Newsletter

ANNO 2024	n. 03/ 2024	marzo 2024

150 Milioni per Innovazione e Tecnologia

Il decreto legge varato il 26 febbraio in Consiglio dei ministri contiene un investimento di 150 milioni di euro destinati a supportare startup e imprese che operano nei settori dell'intelligenza artificiale, della cybersecurity, del 5G, del quantum computing e delle telecomunicazioni.

L'implementazione del piano di investimento del governo mira ad imporsi attraverso le sfide con un approccio proattivo, focalizzandosi sull'ottimizzazione dei processi e sull'efficienza. La trasparenza e l'equità nei criteri di selezione sono priorità, con l'obiettivo di garantire che una vasta gamma di startup innovative possa beneficiare dei fondi. Inoltre, il programma è progettato per offrire un supporto continuativo alle aziende, promuovendo la loro crescita sostenibile nel contesto economico globale. I criteri di selezione per l'accesso ai finanziamenti includono l'innovatività del progetto, il potenziale di crescita e l'impiego di tecnologie avanzate. Le modalità di accesso prevedono una procedura di candidatura e valutazione per assicurare che i fondi siano assegnati alle iniziative più promettenti e in grado di contribuire significativamente alla trasformazione digitale dell'Italia. (https://www.mimit.gov.it/it/pnrr/progetti-pnrr/pnrr-finanziamento-di-start-up)

Nel 2024, Palazzo Chigi e l'Agenzia per la Cybersicurezza Nazionale (ACN) potranno utilizzare fino a 90 milioni di euro per fondi dedicati a tecnologie emergenti, inclusi intelligenza artificiale, quantum computing e cybersecurity. Avranno anche la possibilità di impegnare fino a 44,7 milioni di euro per il settore delle telecomunicazioni, concentrandosi sullo sviluppo del 5G e altre tecnologie come il mobile edge computing e il web3.

Guardando al futuro, l'iniziativa del governo si colloca come un passo importante verso la realizzazione di un'ambizione più ampia: fare dell'Italia un hub di riferimento per l'innovazione tecnologica in Europa e nel mondo. L'efficacia di questi sforzi sarà misurata non solo dagli immediati ritorni economici ma anche dal più ampio impatto sociale, culturale e ambientale delle tecnologie promosse. L'investimento di 150 milioni di euro nel settore delle startup tecnologiche italiane genererà un impatto significativo, sia per l'ecosistema delle startup sia per l'intero contesto economico e tecnologico del paese. Contribuirà all'accelerazione della trasformazione digitale, alla creazione di posti di lavoro qualificati e al rafforzamento della posizione competitiva dell'Italia sul mercato globale.

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 ogni informazione, 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.

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*

VISITA GUIDATA
AL CORPO NAZIONALE DEI VIGILI DEL FUOCO

Il **Centro Studi ed Esperienze (CSE) del Corpo Nazionale dei Vigili del Fuoco** ci ha confermato la visita guidata presso il loro centro situato in Roma, largo Santa Barbara,2 (via delle Capannelle) il giorno

lunedì 8 aprile 2024 mattina.

Il programma di massima (da confermare insieme all'orario preciso) prevede:

- presentazione delle principali attività del Centro Studi ed Esperienze;
- visita ai laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica);
- indicazioni sull'utilizzo dei materiali nella realtà delle costruzioni civili e industriali;
- attività del Nucleo Investigativo Antincendio (NIA).

Poiché la visita è soggetta al numero massimo di 15 partecipanti, vi chiediamo di inviarci la vostra adesione inviando una mail di conferma a segreteria@infrastrutturecritiche.it entro e non oltre il giorno sabato 23 marzo p.v.

A seguito dell'adesione Vi invieremo conferma dell'iscrizione. Qualora il limite dei partecipanti fosse raggiunto Vi comunicheremo l'inserimento in una lista di attesa che attiveremo qualora pervengano

delle rinunce. L'ordine di arrivo della mail sarà quello di inserimento nelle liste (partecipanti confermati o lista d'attesa).

Attenzione! **La visita è riservata ai soli soci AIIC in regola con il pagamento delle quote sociali**. I signori non-soci che volessero partecipare, possono iscriversi all'Associazione AIIC usufruendo di una quota di associazione minima (euro 50 anno + 10 una tantum).
Le modalità per l'iscrizione si trovano sul sito www.infrastrutturecritiche.it o si possono richiedere inviando una mail a segreteria@infrastrutturecritiche.it

Il Centro Studi ed Esperienze (CSE) del Corpo Nazionale Italiano dei Vigili del Fuoco è stato istituito nel 1961 ed è ospitato nelle Scuole Centrali Antincendi di Capannelle a Roma.
Da oltre sessanta anni il contributo del Centro Studi è stato di ricerca applicata attraverso i suoi laboratori di prova dei materiali (Scienza delle costruzioni, Difesa Atomica, Macchine e Termotecnica, Elettrotecnica, Idraulica) con le correlate indicazioni in merito al loro utilizzo nella realtà delle costruzioni civili e industriali del Paese. Nell'ultima legge di riordino del Corpo Nazionale il CSE è stato integrato dalle attività del Nucleo Investigativo Antincendio (NIA).

Un cordiale saluto a tutti.

Silvano Bari
Vice presidente AIIC

NEWS E AVVENIMENTI

5 anni. E' il tempo che gli hacker cinesi di Volt Typhoon sono rimasti all'interno delle infrastrutture critiche statunitensi

Secondo un allarme congiunto emesso il 7 febbraio dalla Cybersecurity and Infrastructure Agency (CISA), dalla National Security Agency (NSA) e dal Federal Bureau of Investigation (FBI), il gruppo di hacker cinese Volt Typhoon, noto anche come Bronze Silhouette, Insidious Taurus, UNC3236, Vanguard Panda o Voltzite ha compromesso alcune delle reti infrastrutturali critiche del paese. La cosa più inquietante, è che tale compromissione è durata per almeno cinque anni. Gli aggressori hanno preso di mira i settori delle comunicazioni, dell'energia, dei trasporti, dell'approvvigionamento idrico e delle fognature negli Stati Uniti e sull'isola di Guam. Le attività degli hacker governativi non erano coerenti con i tradizionali scopi di cyber intelligence e raccolta dati. Con un alto grado di sicurezza, possiamo dire che il Volt Typhoon stava preparando il terreno per un possibile sabotaggio.
Volt Typhoon: Attacchi Persistenti ed Avanzati e ben Finanziati
Una delle tattiche distintive di Volt Typhoon è l'uso di proxy per nascondere la loro vera posizione. Gli hacker stanno compromettendo router e firewall negli Stati Uniti e instradando attraverso di essi il traffico dannoso.
L'obiettivo principale del gruppo è quello di prendere piede per lungo tempo nelle reti hackerate. Nel corso di diversi anni hanno metodicamente ampliato le proprie posizioni, rubando periodicamente le

credenziali di accesso ai conti correnti. Inoltre, gli hacker utilizzano attivamente le vulnerabilità per aumentare i privilegi e ottenere il pieno controllo sui domini. *(Continua…)*
https://www.redhotcyber.com/post/5-anni-e-il-tempo-che-gli-hacker-cinesi-di-volt-typhoon-sono-rimasti-allinterno-delle-infrastrutture-critiche-statunitensi/
Red Hot Cyber *- Redazione RHC – 8 Febbraio 2024*

Quanti conoscono la tecnologia LiFi? - Si chiama Light fidelity-LiFi la nuova tecnologia che consente di espandere le aree di applicazione delle tecnologie Wi-Fi con velocità assolutamente straordinarie. L'approvazione di una norma offre una convalida ufficiale a questa nuova tecnologia.
Nel mondo della connettività senza fili, per molti anni la tecnologia WiFi ha occupato uno spazio assai vasto, in quanto consente di trasmettere segnali radio ad apparati fissi od in movimento.
Ma un nuovo scenario si sta presentando sul mercato, grazie alla recente approvazione della norma IEEE 802.11 bb, che codifica una tecnologia affatto nuova, grazie alla quale le informazioni non vengono trasmesse con segnali radio, ma con segnali luminosi. Il fatto che oggi sia disponibile una norma rappresenta un grande passo in avanti, in quanto chiunque sia interessato ad approfondire le conoscenze su questa tecnologia ha la garanzia che essa è supportata da un documento, che ne attesta la conformità alla regola d'arte.
(continua…)
https://www.puntosicuro.it/security-C-125/quanti-conoscono-la-tecnologia-lifi-AR-24027/
PuntoSicuro *- Adalberto Biasiotti - 09/02/2024*

Smart Building: Nuovo White Paper CEI edifici efficienti e sostenibili - Il CEI ha pubblicato il nuovo White Paper "Smart Building", un documento gratuito e innovativo che è stato redatto con il fine di favorire lo sviluppo delle tecnologie che consentono di realizzare edifici energeticamente altamente efficienti.
Predisposto da un gruppo di lavoro nell'ambito del Tavolo di Confronto 3 "Transizione Energetica", il White Paper fornisce supporto, tra gli altri, a progettisti e installatori del settore delle costruzioni, del terziario e della pubblica amministrazione (PA), anche in un'ottica di interventi nell'ambito del Piano Nazionale di Ripresa e Resilienza (PNRR).
I recenti orientamenti e programmi di intervento nazionali ed europei hanno ulteriormente accelerato i temi inerenti alla decarbonizzazione, l'efficientamento energetico e la modernizzazione, in chiave tecnologica e digitale, dell'intero settore delle costruzioni, determinando quel salto epocale che prevede, già a partire dai prossimi anni, la costruzione e la ristrutturazione profonda degli edifici per renderli a "zero emissioni" (ZEB) e anticipando di fatto gli obiettivi che l'Unione Europea si è prefissata al 2050.
In quest'ottica, lo Smart Building rappresenta la soluzione attraverso la quale è possibile ridurre i consumi energetici finali e favorire la diffusione dell'energia prodotta da fonti rinnovabili, trasformando l'attuale struttura energetica dipendente dai combustibili fossili in un sistema efficiente in termini di sfruttamento delle risorse energetiche.
(continua…)
https://www.snewsonline.com/smart-building-nuovo-white-paper-cei-edifici-efficienti-sostenibili/
SNews *- Redazione - 12/02/2024*

Tlc, via libera Ue al pacchetto connettività. Breton: "Passo avanti verso il Digital Networks Act"
La Commissione punta a promuovere l'innovazione, la sicurezza e la resilienza delle infrastrutture. Al vaglio il fair share per le Big Tech. Focus sul paradigma telco-cloud, il calcolo collaborativo, l'AI e la parità di condizioni competitive. Per i cavi sottomarini, riflettori sulla sicurezza col Cable Security Toolbox. La competitività dell'economia europea dipende dalle reti digitali avanzati e per questo la Commissione europea dedica alla connettività del futuro un pacchetto con una serie di possibili azioni in grado di promuovere l'innovazione, la sicurezza e la resilienza di queste infrastrutture critiche. "La connettività veloce, sicura e diffusa è essenziale per l'implementazione delle tecnologie che ci porteranno nel mondo di domani: telemedicina, guida automatizzata, manutenzione predittiva degli edifici o agricoltura di precisione", si legge nella nota della Commissione.
Due gli elementi principali di questo Digital connectivity package approvato dal collegio dei commissari: il Libro bianco "Come rispondere alle esigenze di infrastruttura digitale dell'Europa?", dove si affrontano le sfide di innovazione, investimento e sicurezza per l'implementazione delle future reti di connettività; e la Raccomandazione per la sicurezza e resilienza delle infrastrutture via cavo sottomarine.
Il white paper è particolarmente rilevante per l'industria delle telco, perché affronta la convergenza tecnologica tra le telecomunicazioni e il cloud, sottolinea l'importanza di realizzare appieno il potenziale del mercato unico digitale per le telecomunicazioni e apre le porte a "misure volte a garantire una vera parità di condizioni" tra operatori diversi. (Continua…)
https://www.corrierecomunicazioni.it/digital-economy/tlc-via-libera-ue-al-pacchetto-connettivita-verso-regole-meno-stringenti-sulle-fusioni/
***CORCOM** – Digital Economy – 21 Febbraio 2024*

Tecnologia a supporto di infrastrutture critiche, agricoltura e sicurezza
Aziende agricole, infrastrutture, reti energetiche e snodi logistici: il global monitoring rappresenta sempre più una risorsa per aziende e istituzioni per garantire sicurezza, qualità ed efficienza a servizi e prodotti. È il tema al centro dell'approfondimento del Corriere della Sera, che dedica tre articoli alle potenzialità derivanti dall'impiego dei droni e dell'intelligenza artificiale in settori quali sicurezza, agricoltura ed edilizia evidenziando l'impegno di Leonardo.
La collaborazione tra tecnologia satellitare, intelligenza artificiale e scansione ottica sta sempre più diventando uno strumento strategico per le attività del mercato civile privato e delle pubbliche amministrazioni, italiane ed europee. L'articolo di Massimiliano Del Barba, "L'AI arriva sul fronte del porto", mette in luce le potenzialità delle tecnologie di Leonardo in materia di global monitoring. Piattaforme secure-by-design, cioè concepite sin dalla fase di progettazione per essere resilienti alle minacce cyber, che garantiscono agli operatori una visione d'insieme del contesto integrata, completa e sempre aggiornata. La valorizzazione delle informazioni raccolte è resa possibile da algoritmi di intelligenza artificiale, in grado di abilitare un processo decisionale consapevole ed efficace.
Tra le applicazioni più recenti, che hanno visto il contributo delle tecnologie di Leonardo, ci sono il progetto europeo SecureGas e il piano Gioia Sicura. Il primo, concluso nel 2021, si è concentrato sui 140mila km della rete europea del gas a copertura dell'intera catena del valore, dalla produzione alla distribuzione. Grazie all'integrazione di sensori fisici e droni, ha fornito metodologie, strumenti e linee guida per proteggere le installazioni esistenti e renderle resistenti alle minacce cyber-fisiche. Il secondo prevede una serie di interventi volti a garantire la sicurezza integrata dell'area portuale di Gioia Tauro, attraverso attività di monitoraggio e controllo. Questa viene effettuata tramite l'ausilio di una flotta di

droni, controllata dalla piattaforma per il comando e controllo sviluppata da Leonardo, che estrae dati e informazioni che agevolano il processo decisionale nella gestione della sicurezza dell'area portuale. *(Continua…)*
https://www.leonardo.com/documents/15646808/28141712/CORRIERE_DELLA_SERA_26022024.pdf?t=1708934886385
Corriere della Sera *- Massimiliano Del Barba – 26 Febbraio 2024*

Nascerà in Sicilia l'impianto fotovoltaico più grande d'Italia - Quando entrerà in funzione, con i suoi 424.638 moduli fotovoltaici, l'impianto genererà circa 400 GWh all'anno.
L'impianto fotovoltaico più grande d'Italia? Attualmente il titolo va al parco solare da 103 MW realizzato in provincia di Foggia dalla danese European Energy. Ma come sempre, soprattutto quando si tratta di rinnovabili, i record sono fatti per essere superati. In questo caso a scippare il primato potrebbe essere Fénix, il nuovo progetto fv del gruppo Iberdrola nel Belpaese. La multinazionale spagnola ha oggi firmato un accordo con IB Vogt per la costruzione di un parco fotovoltaico da 245 MW di potenza. La localizzazione? In Sicilia. La capacità finale renderà l'installazione non solo il nuovo impianto fotovoltaico più grande d'Italia, ma anche anche una sorta di unicum nel panorama nazionale dove, a conti fatti, solo 60 centrali solari superano oggi i 10 MW di capacità unitaria.. *(continua…)*
https://www.rinnovabili.it/energia/fotovoltaico/impianto-fotovoltaico-piu-grande-italia-245-mw-sicilia/
Rinnovabili.it *– 27/02/2024*

Intelligenza artificiale per la gestione degli impianti - Intelligenza artificiale (IA), cos'è? Può realmente ottimizzare la gestione di un impianto? E come può farlo? Nel periodo storico in cui viviamo, dove l'avanzamento tecnologico e informatico lo ha fatto da padrone, questi sono solo alcuni degli infiniti quesiti che ci stiamo ponendo sull'IA. In questo articolo si cerca di fare chiarezza su cosa sia l'IA e la sua applicazione nel settore impiantistico.
I diversi approcci dell'Intelligenza Artificiale
Come prima cosa è importante chiarire cosa sia l'IA. L'intelligenza artificiale è un campo dell'informatica che si occupa dello sviluppo di sistemi e algoritmi in grado di eseguire compiti che richiedono tipicamente l'intelligenza umana. L'obiettivo dell'IA è quello di creare macchine in grado di apprendere da dati, di adattarsi all'ambiente circostante e di eseguire operazioni simili a quelle svolte dall'intelligenza umana.
(continua…)
https://www.ingenio-web.it/articoli/intelligenza-artificiale-per-la-gestione-degli-impianti/
Ingenio *- Samuele Carboni, 29/2/2024*

Biden orders US investigation of national security risks posed by Chinese-made 'smart cars'.
WASHINGTON (AP) — Citing potential national security risks, the Biden administration says it will investigate Chinese-made "smart cars" that can gather sensitive information about Americans driving them. The probe could lead to new regulations aimed at preventing China from using sophisticated technology in electric vehicles and other so-called connected vehicles to track drivers and their personal information. Officials are concerned that features such as driver assistance technology could be used to effectively spy on Americans.While the action stops short of a ban on Chinese imports, President Joe Biden said he is taking unprecedented steps to safeguard Americans' data."China is determined to dominate the future of the auto market, including by using unfair practices,'' Biden said

in a statement Thursday. “China’s policies could flood our market with its vehicles, posing risks to our national security. I’m not going to let that happen on my watch.'' The probe is the latest action by the Biden administration to guard against what officials see as the growing threat of Chinese cyberattacks. Biden signed an executive order this week aimed at better protecting Americans’ personal data such as health and finance records from foreign adversaries like China and Russia.
Biden and other officials noted that China has imposed wide-ranging restrictions on American autos and other foreign vehicles.
Commerce Secretary Gina Raimondo said connected cars “are like smartphones on wheels” and pose a serious national security risk. “These vehicles are connected to the internet. They collect huge amounts of sensitive data on the drivers — personal information, biometric information, where the car goes,'' she told reporters late Wednesday. “So it doesn’t take a lot of imagination to figure out how a foreign adversary like China, with access to this sort of information at scale, could pose a serious risk to our national security and the privacy of U.S. citizens.'' (Continua…)
https://apnews.com/article/china-electric-vehicles-privacy-personal-data-biden-844f2406512b94212ee1a92a61e5a33a
Associated Press - Matthew Daly - February 29, 2024

L’intelligence italiana mappa le strutture sottomarine critiche del Mediterraneo
Anche nella Relazione dell’intelligence italiana si alza l’attenzione sulle infrastrutture critiche sottomarine che solcano il Mediterraneo. C’è una nuova dimensione della guerra subacquea, che tocca gli impianti civili relativi alla vita quotidiana delle collettività.
La prima vittima della prossima crisi militare (o la prossima di questa in corso) potrebbe essere la nostra connessione Internet, colpita perché le infrastrutture che fanno viaggiare i nostri dati – i cosiddetti cavi sottomarini – stanno prendendo centralità tra i potenziali target. Oppure, potrebbero essere le forniture dei nostri servizi primari come l’energia elettrica, che potrebbe subire alterazioni anche nei prezzi da danno a condotte che scorrono sul fondo del mare. Attaccare gli obiettivi dei fondali marini non sarà mai facile. I proclami degli Houthi sulla possibilità di colpire i sistemi che scorrono sotto il Mar Rosso sono per questo sembrati più che altro slanci propagandistici. Tuttavia, l’attenzione resta alta – e quello che è probabilmente stato un incidente, nei giorni scorsi è stato subito descritto come un potenziale attacco.
Colpire sott’acqua, a decine e decine di metri di profondità, è ovvio che sia intrinsecamente più impegnativo che attaccare le infrastrutture fuori terra – in quello stesso quadrante, sempre per restare all’attualità, gli Houthi non hanno avuto problemi a lanciare i missili forniti loro dai Pasdaran contro le grandi navi mercantili che collegano Europa e Asia. Attaccare sotto la superficie richiede un’intelligence di alta qualità (per individuare le infrastrutture) e un’attenta pianificazione, nonché strumenti adeguati. Se per intaccare le connettività internazionali fuori terra basta l’uso di alcuni lancia razzi o sistemi senza pilota (aerei o navali) sotto il controllo di operatori con formazione ed esperienza anche bassa, per colpire tra gli abissi serve preparazione – per esempio, solo alcune unità sceltissime, tra le migliori forze speciali del mondo, hanno mezzi e capacità di andare a danneggiare i cavi, per altro solo nelle porzioni effettivamente raggiungibili.
Tuttavia, visto il valore degli obiettivi (che è nella sostanza il valore inestimabile che i dati hanno in questo momento e quello che altri servizi hanno sempre avuto nella storia recente), molte forze militari regolari e gruppi combattenti si stanno attrezzando per ottenere in qualche modo i mezzi tecnici

necessari a certi gesti. E un numero crescente di produttori di AUV (acronimo da appuntare, sta per autonomous underwater vehicle) ha il know-how necessario per costruire veicoli adatti. *(Continua…)*
https://formiche.net/2024/02/intelligence-italiana-infrastrutture-sottomarine/
Formiche.net *– Emanuele Rossi – 29 Febbraio 2024*

GTPdoor, Italia nel mirino: come proteggere le reti mobili dalla backdoor Linux
Secondo i ricercatori di sicurezza, le minacce dietro GTPdoor prendono di mira le reti degli operatori mobili, utilizzando il protocollo GTP per mascherare le sue comunicazioni C2 e fornire agli aggressori l'accesso diretto alla rete principale di telecomunicazione. Ecco come mitigare il rischio di un attacco nation-state, forse rivolto proprio alle infrastrutture critiche italiane. Il ricercatore di sicurezza HaxRob ha scoperto una backdoor Linux precedentemente sconosciuta, denominata GTPdoor, progettata per operazioni segrete all'interno delle reti degli operatori mobili. L'Italia sarebbe nel mirino di questo attacco, secondo il nostro esperto Pierluigi Paganini.
Si ritiene che gli attori delle minacce dietro GTPdoor prendano di mira i sistemi adiacenti al Gprs roaming eXchange (GRX), come SGSN, GGSN e P-GW, in grado di fornire agli aggressori l'accesso diretto alla rete principale di una telecomunicazione.
"GTPdoor è una nuova backdoor per sistemi operativi Linux che mira alle reti degli operatori mobili, utilizzando il protocollo GTP per mascherare le sue comunicazioni C2", commenta Riccardo Michetti, Threat Intelligence Analyst di Swascan.
"La scoperta della backdoor GTPdoor", conferma Pierluigi Paganini, analista di cyber security e CEO Cybhorus, "è estremamente preoccupante per molteplici fattori". Ecco quali e come proteggersi da un eventuale attacco nation-state, forse rivolto proprio all'Italia. *(Continua…)*
https://www.cybersecurity360.it/nuove-minacce/gtpdoor-italia-nel-mirino-come-proteggere-le-reti-mobili-dalla-backdoor-linux/
Cybersecurity360 *– Mirella Castigli – 04 Marzo 2024*

Quantum revolution: dal CERN le soluzioni per la cybersecurity del futuro
L'avvento dell'era quantistica apre nuove prospettive per la sicurezza informatica. Tra sfide e opportunità, la Quantum Key Distribution emerge come una soluzione promettente. Il ruolo del CERN e l'importanza dell'investimento in formazione e standardizzazione sono fondamentali in questo scenario emergente. Le innovazioni nel campo delle tecnologie quantistiche stanno già rivoluzionando il panorama della sicurezza informatica nel mondo scientifico, ma fra un po' estenderanno anche al livello mainstream della comune cittadinanza: esse porteranno con sé anche nuove sfide, in particolare nel settore della cybersecurity.
Per comprendere meglio l'impatto di queste tecnologie e come affrontare le relative sfide, abbiamo necessità di avviare un'azione sistematica da parte governativa assieme ai centri di eccellenza italiani e comunitari nel campo della ricerca quantistica, affinché si affronti da subito il rischio che le tecnologie quantistiche rappresentano per la sicurezza delle comunicazioni digitali a livello crittografico. *(Continua…)*
https://www.agendadigitale.eu/sicurezza/proteggere-i-dati-nellera-quantistica-dal-cern-le-soluzioni-del-futuro/
Agenda Digitale *– Luciano Magaldi – 5 Marzo 2024*

Cybersecurity nella Pubblica Amministrazione: Garantire la Continuità dei Servizi attraverso la Sicurezza Integrata

Il contesto normativo

Da un punto di vista normativo, i principali riferimenti sono rappresentati dall'art. 51 del Codice dell'Amministrazione Digitale (CAD) e dall'art. 32 del Regolamento Generale sulla Protezione dei Dati (GDPR). Entrambe le discipline sottolineano l'obbligo di garantire la confidenzialità, la riservatezza e l'integrità dei dati. Inoltre, stabiliscono l'importanza di implementare procedure per garantire la continuità dei servizi e il ripristino tempestivo dei sistemi in caso di incidenti fisici o tecnici. Vi sono anche altre misure, obiettivi ed azioni da rispettare in tema di sicurezza informatica nel Piano Triennale per l'Informatica delle PA 2024-2026 che richiamano alla necessità di redigere uno specifico piano di sicurezza.

Tutte queste disposizioni esigono adempimenti che, il più delle volte, si ripetono. Ragion per cui diventa importante coordinare le attività, in modo da non replicare i processi finalizzati a garantire la sicurezza. La chiave per bilanciare il contesto normativo e tecnologico è la gestione organica e strutturata del processo e, nel contesto delle pubbliche amministrazioni, particolare importanza assumono in materia le Linee guida e le circolari messe a disposizione dall'Agenzia per l'Italia Digitale (Agid).

Il contesto organizzativo

In qualsiasi organizzazione, la sicurezza informatica si articola in un processo che coniuga aspetti di natura tecnica ed economica, i quali convergono nel contesto organizzativo. A conferma dell'importanza della sicurezza informatica per gli enti pubblici, il CAD all'art. 17 introduce, nel contesto organizzativo della struttura pubblica, la figura del "Responsabile per la Transizione Digitale" (RTD). Uno dei principali compiti dell'RTD consiste nel sensibilizzare i vertici dell'amministrazione sulla consapevolezza dei rischi da attacco informatico, promuovendo delle best practice in ambito della protezione dei dati e servizi digitali. Questo include la facilitazione di sessioni formative, la diffusione di informazioni sulle minacce attuali e la promozione di politiche e procedure di sicurezza per garantire un ambiente digitale resiliente.

https://www.ictsecuritymagazine.com/articoli/cybersecurity-nella-pubblica-amministrazione-garantire-la-continuita-dei-servizi-attraverso-la-sicurezza-integrata/

ICT Security Magazine *– Daniele De Simone – 5 Marzo 2024*

NIST Cybersecurity Framework 2.0, cambia lo standard della cyber security: ecco come

Il NIST Cybersecurity Framework è sicuramente uno dei più conosciuti e utilizzato in tutte le organizzazioni del mondo per affrontare i rischi informatici in modo strutturato e con l'uso di metodologie standardizzate. È stata ora rilasciata la versione 2.0: ecco cosa cambia e perché è importante anche per l'Italia. ll 26 febbraio 2024 il NIST ha pubblicato in forma ufficiale il Cybersecurity Framework (CSF) versione 2.0: un rilascio atteso e puntualmente avvenuto nei tempi previsti, dopo il rilascio della bozza (Public Draft) ad agosto 2023 sulla quale era stata aperta la fase di "Discussion Draft" con commenti e feedback raccolti fino al 4 novembre 2023.

Il percorso disegnato dal NIST per progettare il CSF 2.0 era partito nel febbraio 2022 attraverso una fase di consultazione, con una richiesta pubblica di informazioni (RFI: Request for Information), "Evaluating and Improving NIST Cybersecurity Resources: The Cybersecurity Framework and Cybersecurity Supply Chain Risk Management".

La RFI richiedeva informazioni sull'uso del NIST Cybersecurity Framework e raccomandazioni per migliorare l'efficacia del framework e il suo allineamento con altre risorse di cybersecurity. L'RFI chiedeva anche suggerimenti per informare altre iniziative di cybersecurity del NIST, in particolare per quanto riguarda i rischi di cybersecurity della catena di approvvigionamento.
Al momento della pubblicazione dell'RFI, il Vicesegretario al Commercio Don Graves ha dichiarato che: "Ogni organizzazione ha bisogno di gestire il rischio di cybersecurity come parte della propria attività, che si tratti di industria, governo o università. È fondamentale per la loro resilienza e per la sicurezza economica della nostra nazione. Ci sono molti strumenti disponibili per aiutarci, e il CSF è uno dei principali framework per la manutenzione della cybersecurity nel settore privato. Vogliamo che le organizzazioni del settore pubblico e privato contribuiscano a renderlo ancora più utile e diffuso, anche per le piccole imprese". *(Continua…)*
https://www.cybersecurity360.it/soluzioni-aziendali/nist-cybersecurity-framework-2-0-cambia-lo-standard-della-cyber-security-ecco-come/
Cybersecurity 360 *– Giorgio Sbaraglia – 5 Marzo 2024*

Improved, Stuxnet-Like PLC Malware Aims to Disrupt Critical Infrastructure
A newly developed PLC malware does not require physical access to target an ICS environment, is mostly platform neutral, and is more resilient than traditional malware aimed at critical infrastructure.
The proliferation of programmable logic controllers (PLCs) with embedded Web servers in them has given attackers a way to launch potentially catastrophic, remote attacks against operational technology (OT) for industrial control systems (ICS) in critical infrastructure sectors.
To highlight the threat, a team of researchers from the Georgia Institute of Technology has developed malware that an adversary could use to remotely access an embedded Web server within a PLC, and attack the underlying physical system. An attacker could use the malware to manipulate output signals to actuators, to falsify sensor readings, disable safety systems, and execute other actions that could trigger potentially devastating outcomes, including even loss of life, the researchers said.
PLCs are the components of ICS that control the operation of physical processes and machinery within various manufacturing, industrial, and critical infrastructure settings. A PLC receives input from various connected sensors and other input sources, and uses the data to send commands to physical systems based on pre-programmed controlled logic. The goal with PLC malware in general is to influence the output in such a way as to disrupt or to sabotage the physical process which a PLC might be controlling.
A Stuxnet-Like, Web-Based PLC Malware
Often, malware targeting PLCs and ICS systems have required attackers to have some kind of prior physical or network access to the target environment, and has often been platform specific and easily erasable via factory resets. In the paper, Georgia Tech researchers Ryan Pickren, Tohid Shekari, Saman Zonouz and Raheem Beyah described their Web-based PLC malware as fundamentally different.
Most PLC malware typically infects the firmware or control logic of the controllers, whereas the new Web-based malware attacks the front-end Web layer in PLCs with malicious JavaScript, eliminating some of the limitations such malicious code has faced in the past. (Continua…)
https://www.darkreading.com/ics-ot-security/improved-stuxnet-like-plc-malware-disrupt-critical-infrastructure
DarkReading*-Jai Vijayan- March 5, 2024*

Southern Company Builds SBOM for Electric Power Substation

The utility's software bill of materials (SBOM) experiment aims to establish stronger supply chain security — and tighter defenses against potential cyberattacks.

Energy giant Southern Company in the past year set out to inventory all of the hardware, software, and firmware in equipment running in one of its Mississippi substations in an effort to create a software bill of materials (SBOM) for the operational technology (OT) site.

The SBOM experiment began with Southern Company's cybersecurity team traveling to the Mississippi Power substation to physically catalog the equipment there, taking photos and gathering data from network sensors. Then came the most daunting — and at times, frustrating — part: acquiring software supply chain details from the 17 vendors whose 38 devices the utility identified in the substation during its reconnaissance mission.

Alex Waitkus, principal cybersecurity architect at Southern Company and head of the SBOM project, said collecting and correlating information on all of the hardware, software, firmware, and interdependencies in the systems for the SBOM supplied the energy company with a deeper understanding of all of the software components in the substation and their potential exploitable vulnerabilities. Prior to the project, Southern had visibility into its OT network assets there via its Dragos platform, but software details were an enigma.

"We had no idea what the different versions of software we were running" before launching the SBOM project, he said in a presentation here this week at the S4x24 ICS/OT security conference. "We had multiple business partners who managed different parts of the substation."

That meant consulting with physical security and maintenance teams, for example, to assist in the utility's gaining the full picture of the substation's software supply chain. Southern cataloged a total of 18 control network system devices from two vendors; eight physical security devices from three vendors; four cybersecurity and telecommunications devices from four vendors; eight OT monitoring systems from six vendors; and one OT fault system device from one vendor.

The next step in the project was gathering SBOMs from each of its vendors represented in the substation. But there were roadblocks, as nearly 60% of the vendors Southern contacted for their products' SBOM information declined to provide the utility with the information. And on average, it took 60 days and a dozen meetings for Southern to actually receive in hand SBOMs from the cooperating vendors.

"So we were updating firmware [in some cases] by the time we received" the SBOM, Waitkus said. That meant an outdated SBOM, added Waitkus, who co-presented Southern's findings here at S4 with Matt Wyckhouse, CEO of software supply chain risk vendor Finite State. The project spun out of an OT SBOM roundtable organized by Wyckhouse at last year's S4 conference.

(Continua...)

https://www.darkreading.com/ics-ot-security/southern-company-builds-a-power-substation-sbom

DarkReading *- Kelly Jackson Higgins - March 6, 2024*

Uncle Sam intervenes as Change Healthcare ransomware fiasco creates mayhem.

As the crooks behind the attack - probably ALPHV/BlackCat - fake their own demise

The US government has stepped in to help hospitals and other healthcare providers affected by the Change Healthcare ransomware infection, offering more relaxed Medicare rules and urging advanced funding to providers.

Change, a UnitedHealth Group-owned IT services firm, provides software to more than 70,000 American pharmacies and healthcare organizations so they can electronically process insurance claims and fill prescription orders.

Many of Change's customers have reported disruptions and severe cash flow issues following the February 21 cyber attack.
On Tuesday, the Department of Health and Human Services (HHS) intervened to assist the healthcare industry and ensure that medical facilities can continue to provide patient care.
"Numerous hospitals, doctors, pharmacies and other stakeholders have highlighted potential cash flow concerns to HHS stemming from an inability to submit claims and receive payments," the department explained in a statement. "HHS has heard these concerns and is taking direct action and working to support the important needs of the healthcare community."
This includes allowing Medicare providers to change clearing houses they use for claims processed during the outage via an expedited process.
The Feds are also "encouraging" Medicare Advantage organizations to offer advance funding to providers more severely affected by the cyber attack. These are the private companies – like UnitedHealthcare and Humana – that Medicare pays to cover individuals' benefits.
Additionally, the government "strongly encourages" Medicaid and Children's Health Insurance Program managed-care plans to either relax or remove prior authorization requirements and offer advance funding to providers.
On top of that, Medicare Administrative Contractors are required to accept paper claims from providers while their electronic billing systems remain down.
"This incident is a reminder of the interconnectedness of the domestic health care ecosystem and of the urgency of strengthening cyber security resiliency across the ecosystem," HHS noted, and directed medical providers to its December concept paper [PDF] that outlines a cyber security strategy for the sector.
A month later, the Feds issued new voluntary cyber security performance goals for hospitals and other healthcare organizations – which some infosec experts predict probably won't be "voluntary" for very long.
'They're really in the hurt locker'
The government stepping in to assist pharmacies and medical providers "is huge," Padraic O'Reilly, co-founder and chief innovation officer of cyber risk firm CyberSaint, told *The Register*.
"The smaller practices are really suffering – they're really in the hurt locker," he added. "It's such a supply chain issue, and it really reaches into the entire infrastructure around healthcare payments, which is really quite scary. It's really high risk to have half the transactions running through one provider." (Continua…)
https://www.theregister.com/2024/03/06/us_government_change_ransomware_intervention/
The Register *- Jessica Lyons – 6 Mar 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

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 Marco Raul Massoni *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.