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 2025 **n. 4/ 2025** **aprile 2025**

Proposta di legge per contrastare il ransomware

Il 20 marzo è stata per la prima volta depositata alla Camera dei deputati una proposta di legge che mira a contrastare la crescente minaccia ransomware, a prima firma Matteo Mauri, parlamentare del Partito Democratico, ma appoggiata anche da Federico Mollicone di Fratelli d'Italia, in rappresentanza della maggioranza di Governo.
I ransomware sono una delle minacce informatiche più insidiose e diffuse degli ultimi anni, software malevoli che si infiltrano nei sistemi informatici e consentono di criptare dati di organizzazioni o individui che vengono poi ricattati dagli aggressori per riavere o evitare la pubblicazione delle informazioni che sono state sottratte. Gli attacchi informatici condotti tramite ransomware hanno dei costi diretti e indiretti pesanti per le aziende colpite, come dimostra il caso di Marposs, azienda bolognese di apparecchi per le misure di precisione, che a seguito di un attacco subito il 26 gennaio è stata costretta a mettere in cassa integrazione parziale i suoi lavoratori per una settimana, in attesa che la crisi rientrasse.
Negli ultimi anni, l'Italia ha assistito a un'escalation significativa degli attacchi ransomware e secondo l'Agenzia per la Cybersicurezza Nazionale (ACN) è il sesto Paese più colpito al mondo e il quarto dell'Unione Europea, registrando nel 2024 circa 145 casi, con un totale di oltre 28 terabyte di dati rubati. Inoltre, secondo l'ultimo Rapporto Cyber Index PMI, realizzato da Generali e Confindustria, con il supporto scientifico dell'Osservatorio Cybersecurity & Data Protection della School of Management del Politecnico di Milano e con la partecipazione dell'Agenzia per la Cybersicurezza Nazionale, l'85% delle piccole e medie imprese italiane non è consapevole dei rischi cyber.
Su questi presupposti si innesta la proposta di legge del deputato Mauri che ha dichiarato in una nota la necessità urgente di un intervento legislativo per contrastare quella che definisce «una vera emergenza nazionale». La strategia delineata dal testo di legge in un unico articolo prende spunto da una proposta che è attualmente al vaglio nel Regno Unito e si articola sui seguenti punti fondamentali della gestione del fenomeno. Innanzitutto, si chiede di stabilire il divieto per i soggetti inclusi nel Perimetro di Sicurezza Nazionale Cibernetica di pagare il riscatto, se non in forza di una deroga del Presidente del Consiglio che valuterà l'eventuale presenza di gravi rischi per la sicurezza nazionale; viene introdotto anche l'obbligo di notificare al CSIRT Italia l'attacco subito entro sei ore dalla sua scoperta. Da un punto di vista finanziario, la legge intende istituire un fondo di supporto per le vittime di attacchi ransomware, in particolare per le PMI, per aiutarle nel recupero e nella ripresa delle attività, il "Fondo nazionale di risposta agli attacchi ransomware". Si prevede anche l'introduzione di incentivi economici per le imprese che investono nell'attuazione di misure per la sicurezza informatica. Infine, la legge propone anche l'istituzione di programmi di formazione per i dipendenti delle aziende e campagne di sensibilizzazione pubblica per aumentare la consapevolezza sui rischi informatici e le buone pratiche di sicurezza.
La proposta di legge Mauri si configurerebbe così come una delle più avanzate in Europa per la difesa del tessuto produttivo nazionale e dei cittadini, con norme che, se approvate, andranno a rafforzare la resilienza del paese e delle sue 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

Ginevra Detti
Laureata in giurisprudenza con un percorso penalistico incentrato sugli aspetti più sociologici dello studio del diritto. Ha sempre ampliato la formazione integrandola con attività associazionistiche di cultura, volontariato e politica. Ricopre il ruolo di analista presso Hermes Bay s.r.l.

Tommaso Diddi
Laureato in ingegneria dell'informazione con un curriculum in telecomunicazioni. Ha maturato esperienza nel settore dell'audio e dell'elettronica. Ricopre il ruolo di Junior Software Developer presso Hermes Bay s.r.l.

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2025

Il 31 dicembre 2024 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo 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 2025".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

Ricordiamo agli associati che non hanno ancora rinnovato la quota: il socio rimane iscritto nel libro soci per tre mesi ma perde il diritto di partecipare alla vita sociale e il diritto di voto e viene cancellato dalle mailing list di distribuzione soci. Scaduti i tre mesi il socio decade per morosità e deve effettuare di nuovo l'iscrizione pagando anche la relativa quota una tantum.

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.

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

PROSSIMO WEBINAR AIIC

Martedì 6 maggio 2025 ore 15:00 - 17:00
"Critical Infrastructure Resilience and Artificial Intelligence"
(in italiano)

Il Gruppo di Lavoro AIIC dedicato all'analisi del ruolo e dell'impatto dell'Intelligenza Artificiale (IA) nelle infrastrutture critiche ha concluso i lavori ed ha pubblicato il relativo documento "Critical Infrastructure Resilience and Artificial Intelligence", scaricabile dal sito www.infrastrutturecritiche.it.

Il rapporto esamina il ruolo e l'impatto dell'Intelligenza Artificiale (IA) nelle infrastrutture critiche, fornendo una panoramica globale di strategie, standard, considerazioni etiche e quadri normativi.

Obiettivo del webinar è l'illustrazione del rapporto e dei diversi aspetti che caratterizzano l'utilizzo della Intelligenza Artificiale allo scopo di aumentare la resilienza delle Infrastrutture Critiche.
A seguire, la locandina dell'evento.

La partecipazione è aperta ai soci e ai simpatizzanti di AIIC, previa iscrizione inviando una mail a:
segreteria@infrastrutturecritiche.it
A coloro che si iscriveranno verrà inviata una mail di conferma con i dati relativi al collegamento.

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

WEBINAR

Critical Infrastructure Resilience and Artificial Intelligence

Webinar a cura AIIC & ISACA Rome Chapter

06 Maggio 2025, ore 15:00

c/o Piattaforma GOTOMeeting

Il rapporto esamina il ruolo e l'impatto dell'Intelligenza Artificiale (IA) nelle infrastrutture critiche, fornendo una panoramica globale di strategie, standard, considerazioni etiche e quadri normativi.
L'obiettivo è identificare le *best practice* e offrire raccomandazioni per promuovere la resilienza e la sostenibilità delle infrastrutture critiche tramite l'uso responsabile dell'IA. Per favorirne la diffusione il rapporto è redatto in lingua inglese

Obiettivo del Webinar è l'illustrazione del rapporto e dei diversi aspetti che caratterizzano l'utilizzo della Intelligenza Artificiale allo scopo di aumentare la Resilienza delle Infrastrutture Critiche.

PROGRAMMA

15:00 - I GdL nella storia di AIIC *Silvano Bari*

15:10 – Applicazioni della Intelligenza Artificiale per la Resilienza delle Infrastrutture Critiche: sono soltanto vantaggi? *Sandro Bologna*

15:30 – Applicazioni della Intelligenza Artificiale tra passato, presente e futuro: cosa ci aspettiamo? *Alberto Stefanini*

15:50 – Vincoli Etici e Sociali nell'utilizzo della Intelligenza Artificiale nelle Infrastrutture Critiche: sono soltanto degli impedimenti? *Luigi Carrozzi*

16:10 – Come affrontare il tema della valutazione del rischio nelle Infrastrutture Critiche che fanno uso della Intelligenza Artificiale: possiamo farne a meno? *Francesca Della Mea*

16:30 – Vincoli Normativi ed Etici non bastano ad assicurare la Resilienza: il caso Heathrow e un auspicabile contributo della intelligenza artificiale *Alberto Caruso De Carolis*

16:50 – Conclusioni: idee per un mondo più resiliente *Luisa Franchina*

17:00 – Chiusura del Webinar

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

NEWS E AVVENIMENTI

L'EHDS, la NIS2 e l'impegno dell'Italia - Lo Spazio Europeo dei Dati Sanitari (EHDS – European Health Data Space) è un'iniziativa dell'Unione Europea volta a creare un quadro comune per la gestione, la condivisione e l'utilizzo sicuro dei dati sanitari tra i Paesi membri. Il suo obiettivo principale è migliorare l'assistenza sanitaria, la ricerca e l'innovazione attraverso un uso più efficace e controllato di queste informazioni.

EHDS, MyHealth@EU e HealthData@EU

L'EHDS si basa su due livelli di utilizzo dei dati. Il primo livello riguarda l'uso primario, che si riferisce all'accesso ai dati sanitari da parte dei cittadini e dei professionisti sanitari per scopi di cura. Questo include le cartelle cliniche elettroniche, le prescrizioni digitali e altri documenti sanitari necessari per garantire continuità nelle cure, indipendentemente dal Paese in cui un paziente si trova. Il secondo livello è l'uso secondario dei dati, che consente il loro utilizzo per la ricerca scientifica, l'innovazione, la politica sanitaria e lo sviluppo di nuovi trattamenti. Questo uso è regolato per garantire la privacy e la sicurezza dei dati. Per assicurarne l'operatività sono stati sviluppati strumenti specifici come, MyHealth@EU, HealthData@EU e ultimo ma non ultimo il Regolamento EHDS.

MyHealth@EU è l'iniziativa pensata per facilitare l'accesso ai dati sanitari quando ci si trova in un altro Stato membro. In pratica, permette ai cittadini europei di ricevere assistenza medica all'estero con la stessa facilità con cui la riceverebbero nel loro Paese d'origine, grazie alla condivisione sicura delle informazioni sanitarie.

Uno degli aspetti più utili di MyHealth@EU è la possibilità di ottenere farmaci prescritti nel proprio Paese anche in una farmacia di un altro Stato membro, senza bisogno di una nuova prescrizione cartacea. Il farmacista locale può accedere ai dati della prescrizione elettronica e fornire il medicinale in base alle indicazioni del medico che lo ha prescritto. Questo è particolarmente comodo per chi viaggia spesso o si trova all'estero per lunghi periodi. Un altro servizio importante è il Patient Summary, un documento che riassume le informazioni essenziali sulla salute di una persona, come allergie, patologie croniche o farmaci in uso. Se un cittadino europeo ha bisogno di assistenza medica mentre è in un altro Paese, i medici locali possono accedere a queste informazioni e offrire cure più sicure e appropriate, evitando errori o trattamenti incompatibili con la sua storia clinica.

(continua….)

https://www.snewsonline.com/ehds-nis2-impegno-italia/

SNews - *di Umberto Saccone - 17 Marzo 2025*

Giornata Mondiale dell'Acqua 2025: l'Italia tra emergenze idriche e soluzioni innovative - La

Il 22 marzo ricorre la Giornata Mondiale dell'Acqua 2025. Il tema di quest'anno è la conservazione dei ghiacciai. Uno sguardo allo stato delle risorse idriche in Italia e all'impatto del cambiamento climatico

L'Italia è in un "paradosso idrico". Pur essendo un paese tradizionalmente ricco d'acqua, deve fare i conti con infrastrutture obsolete, elevata dispersione idrica e impatti crescenti del cambiamento climatico. Nella Giornata Mondiale dell'Acqua 2025 (World Water Day), celebrata ogni 22 marzo, vediamo quali sono le sfide più complesse che il Belpaese deve affrontare nella gestione di questa risorsa vitale.

Indice dei contenuti

Giornata Mondiale dell'acqua 2025: cos'è il World Water Day?

La Giornata Mondiale dell'Acqua 2025 si celebra il 22 marzo e rappresenta un'occasione importante per aumentare la sensibilizzazione sull'importanza dell'acqua dolce e sulla necessità di una gestione sostenibile di questa risorsa vitale.

Istituito dalle Nazioni Unite nel 1992, il World Water Day vuole attirare l'attenzione su temi cruciali legati all'acqua, come l'accesso sicuro per tutti, la scarsità idrica, l'inquinamento e gli effetti dei cambiamenti climatici sulle risorse idriche.

Ogni anno, la Giornata Mondiale dell'Acqua si concentra su un tema specifico: per il 2025 si prevede un'attenzione particolare alla conservazione dei ghiacciai. Dall'acqua di fusione dei ghiacciai in tutto il mondo dipende direttamente la qualità della vita di circa 2 miliardi di persone, sottolineano le Nazioni Unite.

Lo stato critico delle infrastrutture idriche italiane

La situazione delle infrastrutture idriche in Italia ha dati allarmanti che richiederebbero interventi urgenti. In base ai dati più recenti, la dispersione lungo la rete idrica nazionale oscilla tra il 14% e il 72%, con una media nazionale del 42%. Questo significa che quasi metà dell'acqua prelevata viene dispersa prima di raggiungere i rubinetti dei cittadini. La situazione è grave in oltre il 50% dei comuni italiani, dove le perdite idriche superano il 35% dei volumi immessi in rete.

L'obsolescenza delle infrastrutture rappresenta una delle principali cause di questo problema. Circa il 60% della rete idrica italiana ha più di 30 anni e il 25% ha superato il mezzo secolo di vita. Una rete idrica vecchia richiede investimenti consistenti per l'ammodernamento del sistema.

Qualche segnale positivo c'è. Il PNRR ha messo a disposizione 4,3 miliardi di euro per migliorare la qualità dell'acqua, realizzare 25.000 chilometri di nuove reti per la distribuzione, completare le reti di fognatura. E dal 2021 al 2025, i gestori del servizio idrico integrato hanno investito 13,2 miliardi (inclusi gli interventi programmati per quest'anno ma non ancora realizzati), calcola uno studio recente di TEHA.

(continua…)

https://www.rinnovabili.it/clima-e-ambiente/acqua/giornata-mondiale-dellacqua-2025-world-water-day/

Rinnovabili.it – *Redazione - 22 Marzo 2025*

Security Tech That Can Make a Difference During an Attack

The recent report of how Volt Typhoon compromised systems at a water utility highlights security technologies and processes that helped detect the compromise and clean up the network.

When the FBI contacted Massachusetts-based Littleton Electric Light and Water Departments (LELWD) about Volt Typhoon, the small public utility was unaware that the Chinese attack group had been in the company's network for more than 300 days.

While the utility had security controls protecting the perimeter, its security technology and policy had some gaps. A more rigorous update strategy for its network and security appliances would have

prevented the initial compromise. In addition, monitoring of its internal "east-west" traffic could have potentially detected anomalies in how the attackers were using its administrator tools, says John Burns, director of OT threat hunting for Dragos, an OT security firm.

"Once my team went in and actually looked for it, we saw right away that things were happening," Burns says. "That was just with minimal monitoring and minimal checking. We went in and looked, and right away you could tell something was off."

With tactics converging in threat behavior over the past five years, it has become difficult for security teams to detect and attribute activity to specific advanced persistent threat (APT) groups. Cybercriminals, hacktivists, and APT groups are increasingly using the same behaviors, such as targeting vulnerable external-facing network devices, capturing and using legitimate credentials, and executing built-in system commands to move laterally through the network. Even so, organizations can focus their efforts on specific technologies to detect initial attempts at compromise and hunt anomalous behavior that indicate a compromise in progress, says Joe Slowik, principal threat intelligence analyst at MITRE.

"A lot of what Volt Typhoon does — because they eschew using custom tools — really starts [to impact] how you detect malicious entities operating in these environments in a fairly standard or universal way," Slowik says. "If the defensive community can identify effective means of responding to identifying and mitigating against these sorts of behaviors, we then have the ability to really put a variety of threat actors on the back foot quite quickly as a result."

Keep an Eye on Your Edge

APT actors often target N-day vulnerabilities in perimeter devices. In the LELWD case, the attackers exploited a year-old vulnerability in a firewall, giving them an attack window of several months, Dragos said. Keeping these perimeter devices up to date should be the first line of defense against attacks, whether they are from APTs or cybercriminals. Recent research has found that remote access to such devices is the most common way that attackers — especially ransomware groups — compromise a network. (continua…)

https://www.darkreading.com/cybersecurity-operations/east-west-monitoring-visibility-critical-apt-detection

DARKREADING **-** *Robert Lemos,* **-***March 25, 2025*

La progettazione delle infrastrutture viarie secondo il nuovo Codice dei Contratti Pubblici - Il nuovo Codice dei contratti pubblici (D.Lgs. 36/2023), entrato pienamente in vigore il 1° gennaio 2024, digitalizza l'intero ciclo degli appalti per garantire trasparenza ed efficienza. Ha semplificato il quadro normativo con un sistema più strutturato, ma restano criticità da risolvere.

Il 31 marzo 2023 è stato pubblicato in "Gazzetta Ufficiale" il nuovo Codice dei contratti pubblici (D.Lgs.n. 36/2023), con entrata in vigore parziale dal 1° aprile 2023. Tutti gli istituti sono entrati in piena validità ed efficacia a far data dal 1° gennaio 2024. Il digitale è divenuto il protagonista assoluto dell'intero ciclo di vita del contratto, dalla programmazione all'esecuzione ecc., garantendo la trasparenza, la tracciabilità, la partecipazione e il controllo di tutti i procedimenti concorsuali d'appalto.

Il Codice apre la disciplina con il principio del risultato, da cui emerge l'interesse primario che le stazioni appaltanti e gli enti concedenti debbano perseguire ovvero l'affidamento del contratto e la sua esecuzione con la massima tempestività e il miglior rapporto qualità-prezzo, nel rispetto dei principi di legalità, trasparenza e concorrenza e nell'interesse della Comunità, per il raggiungimento degli obiettivi dell'UE.

Sotto il profilo strutturale, il nuovo Codice degli Appalti opera un profondo riordino normativo. Alla coesistenza di varie fonti attuative di diversa natura (regolamenti ministeriali, linee guida ANAC, normativa emergenziale), il nuovo Codice degli Appalti sostituisce un sistema delle fonti strutturato con 229 disposizioni e 40 allegati.
Ciò rende il nuovo Codice degli Appalti immediatamente operativo, senza rinvio a successivi regolamenti attuativi e dà maggiore chiarezza al quadro regolatorio. In conclusione, il nuovo Codice degli Appalti ha introdotto importanti novità nel settore dei contratti pubblici, ma ci sono ancora molte criticità da affrontare per rendere il sistema più efficiente e trasparente.
(continua…)
https://www.ingenio-web.it/articoli/la-progettazione-delle-infrastrutture-viarie-secondo-il-nuovo-codice-dei-contratti-pubblici/
Ingenio - *Guido Caposio - 26.03.2025*

Signalgate: quando la sicurezza delle comunicazioni diventa un boomerang
Il caso Signalgate, e la conseguente fuga di informazioni riservate del governo USA, dovrebbe costituire una lezione di sistema, non solo per le istituzioni governative ma anche per il settore privato, sugli errori che si possono fare in termini di governance della cyber security.
Il mese di marzo 2025 ha segnato un **nuovo punto critico nel dibattito globale sulla sicurezza delle comunicazioni digitali**, con l'esplosione di quello che i media internazionali hanno ribattezzato "Signalgate", lo **scandalo della chat Signal del Governo Usa** in cui si parlava di **piani di guerra contro gli Houthi** e che rappresenta una lezione utile, tanto per uno Stato quanto per le aziende anche strutturate, sugli **errori che si possono fare in termini di governance della cyber security**.
L'evento – che ha visto coinvolti alti funzionari dell'amministrazione Trump e una serie di scelte discutibili nell'uso di strumenti digitali per la pianificazione di operazioni militari – rappresenta **molto più di un semplice scivolone politico**.
Questo incidente costituisce **un caso di studio emblematico sulle insidie dell'adozione non governata di tecnologie di comunicazione cifrate**, sulle **debolezze procedurali in materia di gestione degli accessi** e sulla **pericolosa sottovalutazione degli aspetti di cyber governance** anche in contesti ad alta sensibilità strategica.
Ecco, dunque, una lettura approfondita dell'accaduto, analizzando non solo la cronaca dei fatti ma anche le **implicazioni tecniche e organizzative che ne derivano**. Partiremo dallo scenario specifico che ha dato origine al caso mediatico, per poi estendere la riflessione a temi fondamentali quali la **sicurezza applicativa**, la **gestione dell'identità e degli accessi (IAM)**, l'importanza di **processi di awareness interna** e la necessità – sempre più urgente – di un **approccio integrato e consapevole alla cyber security**, anche (e soprattutto) nei contesti istituzionali.
Indice degli argomenti
- Signalgate: fuga informativa causata da un errore umano
- Uso improprio della crittografia: fra sicurezza del mezzo e insicurezza dell'uso
- Aspetti tecnici e organizzativi evidenziati dal Signalgate
- Reazioni e impatti politici: tra sottovalutazione e danno d'immagine
- Lezioni apprese: come il settore pubblico e privato dovrebbero reagire

Signalgate: fuga informativa causata da un errore umano
L'episodio ha avuto origine da una conversazione su Signal, una popolare app di messaggistica cifrata end-to-end, utilizzata da un ristretto gruppo di funzionari di alto profilo dell'amministrazione Trump – inclusi il vicepresidente J.D. Vance, il segretario alla Difesa Pete Hegseth e il consigliere per la sicurezza

nazionale Mike Waltz – per coordinare, in tempo reale, operazioni militari statunitensi contro i ribelli Houthi nello Yemen.
La chat, denominata "Houthi PC small group", doveva servire come canale alternativo, diretto e sicuro, per discutere decisioni tattiche riservate.
Tuttavia, un evento imprevisto ha alterato completamente l'equilibrio della comunicazione: Waltz, nel tentativo di coinvolgere un giornalista per altri scopi, ha per errore incluso nella chat Jeffrey Goldberg, direttore di *The Atlantic*, senza verificarne l'identità e il contesto.
Goldberg ha successivamente pubblicato una serie di contenuti riservati scambiati nella chat, inclusi dettagli operativi sull'orario esatto degli attacchi militari. Da qui, la deflagrazione mediatica e politica del caso. (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/signalgate-quando-la-sicurezza-delle-comunicazioni-diventa-un-boomerang/
Cybersecurity360 - *Sandro Sana - 2 apr 2025*

Sicurezza cyber, la chiave è la partnership tra umano e intelligenza artificiale
Le capacità di protezione e difesa nella cyber security possono essere migliorate in un mix di collaborazione arricchita ed efficacia aumentata attraverso l'impiego di un "ibrido operativo" formato dall'individuo e agenti di AI. Il perché ce lo spiegano due esperti
La fiducia nella sicurezza informatica dell'AI dipende dalle sue capacità tecniche e anche dalla sua capacità di analizzare in modo affidabile i dati in ambienti reali. In altre parole, **l'AI sta trasformando la sicurezza informatica migliorando la capacità di rilevare, rispondere e monitorare le minacce realizzando una collaborazione uomo-macchina pienamente migliorata**.
Ma nonostante i progressi dell'AI e la persistente crescita degli attacchi cyber, non è realistico affidare il pieno controllo delle decisioni sulla sicurezza all'AI. Piuttosto, **combinare l'intelligenza artificiale (AI) con l'esperienza umana, crea sistemi di sicurezza più forti e adattabili:** gli strumenti AI elaborano rapidamente grandi quantità di dati e individuano modelli che potrebbero indicare minacce, lavorando insieme a esperti umani che apportano una profonda comprensione e pensiero strategico.
Potremmo dire che la collaborazione umana è essenziale per risolvere alcune limitazioni dell'AI: gli esperti di sicurezza umana che possono guidare, supervisionare e valutare gli output degli agenti di AI. Questa partnership migliora la capacità di rilevare e rispondere alle minacce, rendendo gli sforzi di sicurezza informatica più efficaci e resilienti.
In che modo questa collaborazione possa diventare un partenariato di lungo corso, sia sul fronte della difesa e protezione, sia per l'opportunità di crescita specialistica dell'essere umano nell'interazione operativa arricchita con gli agenti AI, lo spiega **Dorit Dor**, Chief Technology Officer di Check Point Software Technologies (CPST) che nella recente conferenza **CPX2025 a Vienna** ha fornito elementi di innovazione in questo senso e ha approfondito ulteriormente l'argomento con noi.
Indice degli argomenti

Il partenariato uomo-AI nella difesa e protezione di cyber security
Alla domanda se possa esistere una vera partnership tra esseri umani e AI per gli obiettivi di sicurezza informatica, Dor spiega che il termine "partnership è ampio e la sicurezza informatica comprende molte sfaccettature".
Quindi suggerisce che "per analizzare efficacemente l'interazione tra IA e sicurezza informatica, sono da considerare cinque aspetti chiave: 1) **attacchi basati sull'AI**, ovvero come gli aggressori utilizzano e utilizzeranno l'AI per migliorare le proprie capacità e il conseguente impatto sul panorama delle

minacce; 2) **l'AI per la difesa che riguarda l'applicazione delle tecnologie di IA** per proteggere in modo proattivo dagli attacchi informatici; 3) **l'AI per le operazioni di sicurezza che sfrutta utilizzo dell'AI per semplificare le operazioni di sicurezza**, inclusa la gestione degli indicatori chiave di prestazione (KPI), la generazione di report e la garanzia della conformità; 4) **la protezione dei sistemi di AI stessi** per la loro salvaguardia da attacchi e vulnerabilità; 5) **la gestione dei rischi sui dati correlati all'AI** per la mitigazione dei rischi sui dati associati allo sviluppo e all'implementazione dei sistemi di AI". (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/sicurezza-cyber-la-chiave-e-una-partnership-tra-umano-e-intelligenza-artificiale/
Cybersecurity360 *- Alessia Valentini* **-** *2 apr 2025*

For flux sake: CISA, annexable allies warn of hot DNS threat
Shape shifting technique described as menace to national security
The US govt's Cybersecurity Infrastructure Agency, aka CISA, on Thursday urged organizations, internet service providers, and security firms to strengthen defenses against so-called fast flux attacks.
Fast flux refers to a technique for obscuring malicious servers by, rather simply, rapidly altering their Domain Name System (DNS) records.
Malicious cyber actors use fast flux to obfuscate the locations of malicious servers
CISA, the FBI, and cyber authorities in Australia, Canada, and New Zealand – evidently still on speaking terms with the US despite threats of annexation – consider such DNS deception a threat to national security. Fast flux may be less troubling than saber-rattling by a head of state but it is an active threat rather than a proposed one.
"Malicious cyber actors, including cybercriminals and nation-state actors, use fast flux to obfuscate the locations of malicious servers by rapidly changing Domain Name System (DNS) records," said CISA in its advisory [PDF]. "Additionally, they can create resilient, highly available command and control (C2) infrastructure, concealing their subsequent malicious operations."
DNS maps domain names, such as google.com, to numeric network IP addresses like 142.250.191.46. When a crook or government spy infects a victim's computer with malware, that software nasty can look up a specific domain name, such as something programmed in like malware.example.com, to get that full domain name's latest IP address from its DNS records. The malware then connects to the server at that IP address to receive instructions from its controllers and to send stolen data.
Every few minutes, typically three to five, the DNS for malware.example.com is automatically updated by the malware's masters so that it resolves to the IP address of another server controlled by those operators. That allows the malware to outrun any network filters that intercept connections to IP addresses of known bad systems. By constantly changing the DNS records from one IP address to another, it turns into a game of Whac-A-Mole.
One could employ DNS filtering, to catch the look ups of known bad domains, but different domain names can be looked up on the fly by the malware, making it another game of Whac-A-Mole. malware.abc.example.com, malware.def.example.com, malware.jkl.example.com, etc, as a trivial example.
As described by MITRE, fast flux comes in two unpalatable flavors: Single flux and double flux. Single flux involves rapidly changing the DNS A record (or AAAA record for IPv6) which binds the domain name to an IP address. Double flux changes both the DNS A record and the authoritative nameserver for that record – the DNS NS record for the DNS zone file (the full set of DNS records for the domain). It may also involve changing the DNS CNAME (Canonical Name) record. (continua…)

https://www.theregister.com/2025/04/03/cisa_and_annexable_allies_warn/?is=0b8f2776946dfb918b4bb1b43d6713cbf6a927ebd5e2184a38ea2f92df6f9da9
The Register - *Thomas Claburn - 3 Apr 2025*

Cavi sottomarini: l'UE svela il piano strategico per difenderli dalla minacce cyber
Dall'Unione Europea un nuovo piano d'azione per rafforzare la sicurezza dei cavi sottomarini. L'obiettivo è continuare a tutelare gli Stati membri nella prevenzione agli attacchi alle infrastrutture sottomarine che trasportano quasi la totalità dei nostri dati internet a livello globale
Dopo l'annuncio dello scorso 9 febbraio a Vilnius da parte della Presidente Ursula von der Leyen in occasione del **Balting Energy Independence Day**, qualche giorno fa è stata presentata dalla vicepresidente esecutiva della Commissione europea per la sovranità tecnologica, Henna Virkunnen, la Comunicazione congiunta della Commissione e dell'Alto Rappresentante dell'UE per gli Affari Esteri, **Joint Communication to the European Parliament and The Council – EU Action Plan on Cable Security**, volta al **potenziamento della sicurezza e della resilienza dei cavi sottomarini**.
Indice degli argomenti

- Un nuovo piano d'azione per i cavi sottomarini
- I punti chiave del piano
  - Prevenzione
  - Rilevamento
  - Risposta e recupero
  - Deterrenza
- Qualche numero sul futuro dei cavi sottomarini
- Azioni future e continuità

Un nuovo piano d'azione per i cavi sottomarini
I cavi sottomarini, è bene ricordarlo, rappresentano **un'infrastruttura fondamentale per il trasporto dei dati internet mondiale**, considerato che vi transita il 99% del traffico. Inoltre, favoriscono l'integrazione dei mercati elettrici degli Stati membri, incrementano la sicurezza di approvvigionamento e forniscono energia rinnovabile offshore alla terraferma.
Già qualche mese fa era stata approvata da parte della Commissione Europea una dichiarazione congiunta sulla sicurezza e sulla resilienza dei cavi sottomarini, proposta dagli Stati Uniti, "The New York Joint Statement on the Security and Resilience of Undersea Cables in a Globally Digitalized World", in occasione dell'Assemblea generale delle Nazioni Unite a New York, che mirava a garantire sicurezza, affidabilità, sostenibilità e resilienza delle infrastrutture che passano sotto i nostri oceani per il trasporto dati di tutto il mondo.
Tra i principi da seguire, esposti nella dichiarazione, anche raccomandazioni sulla selezione dei fornitori di cavi sottomarini a basso rischio, sull'uso delle migliori pratiche di cybersicurezza, sul diversificare le rotte e proteggere le reti via cavo dall'accesso non autorizzato ai dati in transito.
Come dichiarato in quell'occasione dalla vicepresidente esecutiva per Un'Europa pronta per l'era digitale, Margrethe Vestager, "I cavi sottomarini sono un'infrastruttura altamente strategica.
Quasi tutto il traffico dati internazionale viene trasportato attraverso cavi sottomarini, esponendoli a minacce alla sicurezza, dall'hacking alla sorveglianza". (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/cavi-sottomarini-lue-svela-il-piano-strategico-per-difenderli-dalla-minacce-cyber/
Cybersecurity360 *- Marco Santarelli - 3 apr 2025*

Rafts of Security Bugs Could Rain Out Solar Grids

At least three major energy solution and renewable energy companies have nearly 50 vulnerabilities — many of them "basic" mistakes — indicating a lack of developed cybersecurity safeguards.

As climate change continues to show irreversible effects on the planet, the push for more sustainable energy options continues to gain popularity. Solar power systems, in particular, are increasingly becoming more widely used, accounting for a $70 billion market value in 2024. But these eco-friendly options come with downsides, too, specifically when it comes to cybersecurity.

Researchers at Forescout — Daniel dos Santos, Francesco La Spina, and Stanislav Dashevskyi — this week at Black Hat Asia in Singapore detailed close to 50 vulnerabilities impacting the security of at least three leading solar power vendors, Sungrow, Growatt, and SMA.

The researchers found that each vendor has vulnerabilities affecting the whole solar power ecosystem, from power inverters and network connectivity dongles to mobile applications and cloud backends.

A Solar Ecosystem of Problems

In the course of their research, the Forescout analysts found 46 new vulnerabilities across the vendors' gear, which could enable scenarios that affect grid stability and user privacy, or, in residential settings, pivot to hijack other smart devices in users' homes.

For instance, Growatt inverters were susceptible to cloud-based takeover, allowing unauthorized access and control of a user's resources, solar plants, and devices, Forescout found. Sungrow inverters could be hijacked by harvesting communication dongle serial numbers through various insecure direct object references (IDORs), using hardcoded credentials found on the device and publishing messages that lead to remote code execution and full takeover of the inverter.

Once in control of the inverters, attackers can tamper with their power output settings or switch them off and on in a coordinated manner as a botnet. "The combined effect of the hijacked inverters produces a large effect on power generation in a grid," according to Forescout's report. "The impact of this effect depends on that grid's emergency generation capacity and how fast that can be activated." (continua…)

https://www.darkreading.com/vulnerabilities-threats/security-bugs-could-rain-out-solar-grids

DARKREADING - *Kristina Beek - April 4, 2025*

Semiconduttori, IA croce e delizia: le sfide per un futuro sostenibile

La crescita esponenziale dell'IA pone nuove sfide nella produzione e nella supply chain dei semiconduttori, richiedendo investimenti strategici e partnership. Allo stesso tempo, molte aziende già utilizzando la Gen AI per ridurre i tempi di progettazione e accelerare i cicli di sviluppo. Come bilanciare sostenibilità e innovazione

Negli ultimi anni, l'evoluzione tecnologica ha registrato un'accelerazione senza precedenti, spinta dall'**adozione diffusa dell'intelligenza artificiale** in molteplici settori industriali.

In particolare, **l'intelligenza artificiale generativa** sta aprendo nuove frontiere applicative, incrementando la domanda di semiconduttori avanzati.

L'aumento esponenziale della richiesta di chip per AI sta mettendo alla prova l'intero ecosistema produttivo, sollevando interrogativi su capacità di fornitura, **resilienza della supply chain e sostenibilità delle operazioni.**

Inoltre, **il settore sta affrontando sfide complesse legate alla monetizzazione del software integrato nei semiconduttori**, un elemento cruciale per garantire la flessibilità e la scalabilità delle soluzioni.

Indice degli argomenti

- **Strategie per mantenere la competitività e garantire una crescita sostenibile**
  - Ottimizzare la progettazione e la produzione di chip con l'IA
  - Ricerca di nuovi materiali e sviluppo di architetture alternative
  - Diversificare la supply chain
  - L'integrazione tra hardware e software
  - La sostenibilità al centro delle strategie aziendali
  - Soluzioni di sicurezza integrate
- **Strategie olistiche per i semiconduttori AI**

Domanda e personalizzazione dei semiconduttori AI

L'intelligenza artificiale sta ridefinendo il fabbisogno tecnologico delle aziende in numerosi settori, dai data center all'automotive, fino alla sanità e all'industria manifatturiera. Secondo un **report** del Capgemini Research Institute, **la richiesta di chip per AI crescerà del 29% entro il 2026**, un tasso quasi doppio rispetto alla crescita attesa dell'intero settore dei semiconduttori (+15%). (continua…)
https://www.agendadigitale.eu/mercati-digitali/semiconduttori-ia-croce-e-delizia-le-sfide-per-un-futuro-sostenibile/
Agenda Digitale - *Riccardo Dolfi - 4 apr 2025*

AI autonoma: il ruolo degli agenti intelligenti e dei sistemi multi-agente

Gli agenti intelligenti operano autonomamente, adattandosi all'ambiente e interagendo con altri sistemi. Quando combinati in sistemi multi-agente, possono risolvere compiti complessi, con applicazioni in IA, robotica, finanza e logistica, migliorando efficienza e automazione nei diversi settori Cosa sono gli Agenti, e in particolare gli **Agenti Intelligenti**, di cui si sente molto parlare? Gli agenti sono moduli software con una particolare caratteristica: sono autonomi, ossia, una volta attivati, a meno che non vengano fermati, continuano a funzionare portando avanti le loro attività.

Indice degli argomenti

Agenti intelligenti: cosa sono, cosa possono fare

Come il nome suggerisce, **sono capaci di agire sul loro ambiente, mediante opportuni "attuatori",** e dunque devono innanzitutto essere in grado di percepire l'ambiente stesso, mediante "sensori". Gli agenti possono essere intelligenti se basati su tecniche di Intelligenza Artificiale ("Artificial Intelligence", o AI, e dunque "Agenti AI") e opportunamente programmati. Gli agenti sono "situati" in un ambiente, che può essere puramente software oppure fisico. Gli agenti possono costituire la mente pensante dei robot, ossia disporre di un corpo fisico.

Le capacità principali di un agente sono:

- **Reattività**, ossia la capacità di reagire opportunamente ad eventi esterni (cioè provenienti dall'ambiente in cui l'agente è situato) mettendo in atto una o più azioni.
- **Proattività**, ossia la capacità di intraprendere attività ed effettuare azioni per perseguire i propri obiettivi.

Infatti, **gli agenti possono essere programmati per avere intenzioni, perseguire obiettivi ed eseguire compiti.** Per perseguire i propri obiettivi, gli agenti devono essere capaci di costruire un piano (quindi devono avere capacità di pianificazione) ed eseguirlo, e, nel caso, riadattarlo se qualcosa va storto.

La capacità di pianificare è indubbiamente una componente fondamentale dell'intelligenza, e presuppone la capacità di costruire un modello interno del mondo esterno (o almeno del frammento di mondo a cui si è al momento interessati) e delle azioni su di esso possibili da parte dell'agente, date le sue capacità e le risorse disponibili. Sulla base di questa descrizione, un processo di pianificazione

identifica, per un dato obiettivo, una o più sequenze di azioni che possano condurre dallo stato attuale del mondo ad uno stato in cui l'obiettivo sarà stato raggiunto.

Agenti intelligenti e Sistemi Multi-Agente

Gli agenti possono costituire "Sistemi Multi-Agente" (Multi-Agent Systems, o MAS). Gli agenti componenti possono essere cooperativi, ed in tal caso eventualmente possono perseguire intenzioni e obiettivi condivisi. Agenti competitivi possono invece eventualmente negoziare per suddividere fra loro le risorse disponibili. Per far parte di MAS, gli agenti devono possedere "abilità sociali", ossia devono essere in grado di comunicare. A tale scopo sono stati sviluppati i cosiddetti Agent Communication Languages (ACL) che prevedono vari tipi di messaggi, con la propria sintassi e semantica. Ad esempio, un agente può informare un altro agente in merito a qualcosa, o può avanzare una richiesta, o può accettare una richiesta e inviare una risposta, ecc.

Agenti intelligenti e sistemi multi-agente: i principali vantaggi e casi pratici

L'uso di agenti intelligenti e sistemi multi-agente può offrire, già oggi o in prospettiva, numerosi vantaggi agli utenti umani in diversi contesti. Ecco alcuni dei principali potenziali benefici: (continua…)

https://www.agendadigitale.eu/industry-4-0/ai-autonoma-il-ruolo-degli-agenti-intelligenti-e-dei-sistemi-multi-agente/

AgendaDigitale - *Stefania Costantini - 7 apr 2025*

Sistemi robotici e sicurezza: problematiche e raccomandazioni per le aziende - Un documento dell'Agenzia EU-OSHA si sofferma sulle problematiche e opportunità dal punto di vista della sicurezza della robotica avanzata e dei sistemi basati sull'intelligenza artificiale. Focus sulle criticità e sulle raccomandazioni per le aziende.

Bilbao, 8 Apr – In relazione alla campagna " Lavoro sano e sicuro nell'era digitale", promossa dall'Agenzia europea per la sicurezza e la salute sul lavoro (EU-OSHA), sono state svolte in questi ultimi anni diverse ricerche per comprendere l'impatto delle nuove tecnologie e della digitalizzazione nel mondo del lavoro.

Come raccontato, ad esempio, nella relazione " Advanced robotic automation: comparative case study report" sono stati sviluppati vari studi di casi incentrati sui luoghi di lavoro che utilizzano i sistemi robotici avanzati e basati sull'intelligenza artificiale.

Questi sistemi, la cui versatilità rappresenta una delle qualità più note, "possono essere utilizzati in un'ampia gamma di luoghi di lavoro, fornendo supporto e automatizzando numerosi compiti". E se ogni studio di caso può presentare "problematiche e opportunità specifiche al suo scenario, che devono essere affrontate su base individuale", vi sono anche "numerose opportunità e problematiche ricorrenti" in materia di salute e sicurezza sul lavoro (SSL).

A ricordarlo è il documento di sintesi EU-OSHA intitolato "Robotica avanzata e sistemi basati sull'intelligenza artificiale sul luogo di lavoro: problematiche e opportunità dal punto di vista della SSL conseguenti alla loro adozione", un documento a cura di Eva Heinold, Patricia Helen Rosen e Dott. Sascha Wischniewski (Istituto federale per la sicurezza e salute sul lavoro - BAuA).

Se in un primo articolo di presentazione del documento abbiamo parlato delle opportunità, oggi ci soffermiamo su alcune problematiche di queste tecnologie e su alcune raccomandazioni per le aziende:

Problematiche nell'uso della robotica avanzata: i rischi fisici e la paura

Problematiche nell'uso della robotica avanzata: la dequalificazione e il personale

Problematiche nell'uso della robotica avanzata: raccomandazioni per le aziende

(continua)
https://www.puntosicuro.it/robotica-intelligenza-artificiale-C-137/sistemi-robotici-sicurezza-problematiche-raccomandazioni-per-le-aziende-AR-24629
Punto Sicuro – *Tiziano Menduto - 08/04/2025*

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	Glauco Bertocchi

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

Silvano Bari

ai quali potete inviare suggerimenti e quesiti scrivendo a:
segreteria@infrastrutturecritiche.it