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. 8/ 2023** **settembre 2023**

Sfruttare il Potere dell'Intelligenza Artificiale per la Sicurezza delle Infrastrutture Critiche

In un mondo sempre più interconnesso e digitale, la protezione delle infrastrutture critiche non è mai stata così cruciale. Salvaguardare asset essenziali come le reti elettriche, le reti di comunicazione e i sistemi di trasporto è fondamentale per la sicurezza nazionale e la pubblica incolumità. Con l'evoluzione del panorama delle minacce informatiche a un ritmo senza precedenti, organizzazioni come l'Agenzia per la Sicurezza delle Infrastrutture e la Cibersicurezza (CISA) e enti internazionali come la NATO si sono rivolti all'Intelligenza Artificiale (IA) per rafforzare le loro difese e rispondere efficacemente alle sfide emergenti.

1. *Il Ruolo dell'IA per Proteggere le Infrastrutture Critiche*

L'integrazione dell'IA nella protezione delle infrastrutture critiche rappresenta un passo significativo per migliorare le misure di sicurezza. Martin Stanley, il Capo del Dipartimento di Tecnologia Strategica presso la CISA, riconosce il ruolo cruciale dell'IA nel contrastare le minacce in evoluzione. Egli sottolinea che l'IA, in particolare l'IA Generativa, è una spada a doppio taglio. Mentre gli attori malintenzionati possono sfruttarne le capacità per incrementare le loro capacità di cyber attacco, l'IA consente ai difensori di rilevare e respingere più velocemente ed efficacemente gli attacchi informatici e fisici. La CISA, in qualità di Coordinatrice Nazionale per la Resilienza e la Sicurezza delle Infrastrutture Critiche, è stata in prima linea nell'utilizzo dell'IA per analizzare le tendenze e condividere informazioni vitali con i difensori cibernetici della nazione. Il potenziale dell'IA di fornire valutazioni delle minacce più rapide ed accurate rappresenta una svolta nella sicurezza delle infrastrutture critiche.

2. *Il Ruolo dell'IA nella Sicurezza Informatica per Proteggere le Infrastrutture Critiche*

Uno dei problemi più urgenti nella protezione delle infrastrutture critiche è stato il monitoraggio manuale dei sistemi di controllo degli accessi e dei sistemi video. La carenza di personale e l'incremento dei costi hanno reso sempre più difficile mantenere un apparato di sicurezza robusto. Tuttavia, l'IA offre diverse soluzioni in questa situazione. Algoritmi avanzati di IA possono analizzare vaste quantità di dati, inclusi video, audio, testo e registri, per rilevare efficacemente le anomalie. Questa capacità è inestimabile per affrontare il problema delle false allerte generate dai sistemi di controllo degli accessi e dai sistemi video. Inoltre, l'IA può automaticamente filtrare le allerte inutili, consentendo agli operatori di sicurezza di concentrarsi sulle minacce genuine e sulle attività strategiche.

Infine, l'IA può svolgere un ruolo fondamentale nel contrastare il problema del "tailgating" o "piggybacking", in cui individui non autorizzati ottengono l'accesso a strutture sicure attraverso quegli individui che hanno un accesso legittimo. L'analisi video basata su IA può monitorare le operazioni di autenticazione e rilevare eventuali tentativi di accesso non autorizzato, contribuendo a mantenere l'integrità delle misure di sicurezza fisica.

3. *Dove l'IA Non è Sufficiente per Proteggere le Infrastrutture Critiche*

Sebbene l'IA offra un immenso potenziale per migliorare la sicurezza delle infrastrutture critiche, è essenziale riconoscere i suoi limiti. I sistemi di IA dipendono pesantemente dai dati, e la loro efficacia dipende dalla qualità e dalla diversità dei dati che elaborano. Set di dati incompleti o tendenziosi possono portare a risultati inaccurati e a possibili punti ciechi nella sicurezza.

Inoltre, l'IA da sola non può affrontare le cause alla radice delle vulnerabilità della sicurezza. Può automatizzare le attività e individuare modelli, ma potrebbe non riuscire a comprendere gli aspetti

sfumati del comportamento e delle intenzioni e interazioni umane. Pertanto, è fondamentale adottare un approccio olistico che combini le capacità dell'IA con l'esperienza umana nella salvaguardia delle infrastrutture critiche.

4. La Posizione di NIST e CISA

Per garantire l'uso responsabile ed efficace dell'IA nella sicurezza delle infrastrutture critiche, organismi di regolamentazione come l'Istituto Nazionale di Standard e Tecnologia (NIST) svolgono un ruolo vitale. Il NIST ha recentemente pubblicato il quadro di gestione del rischio legato all'IA, sottolineando l'affidabilità dei sistemi di tali tecnologie. Questo quadro fornisce linee guida su come costruire e implementare sistemi di IA che rispecchino dei parametri affidabili e sicuri. Inoltre, il quadro sottolinea l'importanza dell'uso trasparente, legale e autorizzato dei dati per preservare la fiducia pubblica e favorire relazioni positive con gli stakeholder.

Nell'intervista con Martin Stanley, capo del Dipartimento di Tecnologia Strategica presso la CISA (Agenzia per la Sicurezza delle Infrastrutture e la Cibersicurezza), emerge il ruolo cruciale dell'IA nella protezione delle infrastrutture critiche. La CISA, in qualità di coordinatrice nazionale per la resilienza e la sicurezza delle infrastrutture critiche, affronta le minacce in continua evoluzione sia alla cibersicurezza che alle infrastrutture fisiche, sfruttando le capacità dell'IA e della tecnologia quantistica. Mr. Stanley spiega che la CISA risponde a incidenti specifici segnalati e ha l'obiettivo di prestare assistenza, comprendere i rischi potenziali e sviluppare risposte efficaci agli attacchi informatici. L'IA rappresenta sia una minaccia emergente, con attori malintenzionati che possono sfruttarla per scopi nefasti, che un'opportunità, in quanto può aiutare a rilevare e prevenire attacchi informatici e fisici.

Conclusioni

In conclusione, l'integrazione dell'IA nella sicurezza delle infrastrutture critiche rappresenta una promettente via di sviluppo per rafforzare le nostre difese in un'era di crescenti minacce informatiche. Organizzazioni come la CISA e la NATO riconoscono il potenziale trasformativo dell'IA nel rilevare modelli, automatizzare le risposte e ridurre i rischi. Tuttavia, è essenziale essere consapevoli dei limiti dell'IA e valutare più accuratamente l'interazione che c'è tra l'IA e l'esperienza umana nella protezione delle nostre infrastrutture critiche. Adottando le linee guida stabilite da entità come il NIST e promuovendo la collaborazione tra esseri umani e macchine, secondo l'ente, si può migliorare la postura di sicurezza della nostra nazione e garantire la resilienza dei nostri asset critici di fronte alle minacce in evoluzione.

Luisa Franchina
Presidente Associazione Italiana esperti in Infrastrutture Critiche

È stata Direttore Generale della Segreteria per le Infrastrutture Critiche (Presidenza del Consiglio dei Ministri 2010-2013). Ha pubblicato numerosi articoli e libri sulla sicurezza e sulla protezione delle infrastrutture critiche.

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.

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.

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 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*

WORKSHOP SU "GESTIONE DEL RISCHIO NELLA PROSPETTIVA DEI CAMBIAMENTI CLIMATICI" – Roma, 14 novembre 2023

Il Capitolo italiano della Associazione "The International Emergency Management Society", in breve (TIEMS Italia), sta organizzando per il 14 Novembre 2023 un workshop dal titolo "Gestione del Rischio nella prospettiva dei Cambiamenti Climatici".

Il workshop intende evidenziare la necessità di adattare ai Cambiamenti Climatici le strategie per la gestione delle Emergenze e del Rischio e provare ad identificare i punti salienti di una Agenda che tale adattamento dovrà sostenere.

I Cambiamenti Climatici in corso sembrano essere in grado di generare eventi naturali sia più frequenti, sia in grado di produrre, con una frequenza maggiore che nel passato, situazioni complesse da gestire. Oltre che di grande impatto per la popolazione, l'intensità e la frequenza degli eventi tenderanno a produrre conseguenze sugli asset nazionali, in particolare le Infrastrutture Critiche, perturbando in maniera consistente i principali servizi al sistema civile, industriale e della difesa nazionale.

Adattare le Strategie per la gestione del Rischio e delle Emergenze non potrà verosimilmente fare a meno dell'apporto di una maggiore preparatività (preparedness) sia a livello di Operatori, sia a livello di Sistema di gestione delle Emergenze e auspicabilmente ad una gestione comune e condivisa delle infrastrutture del Paese, sempre più dipendenti tra loro.

La nuova Agenda per supportare tali adeguamenti potrà fare leva su una serie di iniziative legislative (in particolare il recepimento della Direttiva Europea 2022/2557 relativa a "Critical Entity Resilience") focalizzate proprio su una maggiore centralizzazione del monitoraggio e dell'analisi di scenari, una migliore conoscenza del parco infrastrutturale del Paese, una maggiore condivisione di informazioni

necessarie ad ottimizzare la gestione delle situazioni di crisi, migliorando anche l'efficienza e l'efficacia delle operazioni di gestione delle Emergenze.

L'Associazione AIIC sostiene l'iniziativa e invita tutti propri Soci a partecipare.

Tra i relatori è prevista la partecipazione del dott. Sandro Bologna, componente del Consiglio Direttivo di AIIC e coordinatore del Gruppo di Studio AIIC su "Resilienza delle Infrastrutture Critiche e cambiamenti climatici" che sta terminando i lavori con la pubblicazione di un apposito report.

Il Workshop si svolgerà **Martedi' 14 Novembre 2023** presso l'Aula Conferenze della Facoltà di Ingegneria della Università di Roma Tre, in Via Vito Volterra 62 a Roma a partire dalle 9:30.

Non appena sarà disponibile il programma definitivo, provvederemo a pubblicarlo sul nostro sito e a darne notizia agli interessati.

NEWS E AVVENIMENTI

Gestione dei rischi Na-Tech in ambito industriale: ricerca, valutazione e progettazione a lungo termine - É sempre più importante definire delle metodologie che possano riportare in controllo la gestione e la mitigazione degli eventi Na-Tech (incidenti tecnologici a seguito di eventi naturali calamitosi) secondo una logica di pianificazione, prevenzione e protezione.
Nel contesto industriale moderno, i rischi Na-Tech (Natural and Technological) rappresentano una preoccupazione rilevante, ma di rado gestita con lungimiranza. Le necessità finanziarie a breve termine, unite alla difficoltà nell'anticipare l'esatta entità delle minacce a venire spingono ad una diffusa procrastinazione che impedisce gli interventi strutturali utili a garantire la continuità operativa dell'impresa anche in condizioni estreme.
Catastrofi annunciate
Mutuando un'espressione tipica della cronaca quotidiana, gli ultimi decenni hanno fornito numerosi esempi di cosiddette "catastrofi annunciate", ossia di eventi naturali avversi (es. terremoti, alluvioni, valanghe ecc.), talvolta d'imponente entità, le cui conseguenze hanno avuto un impatto radicale sia sulle infrastrutture industriali che sull'ambiente circostante.
Con un approccio più strutturato e meno sensazionalistico, la letteratura tecnica classifica questi accadimenti come "eventi Na-Tech" (Natural Hazard Triggering Technological Disasters) qualificandoli come "incidenti tecnologici quali, ad esempio, incendi, esplosioni, cedimenti strutturali, rilascio di sostanze tossiche ecc. che possono verificarsi all'interno di complessi industriali e/o lungo le reti di distribuzione a seguito di eventi calamitosi di matrice naturale".
In quest'ottica, è significativo rilevare innanzitutto come l'interazione fra "rischio naturale" e "rischio industriale" comporti un'amplificazione sovente sottostimata di effetti e danni correlati, determinata sia dalla concomitanza di singoli eventi incidentali (o catene di eventi) di magnitudo superiore, sia dalla possibile indisponibilità dei sistemi di protezione / mitigazione delle conseguenze, ovvero delle risorse operative (es. mezzi, attrezzature, soccorritori specializzati ecc.) usualmente demandate alla gestione dell'emergenza.

Come si può ricostruire facilmente mediante una breve ricerca dedicata all'argomento, gli eventi naturali che hanno colpito negli ultimi anni il nostro Paese hanno non solo provocato il danneggiamento di strutture fisiche e l'interruzione di forniture di energia, originando sensibili perdite economiche (a livello locale o addirittura regionale), ma hanno anche coinvolto decine di lavoratori negli ambiti più disparati, mettendo in evidenza l'elevata vulnerabilità di molte attività produttive nonché del territorio in genere a fronte di circostanze che, non sempre, appartengono alla sfera dell'imponderabile, ma che anzi sono storicamente legate alle caratteristiche geomorfologiche di uno specifico territorio, ovvero che sono state incautamente favorite dalla disattenzione umana (es. con incuria o dolo, in alcune circostanze-limite).
(continua)
https://www.ingenio-web.it/articoli/gestione-dei-rischi-na-tech-in-ambito-industriale-ricerca-valutazione-e-progettazione-a-lungo-termine
***INGENIO** - Alessandro Negrini, 10 luglio 2023*

Sicurezza delle reti di cablaggio sottomarino: un'infrastruttura critica per la connessione internet

La sicurezza delle reti di cablaggio sottomarino rappresenta un aspetto critico per garantire la connettività internet e l'economia digitale dell'Unione Europea, tanto che la gestione dei cavi marini ha ormai assunto una dimensione politica. Ecco le sfide politiche e commerciali

I **cavi sottomarini** rappresentano la **maggior parte del traffico internet mondiale**, ma l'aumento delle preoccupazioni legate agli **attacchi mirati all'infrastruttura internet** sta spingendo l'Unione Europea ad avviare diversi progetti sostenuti da dinamiche politiche nascoste.

Questi cavi in fibra ottica sottomarini **consentono il 99% del traffico internet globale**, secondo la società di ricerca nel settore delle telecomunicazioni TeleGeography, rendendoli una parte cruciale, seppur invisibile, della nostra società.

Negli ultimi anni, la questione di come queste reti potrebbero essere oggetto di attacchi per bloccare o interferire con le comunicazioni e gli scambi di informazioni è stata al centro delle tensioni internazionali tra Stati Uniti e Cina.

Questa **dimensione geopolitica dei cavi transcontinentali** si intreccia inevitabilmente con gli interessi commerciali, poiché l'installazione di cavi internet per migliaia di chilometri è costosa e le grandi aziende del settore tecnologico sono sempre più coinvolte con i propri progetti.

Indice degli argomenti

Garantire la resilienza delle infrastrutture sottomarine

In Europa, **garantire la resilienza delle infrastrutture critiche sottomarine** è un argomento delicato dopo il sabotaggio del gasdotto Nord Stream lo scorso settembre. Il Commissario europeo Thierry Breton ha da allora promosso un'agenda di connettività sicura che combina la diversificazione delle connessioni internet e le comunicazioni basate su satelliti.

L'iniziativa Global Gateway dell'Europa, finalizzata a finanziare progetti internazionali in concorrenza con l'iniziativa Belt and Road della Cina, ha stanziato circa 30 miliardi di euro per progetti di connettività digitale, tra cui cavi sottomarini in fibra ottica, sistemi di comunicazione sicura basati su satelliti e centri di dati.

La maggior parte dei finanziamenti dell'UE verso paesi terzi è destinata all'Africa, dove attualmente il principale progetto ufficiale per la connettività UE-Africa è Medusa, che collega il sud dell'Europa all'Algeria, l'Egitto, il Marocco e la Tunisia attraverso il Mar Mediterraneo.

Secondo una presentazione della Commissione ai rappresentanti nazionali nell'aprile scorso, un altro progetto preso in considerazione è EurAfrica Gateway, che si estenderebbe dalla penisola iberica lungo la costa atlantica dell'Africa occidentale attraverso il Golfo di Guinea fino alla Repubblica Democratica del Congo.
L'obiettivo è quello di connettere paesi con poca copertura e stabilire collegamenti con partner strategici della regione come la Nigeria, il paese africano più popoloso, dove la Commissione ha dichiarato l'intenzione di investire 820 milioni di euro in progetti digitali.
L'interesse si estende anche all'America Latina e ai Caraibi, con il piano iniziale di espandere il programma BELLA, che include EllaLink da Portogallo a Brasile, fino a Colombia, Perù, isole caraibiche come Cuba e la Repubblica Dominicana, e persino fino al Messico attraverso l'America Centrale*.(continua…)*
https://www.cybersecurity360.it/cybersecurity-nazionale/sicurezza-delle-reti-di-cablaggio-sottomarino-uninfrastruttura-critica-per-la-connessione-internet/
Cybersecurity360 *- Tommaso Maria Ruocco - 26 Lug 2023*

SANZIONE SU THIN Dati sanitari, il Garante privacy chiarisce quando è vera anonimizzazione
Il Garante privacy ha sanzionato la società Thin Srl per aver trattato illecitamente i dati sanitari di numerosi pazienti raccolti presso circa 7mila medici di medicina generale (Mmg), senza adottare idonee tecniche di anonimizzazione, chiarendo il corretto ambito di applicazione del GDPR. Ecco cosa impariamo
Nel settore della ricerca scientifica, il tema dell'anonimizzazione dei dati costituisce uno degli argomenti più sensibili e discussi. Da un lato, infatti, la ricerca medica e scientifica necessita di data base quanto più completi possibile per poter effettuare studi efficaci; dall'altro lato, vi è la necessità di tutelare la riservatezza del paziente e delle informazioni che lo riguardano.
Al fine di consentire il rispetto di entrambe le descritte necessità, le Autorità ed i legislatori – sia nazionali che europei – hanno fatto leva sul concetto di anonimizzazione, rendendo anche diverse interpretazioni su cosa debba effettivamente intendersi per "dato anonimizzato".
Indice degli argomenti

Il provvedimento su Thin dal Garante privacy
È in questo filone giurisprudenziale che si colloca il recentissimo provvedimento del Garante Privacy, con il quale è stata comminata ad una società una **sanzione** di 15mila euro per trattamento illecito di dati sanitari dovuto alla mancata adozione di tecniche di anonimizzazione. **Thin ha fatto ricorso.**
L'Autorità, nel provvedimento che si andrà nel seguito meglio a discutere, afferma, richiamando un parere del 2014 reso dal Gruppo di lavoro Articolo 29 (ora EDPB), che per poter considerare un dato sanitario effettivamente "anonimizzato" non è sufficiente la sostituzione dell'ID del paziente con un sistema crittografico o un codice hash irreversibile, non essendo detti sistemi di sicurezza sufficienti rispetto al requisito della rimozione delle singolarità (single out) richiesto per potersi parlare effettivamente di dato anonimizzato.
Sul tema si è formata anche autorevole giurisprudenza della Corte di Giustizia Europea, che ha dettato ulteriori parametri per la qualificazione del dato come "personale", affermando, in particolare, che il dato possa ritenersi non anonimo soltanto quando il destinatario dei dati – anche pseudonimizzati –

abbia la "ragionevole" possibilità di combinare le informazioni in suo possesso con i dati ricevuti, consentendo la re-identificabilità del soggetto cui dette informazioni si riferiscono.
Nota è la sentenza resa nel Caso Deloitte, nel quale si precisava che per poter essere considerati anonimi, i dati dovrebbero essere sottoposti dalle autorità garanti ad un test di re-identificabilità, teso a stabilire se il destinatario dei dati "anonimizzati" abbia effettivamente la possibilità, con gli strumenti concretamente utilizzabili da quest'ultimo, di consentire la re-identificazione di uno specifico soggetto. *(continua…)*
https://www.cybersecurity360.it/legal/privacy-dati-personali/dati-sanitari-il-garante-privacy-chiarisce-quando-si-puo-parlare-correttamente-di-anonimizzazione/
***CYBERSECURITY360**- Marina Rita Carbone – 28 luglio 2023*

Cavi sottomarini, nuovo scenario di guerra tecnologica tra USA e Cina: quali implicazioni
Una delle maggiori aziende di cavi sottomarini al mondo sta supportando gli USA in una nuova guerra tecnologica contro la Cina. Nessuno degli interlocutori coinvolti ha per il momento commentato la notizia. Ecco i possibili scenari
La società tecnologica del New Jersey, **SubCom**, sarebbe al centro della **guerra tecnologica tra Stati Uniti e Cina** in quanto starebbe favorendo la prima potenza, a scapito della seconda, nella **posa di** cavi sottomarini sul **fondo dell'oceano**, incrementandone la forza economica e militare.
La notizia, riportata di recente dall'autorevole testata Reuters, è partita dalle dichiarazioni di quattro persone a conoscenza dei fatti: due dipendenti di SubCom e due membri dello staff della Marina degli Stati Uniti, nessuna delle quali è stata disposta a lasciare le proprie credenziali in quanto non autorizzata a discutere delle operazioni in oggetto.
Indice degli argomenti

- Cavi sottomarini: un'infrastruttura strategica
- SubCom, nuova alleata USA nella cyberwar contro la Cina
- Subcom, tra difesa nazionale ed economia

Cavi sottomarini: un'infrastruttura strategica
Il 10 febbraio dello scorso anno la nave cablata CS Dependable, di proprietà di SubCom, è apparsa al largo dell'isola Diego Garcia, la più grande dell'arcipelago delle isole Chagos, atollo dell'Oceano Indiano sede di una base navale statunitense di una certa importanza.
A marzo dello stesso anno è stata portata a termine l'operazione segreta dal nome in codice "Big Wave", che consisteva nella posa di un cavo di fibra ottica sottomarino fino alla base militare, operazione riportata dai quattro testimoni e da Reuters stessa, che si è affidata ai dati ricavati dalle immagini satellitari e dal tracciamento della nave.
Questo nuovo collegamento internet superveloce all'isola potenzia la prontezza militare USA nell'Oceano Indiano, regione in cui proprio la Cina ha ampliato l'influenza navale negli ultimi dieci anni.
All'uscita delle rivelazioni di Reuters, un portavoce della Flotta del Pacifico della Marina statunitense ha confermato l'esistenza di questo nuovo cavo internet sottomarino ad alta velocità nell'Oceano Indiano ed è stato il primo riconoscimento ufficiale di questa operazione.
Le parole del portavoce della flotta sono state: "La resilienza, la ridondanza e la sicurezza delle nostre infrastrutture di comunicazione rappresentano una priorità assoluta per la Flotta del Pacifico".
Sempre Reuters ha rivelato che la SubCom sta stringendo rapporti sempre più stretti con il Pentagono parlando di un contratto riservato che l'azienda ha sottoscritto con Google per costruire la più grande rete internet privata sottomarina del mondo. Questa partnership è il tipo di progetto che il presidente Joe Biden ha incoraggiato per promuovere le tecnologie avanzate degli Stati Uniti. *(continua…)*

https://www.cybersecurity360.it/cybersecurity-nazionale/cavi-sottomarini-nuovo-scenario-di-guerra-tecnologica-tra-usa-e-cina-quali-implicazioni/
CYBERSECURITY360 -*Marco Santarelli -28 Lug 2023*

Nuovi regolamenti sull'intelligenza artificiale, tra punti di forza e criticità
Su entrambe le sponde dell'Atlantico continuano gli sforzi dei legislatori per creare un quadro normativo che garantisca uno sviluppo sicuro, protetto e trasparente dell'intelligenza artificiale. Tanti i punti di forza, ma anche le perplessità avanzate dagli addetti ai lavori. Facciamo chiarezza
Il 21 luglio 2023 l'amministrazione Biden ha **annunciato** di aver incontrato i dirigenti di sette aziende leader nel settore tecnologico, fra cui Amazon, Anthropic, Google, Inflection, Meta, Microsoft e OpenAI, per raggiungere un accordo su uno sviluppo sicuro, protetto e trasparente dell'intelligenza artificiale (IA). Tale intesa si fonda su tre capisaldi: sicurezza, protezione e fiducia.
Dal punto di vista della sicurezza, le imprese hanno il dovere di garantire che i loro prodotti siano affidabili prima di essere introdotti nel mercato; per quanto riguarda la protezione, è stata manifestata la necessità di mettere a punto soluzioni che salvaguardino i sistemi da minacce informatiche interne ed esterne, condividendo le *best practise* e gli standard per proteggere la sicurezza nazionale.
Infine, le aziende hanno il compito di stabilire e mantenere un rapporto di fiducia e trasparenza con i propri utenti, tutelando i loro diritti alla privacy e informandoli nel caso in cui i contenuti audiovisivi a cui sono sottoposti siano originali o alterati dall'IA.
Indice degli argomenti

- Le misure da adottare per la sicurezza dei sistemi IA
- I punti critici ancora da risolvere
- AI Act: gli impatti del nuovo regolamento europeo
- Nuovi regolamenti sull'intelligenza artificiale: le perplessità
- Intelligenza artificiale: serve collaborazione transatlantica

Le misure da adottare per la sicurezza dei sistemi IA
Nello specifico, tra le misure **proposte** dalle sette multinazionali alla Casa Bianca si rilevano:

1. la conduzione di test di sicurezza interna ed esterna, i cosiddetti *red-teaming*, sui sistemi IA prima del rilascio, affidando parzialmente le verifiche a esperti indipendenti relativamente ai rischi legati alla sicurezza nazionale, quali la capacità di progettare armi di distruzione di massa, le discriminazioni sociali o le minacce cyber;
2. una maggiore condivisione delle informazioni sui progressi raggiunti in campo IA, sulle minacce emergenti e sulle rispettive misure di protezione, non solo all'interno del settore IT ma anche con i governi, la società civile e il mondo accademico*; (continua….)*

https://www.cybersecurity360.it/legal/nuovi-regolamenti-sullintelligenza-artificiale-tra-punti-di-forza-e-criticita/
CYBERSECURITY360*- Luisa Franchina -Davide Agnello- Nunzia Alfano- Gaia D'Ariano -*
01 Ago 2023

Il rischio nelle ferrovie: l'incidente di Brandizzo e la prevenzione - Partendo dal tragico infortunio che è costata la vita di cinque operai sui binari a Brandizzo, alcune riflessioni e un vademecum elvetico con dieci regole vitali per chi lavora nelle ferrovie. Focus sulla pianificazione e sulle regole di sicurezza.
Brescia, 4 Set – Oltre al dolore e al cordoglio per la morte di cinque operai nell'incidente ferroviario avvenuto a Brandizzo, in provincia di Torino, - il Presidente della Repubblica ha sottolineato giustamente che "morire sul lavoro è un oltraggio ai valori della convivenza" – bisogna cominciare a

porsi delle domande. È indubbio che certe dinamiche infortunistiche, probabilmente favorite da un difetto di comunicazione/coordinamento o da un'autorizzazione che non doveva arrivare, dovrebbero e potrebbero essere evitate con il rispetto delle norme, un'adeguata formazione e l'applicazione di idonee procedure e prassi.
A breve partirà una campagna europea che parla di nuove tecnologie, di applicazioni digitali ma poi, come scritto in un interessante articolo del Corriere della Sera (" La sicurezza ferma all'800"), in certi casi sembra di essere rimasti nel passato. Nel 2023 parliamo delle novità dell' intelligenza artificiale, ma nel traffico ferroviario può mancare, come ricorda l'articolo, "un sistema di doppio controllo". E se il più avanzato sistema di sicurezza del traffico (Ertms - European rail traffic management system) oggi copre "900 chilometri su 1.500 della rete ad alta velocità", bisogna comunque arrivare a migliorare gli standard su tutta la rete ferroviaria.
Ma non è nostro compito, oggi, l'analisi dell'infortunio o delle cause e responsabilità per le quali sono ancora in corso delle indagini.
Nostro compito è quello di cercare di fornire qualche spunto di riflessione e qualche indicazione per una eventuale migliore prevenzione del rischio di investimento nelle aree ferroviarie, di cui avevamo recentemente parlato anche in un " Imparare dagli errori", rubrica che racconta gli infortuni professionali.
Rimandando, dunque, ad eventuali articoli futuri l'analisi e l'approfondimento del gravissimo incidente sul lavoro di pochi giorni fa, cerchiamo oggi di comprendere quali materiali possono essere disponibili in rete sul tema della prevenzione degli infortuni in ambito ferroviario.
Un documento disponibile, considerando tuttavia le possibili differenze normative e organizzative tra Italia e Svizzera, è stato prodotto dall'Istituto elvetico per l'assicurazione e la prevenzione degli infortuni (Suva).
Il documento - dal titolo "10 regole vitali per chi lavora nelle ferrovie. Vademecum" contiene dieci diversi principi salvavita, non connessi solo al rischio di investimento.
Ci soffermiamo in particolare su alcune delle regole e indicazioni con riferimento ai seguenti argomenti:

I rischi lavorativi nelle ferrovie: la pianificazione e le responsabilità
I rischi lavorativi nelle ferrovie: la zona dei binari e le regole di sicurezza

(continua)
https://www.puntosicuro.it/trasporti-magazzinaggio-C-27/il-rischio-nelle-ferrovie-l-incidente-di-brandizzo-la-prevenzione-AR-23620
***Punto Sicuro** – Tiziano Menduto, 4 settembre 2023*

Il lavoro ferroviario e la storia infinita dei ritardi normativi - Con riferimento al recente incidente di Brandizzo, un contributo si sofferma sulla tutela della salute e sicurezza nel settore ferroviario. La storia infinita dei ritardi legislativi, l'obsolescenza delle norme e la necessità dell'armonizzazione.
Urbino, 6 Set – Come ricordato in un precedente articolo sul gravissimo incidente ferroviario avvenuto a Brandizzo e sulla prevenzione nella rete ferroviaria, di fronte ai tragici fatti accaduti nella notte del 31 agosto 2023 non ci si può limitare a manifestare sdegno e dolore, ma, "nel pieno rispetto dell'attività degli organi inquirenti", si ha anche "il dovere di interrogarsi su di una vicenda che tuttora riguarda la prevenzione dei rischi lavorativi nel settore ferroviario".
In particolare, con riferimento agli "espliciti e complessi rinvii tra le fonti del diritto evocate" dal Decreto legislativo 81/2008 nonché agli "impliciti e indefiniti rinvii dell'attuazione di alcune di esse". Una vicenda, questa, che "continua ad evidenziare preoccupanti incertezze rispetto ad una trama normativa che affonda le proprie radici in provvedimenti risalenti nel tempo e che oggi debbono confrontarsi con una realtà in profonda trasformazione".

A sottolinearlo e a fornire utili riflessioni sul tema della sicurezza nel lavoro ferroviario è un recente intervento di Paolo Pascucci (professore ordinario di Diritto del lavoro nell'Università di Urbino Carlo Bo) pubblicato sul numero 1/2023 di "Diritto della sicurezza sul lavoro", rivista online dell'Osservatorio Olympus dell' Università degli Studi di Urbino.
L'intervento "La tutela della salute e sicurezza dei lavoratori nel settore ferroviario, tra norme generali e norme speciali", dedicato alla memoria delle cinque vittime dell'incidente, riprende un precedente intervento presentato nel 2022 e nel 2023 nell'ambito del Corso di formazione per gli operatori dei Servizi di prevenzione delle ASL sul tema "Strumenti e indicazioni operative per la vigilanza nel settore ferroviario".
Il saggio analizza, come indicato nell'abstract dell'intervento, la "trama delle fonti normative che disciplinano la salute e la sicurezza sul lavoro in ambito ferroviario sottolineando come, a quindici anni dall'emanazione del d.lgs. n. 81/2008, non siano stati ancora emanati i decreti di armonizzazione tra la disciplina della vecchia legge n. 191/1974 e lo stesso d.lgs. n. 81/2008 e come questo grave ritardo rischi di creare non pochi problemi interpretativi con preoccupanti ripercussioni sulla tutela della salute e della sicurezza dei lavoratori".
Nel presentare l'intervento ci soffermiamo, in particolare, sui seguenti temi:
La sicurezza nel settore ferroviario e la storia infinita dei ritardi
La sicurezza nel settore ferroviario e l'obsolescenza normativa
Ascoltare la voce assordante di chi non può più avere voce
(continua)
https://www.puntosicuro.it/trasporti-magazzinaggio-C-27/il-lavoro-ferroviario-la-storia-infinita-dei-ritardi-normativi-AR-23632
***Punto Sicuro** – Tiziano Menduto, 6 settembre 2023*

China's Winnti APT Compromises National Grid in Asia for 6 Months
Attacks against critical infrastructure are becoming more commonplace and, if a recent PRC-sponsored attack is anything to go by, easier to pull off.
A Chinese threat actor managed to breach the national power grid in an unnamed Asian country earlier this year, compromising multiple computers and using a popular remote access Trojan (RAT) to steal sensitive data.
The perpetrator — an entity within Winnti Group, also known as APT41, Bronze Atlas — has a history of taking on some of the most high-level cyber espionage conducted by the People's Republic of China (PRC), including campaigns against hostile governments and industries abroad. Its wide-ranging and successful campaigns have earned it attention from international law enforcement to a degree matched only by the world's most prolific nation-state and cybercriminal groups.
In this latest campaign, a subsect within Winnti known as "Redfly" or "Red Echo" managed to occupy the network of an Asian national electricity provider for half a year, deploying a Trojan called "ShadowPad" to harvest credentials and obtain privileged information.
According to Dick O'Brien, principal intelligence analyst for the Symantec threat hunter team, this latest case of critical infrastructure attack signals a worrying trend for the sector on the whole. "I think it can be very easy to hear the warnings but not to do anything until something really bad happens," he warns. "The worst case scenario is quite rare, but it does happen from time to time."
Winnti Attack Against a Grid
Researchers from Symantec traced the campaign back to Feb. 28 when ShadowPad was deployed in a single computer in the target network.

ShadowPad, first discovered eight years ago, is a modular backdoor in shellcode format. Like its successor — the long-running PlugX family of Trojans — it was at one point briefly shared with select buyers in the cyber underground, but is generally seen in correlation with Chinese state-sponsored attacks.
In this campaign, the attackers used a distinct variant of ShadowPad which copies itself to disk, disguised as VMWare files and directories.
Redfly deployed ShadowPad for a second time in the target network on May 17, indicating that it had maintained persistence in the three months interim. *(continua….)*
https://www.darkreading.com/ics-ot/chinas-winnti-apt-compromises-national-grid-in-asia-for-6-months
DARKREADING- *Nate Nelson -September 12, 202*

LOCKBIT RANSOMWARE GANG HIT THE CARTHAGE AREA HOSPITAL AND THE CLAYTON-HEPBURN MEDICAL CENTER IN NEW YORK

LockBit ransomware group breached two hospitals, the Carthage Area Hospital and the Clayton-Hepburn Medical Center in New York.
The Lockbit ransomware group claims to have hacked two major hospitals, the Carthage Area Hospital and Claxton-Hepburn Medical Center. The two hospitals serve hundreds of thousands of people in upstate New York.
The cyberattack took place at the end of August and had a severe impact on the two hospitals in the last couple of weeks. The phone systems were restored on September 2, however the cyberattacks impacted several other services. As a precaution, the emergency rooms at Carthage and Claxton have been put on diversion, the patients were hijacked to other area hospitals and most of the appointments were rescheduled.
he two hospitals are still struggling to recover from cyberattacks.
The FBI launched an investigation into the incident along with the New York State Department of Health and the Division of Homeland Security and Emergency Services. *(continua…)*
https://securityaffairs.com/150835/cyber-crime/lockbit-ransomware-carthage-area-hospital.html
Securityaffairs *-Pierluigi Paganini- September 14, 2023*

AI language models need to shrink; here's why smaller may be better

Large language models (LLMs) used for generative AI tools can consume vast amounts of processor cycles and be costly to use. Smaller, more industry- or business-focused models can often provide better results tailored to business needs**.**
Large language models (LLMs) often appear to be in a fight to claim the title of largest and most powerful, but many organizations eyeing their use are beginning to realize big isn't always better.
The adoption of generative artificial intelligence (genAI) tools is on a steep incline. Organizations plan to invest 10% to 15% more on AI initiatives over the next year and a half compared to calendar year 2022, according to an IDC survey of more than 2,000 IT and line-of-business decision makers.
And genAI is already having a significant impact on businesses and organizations across industries. Early adopters claim a 35% increase in innovation and a 33% rise in sustainability because of AI investments over the past three years, IDC found.
Customer and employee retention has also improved by 32%. "AI will be just as crucial as the cloud in providing customers with a genuine competitive advantage over the next five to 10 years," said Ritu Jyoti, a group vice president for AI & Automation Research at IDC.
"Organizations that can be visionary will have a huge competitive edge."

While general purpose LLMs with hundreds of billions or even a trillion parameters might sound powerful, they're also devouring compute cycles faster than the chips they require can be manufactured or upscaled; that can strain server capacity and lead to an unrealistically long time to train models for a particular business use.
"Sooner or later, scaling of GPU chips will fail to keep up with increases in model size," said Avivah Litan, a vice president distinguished analyst with Gartner Research. "So, continuing to make models bigger and bigger is not a viable option." *(continua…)*
https://www.computerworld.com/article/3706510/ai-language-models-need-to-shrink-heres-why-smaller-may-be-better.html
Computerworld - *Lucas Mearian - SEP 14, 2023*

Attacchi informatici in aumento, colpite soprattutto le piccole e medie imprese.
"Il numero degli attacchi informatici cresce costantemente, rispetto allo scorso anno è cresciuto con un incremento di vittime del 185% e l'80% di queste corrisponde al mondo della piccola e media impresa". A spiegarlo è Pierguido Iezzi, esperto di cyber sicurezza e autore del volume "Cyber e potere".
"Ogni attacco informatico nasce da una fase di ricognizione- spiega Iezzi- in cui l'attaccante cerca di identificare una serie di informazioni, pubbliche e semi pubbliche, che terzi hanno pubblicato e hanno reso disponibili".
Nella classifica degli attacchi l'Italia è al terzo posto, dopo Stati Uniti e Giappone. Sul tema è intervenuto il ministro delle Imprese e del Made in Italy Adolfo Urso che ha dichiarato che il tema della cybersecurity "è centrale" e "cornice prodromica a ogni attività in rete". *(continua….)*
https://www.rainews.it/articoli/2023/09/attacchi-informatici-in-forte-aumento-aumento-urso-cybersicurezza-e-una-necessita-e-opportunita-ef08f83a-2f6d-406d-bc4d-bb55771a2f12.html#:~:text=%E2%80%9CIl%20numero%20degli%20attacchi%20informatici,della%20piccola%20e%20media%20impresa%E2%80%9D.
Rai News *– Maria Vittoria Savini – 14/09/2023*

La Soyuz si è agganciata alla Iss: salgono a bordo due russi e un'americana
Due cosmonauti russi e un'astronauta statunitense sono arrivati a bordo di una capsula Soyuz sulla Stazione Spaziale Internazionale (ISS) venerdì, nell'unico caso di **cooperazione nonostante le profonde tensioni tra Mosca e Washington**. Il veterano **cosmonauta russo Oleg Kononenko** e il suo **compagno Nikolai Tchoub**, insieme all'**astronauta della NASA Loral O'HaraLeur**, hanno lasciato il cosmodromo russo di Baikonur, in Kazakistan, alle 15:44 GMT come previsto, a bordo del razzo Soyuz MS-24. L'equipaggio è arrivato alla ISS tre ore dopo, ha annunciato l'agenzia spaziale russa in un comunicato stampa. I tre astronauti sostituiranno i russi Sergei Prokopiev e Dmitri Peteline e l'americano Frank Rubio, arrivati a bordo della ISS un anno fa. La loro missione era stata prolungata a causa di un danno alla navicella di rientro, la Soyuz MS-22, che ha subito una spettacolare perdita mentre era agganciata alla ISS nel dicembre 2022, dovuta, secondo Mosca, all'impatto di un micrometeorite. *(continua…)*
https://www.rainews.it/articoli/2023/09/la-navicella-soyuz-si-e-agganciata-alla-iss-due-russi-e-un-americano-salgono-a-bordo-f1132064-3f9b-45d7-9309-6f5a92095502.html
Rai News *– Spazio – 15/09/2023*

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

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.

NOTIZIE D'INTERESSE:

Le indicazioni per chi vuole iscriversi come nuovo socio sono contenute nel sito AIIC al link *http://www.infrastrutturecritiche.it/new/per-iscriversi/*

Preghiamo i soci che, per vari motivi, modificano la loro anagrafica (recapiti telefonici, indirizzo email o altro) di comunicare I nuovi dati a segreteria@infrastrutturecritiche.it. La mancanza di tali comunicazioni potrebbe impedire, al socio, la ricezione delle comunicazioni.

RIFERIMENTI DELL'ASSOCIAZIONE

AIIC è una associazione apolitica il cui scopo è promuovere attività e conoscenze nell'ambito delle infrastrutture critiche, della loro gestione, protezione e sicurezza.

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

Per ricevere questa newsletter è necessario inviare una richiesta all'indirizzo
segreteria@infrastrutturecritiche.it

L'iscrizione alla newsletter NON comporta alcun onere e non è richiesta la comunicazione di alcun dato personale ad eccezione dell'indirizzo di posta elettronica.

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335

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

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