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

Newsletter

ANNO 2024 | **n. 06/ 2024** | **giugno 2024**

Il futuro della certificazione cyber-security

La relazione dell'Agenzia per la cybersecurity nazionale (Acn) al Parlamento relativa al 2023 parla dei risultati raggiunti e degli investimenti effettuati nell'ambito della sicurezza.
Il 2024 sarà un anno transitorio. Si recepirà la Nis 2 e si implementerà lo schema europeo di certificazione di prodotto per la cyber-security a seguito della pubblicazione dello schema da parte della Commissione europea, avvenuto all'inizio di quest'anno. Con questo arriveranno anche uno schema specifico per il 5G e uno per il cloud. Ne seguiranno altri, suddivisi per tecnologia e per campo di applicazione.
Lo schema di certificazione per la cyber-security di prodotto basato sui Common criteria (Eucc) di livello europeo è stato pubblicato il 31 gennaio 2024. Copre livelli definiti sostanziali o alti: i certificati Eucc di livello sostanziale corrispondono a quelli che coprono i livelli 1 e 2 degli Ava_Van, ossia i livelli di sicurezza delle analisi di vulnerabilità collegate ai Common criteria. I certificati Eucc di livello alto corrispondono a quelli che coprono i livelli 3, 4 e 5 degli Ava_Van. I certificati saranno basati su protection profile come già previsto dallo standard dei Common criteria.
Nel frattempo, dodici sono i certificati Common criteria emanati dall'Ocsi, l'Organismo di certificazione della sicurezza informatica, operante ora all'interno della Acn, nel 2023, in attesa che lo schema europeo abroghi definitivamente lo schema nazionale di certificazione Common criteria emanato del 2003 e oggi ancora operativo.
Sono più di cento i procedimenti Cvcn di scrutinio realizzati nel 2023 per l'impiego di prodotti dell'Ict su servizi del Psnc, mentre sono circa 180 le valutazioni tra tecnologia 5G, notifiche con profili di cyber-security e pre-notifiche realizzate dal Cvcn in applicazione del golden power.
Accanto a questi obiettivi raggiunti fa capolino un altro risultato positivo: l'accreditamento dei laboratori di prova che affiancheranno il Cvcn nelle attività di verifica e certificazione. Cinque laboratori sono ad oggi in corso di valutazione. Tale processo richiede un significativo investimento da parte delle aziende in termini economici e strutturali, nonché di risorse umane. La Acn ha ammesso 27 aspiranti laboratori alla possibilità di un finanziamento in ambito Pnrr per coprire le spese del procedimento di accreditamento. Tuttavia il poco personale disponibile sul mercato per svolgere il ruolo professionalmente rilevante di valutatore disincentiva molto le aziende.
Per quanto riguarda la situazione degli attacchi, il report Clusit evidenziava come nel 2023 il settore più colpito sia stato quello governativo-militare con il 19% degli attacchi, seguiva il comparto manifatturiero con il 13% delle violazioni. Il 30% circa di attacchi viene invece evidenziato nella relazione Acn come indirizzato a Pa locali e centrali, mentre qui il settore manifatturiero risulta target al 4% e le telecomunicazioni hanno il primato con un 20% secco di attacchi. La quantità di attacchi alla Tlc denuncia che sta proseguendo quello che potremmo chiamare un dislocamento di truppe cibernetiche nei sistemi dell'infrastruttura che, insieme a quella energetica, è la più critica.

Quest'ultima scende, rispetto agli anni passati, al circa 6%, attestandosi su valori che ricordano sempre il dislocamento di truppe cibernetiche pronte all'uso, ma con una maggiore capacità che potremmo definire chirurgica.
(da Airpress n. 155, maggio 2024)

Luisa Franchina
presidente dell'Associazione Italiana esperti in Infrastrutture Critiche

Luisa Franchina 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.

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2024

Il 31 dicembre 2023 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare con sollecitudine l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2024".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it.
Ricordiamo che **la data limite per il rinnovo annuale, come da regolamento, è fissata al 31 marzo 2024. 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.**
La nostra segreteria è a disposizione, per informazioni, alla mail segreteria@infrastrutturecritiche.it.

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*

GRUPPO DI LAVORO AIIC
Critical Infrastructures Resilience and Artificial Intelligence
(Resilienza delle Infrastrutture Critiche e Intelligenza Artificiale)

Si è svolta il 30 maggio scorso la prima riunione del nuovo Gruppo di Lavoro AIIC sulla Critical Infrastructure Resilience and Artificial Intelligence.

Coordinatore: Sandro Bologna
Data inizio lavori: 01.06.2024
Durata max: 12 mesi
Lingua di redazione: inglese

Tutte le informazioni di dettaglio e un indice degli argomenti che verranno trattati sono presenti nella Homepage del sito AIIC. Questo indice fornisce un quadro completo per esplorare le interconnessione tra resilienza, infrastrutture critiche e intelligenza artificiale, che coprono vari aspetti come la comprensione della resilienza, le applicazioni di intelligenza artificiale, i casi di studio, la valutazione

dei rischi, le considerazioni politiche, le innovazioni tecnologiche, l'etica, le implicazioni e direzioni future.
La partecipazione al Gruppi di Lavoro AIIC è riservata ai Soci AIIC in regola con i pagamenti associativi.

WEBINAR AIIC SVOLTI

La Direttiva (UE) 2022/2557 sulla resilienza dei soggetti critici
(Critical Entities Resilience)

mercoledì 12 giugno 2024

La nuova direttiva CER completa il panorama normativo europeo sulle infrastrutture critiche, riconciliando, in un mutato quadro geopolitico, la sicurezza negli ambiti cibernetico e cinetico, in una prospettiva all-hazard e risk-based, prevedendo norme armonizzate volte a garantire la fornitura di servizi essenziali nel mercato interno, a migliorare la resilienza degli operatori pubblici e privati, ora definiti soggetti critici, e la cooperazione transfrontaliera tra le autorità competenti, mutuando, di massima, il quadro regolatorio già adottato per il settore dei trasporti, in particolare nell'ambito dell'aviazione civile.

Il webinar è stato tenuto da Alberto Caruso de Carolis.

COLLABORAZIONE ALLE ATTIVITA' AIIC

Si invitano tutti i soci a partecipare alle attività sociali (newsletter, webinar, ecc.) inviando articoli, segnalazioni o dando la disponibilità a tenere webinar o seminari o a partecipare alla stesura e redazione della newsletter mensile.
La mail cui scrivere è segreteria@infrastrutturecritiche.it

NEWS E AVVENIMENTI

GE Ultrasound Gear Riddled With Bugs, Open to Ransomware & Data Theft
Thankfully, GE ultrasounds aren't Internet-facing. Exploiting most of the bugs to cause serious damage to patients would require physical device access.
Researchers have discovered 11 security vulnerabilities in GE HealthCare's Vivid Ultrasound family of products, as well as two related software programs.
The issues are varied, and include missing encryption of sensitive data, use of hardcoded credentials, and more. They range in severity from 5.7 to 9.6 on the CVSS 3.1 scoring system.

As Nozomi Networks explained in its report, the bugs could lead to remote code execution (RCE) with full privileges and any number of attack scenarios such powers would entail. However, the most serious case scenarios also require physical access to the devices in question, massively reducing the potential risk for healthcare facilities.
However, "even when talking about vulnerabilities that indeed require physical access for being exploited, we believe that the likelihood of an attack is far from being negligible," warns Andrea Palanca, senior security researcher with Nozomi Networks. "As a matter of fact,ultrasound machines are used in hospitals and clinics that are frequently accessed by external individuals, and our research showed that just one minute of physical access is sufficient to execute an attack.So, we feel that not only malicious insiders, but also outsiders may have chances to accomplish the attack."
The Bad News
In the course of their study, Nozomi's researchers analyzed three GE creations: the Vivid T9 ultrasound system, designed primarily for cardiac imaging; its pre-installed Common Service Desktop Web application, used for various administrative purposes; and the EchoPAC clinical software package, which doctors use to review and analyze ultrasound images.(continua…)
https://www.darkreading.com/vulnerabilities-threats/ge-ultrasound-gear-riddled-with-bugs-open-to-ransomware-data-theft
DARKREADING *_Nate Nelson-May 16, 2024*

Eccellenza e fiducia nell'intelligenza artificiale - Un'intelligenza artificiale (IA) affidabile può portare molti benefici, quali migliori cure sanitarie, trasporti più sicuri e puliti, processi di produzione più efficienti ed energia più economica e sostenibile. L'approccio dell'UE all'IA permetterà ai cittadini di far proprie tali tecnologie con convinzione, incoraggiando nel contempo le imprese a svilupparle.
L'UE e l'IA
L'intelligenza artificiale (IA) può contribuire a trovare soluzioni a molti dei problemi della società. Ciò è possibile solo se la tecnologia è di alta qualità e viene sviluppata e usata in modo da guadagnare la fiducia dei cittadini. Con un quadro strategico europeo basato sui valori dell'UE si potrà dunque infondere nei cittadini la fiducia necessaria perché accettino soluzioni incentrate sull'IA, incoraggiando nel contempo le imprese a svilupparle e diffonderle.
Per questo motivo la Commissione europea ha proposto una serie di azioni volte a promuovere l'eccellenza nell'IA e norme volte a garantire che la tecnologia sia affidabile.
Il regolamento su un approccio europeo all'intelligenza artificiale e l'aggiornamento del piano coordinato sull'IA garantiranno la sicurezza e i diritti fondamentali delle persone e delle imprese, rafforzando nel contempo gli investimenti e l'innovazione nei paesi dell'UE. *(continua).*
https://www.puntosicuro.it/digitalizzazione-C-147/eccellenza-fiducia-nell-intelligenza-artificiale-AR-24218/
Punto Sicuro – *Redazione, 28/05/2024*

Rete idrica smart come l'elettrica, grazie all'IoT sostenibile - Grazie a dispositivi intelligenti, a bassa potenza e basso costo ma sempre connessi, chi gestisce il sistema idrico diventa in grado di minimizzarne le perdite, potendo conoscere i consumi in modo capillare e puntuale. Con questi "nuovi" dati, si riesce anche a massimizzare il proprio business, sempre garantendo a tutti il servizio idrico e abilitandone anche altri in chiave Smart City
Prima era forse necessario viaggiare, visitando alcuni Paesi o aree definite "a rischio" per toccare con mano e sperimentare sulla propria pelle che l'acqua non è una risorsa infinita e neppure scontata. Negli

ultimi anni, da quando hanno iniziato a spuntare titoli che “denunciano” il divieto di innaffiare giardini e aiuole a nostro piacimento, l’emergenza idrica ha fatto ufficialmente ingresso nella quotidianità anche dei cittadini italiani. Qualcuno ha iniziato a chiudere il rubinetto più spesso, a velocizzare la doccia e ad adottare comportamenti più virtuosi, incoraggiato da vademecum e indicazioni di esperti e influencer. Sempre di più, però, è emersa la chiara necessità di azioni su larga scala, meglio se con l’utilizzo di quelle tecnologie su cui in altri ambiti, anche meno essenziali, investiamo già da diversi anni.
Indice degli argomenti
Il monitoraggio dei consumi e la svolta data driven
Tecnologia e business a braccetto verso il futuro
Dall’IoT “idrico” una spinta ai servizi per smart city
(continua…)
https://www.zerounoweb.it/cio-innovation/rete-idrica-smart-come-lelettrica-grazie-alliot-sostenibile/
ZeroUnoWeb *– Marta Abba', 3 giu 2024*

Russia Aims Cyber Operations at Summer Olympics

As always, Russian APTs are hoping to foment unrest by stoking existing societal divides and fears, this time around the Olympics and EU politics; and, concerns remain around physical disruption.
Two Russian state-aligned threat actors have been carrying out online influence operations designed to undermine the upcoming Olympic Games in Paris.
For a year now, Storm-1679 and the recently disrupted Storm-1099 (aka "Doppelganger") have been spreading fake news, doctored images, and artificial intelligence (AI)-aided videos about the Olympics on social media. According to a Microsoft report this week, the goal seems to be twofold: harm the reputation of the International Olympic Committee (IOC) (which has banned Russia in the past), and stoke fears around potential violence at the Summer Games.
Time will tell whether these operations are a precursor to more direct cyberattacks during the Games themselves.
Last June, Storm-1679 published to Telegram a full feature-length movie titled "Olympics Has Fallen," a play on the popular 2013 blockbuster "Olympus Has Fallen." It came with all the bells and whistles: a fake Netflix intro, fake five-star reviews from major US newspapers, slick special effects, and narration from an AI-generated voice resembling Tom Cruise. The group spread its masterpiece on social media, even commissioning celebrities on Cameo to unwittingly help promote it.
In months since, Storm-1679 has developed as an auteur with videos pretending to come from the CIA, France's General Directorate for Internal Security (DGSI), French broadcaster France24, and the Belgium-based Euro News. All of these videos carried the same theme: warning viewers about terrorist threats to the summer games, in one creative way or another.
In comparison, Storm-1099 has taken a relatively more straightforward approach to fake Olympics-themed content. Particularly in the last couple of months, the group has been using 15 French-language fake news websites to spread rumors about corruption in the IOC, fears about purported violence to come in July, and criticisms of French president Emmanuel Macron.
Concerns About Physical Attacks on Paris Olympics (continua…)
https://www.darkreading.com/threat-intelligence/russia-cyber-operations-summer-olympics
DARKREADING- *Nate Nelson- June 3, 2024*

Ransomware Attack Disrupts Operations Across London Hospitals

The incident affecting pathology-services provider Synnovis demonstrates the ripple effect that cyberattacks have on healthcare systems, and demands immediate security response.

A ransomware attack this week on UK healthcare provider Synnovis has forced several London hospitals to cancel services and surgeries, or redirect them to other facilities. The incident occurred Monday and has had a significant impact on their ability to deliver patient care, demonstrating once again the ripple effect that modern cyberattacks have on healthcare systems, demanding an immediate security response.

Synnovis — a partnership between two London-based hospital trusts and SYNLAB — said June 4 that it was the victim of a ransomware attack the day before that affected all of its IT systems, "resulting in interruptions to many of our pathology services," according to a post on the company's website. Even before the company officially acknowledged the attack, however, social media posts already were reporting the effect it was having on the services of major London hospitals.

One of the key services that Synnovis provides are blood transfusions, which meant that some facilities — including King's College Hospital, Guy's Hospital, St Thomas' Hospital — had to cancel operations. Meanwhile, transplant surgeries at Royal Brompton and Harefield Hospital also were "axed," according to a post on X by Shaun Lintern, health editor at the UK's Sunday Times newspaper. Lintern included a screenshot of a letter sent by the CEO of Guy's and St Thomas NHS Foundation Trust to inform facilities of the situation, mentioning the "major effect" it was having on some facilities.

The UK National Health Service (NHS) also weighed in with a statement on Tuesday, noting that the incident forced hospitals to "prioritize" urgent work. Emergency services across the UK continued to be available as usual, and the NHS directed patients to attend scheduled appointments unless informed otherwise.

Cyberattacks Have Human Consequences

The attack demonstrates once again how repercussions of ransomware attacks can extend "beyond operational and financial disruptions" and into the sphere of public health and well-being, notes one security expert.

The attack directly impacted and endangered patient health, which "not only highlights the immediate impact of ransomware attacks on healthcare facilities but also erodes public trust in the very institutions responsible for safeguarding our health and well-being," says Kevin Kirkwood, deputy CISO at LogRhythm.

Indeed, high-impact attacks on healthcare providers have been ramping up recently, with several high-profile attacks occurring in the US earlier this year. In February, United Healthcare's Change Healthcare was hit by not one but two attacks, a nightmare for the healthcare provider that didn't end even after it paid the ransom demanded by a Black Cat/ALPHV ransomware affiliate**.** (continua…)

https://www.darkreading.com/cyberattacks-data-breaches/synnovis-ransomware-attack-disrupts-operations-london-hospitals

DARKREADING *Elizabeth Montalbano, June 5, 2024*

Trasformazione Urbana "Intelligente": come diventare una smart city - Come la tecnologia plasmerà le città di domani, mettendo in atto una trasformazione urbana intelligente dove digitalizzazione e efficienza avranno un ruolo chiave. Dalla smart mobility, alla smart energy, passando per gli edifici intelligenti fino ad approdare ai sistemi dotati di IoT e IA

Le città giocano un ruolo chiave nel processo di decarbonizzazione essendo responsabili del 70% delle emissioni di gas

Il ruolo delle città nel percorso verso la transizione ecologica non può più essere trascurato. Potrebbero apparire come realtà limitate rispetto alla superficie mondiale, eppure la metà dei quasi 8 miliardi di persone che oggi abitano il Pianeta Terra vive in città, e la cifra è destinata a crescere esponenzialmente da qui al 2050. Ecco perchè è indispensabile ripensare il nostro approccio alla pianificazione, introducendo criteri di trasformazione urbana capaci di garantire al contempo spazi più vivibili per i cittadini, più efficienti nell'uso delle risorse energetiche, resilienti sotto il profilo dei cambiamenti climatici ed adattabili ad un futuro in trasformazione dove sicurezza e prevenzione saranno cruciali.

Gli strumenti per accelerare quest'evoluzione verso città più sostenibili sono molteplici e in gran parte già a nostra disposizione. Il fil-rouge che unisce tutti gli interventi è la digitalizzazione, la componente "smart" capace di ottimizzare le risorse, ridurre i consumi, efficientare i servizi, migliorare la qualità abitativa e la mobilità, ma anche anticipare esigenze future o prevenire eventi catastrofici.

(continua…)

https://www.rinnovabili.it/green-building/smart-city/trasformazione-urbana-intelligente-benefici-tecnologie/

Rinnovabili.it *– Alessia Bardi, 6 Giugno 2024*

IA, i rischi cyber che ceo e cda devono conoscere

L'intelligenza artificiale rivoluziona industria e società, richiedendo alle aziende di sfruttare i dati per ottenere vantaggi competitivi. La trasformazione include rischi di cybersecurity e questioni di proprietà intellettuale, necessitando di cambiamenti strategici e culturali guidati dal consiglio di amministrazione. La supervisione della cybersecurity è fondamentale per la resilienza aziendale e la gestione delle crisi **dell'industria e della società**, con molti che prevedono un impatto paragonabile a quello dell'elettricità durante la rivoluzione industriale.

Trasformare un'azienda in un'organizzazione guidata dall'AI è un'impresa complessa, sistemica e di lungo termine che richiede a tutte le aziende di potenziare, proteggere e sfruttare il loro bene più prezioso in questo nuovo mondo: i dati.

Questa trasformazione richiede **un cambio strategico, culturale e organizzativo** guidato direttamente dall'amministratore delegato e dal consiglio di amministrazione.

Indice degli argomenti

Il rischio crescente della cyber security nell'era dell'AI

L'ascesa dell'AI aumenta inoltre i rischi connessi alla cybersecurity. Tuttavia, poiché la cybersecurity è stata oggetto di attenzione per molti anni, alcune aziende hanno sviluppato un falso senso di sicurezza. Per i consigli di amministrazione e gli amministratori delegati, sarà sempre più

importante rinnovare la loro attenzione sui rischi informatici e implementare metodologie e pratiche più sofisticate.

L'emergere dell'AI generativa: opportunità e rischi

L'emergere dell'AI generativa (GenAI) e del machine learning, inclusi i modelli basati su tecnologie di linguaggio come **ChatGPT**, crea innumerevoli opportunità e rischi per le aziende che molti consigli stanno solo iniziando a comprendere. Le opportunità includono la creazione di business adiacenti per monetizzare gli asset dati, migliorare i percorsi e il servizio clienti, automatizzare compiti qualificati e ottimizzare il processo decisionale e l'efficienza in aree come previsioni di vendita, gestione dell'inventario, gestione/efficienza operativa, controllo di qualità, miglioramenti nella produzione e programmazione informatica, solo per citarne alcuni.

La questione dei diritti di proprietà intellettuale nell'AI generativa

Un problema attualmente oggetto di contenzioso è inoltre **la questione dei diritti di proprietà intellettuale e dell'AI generativa**. Quando gli ingegneri del software utilizzano GenAI per sviluppare codice, per esempio, è finora incerto chi possieda i diritti di proprietà intellettuale su questo codice. I modelli AI sono "addestrati" su vasti set di dati, il che significa che è fondamentale comprendere non solo l'accuratezza del modello, ma anche i dati su cui è stato addestrato, e come vengono utilizzati e protetti i dati proprietari o sensibili. Ad esempio, le informazioni condivise con ChatGPT nelle conversazioni con gli utenti sono memorizzate per migliorare l'accuratezza dell'algoritmo. Questo rappresenta una sfida per l'uso di queste tecnologie per le aziende che hanno bisogno di proteggere dati sensibili di clienti o aziendali. Molte aziende GenAI stanno sviluppando versioni aziendali chiuse dei loro modelli per migliorare la privacy, ma queste soluzioni sono ancora nelle fasi molto iniziali di sviluppo.(continua…)

https://www.agendadigitale.eu/sicurezza/ia-e-rischi-cyber-strategie-e-responsabilita-di-consigli-di-amministrazione-e-ceo/

AGENDA DIGITALE – *Fabio Moioli 6 giu 2024*

L'IA in Sanità: applicazioni, rischi e compliance normativa

L'introduzione dell'IA in sanità rivoluziona il settore, incrementando sia l'efficienza che i rischi. Il regolamento europeo AI Act e la direttiva NIS2 stabiliscono requisiti rigorosi per garantire sicurezza e conformità. La gestione del rischio cyber implica approcci olistici e contratti robusti per mitigare vulnerabilità e garantire continuità operativa

La **pervasiva introduzione di sistemi di intelligenza artificiale** in pratica in ogni settore, pubblico e/o privato, è un dato che possiamo dare come acquisito, così come anche la grande profusione di sforzi e risorse per l'evoluzione e il miglioramento dei modelli. Così come anche si deve registrare la rapidità con cui la complessità e l'ampiezza di questi sistemi sta crescendo.

Per quanto sia una tecnologia frutto di una ricerca pluridecennale, le sue ulteriore evoluzioni e possibili sviluppi sono a**ncora difficilmente prevedibili,** rappresentando un caso, forse IL caso di ignoto tecnologico.

Nel frattempo, mentre ancora se ne mappano e registrano i rischi intrinsechi, sviluppare ed adottare sistemi di IA è divenuto **un fattore competitivo discriminante** che a diversi livelli "obbliga" all'adozione di queta tecnologia, sia per ottimizzare processi (ridurre tempi e consti) ma anche per rispondere alle richieste del mercato e delle scelte dei "consumatori".

Appare intuitivo che questa adozione precoce di una tecnologia che ha ancora molteplici elementi "incogniti", presenti **livelli di rischio più o meno rilevanti** in dipendenza della sensibilità del settore di applicazione.

Indice degli argomenti

L'IA in Sanità: vantaggi e rischi

Una delle applicazioni che certamente può definirsi sensibile è quella nel settore sanitario.
Affrontare correttamente la questione dei rischi (e della gestione di questi) delle applicazioni dei sistemi di IA in sanità, rende necessario alcune precisazioni preliminari.
Il sistema sanitario, è un sistema sociotecnico complesso che ha come punto di emersione le erogazioni di prestazioni di assistenza sanitaria verso il pubblico, ma che, al contempo, non si esaurisce esclusivamente in quella.
Il sistema sanitario per attuarsi include: la scoperta e sviluppo del farmaco, le fasi di validazione clinica, logistica, stoccaggio, distribuzione, vigilanza sui farmaci, l'erogazione delle prestazioni, i processi di immissione sul mercato, pagamento e rimborso nonché "in esteso" anche il sistema di qualificazione delle professionalità impiegate, considerato l'impatto che la formazione ha sulla qualità delle prestazioni sanitarie erogate dal e nel sistema.
Ognuno di questi elementi è parte essenziale di quello che si definisce sistema sanitario ed ognuno di questi vede, con livelli diversi, applicazioni di Intelligenza Artificiale che parimenti ai vantaggi promessi, presentano specifici **rischi che impattano sul sistema sanitario nel suo complesso.**
La qualità (e la sicurezza) delle prestazioni erogate da un sistema sanitario, dipende dalla qualità di medicinali e terapie, dalla disponibilità di questi, dalla preparazione del personale medico e sanitario, incluso quello applicato alle attività amministrative. (continua….)

https://www.agendadigitale.eu/sanita/lia-in-sanita-applicazioni-rischi-e-compliance-normativa/
***Agendadigitale**-Gianluca Rotino- 7 giu 2024*

Cosa sappiamo del maxi attacco ransomware che ha colpito la sanità di Londra
Qilin, gruppo con sede in Russia, ha colpito Synnovis spingendo alcuni ospedali della capitale britannica a dichiarare lo stato d'emergenza. Il ransomware si conferma un problema globale nel settore
È stato uno dei più gravi attacchi informatici condotti di recente contro le istituzioni e i servizi pubblici del Regno Unito. I principali ospedali londinesi sono stati costretti a cancellare alcuni interventi chirurgici e molti hanno dichiarato lo stato d'emergenza. Ci sono stati problemi in particolare sulle trasfusioni di sangue e sui referti degli esami clinici. A essere stato colpito, lunedì, è stato Synnovis, nato da una partnership tra il Guy's and St Thomas' NHS Foundation Trust e il King's College Hospitals NHS Trust, che ospita il Synlab, il più grande fornitore di test e diagnostica medica in Europa. A colpire sembra essere stato il gruppo Qilin, con sede in Russia, specializzato in *ransomware-as-a-service* con la doppia estorsione, ovvero criptare i dati e minacciare di pubblicarli se non viene pagato un riscatto (che, in base alla linea indicata dal governo, non è previsto nel Regno Unito).
Il gruppo
Qilin, noto anche come Agenda, è attivo dal luglio 2022, secondo SentinelOne. A ottobre dello stesso anno quando ha lanciato la sua prima ondata di attacchi contro aziende tra cui la società francese Robert Bernard e la società australiana di consulenza informatica Dialog. Come detto l'approccio è quello del *ransomware-as-a-service*. Ciò consente agli hacker indipendenti di utilizzare gli strumenti e l'infrastruttura del gruppo in cambio di una percentuale compresa tra il 15 e il 20% dei proventi. Il colpo più recente è stato quello contro l'editore del giornale di strada *The Big Issue* a marzo: il gruppo ha distrutto i sistemi della società prima di rubare e pubblicare dati riservati. Dopo il rifiuto di pagare il riscatto, sono stati pubblicati sul dark web oltre 500 gigabyte di informazioni sottratte all'editore, tra cui le scansioni dei passaporti dei dipendenti e le informazioni sulle buste paga.(continua…)
https://formiche.net/2024/06/londra-la-sanita-target-preferito-ransomware/
Formiche- *Gabriele Carrer -07/06/2024*

Russian hacktivists vow mass attacks against EU elections
But do they get to wear 'I DDoSed' stickers?
A Russian hacktivist crew has threatened to attack European internet infrastructure as four days of EU elections begin on Thursday.
The NoName57(16) crew, which is one of the pro-Russia hacktivist gangs that sprung up shortly after the invasion of Ukraine, said seven other groups (plus "more teams that wish to remain anonymous") plan to participate in the plan to punish the EU for opposing the illegal invasion of Ukraine.
The digital assault, according to a post shared by Daily Dark Web, would be in retaliation for European Parliament-issued sanctions along with "Russophobia and double-standards of European authorities." They claim that the EU has ignored an alleged genocide in the Ukrainian region of Donbas – territory which is now under heavy attack from Russia.

And while the groups don't specify what they have planned, we'd assume any cyber attacks – if they materialize at all – will include the usual distributed denial of service (DDoS) disruption, which is the preferred menace from NoName and its fellow hacktivist crews like KillNet, Anonymous Russia, and the People's Cyber Army.
While NoName's earlier network-traffic-flooding attacks targeted Ukrainian websites, including media outlets, the gang has also claimed responsibility for DDoS attacks against European sites – usually in response to those governments' support of Ukraine.
More recently, some of these pro-Russia crews have turned their attention to attacking drinking water and other critical systems, prompting an alert from government agencies in the US, UK and Canada. In a May notice [PDF], the authorities warned of "pro-Russia hacktivists targeting and compromising small-scale OT systems in North American and European water and wastewater systems, dams, energy, food and agriculture sectors." (continua…)
https://www.theregister.com/2024/06/07/russian_hacktivists_eu_elections/
***TheRegister**- Jessica Lyons - Fri 7 Jun 2024*

NOTIZIE D'INTERESSE:

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

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

RIFERIMENTI DELL'ASSOCIAZIONE

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

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

ATTENZIONE

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

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

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Urbino 31 – 00182 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirsi al gruppo si può usare il link http://www.linkedin.com/ groups/96335
Versione stampabile della newsletter	Nella sezione "Newsletter"del sito http://www.infrastrutturecritiche.it è disponibile l'archivio delle Newsletter.
Comitato di Redazione	Alberto Traballesi Glauco Bertocchi Silvano Bari Gianluca Cipriani *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.