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. 5/ 2023	Maggio 2023

Chat GPT, OPEN AI
e le considerazioni sulla sicurezza informatica e su quella per l'individuo

Da qualche tempo tutti sono alle prese con gli interrogatori ai sistemi di OPEN AI specialmente quello noto con il nome di CHAT GPT. Se sia per simulare un test di Turing o se sia per sentirsi parte della folta comunità che si fa una propria opinione su questi strumenti, nessuno sembra resistere al fascino di "chattare" con un algoritmo per verificarne le capacità, per testarne la prontezza e la qualità delle risposte, per cercare di provare che così intelligente non è, o per svago, curiosità, per capire come funzioni, sentirsi parte dell'ultimo trend…
Ma di cosa si tratta davvero e che implicazioni di sicurezza potrebbero esserci nell'uso di un algoritmo di Chat GPT? La domanda non ha molto senso se non ci chiediamo prima "sicuro rispetto a cosa e rispetto a quale ambito di applicazione?"
Andiamo con ordine. Per iniziare è bene chiarire che Chat GPT è definito dall'organizzazione OPEN AI che l'ha concretizzato, come un modello che interagisce in modo conversazionale. Il formato del dialogo abilita l'algoritmo nella risposta a domande, contestare premesse errate e rifiutare richieste inappropriate o ammettere i propri errori, ma è anche capace di fornire una risposta dettagliata ad una istruzione fornita da "Prompt dei comando". L'organizzazione no profit che ha generato questo modello di Intelligenza Artificiale si chiama OpenAI ed è un laboratorio di ricerca americano sull'intelligenza artificiale (AI o IA) costituito nel 2015 dalla OpenAI Incorporated (OpenAI Inc.) senza scopo di lucro e dalla sua società controllata che invece è a scopo di lucro, OpenAI Limited Partnership (OpenAI LP). Dalla sua fondazione OpenAI conduce ricerche sull'IA con l'intenzione dichiarata di promuovere e sviluppare un'AI amichevole. I sistemi OpenAI girano sul quinto supercomputer più potente al mondo. (Fonte sito Open AI). I diversi progetti in cui sono adottati algoritmi di intelligenza artificiale spaziano dalle capacità di dialogo (Chat GPT), alla produzione di immagini a partire da descrizioni in linguaggio naturale (progetto DALL E2), dalla produzione di codice a partire dal linguaggio naturale (Open AI Codex) alla produzione di musica e canto (livello rudimentale (Progetto Jukebox).
In relazione alla domanda sulla sicurezza, posta poche righe fa, vale la pena segnalare come nel 2018 gli stessi ricercatori di OpenAI si siano posti il problema di come una AI potesse essere usata in modo malevolo (Malicious use of AI n.d.r.), al fine di poter porre rimedio a questa eventualità. Per loro stessa ammissione e preoccupazione di un uso duale di questa tecnologia, dichiararono apertamente l'ovvia verità tautologica applicabile ad ogni tecnologia: "l'intelligenza artificiale è una tecnologia capace di applicazioni immensamente positive e immensamente negative" (fu vero per la dinamite e per la scissione dell'atomo per citare due esempi noti a tutti n.d.r.). La buona notizia è che i ricercatori fin dal 2018 hanno voluto ispirarsi ai principi della Cybersecurity (perlomeno nelle loro dichiarazioni n.d.r.) segnalando come l'utilizzo di pratiche di "red teaming" per sovvertire i sistemi, di previsione delle minacce prima che si manifestino e di scoperta di vulnerabilità nei sistemi di AI, li abbiano guidati rispettivamente per intervenire nella difesa e nel patching. Ma purtroppo oggi non abbiamo strumenti per valutare se quelle azioni di "fortificazione" abbiano funzionato completamente o solo parzialmente e temporaneamente. L'esperienza ci insegna purtroppo che il codice digitale è "sicuro" e "al sicuro" solo fino a quando non si manifesta un soggetto capace di produrre un attacco con successo su quel codice.

La brutta notizia è che una risposta definitiva all'uso malevolo delle AI non è stata data nemmeno da OpenAI, che anzi segnala casistiche di esempio, sulle quali è disposta a ragionare con la community tecnologica e politica, ma sulle quali non è in grado di agire da sola: reti neurali e tecniche di "fuzzing" usate per creare virus informatici con capacità di generazione automatica di exploit, attori malintenzionati capaci di violare un robot delle pulizie in modo che consegni un carico utile di esplosivi a un soggetto target, o come Stati canaglia che utilizzano sistemi di sorveglianza potenziati dall'AI per arrestare preventivamente le persone che si adattano a un profilo di rischio predittivo…. e così via.
Quindi il problema è lungi dall'essere risolto perlomeno da OpenAI. Ma fortunatamente la community scientifica è ampia come è ampia la community dedicata alla sicurezza. In particolare il gruppo di standardizzazione ETSI dedicato alla sicurezza dell'intelligenza artificiale (Industry Specification Group – Securing Artificial Intelligence) ha rilasciato uno specifico paper sulla sicurezza dell'IA già nel 2021: "Securing Artificial Intelligence (SAI)" . più di recente è l'intervento normativo della UE ad aver segnato il passo dell'uso sicuro delle AI. Infatti l'Artificial Intelligence ACT, mira proprio a bilanciare l'uso delle AI fra i *"benefici socio-economici dell'IA e i rischi o le conseguenze negative per gli individui o la società…. e per delineare un approccio europeo sulle implicazioni umane ed etiche dell'IA."* Nel documento si legge che l'impostazione della proposta "*stabilisce norme armonizzate per lo sviluppo, l'immissione sul mercato e l'uso dei sistemi di IA nell'Unione secondo un approccio proporzionato basato sul rischio. Propone un'unica definizione di IA a prova di futuro. Alcune pratiche di IA particolarmente dannose sono vietate in quanto contrarie ai valori dell'Unione, mentre sono proposte restrizioni e salvaguardie specifiche in relazione a determinati usi di sistemi di identificazione biometrica remota a fini di contrasto. La proposta stabilisce una solida metodologia di rischio per definire i sistemi di IA "ad alto rischio" che comportano rischi significativi per la salute e la sicurezza o per i diritti fondamentali delle persone. Tali sistemi di IA dovranno rispettare una serie di requisiti orizzontali obbligatori per un'IA affidabile e seguire le procedure di valutazione della conformità prima che tali sistemi possano essere immessi sul mercato dell'Unione*".
Parallelamente alle norme e regole la ricerca non si è fermata e si va affermando l'AI Trust, Risk and Security Management (AI Trism), un'area di ricerca che cerca di garantire che i sistemi di Intelligenza artificiale siano sicuri e affidabili e che i rischi associati al loro utilizzo siano ridotti al minimo. (Per approfondire si veda la pagina Gartner dedicata al tema).
Tutto risolto quindi fra norme e ambiti di ricerca? Ovviamente no, perché il resto sta a noi. Come esseri umani "senzienti" abbiamo il diritto/dovere di sapere, per imparare a dubitare e a capire quando e come affidarci o meno ad una tecnologia, non perché decida per noi, ma perché ci supporti nelle decisioni da prendere, non per arrenderci ad essa, ma per vivere meglio grazie ad essa. D'altra parte, il progresso tecnologico ci ha permesso di evolvere dalla primitiva "clava", ma è sempre la nostra mano che deve effettuare la prima mossa, e che sia un gesto di polso per muovere la clava o che sia un "click", dovrebbe sempre essere un gesto pienamente consapevole e responsabile.

Alessia Valentini
Consulente di cybersecurity, advisor e giornalista. Fa parte delle "Women for Security", la community di Cyberladies nata nell'ambito del Clusit. È giornalista presso l'OdG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016.

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

ATTIVITA' 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.

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 ai soci che non hanno ancora rinnovato 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.

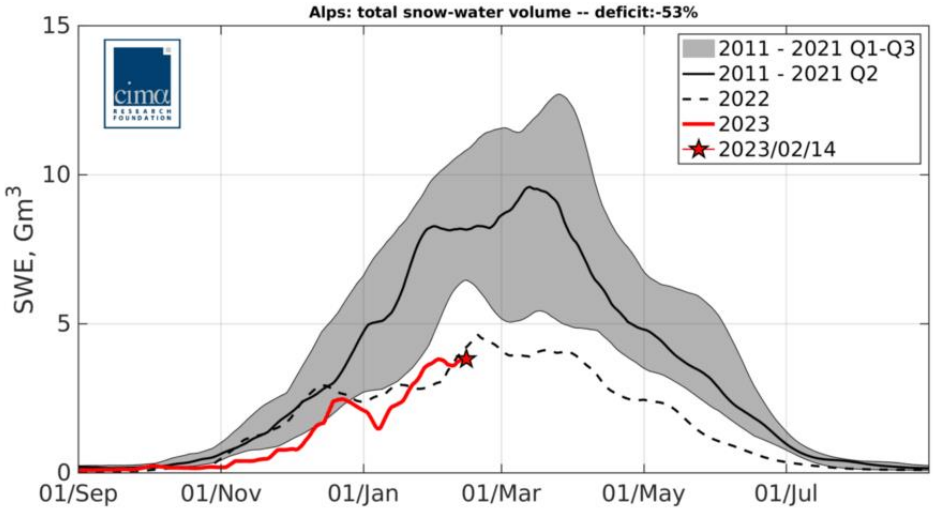
È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

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.
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

La neve di oggi è l'acqua di domani: lo strumento IT-SNOW - Conoscere la quantità d'acqua contenuta nella neve ha profonde implicazioni per la gestione della risorsa idrica, specialmente alla luce degli impatti che la crisi climatica ha sulla disponibilità d'acqua e i suoi molteplici usi: umano, agricolo ed energetico. La neve che si accumula in inverno è, infatti, acqua che useremo in estate.
Lo scorso 8 febbraio è stato pubblicata, sulla rivista scientifica Earth System Science Data, la prima analisi a livello nazionale sulla risorsa idrica nivale italiana e sulla sua evoluzione nel corso degli ultimi 12 anni, IT-SNOW.
Francesco Avanzi di Fondazione CIMA ha coordinato lo studio e spiega che "l'analisi è basata sull'integrazione tra dati raccolti a terra dai molteplici soggetti ed enti che si occupano di neve a livello nazionale, immagini satellitari e modelli fisici che consentono di stimare non solo la presenza di neve a terra, ma anche il suo spessore e quindi la quantità d'acqua contenuta, producendo mappe giornaliere a scala nazionale.
Per la prima volta quindi disponiamo di un'informazione, prodotta in modo omogeneo su tutto il territorio nazionale, che ci consenta di conoscere in tempo reale l'evoluzione di una delle risorse strategiche più importanti per il nostro Paese, in un contesto di crisi idriche sempre più frequenti indotte dalla crisi climatica."
Un importante contributo allo sviluppo del modello deriva anche dall'esperienza maturata in Valle d'Aosta.
"La Valle d'Aosta è stata una delle palestre dove è stata sviluppata l'esperienza che ci ha portato a questo grande risultato. Questo lavoro sulla modellazione della risorsa idrica nivale è infatti iniziato qui più di 10 anni fa. È stata una importante intuizione del gruppo di lavoro che comprende Fondazione CIMA, ARPA Valle d'Aosta, CVA e il Centro Funzionale della Regione Autonoma Valle d'Aosta e che ci ha consentito di sviluppare competenze innovative e testare metodi accurati per arrivare a quantificare nel modo più preciso possibile lo stato dei nostri serbatoi d'acqua in quota.
Questo ci ha consentito di avere a disposizione una catena di raccolta dati in campo e analisi che ci permette di avere un quadro sempre aggiornato dell'evoluzione della risorsa idrica nivale. In questo abbiamo anticipato i tempi, e ora ci troviamo ad avere uno strumento fondamentale che contribuisce a gestire i sempre più frequenti anni di siccità, come sembra purtroppo essere anche il 2023" spiega ARPA Valle d'Aosta.
A proposito di siccità, i dati di IT-SNOW mostrano un profondo deficit per l'anno in corso, con circa metà risorsa idrica nivale a scala nazionale oggi rispetto al periodo 2011-2021 (-45%). Nel bacino del Po, ad esempio, abbiamo un terzo di neve rispetto all'ultimo decennio e circa la stessa quantità rispetto all'anno scorso. Il Po ospita la metà della risorsa idrica nivale nazionale, e qui il volume di picco della neve può essere anche pari o superiore al 60% della portata annuale. Questo deficit di neve è l'acqua che avremo (o non avremo) in estate.



Andamento dell'equivalente idrico nivale alpino. La linea rossa rappresenta l'equivalente idrico nivale per la stagione in corso, totale su tutte le alpi italiane. La linea tratteggiata rappresenta l'equivalente idrico nivale totale per la scorsa stagione, mentre la linea nera e la banda grigia rappresentano, rispettivamente, la media sul periodo storico e la variabilità interannuale. Fonte: Snpa
https://www.puntosicuro.it/archivio-news-brevi/la-neve-di-oggi-l-acqua-di-domani-iNews1-2275.php?
Punto Sicuro *– 4 aprile 2023*

Direttiva NIS 2: la sicurezza delle infrastrutture critiche, tra normativa e buone prassi - La Direttiva NIS 2, che nasce da una profonda revisione della NIS, segna un altro importante passo verso la piena definizione della strategia cyber dell'Unione Europea, predisponendo adeguate risposte coordinate e innovative da parte di tutti gli Stati membri per garantire la continuità dei servizi digitali in caso di incidenti di sicurezza. Ecco il quadro normativo in cui si inserisce e i suoi punti salienti
L'entrata in vigore, lo scorso 17 gennaio 2023, della Direttiva NIS 2 (Direttiva UE 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022 sulla sicurezza delle reti e delle informazioni) segna un altro importante passo verso la piena definizione della strategia per la cyber sicurezza dell'Unione Europea, nella quale la Direttiva stessa si inserisce a pieno titolo partendo dal presupposto secondo il quale, ormai, i sistemi informatici e di rete usati per fornire servizi essenziali in settori chiave, occupano una pozione centrale nel percorso sempre più rapido di trasformazione digitale e di interconnessione della società (ricordiamo che NIS è, per l'appunto, l'acronimo di Network and Information Security).
Vero è, infatti, che i cyber attacchi alle infrastrutture critiche possono causare impatti economici e sociali di massa. Non esistono strategie migliori dei cyber attacchi per causare ansia e instabilità, soprattutto quando a essere presi di mira sono i sistemi e le reti che consentono le nostre attività quotidiane. I cyber attacchi perpetrati contro le infrastrutture critiche, quindi, sono diventati un'altra potentissima arma di interruzione di massa[1].
Tutto questo, insieme alla sempre più stringente necessità di gestire in sicurezza e in piena conformità normativa gli scambi transfrontalieri di dati di fronte a un'espansione delle minacce informatiche, ha spinto il legislatore europeo a trovare nuove e più adeguate risposte coordinate e innovative, da parte di tutti gli Stati membri, per garantire la continuità dei servizi digitali in caso di incidenti di sicurezza.
Ecco, dunque, che la Direttiva NIS 2 nasce in seguito a una profonda revisione della precedente Direttiva NIS (la Direttiva UE 2016/1148 del 6 luglio 2016 attuata in Italia con D.lgs. n. 65 del 18 maggio 2018) che, sebbene abbia consentito di sviluppare le capacità di cyber sicurezza di tutta l'Unione,

contribuendo al funzionamento efficace della sua economia e della società, ha rivelato alcune carenze intrinseche che di fatto hanno impedito di affrontare efficacemente le sfide attuali ed emergenti in materia di sicurezza informatica.

Indice degli argomenti

Dove non ha funzionato la Direttiva NIS
Dove, quando e a chi si applica la Direttiva NIS 2
La Direttiva NIS 2 nella strategia nazionale di cyber security
Direttiva NIS 2 e armonizzazione normativa tra Stati UE
Le sanzioni previste dalla Direttiva NIS 2
(continua)

https://www.cybersecurity360.it/cybersecurity-nazionale/direttiva-nis-2-la-sicurezza-delle-infrastrutture-critiche-tra-normativa-e-buone-prassi/

Cybersecurity360 *– Cristina Spagnoli - 05 Apr 2023*

Finalmente ufficialmente riconosciuta la figura del security manager - L'articolo 52 della legge regionale 3 marzo 2023 della regione Friuli Venezia Giulia fa riferimento al "Security manager regionale per le infrastrutture critiche regionali", conforme alla norma UNI 10459, debitamente certificato.

La regione Friuli-Venezia Giulia approvato recentemente una legge, un articolo della quale ha particolarmente attratto l'attenzione di chi scrive. Ecco i riferimenti ufficiali:

Legge regionale 3 marzo 2023, n. 10 Misure per la semplificazione e la crescita economica.
Capo II Incremento dei servizi
Art. 52 (Security manager regionale per le infrastrutture critiche regionali)

1. La Regione, nel rispetto della direttiva 2008/114/CE relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione, individua le infrastrutture critiche regionali quali elementi essenziali al mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico e sociale dei cittadini, il cui danneggiamento o la cui distruzione avrebbe un impatto significativo.

2. Le infrastrutture critiche regionali individuate con deliberazione della Giunta regionale ai sensi del comma 1 sono dotate di una gestione integrata di tutti i rischi di natura dolosa e/o criminosa, colposa o accidentale a cura di specifiche figure professionali, quali il Security manager UNI 10459 con certificazione, individuate in modo da garantire la gestione complessiva del processo conformemente alle norme tecniche di settore.

Sino ad oggi, gli unici testi non legislativi, ma regolamentari, nei quali compariva un riferimento al profilo del security manager secondo UNI 10459 erano i documenti prodotti dal ministero dell'interno, ed in particolare riferiti agli istituti di vigilanza privata. Il fatto che in questa legge regionale si faccia un esplicito riferimento a questo profilo professionale, incaricato di condurre le analisi di rischio e di predisporre le misure di messa sotto controllo di ogni tipologia di rischio, dimostra come il legislatore regionale abbia pienamente compreso il valore di questa qualificazione.

Particolare attenzione merita il fatto che il legislatore non solo abbia fatto riferimento a questa norma, che in Italia non viene apprezzata come meriterebbe, ma ha anche precisato che il soggetto in questione deve essere certificato. Ciò significa che una auto dichiarazione di conformità, rilasciata dal soggetto fisico, in merito alle sue capacità di svolgere con profitto il compito impegnativo di responsabile della security, non è sufficiente. In altre parole:

"Non basta che io dica che sono bravo, bisogna che lo dica un organismo terzo accreditato!"

Per dare un'idea della possibile estensione delle infrastrutture critiche regionali, che possono essere individuate come tali dalla regione, mi permetto di ricordare ai lettori tutte le strutture sanitarie, le

stazioni delle auto corriere, le stazioni ferroviarie, i musei, le infrastrutture energetiche e via dicendo. Non ho specificamente menzionato agli aeroporti, in quanto essi sono già assoggettati a controlli da parte dell'ENAC.
A questo punto confidiamo che anche altre regioni vorranno seguire il percorso indicato dalla regione Friuli-Venezia Giulia e dotarsi di personale con idoneo e certificato profilo professionale.
Cari colleghi professionisti certificati, un augurio di proficuo lavoro da tutti coloro che amano la vera security!
https://www.puntosicuro.it/security-C-125/finalmente-ufficialmente-riconosciuta-la-figura-del-security-manager-AR-23273/
PuntoSicuro *- Adalberto Biasiotti, 19/04/2023*

Cybersecurity, Milano diventa laboratorio di sicurezza informatica - Firmato il protocollo d'intesa tra la Città metropolitana e il Centro Operativo Sicurezza Cibernetica della Polizia Postale per la prevenzione e il contrasto degli attacchi alle infrastrutture critiche. Avanti sul progetto Deda Next per l'innovazione della gestione finanziaria.
(continua)
https://www.corrierecomunicazioni.it/cyber-security/cybersecurity-milano-diventa-laboratorio-di-sicurezza-informatica/
Corriere delle comunicazioni *– L.O. – 27/04/2023*

ChatGPT adempie alle prescrizioni del Garante Privacy e riapre in Italia garantendo più trasparenza e più diritti a utenti e non utenti europei - OpenAI, la società statunitense che gestisce ChatGPT, ha fatto pervenire al Garante per la protezione dei dati personali una nota nella quale illustra le misure introdotte in ottemperanza alle richieste dell'Autorità contenute nel provvedimento dello scorso 11 aprile, spiegando di aver messo a disposizione degli utenti e non utenti europei e, in alcuni casi, anche extra-europei, una serie di informazioni aggiuntive, di aver modificato e chiarito alcuni punti e riconosciuto a utenti e non utenti soluzioni accessibili per l'esercizio dei loro diritti. Alla luce di questi miglioramenti OpenAI ha reso nuovamente accessibile ChatGPT agli utenti italiani.
(*continua*)
https://www.federprivacy.org/informazione/garante-privacy/chatgpt-adempie-alle-prescrizioni-del-garante-privacy-e-riapre-in-italia-garantendo-piu-trasparenza-e-piu-diritti-a-utenti-e-non-utenti-europei
Federprivacy – *28/04/2023*

Cybersecurity per le infrastrutture critiche: una panoramica degli strumenti impiegati nel settore nucleare - La cyber sicurezza per le infrastrutture critiche presenta delle peculiarità che vanno approfondite con un approccio diverso rispetto alla normale attività di un SOC. Abbiamo pertanto considerato il settore "critico" per eccellenza che una potenziale riuscita di un cyber attacco implica per i risvolti ambientali, psicologici sulla popolazione, economici e di security&safety. Come viene affrontata e valutata la cyber resilienza nel settore nucleare e su quali linee guida e standards specifici si basa è lo scopo che ci prefiggiamo per fornire a chi si occupa di altre infrastrutture critiche spunti di riflessione e di confronto.
(continua)
https://www.ictsecuritymagazine.com/articoli/cybersecurity-per-le-infrastrutture-critiche-una-panoramica-degli-strumenti-impiegati-nel-settore-nucleare/
ICT Security Magazine *– Alberto Monici – 03/05/2023*

2 Years After Colonial Pipeline, US Critical Infrastructure Still Not Ready for Ransomware - Sweeping changes implemented since the May 2021 cyberattack are helping — but more work remains to be done, security experts say.

As the second anniversary of the massive ransomware attack on Colonial Pipeline nears, experts warn that efforts to thwart the potentially debilitating threat to US critical infrastructure have not been enough.

The cyberattack on its IT infrastructure forced Colonial Pipeline to shut down its entire operations for the first time ever, triggering a fuel shortage and price hikes that prompted four US states along the East Coast to declare a state of emergency. The incident immediately elevated ransomware to a national security level threat and galvanized concerted action from the Executive Branch down.

Since the attack — and another one shortly thereafter on JBS that threatened domestic meat shortages — the US government has said it would treat the use of ransomware on critical infrastructure as terrorism. An Executive Order signed by President Biden just days after the Colonial Pipeline attack mandated new security requirements for critical infrastructure organizations. And there have been numerous other initiatives at the federal level and by regulatory bodies to bolster resilience to attacks on US critical infrastructure.

However, two years on, the ransomware threat to critical infrastructure remains high, as a recent attack on America's largest cold-storage provider, Americold, showed. The attack — like the one on Colonial Pipeline — forced Americold, to shut down cold-storage operations while it worked to remediate the threat. Last year 870 of the 2,385 ransomware complaints that the FBI received involved critical infrastructure organizations. The FBI's data showed 14 of the 16 designated critical infrastructure sectors had at least one ransomware victim.

The trend continues unabated in 2023: BlackFog's State of Ransomware Report for April 2023 showed ransomware attacks on healthcare, government, and the health sector are continuing to grow, despite other vendor reports of a slowdown in attack volumes.

Unfinished Business

Security experts view the situation as one where for all the work done so far, there's a lot more to do. (*continua….*)

https://www.darkreading.com/ics-ot/2-years-after-colonial-pipeline-attack-us-critical-infrastructure-remains-as-vulnerable-to-ransomware

***Dark Reading** -Jai Vijayan- May 05, 2023*

NextGen Healthcare suffered a data breach that impacted +1 Million individuals - NextGen Healthcare suffered a data breach, the security incident exposed the personal information of approximately 1 million individuals. NextGen Healthcare, Inc. is an American software and services company that develops and sells electronic health record (EHR) software and practice management systems to the healthcare industry. NextGen Healthcare also provides population health, financial management, and clinical solutions for medical and dental practices.

NextGen Healthcare last week notified the Maine Attorney General's Office and started sending notification letters to the impacted individuals.

The data breach impacted 1049375 individuals, the company has contacted law enforcement and is working with them on the investigation.

According to the letters, the data breach was discovered on April 24, 2023. The company immediately launched an investigation and determined that threat actors had access to the systems at the company between March 29 and April 14, 2023. (continua…)
https://securityaffairs.com/145935/data-breach/nextgen-healthcare-data-breach.html
SecurityAffairs *-Pierluigi Paganini- May 8, 2023*

IA, cosa temono i massimi esperti - Hinton che ha lasciato Google è in buona compagnia sui molti timori nei confronti dell'intelligenza artificiale, per il breve e lungo periodo. Ecco il contesto in cui si esprimono, nella community scientifica di riferimento
Diremo tra poco chi è e cosa rappresenta Geoffrey Hinton nel campo dell'Intelligenza artificiale, per capire l'importanza delle sue considerazioni e dell'inquietudine che necessariamente esse sollevano.
In una recente intervista, egli ha affermato che quando le persone gli chiedevano come poteva lavorare su una tecnologia potenzialmente pericolosa, ricorreva a quanto dichiarava Robert Oppenheimer, uno dei padri della bomba atomica USA: "Quando vedi qualcosa che è tecnicamente fattibile, vai avanti e fallo".
Indice degli argomenti

Geoffrey Hinton e l'AI
Oggi, quando affronta il tema dell'I.A., non se la sente più di sposare questa posizione. Geoffrey Hinton è stato un pioniere dell'intelligenza artificiale. Poco più di dieci anni fa ha creato, insieme a due suoi studenti laureati all'Università di Toronto, una tecnologia che è diventata la base per i sistemi di intelligenza artificiale. In sostanza, ha cambiato il modo in cui le macchine vedono il mondo, realizzando un sistema in grado di analizzare migliaia di foto e, imparando da solo grazie al machine learning, ad identificare oggetti come fiori e automobili con precisione pressoché assoluta.
Il professore e i due studenti sono stati presto ingaggiati da Google, e il sistema, chiamato rete neurale, si è affermato consentendo, ad esempio, alle auto a guida autonoma di riconoscere segnali stradali e pedoni. Qualche giorno addietro, tuttavia, si è ufficialmente unito ai critici che affermano che le aziende tecnologiche stanno correndo verso il pericolo con la loro campagna aggressiva per creare prodotti basati sull'intelligenza artificiale generativa, la tecnologia che alimenta popolari chatbot come ChatGPT.
Il Dr. Hinton ha lasciato Google, dove ha lavorato per più di un decennio divenendo una delle voci più rispettate nel settore, quindi può parlare liberamente dei rischi dell'IA. Ora si rammarica del lavoro della sua vita. (continua…)
https://www.agendadigitale.eu/cultura-digitale/ia-i-principali-timori-dei-massimi-esperti/
AgendaDigitale*- Antonino Mallamaci -9 mag 2023*

Stop agli spyware e con gli Usa… I consigli del Parlamento europeo - *La commissione speciale dell'Eurocamera ha approvato una relazione e una raccomandazione non vincolanti sull'uso di Pegasus e dei suoi fratelli. Chiesto un divieto a meno che non vengano soddisfatte determinate condizioni entro la*

fine dell'anno e auspicata una strategia congiunta Bruxelles-Washington. La commissione speciale del Parlamento europeo su Pegasus ha termine i suoi 14 mesi di indagini concludendo che Polonia e Ungheria hanno usato lo spyware israeliano per monitorare illegalmente giornalista, politici e attivista. Inoltre, ha affidato una raccomandazione all'Unione europea: rafforzare la regolamentazione del settore. Gli eurodeputati hanno approvato a larghissima maggioranza una relazione e una raccomandazione non vincolanti sull'uso di Pegasus e di altri spyware nell'Unione europea, chiedendo un divieto effettivo della tecnologia a meno che non vengano soddisfatte determinate condizioni entro la fine dell'anno.
Per quanto riguarda i Paesi terzi e gli strumenti di politica estera dell'Unione europea, gli eurodeputati auspicano: un'indagine approfondita sulle licenze di esportazione di spyware; un'applicazione più rigorosa delle norme europee in materia di controllo delle esportazioni; una strategia congiunta tra Unione europea e Stati Uniti in materia di spyware; colloqui con Israele e altri Paesi terzi per stabilire norme sulla commercializzazione e l'esportazione di spyware; la garanzia che gli aiuti allo sviluppo dell'Unione europea non sostengano l'acquisizione e l'uso di spyware.(continua…)
https://formiche.net/2023/05/spyware-parlamento-europeo/
Formiche **-** *Gabriele Carrer* **-** *09/05/2023*

Digital Twin delle infrastrutture: i vantaggi e come realizzare un buon progetto
Avere un gemello digitale di una infrastruttura fisica permette di ottenerne la ricostruzione logica e digitale come se vivesse un mondo parallelo a quello reale ma replicando istante per istante ciò che accade realmente. Ma cosa serve per realizzare un buon progetto di digital twin e quali sono le difficoltà da superare?
Nell'evoluzione delle tecnologie e della digitalizzazione di tutto ciò che ci circonda stanno emergendo tutta una serie di applicazioni e soluzioni raccolte sotto il nome di **digital twin**, il gemello digitale di ogni opera ed infrastruttura che digitale non è.
Il concetto non è nuovo ma oggi sta emergendo un mercato ed una economia legata a questo settore di applicazione industriale che promette di cambiare il modo in cui gestiamo le nostre infrastrutture e di creare nuove professioni.
Indice degli argomenti

- I vantaggi di avere un gemello digitale
- Cosa occorre per realizzare un buon progetto di digital twin
- Gli attori coinvolti in un progetto di digital twin
- Conclusioni

I vantaggi di avere un gemello digitale
Il gemello digitale nasce dall'evoluzione delle tecniche di telecontrollo e di monitoraggio in verità presenti da anni sul mercato. Ad esempio, nel settore delle **automazioni industriali** i segnali di allarme e di gestione remota delle infrastrutture elettriche ed elettroniche sono da sempre, per definizione, prelevate sulla macchina oggetto di osservazione e trasportate in una sala di controllo o in una stazione con operatore che ne può leggere ed interpretare i valori ed i risultati. (*continua…*)
https://www.agendadigitale.eu/industry-4-0/digital-twin-delle-infrastrutture-i-vantaggi-e-come-realizzare-un-buon-progetto/
AgendaDigitale **-** *Nicola Ruggiero-10 Mag 2023*

NOTIZIE D'INTERESSE:

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

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 Andrea Agostino Fumagalli *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.