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. 6/ 2023** **giugno 2023**

L'intelligenza artificiale: un alleato nella sicurezza delle infrastrutture critiche

L'intelligenza artificiale (IA) è una tecnologia in continua evoluzione che ha dimostrato un enorme potenziale in diversi settori. Un'applicazione promettente dell'IA riguarda la sicurezza delle infrastrutture critiche. In questo articolo, esploreremo come l'intelligenza artificiale possa migliorare la sicurezza e la gestione delle infrastrutture critiche, fornendo una maggiore efficienza operativa, rilevazione precoce delle minacce e risposta rapida alle emergenze.

IA per il monitoraggio e la manutenzione predittiva

Le infrastrutture critiche richiedono un monitoraggio costante per garantire il loro corretto funzionamento. L'IA può essere utilizzata per analizzare enormi quantità di dati provenienti da sensori, apparecchiature e altre fonti per rilevare anomalie e prevedere potenziali guasti. Ciò consente di pianificare interventi di manutenzione preventiva prima che si verifichino problemi critici, riducendo al minimo le interruzioni e i costi operativi.

Rilevamento delle minacce e prevenzione degli attacchi

L'integrazione dell'IA nei sistemi di sicurezza può migliorare significativamente la capacità di rilevare e prevenire minacce alle infrastrutture critiche. I modelli di intelligenza artificiale possono analizzare in tempo reale i dati provenienti da telecamere di sorveglianza, sensori di movimento e altre fonti per identificare comportamenti sospetti o attività non autorizzate. Questo consente di intervenire prontamente e impedire potenziali attacchi o intrusioni.

Gestione intelligente del traffico e delle risorse

Le infrastrutture critiche, come le reti di trasporto e le forniture di energia, possono beneficiare dell'IA per una gestione più efficiente delle risorse. Ad esempio, l'IA può essere utilizzata per ottimizzare i flussi di traffico, identificando i punti critici e suggerendo soluzioni per evitare congestioni o incidenti. Inoltre, l'IA può contribuire a ridurre il consumo energetico e migliorare l'efficienza operativa attraverso l'analisi dei dati e l'ottimizzazione dei processi.

Risposta rapida alle emergenze

In situazioni di emergenza, come disastri naturali o attacchi terroristici, il tempo è cruciale. L'IA può supportare le infrastrutture critiche nella gestione delle crisi fornendo una risposta rapida e coordinata. Sistemi di intelligenza artificiale possono analizzare i dati provenienti da diverse fonti, come telecamere di sorveglianza, sensori di rilevamento e segnalazioni degli utenti, per identificare e localizzare tempestivamente gli eventi critici. Ciò consente di avviare misure di evacuazione, ripristino dei servizi e coordinamento delle risorse in modo più efficiente ed efficace.

Sfide e considerazioni etiche

L'adozione dell'intelligenza artificiale nelle infrastrutture critiche comporta anche sfide e considerazioni etiche. È fondamentale garantire la sicurezza dei dati e prevenire possibili manipolazioni o attacchi informatici alle reti di intelligenza artificiale stesse. Inoltre, l'uso dell'IA deve essere accompagnato da una rigorosa governance e da meccanismi di trasparenza per garantire la responsabilità e l'equità delle decisioni automatizzate.

Conclusioni

L'intelligenza artificiale offre un'enorme opportunità per migliorare la sicurezza e la gestione delle infrastrutture critiche. Dal monitoraggio predittivo alla prevenzione degli attacchi, dall'ottimizzazione delle risorse alla gestione delle emergenze, l'IA può fornire una maggiore resilienza e una risposta più rapida alle sfide che affrontano le infrastrutture critiche. Tuttavia, è fondamentale adottare un approccio equilibrato, garantendo la sicurezza dei dati e affrontando le sfide etiche per massimizzare i benefici dell'IA senza compromettere la sicurezza e la privacy delle infrastrutture critiche e dei loro utenti.

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

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

Proseguono le attività di formazione per soci e simpatizzanti per l'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.

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 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

Un cyberattacco blocca la Sanità lombarda, il caso Multimedica - La sanità pubblica italiana sotto scacco da parte del cyber crimine per quella che si sta rivelando essere una primavera movimentata. L'attacco a Multimedica sta paralizzando dal 25 aprile ambulatori lombardi e l'ospedale San Giuseppe di Milano, si tratta di un ransomware e oltre al disservizio il pericolo è il furto di dati sensibili sanitari

Il San Giuseppe di Milano, uno dei principali ospedali della città, è stato colpito da un attacco ransomware rivendicato dal gruppo criminale Lockbit. L'attacco ha causato gravi danni all'ospedale, bloccando molti dei suoi sistemi informatici e impedendo il normale svolgimento delle attività sanitarie.

Indice degli argomenti

Attacco a Multimedica, bloccato l'ospedale San Giuseppe di Milano

L'attacco è avvenuto circa quindici giorni fa contro il gruppo aziendale Multimedica, che gestisce appunto il San Giuseppe e altri ambulatori lombardi, ha subito immediatamente allertato sulla situazione, cercando di contenere i danni e di ripristinare i sistemi colpiti. Tuttavia, l'attacco si è dimostrato, come spesso accade con gli attacchi ransomware, particolarmente aggressivo e complesso, rendendo difficile il lavoro degli esperti informatici che stanno cercando di risolvere il problema.

Tuttavia ancora oggi sul sito Web di Multimedica (indisponibile) viene comunicato "Ci scusiamo per il disagio. Il servizio non è attualmente disponibile e sarà ripristinato il prima possibile". In effetti l'attacco sembra partito il 21 aprile e dalle dichiarazioni fornite alla stampa si legge di un secondo tentativo effettuato il 25 aprile appena passati.

(continua)

https://www.cybersecurity360.it/nuove-minacce/ransomware/un-cyberattacco-blocca-la-sanita-lombarda-il-caso-multimedica/

Cybersecurity360 *– Dario Fadda, 8 maggio 2023*

L'IA spaventa, il mondo reagisce: verso nuove regole UE, USA, Cina - Cresce la consapevolezza delle istituzioni sui rischi dell'IA. La legislazione in Ue e Usa sta facendo progressi per rimanere al passo con le innovazioni tecnologiche; lo stesso stanno facendo altri paesi come Canada e Cina. Una panoramica sul NIST AI Risk Framework e sulle raccomandazioni dell'osservatorio AI dell'OECD.

L'evoluzione delle normative sull'intelligenza artificiale evidenzia un crescente interessamento delle istituzioni rispetto ai rischi legati ai possibili usi distorti della tecnologia.

Dall'"AI Risk Management Framework" pubblicato dal NIST negli Usa all'osservatorio sull'IA dell'OECD, ecco le soluzioni proposte.

Indice degli argomenti

(continua)

https://www.agendadigitale.eu/sicurezza/rischi-dellintelligenza-artificiale-inizia-lera-delle-regolamentazioni/

Agenda Digitale *- Irene Parodi, Lorenzo Visaggio – 5 maggio 2023*

Digitalizzazione e cobot: come valutare la resilienza organizzativa? - Una scheda informativa dell'Inail riporta indicazioni su uno strumento per valutare la resilienza organizzativa nella transizione digitale e nell'uso di robot collaborativi. Il modello RAG e lo strumento operativo per valutare la resilienza.

Con "resilienza organizzativa" si può intendere "la capacità di un'organizzazione di anticipare, prepararsi, rispondere e adattarsi al cambiamento incrementale e agli inconvenienti improvvisi, con l'obiettivo di sopravvivere e prosperare". In particolare Hollnagel (2006) la "definisce come l'abilità intrinseca di un sistema di aggiustare il proprio funzionamento in presenza di disturbi o di cambiamenti imprevisti, interni o esterni a esso".
A parlare di resilienza organizzativa in connessione all'introduzione delle nuove tecnologie e alla trasformazione digitale in atto è una nuova scheda informativa (factsheet) prodotta dal Dipartimento di medicina, epidemiologia, igiene del lavoro e ambientale (Dimeila) dell' Inail.
La scheda – dal titolo "Transizione digitale, Cobot e SSL: uno strumento per valutare la resilienza organizzativa" e a cura di S. Stabile, E. Pietrafesa, R. Bentivenga e E. Sorrentino (Dimeila, Inail) e F. Costantino (Sapienza Università di Roma) – ricorda che l'implementazione di advanced manufacturing solutions nelle imprese "permette di migliorare la produttività, la qualità e la flessibilità della produzione", ma introduce "nuovi tipi di interazioni uomo-macchina che richiedono un'adeguata valutazione in un'ottica di salute e sicurezza sul lavoro (SSL)". Si sottolinea poi che, come richiesto dal Decreto legislativo 81/2008, il datore di lavoro procede alla rielaborazione della valutazione dei rischi "ogni qual volta siano introdotte modifiche del processo produttivo o della organizzazione del lavoro significative ai fini della SSL". E come ricordato dall'Agenzia europea per la sicurezza e la salute sul lavoro "l'automazione dei processi e il numero crescente di robot mobili e intelligenti negli ambienti lavorativi possono contribuire a rendere più complessa la gestione della SSL e aumentare il rischio di infortuni". Tuttavia per rendere il processo di valutazione dei rischi più aderente ai cambiamenti tecnologici e organizzativi, "è importante individuare e sviluppare metodologie e strumenti in grado di supportare le aziende nella prevenzione dei rischi nuovi ed emergenti in modo da adattarsi ai cambiamenti e anticiparne gli effetti, acquisendo una resilienza organizzativa per perseguire il miglioramento delle condizioni di lavoro".
L'articolo di presentazione della scheda si sofferma sui seguenti argomenti:
Un modello per la rilevazione della resilienza organizzativa
Lo strumento operativo e l'applicazione nell'utilizzo di cobot
Una guida nella misurazione della resilienza organizzativa
(continua)
https://www.puntosicuro.it/digitalizzazione-C-147/digitalizzazione-cobot-come-valutare-la-resilienza-organizzativa-AR-23327/
Punto Sicuro *- Tiziano Menduto, 17/05/2023*

La crisi dei trasporti richiede miglioramenti nella catena logistica - Il ritardo nella movimentazione di merci ha riflessi negativi su produzione, distribuzione e costo dei prodotti. Come migliorare la catena logistica? L'aggiornamento della norma ISO 28000 e il miglioramento di un manuale per il trasporto merci del GAO.
La pandemia di COVID-19 ha portato alla congestione dei container nei porti marittimi e nei magazzini. Queste sfide hanno ritardato la consegna delle merci ai consumatori e hanno portato a fluttuazioni dei prezzi.
La necessità di ridurre i ritardi nella catena logistica hanno fatto sì che, sia di qua, sia di là dell'Oceano Atlantico, gli enti preposti si siano attivati.
Ecco cosa succede di là dell'Atlantico.
Nel febbraio 2021, il presidente degli Stati Uniti ha emesso l'ordine esecutivo 14017, chiedendo una migliore resilienza delle catene di approvvigionamento statunitensi.

Il rapporto del comitato della Camera, che accompagna il disegno di legge sugli stanziamenti del Dipartimento per la sicurezza interna, nel 2022, include una disposizione per il GAO per rivedere i fattori, che influenzano la creazione di strutture di trasporto intermodale interno.
Questo rapporto affronta, tra gli altri obiettivi, il modo in cui le parti interessate del trasporto merci utilizzano le strutture di trasporto intermodale interno e la misura in cui la Federal Highway Administration (FHWA) ha aggiornato e comunicato il suo manuale sull'uso del trasporto e del territorio.
(continua)
https://www.puntosicuro.it/terziario-servizi-C-30/la-crisi-dei-trasporti-richiede-miglioramenti-nella-catena-logistica-AR-23346/
***Punto Sicuro** – Adalberto Biasiotti, 19/05/2023*

Se hai un pacemaker gli hacker ti possono colpire dritto al cuore - Un dispositivo medico, dal pacemaker al defibrillatore, una connessione wireless e adesso l'hacker può non limitarsi più a una "semplice" violazione della privacy, ma si apre piuttosto la porta a un nuovo e più crudele tipo di cybercrime per poter manipolare i software medicali e creare un serio pericolo proprio al cuore del bersaglio, nel verso senso della parola. L'obiettivo del cyber criminale può essere l'azienda che produce i dispositivi medici, ma anche lo stesso paziente che li indossa.
Attacchi hacker a pacemaker e defibrillatori: "Troppo vulnerabili, oltre 150-200 violazioni"
Già Dick Cheney quando era vice presidente degli Usa chiese ai suoi cardiologi di rimuovere la funzione wireless dal proprio defibrillatore per paura di poter subire un attacco terroristico nei suoi confronti, ma se allora quella sembrò una mossa da 'spy story', oggi la minaccia ai dispositivi medici è diventata un filone da osservare con molta attenzione.
A spiegarlo all'Adnkronos Salute, è Gaetano Marrocco, professore ordinario di Campi Elettromagnetici dell'Università Tor Vergata di Roma e coordinatore del corso di studi in Ingegneria Medica, dipartimento di Ingegneria Civile e Ingegneria informatica.
(continua)
https://www.federprivacy.org/informazione/societa/se-hai-un-pacemaker-ora-l-hacker-ti-puo-colpire-dritto-al-cuore
***Federprivacy –** 21 Maggio 2023*

Nuova specie di gallerie ferroviarie profonde e lunghe - Analisi delle particolari e complesse problematiche della costruzione delle nuove linee ferroviarie caratterizzate da elevate lunghezze e profondità.
Le future linee ferroviarie
I futuri trasporti di persone e merci attraverso grandi aree continentali, tipo la euroasiatica nella quale viviamo, saranno sviluppati via terra, grazie alla grande capacità trasportistica dei treni (più lunghi, pesanti e veloci) ed ai connessi risparmio energetico e sostenibilità ambientale, vincolando sin da ora la concorrenza con il traffico aereo.
Saranno costruite nuove linee ferroviarie ad alta velocità che correranno quasi su un piano orizzontale: e dovranno essere in galleria, per raggiungere velocemente le grandi aree urbanizzate, ed i connessi nodi di interscambio, sottopassando ogni tipo di ostacolo, naturale e/o costruito.
In ogni caso, queste reti ferroviarie dovranno essere costituenti privilegiati di un territorio vario già piuttosto ingombro, ma che comunque dovrà rimanere il più possibile libero per consentirvi la produzione di cibo (erba e carne).

Le nuove linee ferroviarie scenderanno dunque in galleria: a non grande profondità per sottopassare vaste aree urbanizzate o corsi d'acqua, come anche a profondità molto grandi (meglio dire con coperture molto grandi!) di un migliaio e più metri, per attraversare alla quota di base della rete ferroviaria vaste catene montuose.
E' proprio la profondità che le caratterizza come una nuova specie, giacché la profondità rende molto più complessi i comportamenti geomeccanici delle masse rocciose attraversate e quindi altrettanto complessi gli studi che vengono richiesti in sede di progettazione ed analogamente complesse le indagini "geologiche, geomeccaniche ed idrogeologiche" preliminari che saranno indispensabili.
Purtroppo le esperienze di studio e costruzione di opere sotterranee similari è ancora molto scarsa: solo un traforo è terminato ed è stato aperto al traffico nel 2016, un secondo è ancora in costruzione e per il terzo sono appena stati assegnati quasi tutti i lotti di lavoro tutti attraverso le Alpi:
il San Gottardo in Svizzera lungo circa 57,5 km che è già stato aperto al traffico nel 2016;
il Brennero circa 55,5 km, sulla linea Verona Innsbruck Monaco, tra Italia ed Austria, che è in avanzato stato di costruzione;
il Moncenisio circa 55,5 km sulla linea Torino Lione, tra Italia e Francia, i cui lavori stanno per iniziare essendo già stati assegnati gli appalti per la costruzione.
(continua)
https://www.ingenio-web.it/articoli/nuova-specie-di-gallerie-ferroviarie-profonde-e-lunghe/
***Ingenio** – Sebastiano Pelizza, 19 maggio 2023*

Gamp5 (2nd Edition) e la Security - Presentate al Simposio AFI 2023 (https://simposio.afiscientifica.it/) le "nuove" GAMP (Good Automated Manufacturing Practices), il "vangelo" per chi sviluppa e convalida sistemi computerizzati destinati all'utilizzo nell'industria del Life-Science (Farmaceutico, Biotech, Medical Devices, Nutritionals, ecc.): sono state pubblicate nel 2022 (l'edizione precedente era del 2005) ed il volume di oltre 400 pagine tra testo, appendici e glossari ha come sottotitolo "A Risk-Based Approach to Compliant GxP Computerized Systems".
Come enunciato nell'incipit, la Guida, creata dal gruppo di lavoro Gamp di ISPE (www.ispe.org, l'associazione internazionale che raggruppa i professionisti dell'industria Life Science), ha lo scopo di essere di supporto alle aziende dei comparti regolati dalle GxP (le linee guida per lo sviluppo, produzione e distribuzione di farmaci): non è un documento di regolamentazione, non è uno standard "de Jure" e non è automatico che sistemi sviluppati in accordo alle Gamp vengano accettati dalle autorità di vigilanza e controllo in ambito farmaceutico, che operano secondo protocolli condivisi a livello sovranazionale. Ricordiamo che per le regolamentazioni bisogna fare riferimento in Italia all'Agenzia Italiana del Farmaco, mentre l'organo di supervisione dell'Unione Europea è la European Medicines Agency (EMA). Negli Stati Uniti e per tutti gli stabilimenti che intendono esportare prodotti negli USA opera invece la U.S. Food and Drug Administration (FDA).
È però innegabile che le GAMP siano uno standard industriale "de Facto" alle quali si attengono tutti i partecipanti alla catena di fornitura nell'industria farmaceutica, dai costruttori di macchinari ed impianti, ai produttori e fornitori di materie prime, semilavorati, principi attivi, prodotti complementari e di confezionamento, consulenti e fornitori di servizi per l'industria del Life Science e naturalmente tutti i produttori e confezionatori di farmaci operanti nei paesi soggetti a stringenti regolamentazioni del settore.
Nella prefazione di questa seconda edizione della GAMP5, che volutamente non sono passate alla numerazione GAMP6 proprio per dare continuità di visione, si fa presente che il recente periodo di pandemia globale di Codid-19 ha sottolineato il ruolo essenziale delle nuove tecnologie per la

protezione della salute pubblica: in particolare questa guida GAMP5 tende a promuoverne l'utilizzo proprio per salvaguardare la qualità del prodotto e la sicurezza per il paziente.
Le innovazioni sono essenziali per l'Industria del Life Science per aumentare il valore per l'intera società, controllando i costi e ridurre il time-to-market.
La vasta regolamentazione di questo settore industriale potrebbe portare ad adottare approcci troppo rigidi per rispettare le norme, che spesso non sono commisurati all'effettivo rischio in essere per la qualità del prodotto e la salute per il paziente: in questa visione la revisione delle GAMP5 propone innovazione per la valutazione del rischio ed un uso efficiente ed efficace delle risorse anche applicando nuovi approcci nello sviluppo di sistemi ed utilizzo di tecnologie di mercato.
Il WhitePaper su GAMP5 2nd edition è scaricabile al link https://www.servitecno.it/wp-content/uploads/2023/05/Gamp5-2nd-Edition-e-la-Security.pdf
Enzo M. Tieghi – *etieghi@servitecno.it*

ChatGPT Hallucinations Open Developers to Supply Chain Malware Attacks
Attackers could exploit a common AI experience — false recommendations — to spread malicious code via developers that use ChatGPT to create software.
Attackers can exploit ChatGPT's penchant for returning false information to spread malicious code packages, researchers have found. This poses a significant risk for the software supply chain, as it can allow malicious code and Trojans to slide into legitimate applications and code repositories like npm, PyPI, GitHub, and others.
By leveraging so-called "AI package hallucinations," threat actors can create ChatGPT-recommended, yet malicious, code packages that a developer could inadvertently download when using the chatbot, building them into software that then is used widely, researchers from Vulcan Cyber's Voyager18 research team revealed in a blog post published today. In artificial intelligence, a hallucination is a plausible response by the AI that's insufficient, biased, or flat-out not true. They arise because ChatGPT (and other large language models or LLMs that are the basis for generative AI platforms) answer questions posed to them based on the sources, links, blogs, and statistics available to them in the vast expanse of the Internet, which are not always the most solid training data.
Due to this extensive training and exposure to vast amounts of textual data, LLMs like ChatGPT can generate "plausible but fictional information, extrapolating beyond their training and potentially producing responses that seem plausible but are not necessarily accurate," lead researcher Bar Lanyado of Voyager18 wrote in the blog post, also telling Dark Reading, "it's a phenomenon that's been observed before and seems to be a result of the way large language models work."
He explained in the post that in the developer world, AIs will also generate questionable fixes to CVEs and offer links to coding libraries that don't exist — and the latter presents an opportunity for exploitation. In that attack scenario, attackers might ask ChatGPT for coding help for common tasks; and ChatGPT might offer a recommendation for an unpublished or non-existent package. Attackers can then publish their own malicious version of the suggested package, the researchers said, and wait for ChatGPT to give legitimate developers the same recommendation for it. *(continua…)*
https://www.darkreading.com/application-security/chatgpt-hallucinations-developers-supply-chain-malware-attacks
***DARKREADING** -Elizabeth Montalbano -June 06, 2023*

Le due facce dell'intelligenza artificiale, tra nuovi rischi cyber e più efficaci sistemi di difesa proattiva

Le nuove tecnologie basate sull'intelligenza artificiale stanno cambiando il mondo e allo stesso tempo i rischi per la sicurezza, ma introducono anche un elemento di proattività nella difesa cyber verso le nuove minacce. Serve, però, un salto di qualità e una combinazione di approcci tecnici e strategici. Ecco perché

Le nuove tecniche di AI introducono sicuramente un **elemento di proattività nella difesa verso le nuove minacce** ma divengono anche uno strumento portentoso per la creazione di algoritmi malevoli che incrementano la capacità degli attaccanti di sfuggire ai sistemi di rilevazione tradizionali. **Le minacce divengono**, in questo modo, **sempre più sofisticate** proprio per la facilità di accesso a strumenti e metodologie impensabili fino a poco tempo fa.

Indice degli argomenti

- **Intelligenza artificiale e nuovi rischi cyber: il caso ChatGPT**
- **Intelligenza artificiale alleata della cyber security**
- **AI e difesa proattiva: quali soluzioni**

Intelligenza artificiale e nuovi rischi cyber: il caso ChatGPT

Abbiamo visto in questi giorni, da numerosi articoli, come anche tramite l'uso di ChatGPT un professionista possa essere assistito nello sviluppare linee di codice dannoso producendo una minaccia "Zeroday" (minaccia mai vista in precedenza per cui non è ancora disponibile una protezione specifica).

La **difesa contro le nuove tecniche di attacco basate sull'intelligenza artificiale** richiede un salto di qualità e una combinazione di approcci tecnici e strategici. Ne è un esempio l'utilizzo di approcci "Zero Trust" (non fidarsi mai, verificare sempre) i quali sono indispensabili per fronteggiare le nuove minacce. Tale approccio deve essere sempre applicato a 360° (per le identità, per gli accessi ai sistemi, per i contenuti).

Basti pensare ai file scambiati su ambienti ibridi dove non basta una classica verifica basata su signature ma occorre appunto un approccio che consenta di verificare minacce zero day (e quindi non ancora conosciute) andando ad applicare tecniche evolute come la CDR (Content Disarm and Reconstruction)

(continua..)

https://www.cybersecurity360.it/soluzioni-aziendali/l-intelligenza-artificiale-ed-il-suo-nuovo-ruolo-nella-cybersecurity/

***CYBERSECURITY 360** -Alessandro Gioso; Roberto Marzocca -07 Giu 2023*

Cybercrooks Scrape OpenAI API Keys to Pirate GPT-4

With more than 50,000 publicly leaked OpenAI keys on GitHub alone, OpenAI developer accounts are the third-most exposed in the world.

Yesterday, moderators of the r/ChatGPT Discord channel banned a script kiddie who was freely sharing stolen OpenAI API keys with hundreds of other users.

API keys allow developers to integrate OpenAI's technologies — particularly its latest language model, GPT-4 — into their own applications. Often, however, developers forget their keys in their code, making account theft a matter of just a few clicks.

Since at least March, a user by the name "Discodtehe" has been scraping API keys from source code published to the software collaboration platform Replit. The person shared free access to the booty on r/ChimeraGPT, where a community of more than 800 members began racking up usage charges to the stolen accounts. Following Vice reporting on June 7, Discodtehe can no longer be found on Discord or Reddit. But the story isn't over, experts emphasize : Tens of thousands of exposed API keys are still out

in the wild."The core of the story is: Don't put credentials in your source code," says Chris Anley, chief scientist at NCC Group. "And certainly don't then publish that source code."
OpenAI Keys Are Everywhere
As ChatGPT exploded in popularity, its keys began proliferating on the open Web. In The State of the Secrets Sprawl 2023 report, published March 8, GitGuardian observed thousands of exposed OpenAI keys in public repositories, rising in proportion to the newfound popularity ChatGPT. As of this writing, GitGuardian tells Dark Reading there are more than 50,000 publicly leaked OpenAI keys on GitHub alone. (*continua…)*
https://www.darkreading.com/application-security/cybercrooks-scrape-openai-keys-pirate-gpt-4
***DARKREADING** - Nate Nelson- June 08, 2023*

La certificazione di sicurezza dei prodotti ICT: cos'è, le origini e gli sviluppi futuri
La certificazione di sicurezza di un prodotto ICT è un processo articolato e complesso che richiede un contesto normativo ben definito e coinvolge un certo numero di soggetti. Ecco tutto quello che c'è da sapere.
La **certificazione di sicurezza dei prodotti** è un'esigenza sentita da tempo, ma solo negli ultimi anni ha registrato un interesse sempre maggiore a causa dell'aumento esponenziale degli **attacchi cyber** che hanno reso la **cybersecurity** un'emergenza all'attenzione di tutte le Istituzioni mondiali.
Indice degli argomenti

Cosa vuol dire certificare un prodotto ICT e la sua sicurezza
Una definizione consolidata del processo di certificazione, indipendentemente da quale sia l'oggetto in esame, è la seguente: "la certificazione è il risultato di una attività di valutazione eseguita da una terza parte indipendente (organismo di certificazione) sulla base di standards e metodologie riconosciute, e per le quali l'organismo di certificazione è stato preventivamente accreditato da un ente di accreditamento specifico".
Come si evince dalla definizione, **la certificazione è un processo articolato e complesso che richiede un contesto normativo ben definito** (una norma di riferimento, uno schema di certificazione, un gestore dello schema e un garante dello schema) e coinvolge un certo numero di soggetti (un ente accreditatore, un certificatore, un valutatore, un cliente, un oggetto da certificare e i fruitori della certificazione).
Pertanto, la certificazione di sicurezza di un prodotto ICT si può definire come "attività che in maniera probabilistica consente di rispondere circa le capacità di un sistema (assurance) di rispettare le specifiche di sicurezza che sono state stabilite in relazione al suo utilizzo/funzionamento."
Le caratteristiche della certificazione
Per poter raggiungere tali obiettivi, una certificazione deve avere delle caratteristiche essenziali quali: *(continua…)*
https://www.agendadigitale.eu/sicurezza/la-certificazione-di-sicurezza-dei-prodotti-ict-cose-le-origini-e-gli-sviluppi-futuri/
***AGENDA DIGITALE-** Garibaldi Conte - 9 giu 2023*

GPT-4, per alleggerire il lavoro dei medici: meno burocrazia, più cura

L'applicazione Dragon Ambient eXperience, o DAX, incorporerà presto GPT-4 grazie alla partnership tra Microsoft e OpenAI. I medici "cederanno il controllo" a "macchine imperfette" per utilizzare parte del loro tempo diversamente? Vediamo i vantaggi e le criticità

Uno tra i più gravosi compiti che i **medici** si trovano ad affrontare quotidianamente è il loro rapporto con la "**burocrazia**". Molti medici, infatti, passano ore ed ore della loro giornata lavorativa a compilare documenti e redigendo atti. Compiti che, peraltro, in molti paesi sono **obblighi di legge**; per cui, la loro compilazione non è facoltativa e comporta un pesante carico emotivo per i medici (in aggiunta a una professione già di per sé stressante e a costante rischio di burnout).

Indice degli argomenti

Le potenzialità di Dragon Ambient eXperience

Negli ultimi anni, negli Stati Uniti è stata testata una tecnologia che ha il potenziale di **alleviare parte del carico di lavoro dei medici**, ossia un'applicazione che registra le interazioni dei medici con i pazienti e utilizza l'Intelligenza Artificiale per generare note da inserire nella cartella clinica elettronica. L'applicazione, chiamata **Dragon Ambient eXperience**, o DAX, è stata sviluppata da Nuance Communications, azienda di Intelligenza Artificiale acquisita da Microsoft nel 2022.

Tra i primi ad utilizzare l'applicazione vi è la non-profit statunitense "**Providence Health & Services**" di Renton (Washington), che gestisce diversi ospedali e cliniche statunitensi. Sebbene molti degli oltre quattrocento medici del **Providence Health & Services** che finora hanno utilizzato DAX lo apprezzino, ci sono stati due ostacoli principali quando si è trattato di convincere un maggior numero di medici a utilizzarlo: ossia, la resistenza al cambiamento e la rinuncia al controllo della scrittura degli appunti (per quanto non sia una pratica apprezzabile dai medici, come accennato in precedenza). Finora, **il lavoro dell'Intelligenza Artificiale di DAX viene controllato da professionisti "umani"** prima di essere inviato al medico per la revisione finale. *(continua…)*

https://www.agendadigitale.eu/sanita/gpt-4-un-aiuto-per-i-medici-cosa-ci-riservano-gli-sviluppi-della-tecnologia/

AGENDADIGITALE- *Luigi Mischitelli- 9 giu 2023*

City of Dallas Still Clawing Back Weeks After Cyber Incident

The Texas city's networks have returned to 90% functionality following the May 3 Royal ransomware attack.

A month after the city of Dallas experienced a ransomware attack that took down major city services, city officials have announced that they have made significant progress, but there is still a substantial amount of work left to be done.

The Royal ransomware attack on May 3 affected services such as 311 (for non-emergency services), public libraries, animal shelters, safety departments, and online payment systems, though the Dallas IT team has now restored 90% of the network, it said.

The threat actor responsible for the attack, Royal ransomware, threatened to leak sensitive private data if a ransom wasn't paid by the city, though any threats made have yet to come to fruition. In the meantime, during this period of recovery, officials have boosted the software and functionality in many of the city's public departments.
"Our staff has worked tirelessly to restore and rebuild systems and return all systems to full functionality as quickly and securely as possible. At this time, we are more than 90 percent restored, with most public-facing services restored," the city of Dallas said in a statement. "We continue working diligently to restore full functionality as quickly as possible and will continue to keep the community informed with relevant updates throughout this process."
The city's update to residents also added that rebuilt and restored systems include the Dallas Water Utilities' payment and meter reading system as well as the Dallas Municipal Court. Dallas Public Library systems remain in the process of being restored and upgraded. *(continua…)*
https://www.darkreading.com/ics-ot/city-of-dallas-clawing-back-to-recovery-following-cyber-incident
DARKREADING-*Dark Reading Staff- June 09, 2023*

PROSSIMI EVENTI

La "AEIT - Associazione Italiana di Elettrotecnica, Elettronica, Automazione, Informatica e Telecomunicazioni", costituita il 1° gennaio 1897, dal 1° novembre 2013 ha assunto la attuale denominazione. Nella AEIT è confluita la AIIT - Associazione Italiana Ingegneri delle Telecomunicazioni, fondata nel 1962. Dal 1910, con un Regio Decreto, la AEIT ha ricevuto il riconoscimento di "Ente Morale".
Da 5 al 7 ottobre AEIT terrà la 115 International conference. La call for papers è a: https://convegni.aeit.it/aeit2023/documenti/aeit2023_save_the_date.pdf

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	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani Andrea Agostino Fumagalli *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.