supply chain cyber risks pose a serious challenge in many instances.
This article examines the major supply chain implications of these breaches and how they can inform cybersecurity strategies moving forward.

Change Healthcare: $17.9-billion wake-up call

The ransomware attack on Change Healthcare, which compromised 100 million records, was tied as the most severe breach of 1H 2024, with a Risk Exposure Index score of 9.46. The breach, which exposed sensitive health data, including medical and billing information, disrupted patient care across numerous facilities.

Supply chain impact:

- **Third-party risks:** As healthcare organizations outsource many IT services, third-party vendors often handle sensitive data. In Change Healthcare's case, the attack could have been exacerbated by a weak link in the digital supply chain. Healthcare systems frequently interact with external entities like insurance providers, diagnostic labs, and payment processors, increasing the risk of exposure if these third parties are not secured.
- **Operational continuity:** The attack's disruption of healthcare services shows that supply chain integrity is not just a data issue but a matter of operational continuity. When ransomware locks down systems, critical healthcare operations reliant on external suppliers or services can come to a halt.

National Public Data: 2.9 billion records compromised

Tied with the highest Risk Exposure Index score at 9.46, the data breach at National Public Data affected 2.9 billion records, exposing personally identifiable information (PII), including Social Security numbers. With a staggering financial impact of $501.7 billion, this incident underscores the immense value of sensitive data managed by data brokers.

Supply chain impact:

- **Data brokers as critical supply chain nodes:** National Public Data acts as a data broker that sells personal information to numerous industries, including fraud prevention services, banking, and retail. The sheer volume of records compromised reflects how interconnected data brokers are within the digital supply chain. A breach in such a node can cascade down the supply chain, affecting the security of thousands of businesses that depend on their data.
- **Regulatory scrutiny:** As data brokers are subject to regulations like the CCPA, HIPAA, and GDPR, a breach of this magnitude places every downstream company at risk of compliance violations. Companies relying on external data services must enforce strict third-party management protocols to mitigate cascading risks.

AT&T: Telecommunications on the edge

AT&T's two breaches, with a Risk Exposure Index score of 9.37, impacting 110 million customer records, exposed phone numbers, call records, and other aspects of PII. With an estimated financial impact of $19.7 billion, the incident attracted significant regulatory and reputational *back*lash. (continua…)

https://www.scmr.com/article/analyzing-the-supply-chain-risks-behind-the-top-data-breaches-in-2024/procurement

SMCR - *Tim Freestone - November 4, 2024*

AI e copyright: la partita si gioca su revenue sharing e equo compenso

Il caso Perplexity riaccende il dibattito sulla remunerazione dei contenuti usati per addestrare l'AI. Mentre i grandi editori negoziano accordi milionari, emerge la necessità di un sistema equo che tuteli anche i piccoli creator. La sfida è bilanciare innovazione e diritti d'autore

Le dispute legali che ruotano intorno all'addestramento dei modelli di intelligenza artificiale si sono arricchite di elementi che, soprattutto da un punto di vista strategico-processuale, permettono di effettuare alcune considerazioni sia in seno all'**utilizzo delle generazioni di tali modelli in campo**

aziendale, sia sugli equilibri generali che potranno, eventualmente, essere raggiunti, garantendo quella certezza sugli u**tilizzi capaci di fornire equilibrio e sostenibilità all'intero ecosistema digitale**.
Un assetto più certo consentirebbe non solo di ridurre i rischi legali, ma anche di favorire un approccio responsabile all'intelligenza artificiale, in cui le aziende possano investire con maggiore fiducia e i creatori di contenuti vedano riconosciuto il valore delle loro opere in modo equo e sostenibile.
Indice degli argomenti

Il caso emblematico di Perplexity
Un esempio rilevante in questa disputa riguarda il modello di AI Generativa creato da **Perplexity**, una delle aziende più discusse in questo momento, sia per la specificità di utilizzo che per la capacità, qui analizzata nei mesi scorsi, di **fornire fonti e contributi direttamente verificabili e con espliciti link di collegamento**.
Tale è stata la diffusione negli ultimi mesi del modello Perplexity che l'azienda, **come riportato dal *Wall Street Journal***, si è trovata, in un buona compagnia insieme ad OpenAI, al centro di un procedimento legale intentato dal *New York Post* per violazioni di copyright.
Perplexity ha la specificità di utilizzare l'intelligenza artificiale generativa per creare risposte alle *query* (domande poste attraverso *prompt*) degli utenti, posizionandosi come concorrente di Google nel campo dei motori di ricerca. Il fondatore Aravind Srinivas ha comunicato l'ambizioso obiettivo di raggiungere mezzo miliardo di *query* giornaliere entro il 2026.
Per comprendere la portata economica, oltre quella meramente tecnica, può essere utile sapere che la compagnia, sostenuta da Jeff Bezos e Nvidia, è in trattative per un finanziamento che potrebbe raddoppiare la sua valutazione a oltre 8 miliardi di dollari.
La startup ha un ricavo annualizzato stimato intorno ai 50 milioni di dollari.
Le proposte di Perplexity per risolvere le dispute
Nonostante questi numeri siano poco equivocabili, **Perplexity** ha dichiarato, attraverso i propri funzionari, di essere stata colta di "sorpresa" dal contenzioso poiché la società era aperta a una "conversazione commerciale appropriata."Come segno di apertura, l'azienda ha proposto un modello di *revenue-sharing*, suggerendo ai ricorrenti di partecipare alla suddivisione dei proventi generati dall'utilizzo dei contenuti.Da un punto di vista processuale, è chiaro che questo approccio non solo eviterebbe una lunga disputa giudiziaria, ma permetterebbe di stabilire una forma ulteriore di compenso per l'uso dei contenuti protetti. News Corp, proprietaria del *Wall Street Journal* e del *Post*, ha già stabilito un accordo di licenza con OpenAI per 250 milioni di dollari, della durata di cinque anni.
(continua…)
https://www.agendadigitale.eu/mercati-digitali/ai-e-copyright-la-partita-si-gioca-su-revenue-sharing-e-equo-compenso/
Agenda Digitale - *Alfredo Esposito - 7 nov 2024*

GitHub Spark, l'AI diventa multi-modello: perché è una svolta
Github ha recentemente annunciato **Github Spark**, un nuovo servizio per generare delle "micro app" con l'ausilio dell'**intelligenza artificiale**. L'annuncio colpisce non solo perché promette l'automazione

della generazione del codice, ma soprattutto perché supporta più modelli di **AI generativa** anche da parte di più vendor come **OpenAI** e Anthropic.
Questa capacità colpisce per almeno due ragioni: da una parte il software deve adattarsi a più intelligenze artificiali per funzionare, dall'altra **Microsoft introduce in uno dei suoi servizi modelli AI che non sono di OpenAI.**
Cerchiamo di capire **le sfide da affrontare nello sviluppo di software** capace di sfruttare più modelli di AI e le implicazioni che può avere per il futuro. La scelta di Microsoft di differenziare il supporto per i modelli AI può suggerire che quella sia la via da seguire.
Indice degli argomenti

GitHub Spark in breve
Il servizio sembra istituzionalizzare l'idea che sia possibile generare codice automaticamente che realizzi semplici funzioni applicative usando modelli AI, un po' come succede per gli artifact realizzati con **Claude**, tenendo però conto che GitHub vive di sviluppo e sviluppatori e promette quindi la generazione di veri e propri programmi usando l'AI.
Il servizio è per ora in technical preview ed è quindi presto per potersi formare delle opinioni proprie, ma dalle informazioni che si trovano sembra che se si ha bisogno di un'applicazione che svolga una funzione specifica, o di generare un semplice videogame arcade, il risultato sia decisamente buono e più curato di quanto possano essere gli artifacts di Anthropic. (continua…)
https://www.agendadigitale.eu/cultura-digitale/github-spark-lai-diventa-multi-modello-perche-e-una-svolta/
***AGENDA DIGITALE** - Antonio Cisternino - 7 nov 2024*

La Strategia Italiana per l'Intelligenza Artificiale 2024-2026 - Un documento che definisce uno sviluppo etico e inclusivo dell'IA, articolato in Ricerca, Pubblica Amministrazione, Imprese e Formazione, con azioni mirate a favorire innovazione e competitività nel contesto italiano. Cosa prevede questa strategia?
La Strategia Italiana per l'Intelligenza Artificiale 2024-2026 è stata sviluppata da un Comitato di esperti per aiutare il Governo nella regolamentazione e promozione dell'IA in Italia. Redatta da un team coordinato da Gianluigi Greco, professore di informatica e presidente di AIxIA, e composta da quattordici esperti tra cui Viviana Acquaviva e Maria Chiara Carrozza, la strategia mira a posizionare l'Italia come leader nella transizione tecnologica e nello sviluppo dell'IA, sfruttando anche il ruolo guida della presidenza italiana del G7.
Il documento propone un quadro di sviluppo etico e inclusivo, massimizzando i vantaggi dell'IA e riducendo i rischi. La strategia, che affronta il contesto globale e la posizione italiana nel settore, si articola in quattro aree principali: Ricerca, Pubblica Amministrazione, Imprese e Formazione. In ciascuna area, sono previste azioni mirate per supportare l'innovazione, favorire la competitività e incentivare l'adozione di soluzioni IA nella società e nell'economia italiane. *(continua…)*
https://www.puntosicuro.it/nuove-tecnologie-C-148/la-strategia-italiana-per-l-intelligenza-artificiale-2024-2026-AR-24822/

Punto Sicuro - *Redazione - 07/11/2024*

Mystery Hackers Target Texas Oilfield Supplier in Ransomware Attack

It remains unclear how the attackers gained access to Newpark Resources' system, or what they plan to do with any stolen data the strike may have spewed out.

Newpark Resources, a Texas-based oil drilling fluids system and composite matting systems provider, announced in a filing with the Securities and Exchange Commission (SEC) that it is dealing with the fallout of a ransomware attack it faced earlier this week.

The company has not shared details as to how the attackers gained access to its network, nor who the threat actors are or why they may have targeted Newpark. But after the breach was discovered, Newpark engaged its security response plan as expected and limited access to certain parts of its systems.

"The incident has caused disruptions and limitation of access to certain of the company's information systems and business applications supporting aspects of the company's operations and corporate functions, including financial and operating reporting systems," Newpark said.

According to Matt Hull, global head for Strategic Threat Intelligence at cybersecurity consultancy NCC Group, any data stolen from the critical infrastructure company has not yet appeared on any leak sites.

And because the company reverted to downtime procedures in response to the attack, it was able to continue manufacturing, and its field operations were uninterrupted. It hopes the attack will not have an effect on its financial conditions, it said. (continua…)

https://www.darkreading.com/cyberattacks-data-breaches/mystery-hackers-texas-oilfield-supplier-ransomware-attack

DARK READING - *Dark Reading Staff, - November 8, 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/*

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

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

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	Glauco Bertocchi Silvano Bari Alberto Traballesi *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.