AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Newsletter

ANNO 2022	N. 8/ 2022	Settembre 2022

Nuovi anticorpi per un'Italia cyber-sicura*

La strategia italiana di sicurezza nazionale cibernetica è stata aggiornata al 2022 e alle nuove sfide che, nella visione dell'Agenzia per la cybersicurezza nazionale (Acn), diventano obiettivi. L'alba del nuovo mondo si vede prima di tutto dalla postura, consapevole e ottimista, che coglie opportunità per un lavoro coordinato, consapevole e smart così da guardare al futuro con serenità.
Una visione a quattro anni per la quale l'Acn pone gli obiettivi strategici su tre binari: protezione, risposta e sviluppo. Nel primo troviamo i temi della certificazione di prodotto per la sicurezza, che porterà questa disciplina a essere una professione e non un'arte, e il contrasto alla disinformazione. Alla voce risposta c'è la deterrenza, con squadre specializzate e multidisciplinari, e la reazione agli attacchi basata sulla condivisione delle informazioni. A tal proposito è prevista finalmente la creazione degli Information sharing and analysis centre (Isac) con al centro l'Acn e intorno una costellazione di hub per scambi informativi. Infine lo sviluppo, legato alla creazione del Centro nazionale di coordinamento e alla creazione di un parco nazionale per la sicurezza cibernetica legato agli hub locali.
Si parla anche di un'autonomia digitale nazionale soft, che considera le risorse umane e la formazione. Questa è quella che ci dovrebbe interessare di più. Il mercato del lavoro della cyber-security è, con una metafora, "rinascimentale", con grandi aziende che fanno da mecenate e che premono il settore giocando al rialzo continuo delle offerte, di fatto escludendo le Pmi.
Il problema è risolvibile solo con l'espansione dei percorsi formativi e con una crescita della quantità dei profili disponibili. Se non iniziamo a produrre cyber-professionisti questa disciplina resterà appannaggio di pochi, una situazione che non possiamo permetterci.
Il piano di implementazione è il punto di partenza per realizzare la strategia. Mette a terra gli obiettivi di medio e lungo termine, ne sostanzia il significato e le azioni da intraprendere.
Ancora una volta l'obiettivo è l'autonomia tecnologica digitale: l'Acn promuove un Piano per l'industria cyber nazionale a sostegno di imprese e start up per progettare e realizzare prodotti e servizi ad alta affidabilità, tra i quali un'infrastruttura di comunicazione nazionale. Le industrie dovranno sostenere un grande balzo in avanti in termini di tecnologia e il Piano spiega il metodo per effettuarlo.
L'attuazione ruota intorno alla capacità dei servizi digitali nazionali ed è focalizzato sull'accrescimento di tutte le competenze, tecniche, scientifiche e anche umanistiche.
L'Acn gestirà i 623 milioni del Pnrr destinati alla cyber-security su tre aree principali: amministrazione resiliente, servizi nazionali cyber e laboratori di valutazione e certificazione. Inoltre l'Acn opererà quale ente regolatore, certificatore e di vigilanza del settore, definendo i livelli minimi di sicurezza nei diversi ambiti, potendo anche effettuare ispezioni e irrogare sanzioni.
E infine si parla del Centro di valutazione e certificazione nazionale (Cvcn) e degli schemi di certificazione e valutazione. Con questo e con il provvedimento sulla identificazione della Autorità nazionale di sicurezza capiremo qual è il futuro che ci si prospetta e che rappresenta il passaggio della cyber-security dall'artigianato al professionismo. L'Acn, poi, ha nominato anche il Comitato tecnico scientifico. Nove membri, quattro dall'industria, quattro dall'accademia e un presidente pro tempore di

una associazione di security aziendale, verranno chiamati a promuovere la collaborazione tra università, ricerca e sistema produttivo nazionale.

* AirPress, n.135, luglio-agosto 2022

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

ATTIVITA' DI EDUCATION

Sono in corso di programmazione le attività di formazione per soci e simpatizzanti che si svolgeranno nella seconda parte dell'anno 2022.

Anzitutto, l'accordo con IsacaRoma consentirà ai soci AIIC di partecipare ai loro seminari (svolti principalmente in modalità webinar) su cybersecurity, risk management e protezione dei dati.

Per quanto riguarda i nostri "Colloquia", abbiamo in cantiere per metà novembre un evento molto interessante sulla protezione delle infrastrutture critiche tramite "droni" mentre stiamo organizzando, con una startup del settore, un evento di illustrazione di soluzioni innovative di predizione e anticipazione degli eventi negativi per tendere al rischio minimo nelle realtà RIR (Rischio Incidente Rilevante) e in generale dove il Real Time Risk Management e la Resilience Engineering rappresentano aspetti qualificanti e determinanti nella gestione.
Stiamo valutando le modalità di svolgimento di questi eventi, possibilmente – se le condizioni pandemiche lo consentiranno – in modalità mista, presenza e distanza.
Inoltre, stiamo già prendendo accordi per una ripresa delle visite aziendali presso enti/imprese di rilevanza nazionale.
Vi terremo informati.
Vi ricordiamo anche che proprio per fornire un valore aggiunto ai nostri associati, alcuni eventi saranno riservati soltanto a chi è in regola con il pagamento delle quote associative.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.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.

AIIC ha sottoscritto convenzioni di collaborazione con altre Associazioni. In particolare con:

- **ARPIC –** La convenzione tra AIIC e ARPIC (Romanian Association for Critical Infrastructures and Services Protection) è entrata in vigore il 01/04/2012. ARPIC e AIIC, hanno concordato di collaborare sulla base di una partnership attiva, con lo scopo di:
usare la loro esperienza comune per aiutare l'implementazione di aspetti critici del concetto di infrastruttura nell'ambito dell'UE e del quadro giuridico nazionale,
costruire e promuovere una rete europea di organizzazioni professionali ed esperti che lavorino nel campo dei servizi e della protezione delle infrastrutture critiche.
- **CENTRO RICERCHE THEMIS** – la convenzione tra AIIC e THEMIS è stata firmata il 21 marzo 2016. Le due Associazioni si sono impegnate a collaborare per la realizzazione congiunta di iniziative e servizi da proporre agli associati, secondo forme e modalità da stabilire con appositi accordi.
- **EUCONCIP** – AIIC è membro fondatore di EUCONCIP (European Cooperation Network on Critical Infractructures Protection) assieme a Fondazione Formit, ARPIC (Romanian Asociation for Critical Infrastructures and Services Protection), CCI (Centro de Ciberseguridad Industrial), CESS (Centre for European Security Strategies), S21Sec. EUCONCIP è un'associazione con sede legale in Italia, costituita nel 2016 con lo scopo di promuovere la cooperazione tra paesi e tra settori nel campo della protezione delle infrastrutture critiche. L'obiettivo principale di EUCONCIP è contribuire allo sviluppo di un approccio armonizzato da adottare per la protezione delle infrastrutture critiche che sono essenziali per il mantenimento delle funzioni vitali della società, della salute, della sicurezza, del benessere economico e sociale delle persone (Direttiva UE 2008/114 / CE).
- **AFCEA ROMA** - la convenzione tra AIIC e AFCEA – Armed Forces Communications & Electronics Association – Capitolo di Roma è stata firmata il 18 settembre 2017. Scopo della convenzione è di promuovere principi e tecniche professionali reciproche e di interesse per entrambe le Associazioni, avvicinando così le due community nazionali su tematiche comuni. La collaborazione permetterà di dare evidenza a eventi organizzati da ciascuna associazione, attraverso i propri canali di comunicazione, e di sviluppare e sostenere iniziative congiunte su temi di comune interesse.
- **AIAS** – la convenzione tra AIIC e AIAS Associazione professionale Italiana Ambiente e Sicurezza) è stata firmata il 15 febbraio 2016 con durata triennale. Le due associazioni intendono promuovere forme di collaborazione tra le attività di AIAS e delle sue società appartenenti al Networkaias e

precisamente AIAS Academy e di AIASCert e le attività di AIIC al fine di promuovere una cultura applicativa di una prevenzione efficace che tenga conto di tutti gli aspetti di sicurezza

- **CLOUD SECURITY ALLIANCE ITALY CHAPTER –** la convenzione tra AIIC e CLOUD SECURITY ALLIANCE ITALY CHAPTER è stata firmata il 26 aprile 2012, con l'intento di collaborare per dare reciprocamente visibilità alle iniziative sviluppate autonomamente da ciascuna delle due associazioni in occasione di incontri, corsi e seminari di studio.
- **ISACA Rome Chapter** La convenzione con ISACAROMA (capitolo di Roma della *Information Systems Audit And Control Association*, associazione internazionale con circa 140.000 soci nel mondo) è stata firmata il 7 dicembre 2018 con l'intento promuovere la collaborazione tra le due associazioni per l'organizzazione di eventi, seminari sulla cyber security e le infrastrutture critiche.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.
Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.
Potete scriverci al nostro solito indirizzo email: *segreteria@infrastrutturecritiche.it*

NEWS E AVVENIMENTI

IoT, come la tecnologia migliora la sicurezza sul lavoro: ecco le ricerche - Le tecnologie IoT, in particolare le innovazioni Machine-to-machine, augmented e virtual reality, in ambito industriale possono svolgere un ruolo rilevante per la sicurezza del lavoratore: vediamo la situazione, analizzando anche i risultati del progetto Smartgrind.
Lo sviluppo di progetti di ricerca applicata sulla tecnologia IoT consente di supportare, con metodologia scientifica, il miglioramento della produttività, le attività manutenzione, i controlli nonché di studiare le migliori modalità applicative per la sicurezza degli operatori coinvolti nei processi produttivi industriali. All'interno dei nuovi sistemi di produzione le tecnologie, legate all' IIoT "Industrial Internet of Things" e al mondo delle M2M "Machine -to- Machine", soluzioni di Augmented reality (AR) e Virtual Reality (VR), rappresentano un ruolo importante nell'ambito della sicurezza del lavoratore.
La connessione in rete, offerta da queste nuove frontiere digitali, dei diversi elementi costituenti l'ambiente di lavoro e lo scambio di dati e informazioni in tempo reale consentono di creare sistemi cyber fisici che contribuiscono a migliorare gli standard di sicurezza dell'operatore coinvolto nel processo produttivo industriale. Le potenzialità offerte dall'adozione di queste tecnologie abilitanti si esaltano in contesti nei quali è possibile stabilire un'integrazione con i dati provenienti da sensori di macchine, sistemi cloud e da sistemi informativi aziendali.
Avere a disposizione, in tempo reale, informazioni e dati real time facilmente elaborabili e consultabili, consente un uso delle macchine più sicuro per l'operatore e offre allo stesso tempo la possibilità di eseguire interventi di manutenzione predittiva. In tale contesto anche i DPI – Dispositivi di protezione individuale – che sono utilizzati al fine di gestire il cosiddetto rischio residuo e sono considerati da sempre come l'ultimo baluardo per proteggere chi li indossa dalle conseguenze di un incidente – si innovano, adeguano e integrano con le nuove tecnologie.
Indice degli argomenti

(continua)
https://www.agendadigitale.eu/sanita/iot-come-la-tecnologia-migliora-la-sicurezza-sul-lavoro-ecco-le-ricerche/
Agenda Digitale - *Alessandra Ferraro, Anna Palermo, Marco Pirozzi - 01 Lug 2022*

Connected car e smart mobility, la crescita guida il cambiamento dei modelli di business - Gli ultimi dati dell'Osservatorio Connected Car & Mobility della School of Management del Politecnico di Milano confermano sia l'incremento delle auto "intelligenti", che oggi rappresentano quasi la metà del parco circolante in Italia, sia la trasformazione dell'automotive in un mercato basato sempre di più su meccanismi di servitizzazione.
Arrivano almeno due conferme dagli ultimi risultati dell'Osservatorio Connected Car & Mobility della School of Management del Politecnico di Milano, presentati pochi giorni fa. Anzitutto, che i trend di

crescita di questo ampio comparto continuano a essere molto sostenuti e in secondo luogo che il segmento non solo coinvolge un insieme di tecnologie sempre più integrate all'interno del settore automotive ma abilita anche nuovi modelli di business. In merito alla prima conferma, il mercato della Connected Car nel 2021 ha raggiunto una cifra pari a 1,92 miliardi di euro, l'8% in più rispetto al 2020, con una netta prevalenza delle soluzioni per l'auto connessa che, nel loro insieme, valgono 1,28 miliardi di euro. A queste si aggiungono i sistemi di Advanced Driver Assistance Systems (ADAS) presenti di default nei nuovi modelli, che vanno dalla frenata automatica d'emergenza al mantenimento del veicolo in corsia per un ammontare di 640 milioni di euro. L'incremento della smart mobility è trainato anche dalla diffusione di auto nativamente connesse tramite SIM (il 19% del totale) e dalla capacità degli attori della filiera di raccogliere grandi quantità di dati dai veicoli. In termini complessivi, alla fine del 2021 nel nostro paese quasi la metà del parco circolante, cioè 18,4 milioni di auto, era formato da auto connesse.

Indice degli argomenti

La servitizzazione come nuova frontiera della Connected Car
Tecnologie V2X, 5G nella Release 16 e veicoli a guida autonoma
Dalla logistica alla smart road del futuro *(continua)*
https://www.internet4things.it/automotive/connected-car-e-smart-mobility-la-crescita-guida-il-cambiamento-dei-modelli-di-business/
Internet4things *- di Maria Teresa Della Mura - 1 Luglio 2022*

Intelligenza artificiale e rischi connessi - Oggi l'IA (AI in inglese) è una tecnologia parecchio usata ma, come spesso accade i rischi connessi, che potrebbero portare alle situazioni descritte da Huxley in "A brave new world", non sono ancora correttamente percepiti.

Da "2001 Odissea nello spazio" a "A Brave new world" e "1984"

Già agli inizi degli anni '70, quando un minicomputer con una memoria di 32 kilobytes costava quanto una Rolls Royce e i cicli macchina si misuravano in millisecondi, si lavorava all'intelligenza artificiale, ma con progressi modesti rispetto agli altri settori. Nell'ottobre 2015 un evento eccezionale, forse non noto quanto merita, attestò il grande salto di qualità di questa disciplina.

Il programma AlphaGo(1) riuscì a battere uno dei più forti giocatori professionisti di Go. Per decenni programmatori di tutto il mondo si erano impegnati in tentativi vani di vincere il premio milionario collegato a questa sfida, faticando a raggiungere il livello di un buon dilettante. E questo quando già esistevano già da anni programmi in grado di battere inesorabilmente il campione mondiale di scacchi.

Il buono e il cattivo delle tecnologie

Oggi l'IA (AI in inglese) nelle sue varie accezioni è diventato un argomento comune, ma anche una tecnologia parecchio usata ed incentivata dai governi. Inoltre, grazie alle possibilità offerte dal cloud computing, molte sue funzioni sono rese accessibili a prezzi abbordabili.

L'attualità dell'argomento ha aperto il dibattito tra chi la considera una tecnologia "buona" ne vede solo vantaggi, come quello di viaggiare senza la fatica di tenere il volante e chi invece la considera "cattiva" magari influenzato dal ricordi di HAL, il computer impazzito di "2001 Odissea nello spazio".

In realtà le tecnologie in sé non sono né buone né cattive, mentre lo può essere l'uso che se ne fa.

Per esempio l'auto elettrica è considerata "buona" dalla massa perché non inquina. In realtà, considerando il ciclo completo di vita, dalla produzione allo smaltimento, comprendendo l'estrazione delle terre rare per le batterie, inquina più delle auto a benzina; se poi pensiamo a come viene prodotta l'elettricità, in paesi come la Germania possiamo affermare che le auto elettriche vanno prevalentemente a carbone.

I rischi connessi all'IA
L'importante è utilizzare le tecnologie quando danno veri vantaggi e non secondo la moda del momento od il grado di innovazione. Inoltre è necessario valutare attentamente i rischi connessi, sia in sede di progettazione che di esercizio.
Per esempio, alla luce del progresso attuale il rischio del computer impazzito sembra abbastanza lontano, non mancano però rischi di altro tipo, non meno gravi se sottovalutati.
Un articolo di IEEE del 3 gennaio elenca 6 punti da prendere in considerazione.
(continua)
https://www.ingenio-web.it/35299-intelligenza-artificiale-e-rischi-connessi
Ingenio *- Mariani Enrico - 12/07/2022*

Sicurezza cloud: le sfide che le aziende devono affrontare per una corretta migrazione - Sono sempre di più le aziende che migrano sul cloud per fare business. Proprio per questo motivo è importante avere una strategia chiara di come farlo in maniera sicura, senza esporre i processi di business a vulnerabilità. Ecco quali sono i capisaldi una buona strategia di migrazione
Vuoi per ampliare il loro portfolio di servizi, vuoi per ridurre i costi di manutenzione della loro infrastruttura IT, vuoi per tentare di sfuggire all'obsolescenza, sono sempre più numerose le aziende che decidono di migrare su uno o più cloud service provider commerciali (Azure, AWS, Google). Si stima infatti che l'88% delle aziende pensa di adottare il cloud o lo ha addirittura già fatto (Cloud Statistics: 10 Current Adoption and Usage Metrics – Axeleos Technology Consulting).
Indice degli argomenti
Ma il cloud è sicuro?
Come mettere a terra una buona strategia di migrazione
Protezione dei dati
Integrazione dei processi di manutenzione dell'infrastruttura
Conclusioni
(continua)
https://www.cybersecurity360.it/soluzioni-aziendali/sicurezza-cloud-le-sfide-che-le-aziende-devono-affrontare-per-una-corretta-migrazione/
Cybersecurity360 *- Giulia Traverso - 13 Lug 2022*

Linee guida ANSFISA per la gestione della sicurezza su strade e autostrade - Attraverso tre video presentazioni ad alcune figure di prim'ordine di ANSFISA si presentano i contenuti delle Linee guida per la implementazione, certificazione e valutazione delle prestazioni dei Sistemi di Gestione della Sicurezza (SGS) per le attività di verifica e manutenzione delle infrastrutture stradali e autostradali, realizzate con lo scopo di fornire uno strumento utile per la valutazione e gestione delle infrastrutture e per la pianificazione della manutenzione.
Le "Linee guida per la implementazione, certificazione e valutazione delle prestazioni dei Sistemi di Gestione della Sicurezza (SGS-ISA) per le attività di verifica e manutenzione delle infrastrutture stradali e autostradali", dopo un articolato iter di consultazione e confronto con gli operatori, sono state approvate con il decreto direttoriale del 22 aprile scorso e adottate da ANSFISA lo scorso 4 maggio 2022. Le Linee Guida sono disponibili sul sito di ANSFISA

Attraverso le "Linee guida per la implementazione, certificazione e valutazione delle prestazioni dei Sistemi di Gestione della Sicurezza (SGS) per le attività di verifica e manutenzione delle infrastrutture stradali e autostradali", ANSFISA ha voluto raggiungere il massimo livello di integrazione, armonizzando norme di alto livello per i Sistemi di Gestione della Sicurezza dell'ICAO (International Civil Aviation Organization), dell'EASA (European Aviation Safety Agency), dell'ERA (European Railway Agency) e della Direttiva Seveso III per elaborare una norma orizzontale indipendente dal dominio di applicazione. Dopodichè, si è proceduto a verificare tutte le connessioni tra la norma orizzontale e quelle verticali, ovvero le linee guida:
Road Infrastructure Safety Management – RISM, sviluppate dall'International Transport Forum,
Linee guida per la classificazione e gestione del rischio, la valutazione della sicurezza ed il monitoraggio dei ponti esistenti, adottate dal MIMS,
quelle relative al d.Lgs. 35/2011 di recepimento della Direttiva 2008/96/CE delle gallerie stradali, di prossima pubblicazione
Il risultato concettuale e logico è quello di un sistema di gestione che raccorda funzioni generali della sicurezza, con quelle più specifiche legate alle attività su una rete di traffico e in particolare legate alle infrastrutture stradali e autostradali ed infine con quelle ancora più specifiche focalizzate sulla singola tipologia di infrastruttura o al singolo componente, come ad esempio i ponti, i viadotti o i cavalcavia, le gallerie, la segnaletica, le barriere di sicurezza, le pavimentazioni.
(continua)
https://www.ingenio-web.it/35366-linee-guida-ansfisa-per-la-gestione-della-sicurezza-su-strade-e-autostrade
***Ingenio** - Frumento Sara - 19/07/2022*

Industria 4.0 e cyber security: tra protezione della produzione e business continuity - Per poter affrontare le sfide dell'Industria 4.0 è fondamentale un'evoluzione del mindset che porti a percepire l'investimento in cyber security come qualcosa di indispensabile e non opzionale, che porta beneficio all'intera società. Ecco perché e le soluzioni da adottare
In Italia sono più di 9mila le PMI che fanno parte dell'industria manifatturiera, settore che nell'ultimo anno sta vivendo la quarta rivoluzione industriale, anche detta Industria 4.0.
Fondamentalmente, con Industria 4.0 si intende quella transizione che le aziende produttive italiane stanno sperimentando, da una produzione manuale e analogica ad una produzione sempre più automatica e interconnessa.
Tale processo di innovazione e miglioramento delle performance nasconde tuttavia delle insidie da ricondurre alla protezione dei nuovi confini e paradigmi digitali all'interno e all'esterno delle aziende.
In questo contesto di digitalizzazione e connessione la cyber security diventa quindi non più opzionale, ma indispensabile per la business continuity e la prosperità del tessuto produttivo italiano.
È bene ricordare che un attacco informatico in contesto industriale può avere gravi ricadute non solo a livello di produzione, con fermi macchina o produzione difettosa, ma anche ricadute sulla sicurezza delle persone.
Indice degli argomenti
La crescente digitalizzazione dell'industria manifatturiera italiana
I cyber attacchi dell'industria manifatturiera italiana
Le sfide delle PMI dell'industria manifatturiera italiana
Le soluzioni in uso
Altre soluzioni per salvaguardare sicurezza e operatività
(continua)

https://www.cybersecurity360.it/soluzioni-aziendali/industria-4-0-e-cyber-security-tra-protezione-della-produzione-e-business-continuity/
Cybersecurity360 *- Andrea Filippo Marini, 20 Lug 2022*

Dominio aerospaziale, il nuovo ruolo dell'Intelligence: come cambiano gli scenari -
Il Copasir ha pubblicato la "Relazione annuale sul dominio aerospaziale quale nuova frontiera della competizione geopolitica". Tra gli obiettivi, il potenziamento delle strutture di governance per l'interesse nazionale. Analizziamoli nel dettaglio
Il Copasir, Comitato parlamentare per la sicurezza della Repubblica, ha di recente pubblicato la "Relazione sul dominio aerospaziale quale nuova frontiera della competizione geopolitica", approvata nella seduta del 7 luglio 2022 e trasmessa alle Presidenze delle Camere il giorno stesso.
Il dominio aerospaziale oggi rappresenta il campo di massima competizione a livello mondiale in ambito scientifico, economico e militare e anche l'Italia deve allinearsi agli altri Paesi, potenziando strutture di governance per l'interesse nazionale e la collaborazione a livello internazionale.
Indice degli argomenti
Il dominio aerospaziale e l'Italia
Spazio e Intelligence
L'asse Cina-Russia
(continua)
https://www.cybersecurity360.it/cybersecurity-nazionale/dominio-aerospaziale-il-nuovo-ruolo-dellintelligence-come-cambiano-gli-scenari/
Cybersecurity360 *- Marco Santarelli, 7 ago 2022*

Cambiamento climatico: sarà il quantum computing il deus ex machina? - Secondo gli analisti di McKinsey la tecnologia quantistica potrà contribuire ad abbattere le emissioni di CO2 fino a 7 gigatoni annui entro il 2035, portando il pianeta in linea con il target di 1.5°C in meno.
Il raggiungimento del net zero non sarà possibile senza enormi progressi nella tecnologia climatica. Ma il quantum computing potrebbe essere rivoluzionario in questo senso, contribuendo allo sviluppo di tecnologie climatiche capaci di abbattere le emissioni aggiuntive di CO2 fino a 7 gigatoni annui entro il 2035 (o, complessivamente, fino a 150 gigatoni nei prossimi trent'anni), rispetto alla traiettoria attuale, e di portare il pianeta in linea con il target di 1.5°C in meno.
Lo afferma il report "Quantum computing might just save the planet", con cui McKinsey & Company analizza le potenzialità offerte dal quantum computing in termini di riduzioni delle emissioni di anidride carbonica. L'indagine rivela che, in particolare, il quantum computing potrebbe aiutare a ridurre le emissioni in alcuni dei settori più sfidanti o a maggiore intensità di emissioni, come l'agricoltura, e potrebbe accelerare lo sviluppo di tecnologie necessarie su larga scala, come i pannelli solari e le batterie. Inoltre potrebbe contribuire a risolvere problemi di sostenibilità persistenti come il miglioramento delle batterie elettriche per il settore automotive, la produzione di cemento a emissioni zero, lo sviluppo di una tecnologia solare rinnovabile più avanzata, l'identificazione di modalità più rapide per ridurre il costo dell'idrogeno rendendolo una valida alternativa ai combustibili fossili e, infine, l'impiego dell'ammoniaca green come combustibile e fertilizzante.
Ma ecco il dettaglio delle singole potenzialità applicative.
Indice degli argomenti
La sfida della densità energetica delle batterie
Riduzione dell'impatto dei clinker
La decarbonizzazione dell'energia

Ottimizzare l'efficienza per ridurre il costo dell'idrogeno
Migliorare il tasso di produzione dell'ammoniaca
Potenziamento delle attività di cattura e sequestro del carbonio
Trasformazione del settore alimentare e forestale
(continua)
https://www.corrierecomunicazioni.it/green-economy/cambiamento-climatico-sara-il-quantum-computing-il-deus-ex-machina/
CorCom *- Veronica Balocco.17 Ago 2022*

A 'nightmare scenario': Data-tampering attacks are hard to detect, with devastating consequences
Attacks involving manipulation of data could pose an even more severe threat than data theft or ransomware in some cases, but are not top of mind for most businesses, experts told Protocol.
"If you're not looking for the threat, you pretty much fall for it every time," one cyber security expert said of data manipulation. Imagine a cybersecurity catastrophe like this one: A pharmaceuticals maker suffers a data breach, but no data is stolen and no ransomware is deployed. Instead the attacker simply makes a change to some of the data in a clinical trial — ultimately leading the company to release the wrong drug. It's a hypothetical scenario, for now. Ransomware and the theft of sensitive data remain massive top-of-mind security concerns, of course, but at least there are tools and procedures available to mitigate those issues. Data-tampering represents a different type of threat, and one that could be potentially even more serious for certain organizations, depending on the situation. And yet it's not on the radar for many businesses, experts told Protocol, due to the fact that few such attacks have occurred and come to light. But this type of attack is not totally unprecedented. In early 2021, for instance, a hacker who broke into a Florida water treatment plant was able to elevate the sodium hydroxide, or lye, in the water to an unsafe level. (The modification was quickly caught by an operator.)
Will Ackerly, a former NSA security architect who invented a data-protection standard used by U.S. defense and intelligence agencies, is among those who believe that data manipulation is poised to become a burgeoning threat in coming years.
Compared with other threats to data security, the manipulation of data is probably the "most nefarious and hardest to detect," said Ackerly, who is now co-founder and CTO of data security startup Virtru. And on the attacker side of the equation, the fact remains that today, "there are a lot of adversaries looking to trick someone into thinking something that's not true," he said. Another example is the growing use of deepfake audio and video in cyberattacks. A recent VMware study found that two-thirds of cyber incident responders investigated attacks that involved fabricated audio or video over the past year, up 13% from a year ago.
But as jarring as it is, the deepfake phenomenon is just one part of the larger threat that businesses are facing from manipulated data, experts told Protocol. (*continua…)*
https://www.protocol.com/enterprise/data-integrity-security-cyberattacks-threat
PROTOCOL -*Kyle Alspach August 22, 2022*

Privacy complaint targets Google over unsolicited ad emails
PARIS, Aug 24 (Reuters) - Google has breached a European Union court ruling by sending unsolicited advertising emails directly to the inbox of Gmail users, Austrian advocacy group noyb.eu said on Wednesday in a complaint filed with France's data protection watchdog.

The Alphabet unit (GOOGL.O), whose revenues mainly come from online advertising, should ask Gmail users for their prior consent before sending them any direct marketing emails, noyb.eu said, citing a 2021 decision by the Court of Justice of the European Union (CJUE).
While Google's ad emails may look like normal ones, they include the word "Ad" in green letters on the left-hand side, below the subject of the email, noyb.eu said in its complaint. Also, they do not include a date, the advocacy group added.
"It's as if the postman was paid to remove the ads from your mailbox and put his own instead," said Romain Robert, programme director at noyb.eu, with reference to Gmail's anti-spam filters that put most unsolicited emails in a separate folder.
Google did not immediately respond to requests seeking comment. A spokesperson for the CNIL confirmed the authority had received the complaint and that it was being registered. *(continua…)*
https://www.reuters.com/technology/privacy-complaint-targets-google-over-unsolicited-ad-emails-2022-08-24/
***REUTERS-** Mathieu Rosemain - August 24, 2022*

Scammers Create 'AI Hologram' of C-Suite Crypto Exec

Fraudsters used deepfake technology to impersonate the identity of a senior Binance official in online meetings with clients, the crypto exec has claimed.
Binance claims to be the world's largest cryptocurrency exchange by daily trading volume, making it a popular target for threat actors.
Chief communications officer (CCO) Patrick Hillmann said in a new blog post that he was shocked at the "layers of security protocols" new starters had to navigate during onboarding.
"Despite having previously led one of the world's largest cybersecurity teams and managed some of the largest data breaches in history (US OPM, Ashley Madison, etc.), I was not prepared for the onslaught of cyber-attacks, phishing attacks, and scams that regularly target the crypto community. Now I understand why Binance goes to the lengths it does," he explained.
"However, criminals will almost always find a way to adapt to and circumvent even the most secure system. Over the past month, I've received several online messages thanking me for taking the time to meet with project teams regarding potential opportunities to list their assets on Binance.com. This was odd because I don't have any oversight of or insight into Binance listings, nor had I met with any of these people before."
It transpired that fraudsters had impersonated Hillmann using AI-based technology, he claimed.
"It turns out that a sophisticated hacking team used previous news interviews and TV appearances over the years to create a 'deep fake' of me," he said.
"Other than the 15 pounds that I gained during COVID being noticeably absent, this deepfake was refined enough to fool several highly intelligent crypto community members." *(continua…)*
https://www.infosecurity-magazine.com/news/scammers-create-ai-hologram-csuite/
***INFOSECURITY -** Phil Muncaster- 25 AUG 2022*

Increasing cybersecurity awareness in critical infrastructure

Imagine this: the power grid has been hacked by a nation-state and has catapulted us back to the Stone Age. No power, water, fuel, online communications or banking. No, this isn't a story out of a Michael Crichton novel. In 2018, a dire warning from former British Secretary of Defense, Gavin Williamson, indicated Britain's energy infrastructure had been spied on by Russia. He predicted countless deaths would result if their power grid was ever crippled.

The critical infrastructure space is hardly an emerging topic in terms of cybersecurity. Case in point — in the spring of 2021, the Colonial Pipeline was hacked, leaving consumers from Texas up to New Jersey and New York vulnerable without a basic need: gas. Thankfully, the issue was resolved, but the implications of cyberattacks on critical infrastructure were exemplified by this incident.

The power of security awareness

There are key concerns revolving around device capabilities, supply chain, security and safety in the critical infrastructure sector. According to Brian Wrozek, Principal Research Analyst with Forrester and former CISO of Texas Instruments and Optiv, an organizational focus on security awareness can help critical infrastructure organizations harden their operational technology (OT) and information technology (IT) against threats.

The OT space has been a more challenging space to manage and prevent attacks primarily because OT utilizes unique equipment that is not able to leverage the common security controls used in IT environments. Systems were created to operate uninterrupted for a long period of time in specialized use cases and security was not built into the original design. Wrozek highlights that "on the plus side, OT environments have robust physical security controls and manual safety mechanisms that can provide protection to minimize potential damages."

This is a prime time for IT and cybersecurity executives to revisit and re-strategize security awareness training around this space. The IT and OT environments can never be treated in the same manner, which means companies will need to adjust their delivery methods and timing to align with the unique characteristics of the OT environments. Structuring security awareness training to fit critical infrastructure challenges and meet employees where they are in terms of cybersecurity knowledge may lead to more successful security outcomes. Wrozek recommends "holding a live workshop during lunch time at the factory, as all operators may not have a traditional office desk and laptop."

Regardless, all OT operators and administrators should participate in the standard cybersecurity training curriculum offered by their companies, but taking it a step further, Wrozek emphasizes "incorporating cybersecurity training into the physical security and safety educational programs common in OT environments will improve participation and adoption." *(continua…)*

https://www.securitymagazine.com/articles/98233-increasing-cybersecurity-awareness-in-critical-infrastructure

SecurityMagazine *-Ellen M. Sturgeon - August 26, 2022*

James Webb Telescope Images Loaded With Malware Are Evading EDR

New Golang cyberattacks use deep space images and a new obfuscator to target systems — undetected.

Threat hunters are warning security teams to be on the lookout for new cyberattack that uses a chance to see historic James Webb space telescope deep field images as a lure. The campaign's victims are infected with Golang malware.

Besides the novel lure strategy, the Go programming-based malware gives threat actors added flexibility across platforms and frameworks, in addition to providing reverse-engineering protections and obfuscation benefits, the Securonix research team reported. They dubbed the new cyberattack chain GO#WEBFUSCATOR for its ability to get around extended detection and response (EDR) defenses.

"The image contains malicious Base64 code disguised as an included certificate," *(continua…)*."

https://www.darkreading.com/vulnerabilities-threats/james-webb-telescope-images-loaded-with-malware-are-evading-edr

Dark Reading *- Staff - August 31, 2022*

Cyber-attacchi ad aziende energetiche in crescita. La nota dell'Acn

Dopo la riunione interministeriale convocata ieri dal presidente Draghi, oggi si è riunito il Comitato interministeriale per la cybersicurezza. "L'Italia risulta essere un target particolarmente colpito". Nel mirino l'interna catena di approvvigionamento e distribuzione del settore energetico

Il Nucleo per la Cybersicurezza si è riunito oggi dopo i cyber-attacchi che negli scorsi giorni hanno coinvolto operatori italiani del settore energetico. Il comitato, convocato in composizione ristretta nelle sue componenti tecnico-operative e integrato per l'occasione dai rappresentanti del settore, ha analizzato le attività cyber ostili rivolte alle infrastrutture nazionali.

"L'incremento generalizzato di attività malevole, confermato dai dati di monitoraggio dell'Agenzia, evidenzia il perdurare di diverse campagne globali di tipo DDOS e intrusivo, nell'ambito delle quali l'Italia risulta essere un target particolarmente colpito", si legge in una nota diffusa dall'Agenzia per la cybersicurezza nazionale diretta da Roberto Baldoni. "In tale contesto, si osserva un trend crescente di azioni apparentemente riconducibili al *cyber crime* che includono campagne di *social engineering* volte a individuare target aziendali particolarmente sensibili (singoli dipendenti o intere articolazioni), unitamente a campagne di *phishing*. Queste ultime perpetrate allo scopo di appropriarsi di informazioni sensibili o di credenziali di accesso, utilizzate poi direttamente dall'attaccante, ovvero 'vendute' ad un committente o altra gang criminale", conclude la nota.

Nel corso della riunione, è stato, inoltre, "evidenziato come sempre più spesso gli obbiettivi di tali azioni siano non solo le principali aziende del settore energetico ma anche tutta la catena di approvvigionamento e di distribuzione dei prodotti o servizi ad esse connesse". I tecnici dell'Agenzia per la cybersicurezza nazionale, in stretto contatto con le omologhe agenzie europee e internazionali, hanno diffuso le raccomandazioni tecniche per l'innalzamento dei livelli di protezione delle infrastrutture digitali degli operatori energetici, adeguandole costantemente alle più recenti informazioni sulla minaccia.

La nota è stata pubblicata all'indomani della riunione del Comitato interministeriale per la cybersicurezza convocata dal presidente del Consiglio Mario Draghi, a cui hanno partecipato il direttore Baldoni e la sua vice, Nunzia Ciardi. *(continua….)*

https://formiche.net/2022/09/cyber-attacchi-aziende-energetiche-in-crescita-acn/

Formiche- *Gabriele Carrer - 02/09/2022*

Nuovo data breach in casa Samsung: ecco i rischi per i clienti

La storia si ripete per Samsung, dopo circa sei mesi un altro attacco ha causato il furto di dati interni. Ecco cosa è successo con il nuovo attacco. Il rischio per i clienti Samsung sono ora nuove campagne di phishing.

Il colosso della tecnologia **Samsung** è stata colpita da attacco informatico, con conseguente **furto di dati** interni da entità non autorizzate. A riferirlo è la stessa società in un comunicato datato 2 settembre.

Indice degli argomenti

Il secondo furto di dati dell'anno per Samsung

Un fatto analogo è stato analizzato a marzo 2022, quando la cyber gang LAPSUS$ ha rivendicato l'attacco con la diffusione di GB di dati interni alla società tra cui il codice sorgente di un progetto legato al prodotto smartphone Galaxy.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Nella giornata di ieri la storia per il gigante sud coreano, si ripete**.** Stavolta non segue una rivendicazione criminale ma arriva a circa un mese dall'effettivo attacco. "Alla fine di luglio 2022, una terza parte non autorizzata ha acquisito informazioni da alcune unità statunitensi di Samsung", ha rivelato la società nella nota. "Intorno al 4 agosto 2022, tramite la nostra indagine in corso, abbiamo identificato che le informazioni personali di acquirenti specificati erano state interessate". *(continua…)*
https://www.cybersecurity360.it/nuove-minacce/nuovo-data-breach-in-casa-samsung-ecco-i-rischi-per-i-clienti/
Cybersecurity360 -*Dario Fadda -04/09/2022*

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.

AIIC (Associazione Italiana esperti in Infrastrutture critiche)
00185 Roma, Via Palestro, 95 c/o Nitel - Tel. +39/0664871209
e-mail:segreteria@infrastrutturecritiche.it
www.infrastrutturecritiche.it

Sede operativa e servizio di segreteria	AIIC c/o NITEL – via Palestro 95 – 00185 ROMA Tel. +39 06 64871209 E-mail: segreteria@infrastrutturecritiche.it
Gruppo di user all'interno della community	Si informa che AIIC ha costituito un proprio gruppo di user all'interno della community di LinkedIn: per unirti al gruppo è sufficiente usare il seguente 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 *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.