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

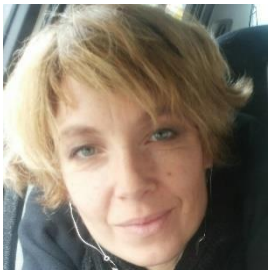
ANNO 2025	n. 7/ 2025	luglio 2025

Strategia, stato di salute e stress test europei di Cybersecurity: un esempio metodologico di gestione

Probabilmente molti di voi già sanno che la missione dell'Agenzia dell'Unione Europea per la Cybersecurity (ENISA) è raggiungere un elevato livello comune di sicurezza informatica in tutta l'Unione. Quello che forse potreste non sapere è che tutte le attività dell'ENISA sono finalizzate in pubblicazioni ad hoc; che sia un report, uno studio, un insieme di linee guida o una metodologia, il risultato finale è una produzione "monumentale" di approfondimenti in tema di Cyber security e dei suoi ambiti specialistici, che già da soli basterebbero a colmare lo "scibile" di sapere e guidare i meno avvezzi alla materia verso l'adozione di pratiche di sicurezza informatica.
Fra tutte le pubblicazioni più recenti (dedicate alla corretta applicazione della NIS2, agli studi sulle minacce (generali, tematici e specifici), o su questa o quella tecnologia), vi sono tre pubblicazioni che possono costituire un esempio da replicare per qualsiasi azienda in termini di metodologie di gestione e rapporto con il mercato per essere efficaci: la nuova strategia ENISA (febbraio 2025), il manuale per i Cyber stress test (maggio 2025) e l'indice di Cybersecurity dell'UE (EU-CSI emesso a giugno 2025 ma relativo al 2024).
La prima, la Strategia ENISA, rappresenta la versione aggiornata di visione e missione dell'ENISA seguita dalla lista di valori, dagli obiettivi strategici e operativi, allineati alla missione e per ciascuno di essi è riportata la lista di obiettivi verticali, senza dimenticare il set di indicatori di misurazione per la verifica degli avanzamenti. Sedici pagine in tutto che sinteticamente e in modo semplice e chiaro spiegano chi è l'ENISA e cosa si propone di fare e come. Questo documento, in questa precisa forma sintetica è un esempio da replicare per ogni organizzazione perché anno dopo anno i cambiamenti di mercato, in termini di concorrenti, tecnologie e normative possono incidere sulle modalità di raggiungere la missione aziendale e si rende necessario l'adattamento o adeguamento dell'intera postura aziendale. Potrebbero sembrare futile indicare l'ovvio; potrebbe sembrare scontato, quasi lapalissiano addirittura, ricordare di riemettere ogni anno la strategia aziendale e darne diffusione ai dipendenti, eppure, non viene fatto puntualmente da tutte le aziende, specie le piccole, a gestione familiare o quelle anche medie che hanno una gestione manageriale semplicistica. Non ci è dato sapere il motivo di tale "pigrizia", ma emettere un aggiornamento di strategia, completa di missione aziendale, valori, etica aziendale e soprattutto obiettivi non è solo una buona prassi, ma da parte del vertice, richiede una consapevolezza di dove si è e di dove si vuole andare e fa da guida ai cambiamenti organizzativi; delinea le modifiche di ruoli e responsabilità come anche i budget e gli incentivi per obiettivo sulle risorse. In definitiva aiuta a dare la direzione da prendere per "remare" tutti insieme nella stessa traiettoria. Anche se nel mercato delle tecnologie ed in particolare nella cybersecurity come contesto di mercato, tutto corre e tutto si sviluppa rapidamente, i metodi e le modalità di gestione impresa, spesso anche certificate da sistemi di gestione ISO, vengono tralasciati in funzione di una "foga" a vendere che potrebbe perdere di significato se non si ha chiaro quale business deve essere consolidato nel tempo. Il "cosa" si fa è importante tanto quanto il "come". Solo per citare un esempio pratico, a fronte dei requisiti imposti dalla direttiva NIS2, le aziende devono predisporsi. Come? La risposta arriva sempre dall'ENISA che ha emesso la pubblicazione "Cybersecurity roles and skills for NIS2 Essential

and Important Entities" come guida di orientamento alle aziende ed esortarle ai cambi organizzativi aziendali necessari ad una migliore risposta di adeguamento alla direttiva NIS2.
Ma fra i cambiamenti di mercato che ogni azienda dovrebbe studiare, vi sono sia le normative sia i concorrenti di cui approfondire capacità e postura. Nell'esempio dell'ENISA e rispetto alla sua strategia, questo significa studiare l'ecosistema informatico dell'UE per avere una comprensione completa dello stato attuale di maturità della sicurezza informatica degli Stati membri dell'UE. Il monitoraggio continuo e coerente dei livelli di sicurezza informatica in tutta l'UE nel tempo è il mezzo principale per valutare le attuali capacità di sicurezza informatica e individuare le aree di miglioramento. Per questo motivo tale studio approfondito è stato oggetto di una specifica pubblicazione ENISA, "the EU-cybersecurity index 2024" che descrive appunto la postura a livello di stati dell'Unione grazie ad un sistema di misura basato su indici quantitativi e qualitativi e una analisi multidimensionale. In parallelo, una qualsiasi azienda che abbia come business la cybersecurity dovrebbe poter conoscere approfonditamente il mercato a cui si rivolge, i concorrenti e le loro capacità con almeno, una analisi equivalente per determinare dove si trova lei stessa rispetto ai concorrenti ed anche per delineare criteri distintivi e di miglioramento della propria performance. Attenzione, in questa valutazione la postura stessa di cyber security dell'azienda è un elemento di garanzia e solidità e non dovrebbe essere tralasciata o trascurata o affrontata superficialmente perché la propria postura di cyber sicurezza è uno dei rischi operativi dell'impresa e dovrebbe figurare proprio nella strategia aziendale come elemento di consolidamento.
Se non sapete come procedere per valutarlo, niente paura. Ci pensa ENISA. Nel suo immenso set di kit di lavoro trovate pure "l'Handbook for Cyber Stress Tests" uno strumento di valutazione mirata della resilienza per ogni organizzazione e della sua capacità di resistere e riprendersi da incidenti di sicurezza informatica significativi, continuando a garantire la fornitura di servizi critici in diversi scenari di rischio. Il manuale è un guida in cinque fasi allo stress test informatico:
1. definizione dell'ambito e degli obiettivi del test, coinvolgimento degli stakeholder;
2. progettazione del test, scelta della metodologia, perfezionamento degli scenari;
3. esecuzione dello stress test informatico;
4. analisi dei risultati e identificazione delle lacune;
5. follow-up delle lacune e delle problematiche identificate nello stress test.
Gli stress test si concentrano sulla resilienza, utilizzano metriche di resilienza e possono essere utilizzati per testare sia le misure di preparazione che le misure di recupero reattivo. Le lacune evidenziate dagli stress test possono essere discusse in contesti collaborativi e volontari, ma possono anche essere analizzate in un contesto di supervisione più rigoroso generando interventi di direzione e riassetto aziendale.
Insomma, l'ENISA insegna, ma tutti gli altri dovrebbero imparare e fare pratica……

Alessia Valentini



Consulente di Cybersecurity, Advisor e Giornalista. Fa parte delle "Women for Security" la community di Cyberladies nata nell'ambito del Clusit. È Giornalista presso l'ODG del Lazio dal 2013. Ha conseguito la certificazione CISA /ISACA nel 2017. È stata consigliere direttivo in Afcea (Armed Forces Electronic Association) dal 2014 al 2016.

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

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.

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

Vi 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.

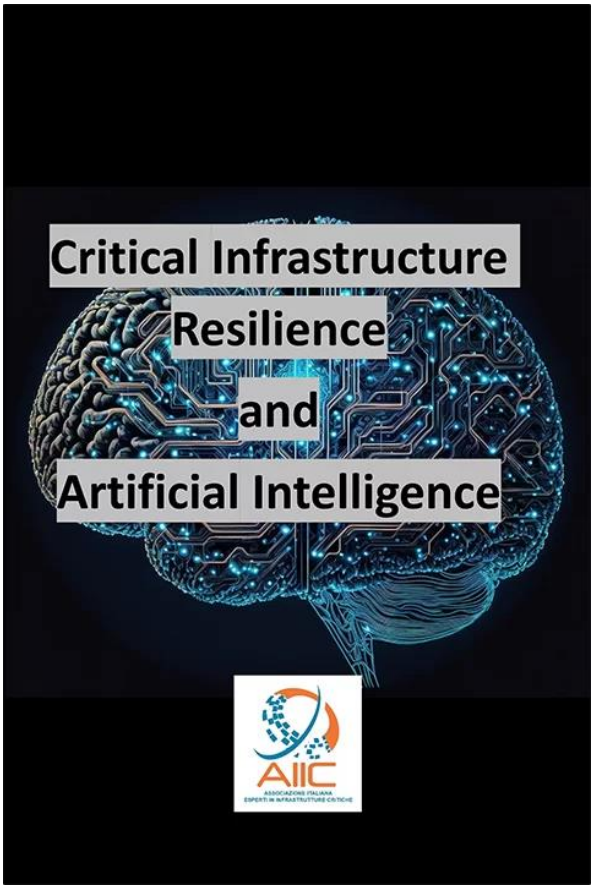
COLLABORAZIONE ALLE ATTIVITA' AIIC

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

IL REPORT AIIC "CRITICAL INFRASTRUCTURE RESILIENCE AND ARTIFICIAL INTELLIGENCE" NEL SITO DELLA COMMISSIONE EUROPEA

Il Report "Critical Infrastructure Resilience and Artificial Intelligence" è stato inserito nel sito web della Commissione Europea, al seguente link:

https://ec.europa.eu/newsroom/cipr/items/884567/en



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

E' un'ottima notizia per AIIC e per tutti i Soci che hanno collaborato.
La versione finale del report, oltre che dal sito AIIC, può essere scaricata dal sito della Commissione.

AIIC – GRUPPO DI LAVORO

Artificial Intelligence and Climate Change

INVITO A PARTECIPARE

Il nuovo Consiglio Direttivo AIIC, a valle della nomina e della distribuzione delle nuove cariche sociali del 18 Giugno 2025, ha approvato la nascita del GdL **"Artificial Intelligence and Climate Change"**. Tutti i Soci AIIC che intendono partecipare sono invitati a manifestare la loro disponibilità, mandando una mail al Coordinatore s.bologna@infrastrutturecritiche.it e per conoscenza alla Segreteria segreteria@infrastrutturecritiche.it
Di seguito i dati salienti del GdL proposto.
Coordinatore: Sandro Bologna
Data inizio lavori: 08. 09. 2025
Durata max: 12 mesi
Lingua di redazione: inglese
Riferimenti: Rapporti AIIC "Resilienza delle Infrastrutture Critiche e Cambiamenti Climatici" 2023 e "Critical Infrastructure Resilience and Artificial Intelligence" 2024; disponibili nel sito AIIC, sezione Pubblicazioni.

descrizione del gdl e lista degli argomenti trattati

A possible index for the Report on "Artificial Intelligence and Climate Change" could be the following. This index provides a comprehensive framework for exploring the intersection of artificial intelligence and climate change, covering various aspects such as understanding AI energy consumption, AI applications for energy optimisation, policy considerations, technological innovations, ethical implications, and future directions.
Any improvement of the proposed Index is welcome.

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

Introduction
AI and climate change
Understanding the energy-AI nexus
Energy demand from AI
Energy supply for AI
AI for energy optimisation and innovation
AI and energy security
Conclusions

NEWS E AVVENIMENTI

Conflitto Israele-Iran, ecco gli impatti sulle Tlc (e come affrontarli) - La guerra mette alla prova la resilienza delle infrastrutture di telecomunicazione e dei quadri di sicurezza informatica. Gli operatori attivi anche su mercati esterni al Medio Oriente e i provider delle comunicazioni satellitari potranno salvaguardare il business

Il conflitto Israele-Iran si è evoluto in un'arena ad alto rischio per i servizi Tlc globali e mette alla prova la resilienza delle infrastrutture di telecomunicazione e dei quadri di sicurezza informatica. Con i blackout quasi totali di Internet in Iran, la proliferazione degli attacchi informatici e il controllo di Teheran sulle comunicazioni, il settore affronta rischi operativi e finanziari senza precedenti. Tuttavia, all'interno di questa turbolenza gli investitori possono trovare opportunità in aziende che offrono soluzioni di cybersecurity, alternative come le Tlc satellitari e attività legate alla ricostruzione post-conflitto, secondo un'analisi firmata da Theodore Quinn su ainvest.com.

Indice degli argomenti

Conflitto Israele-Iran, le vulnerabilità per le Tlc

Il conflitto tra Israele e Iran ha messo in luce le debolezze critiche nelle reti di telecomunicazioni, in particolare in Iran. I recenti blackout nazionali di 36 ore hanno ridotto la connettività al 3% dei livelli normali, paralizzando i servizi di ogni genere, da quelle bancari alle comunicazioni di emergenza. I principali operatori Tlc come Irancell e MCCI affrontano rischi esistenziali, perché il regime iraniano dà la priorità alle reti controllate dallo Stato rispetto all'accesso aperto a Internet.
(continua…)
https://www.corrierecomunicazioni.it/telco/conflitto-israele-iran-ecco-gli-impatti-sulle-tlc-e-come-affrontarli
CorCom - *Patrizia Licata, 24 giu 2025*

La Terra si sta riscaldando molto più velocemente del previsto - Lo squilibrio energetico terrestre è più che raddoppiato negli ultimi due decenni.
Il calore intrappolato dalla Terra è molto di più rispetto a quanto avevano previsto i modelli climatici e il tasso attraverso cui tale calore viene immagazzinato è raddoppiato negli ultimi 20 anni. Un modo utile a misurare il riscaldamento globale è considerare appunto il bilancio energetico terrestre, vale a dire valutare quanto calore entra nell'atmosfera e quanto ne esce. Adesso questo bilancio è completamente squilibrato.
Una nuova ricerca pubblicata sul giornale scientifico AGU Advances e ripresa dal sito Phys.org ha dimostrato che lo squilibrio energetico terrestre è più che raddoppiato negli ultimi due decenni. Inoltre, tale squilibrio era stato sottostimato dai modelli climatici.
INDICE DEI CONTENUTI

Più calore intrappolato dalla Terra
Il riscaldamento globale è dovuto alle emissioni di gas serra causate dalle attività umane, tali attività sono capaci di alterare il delicato equilibrio tra il calore dei raggi in arrivo dal Sole e le radiazioni riflesse ed emesse dalla Terra. Lo squilibrio di tale processo porta all'accumulo di energia nell'atmosfera, nell'oceano e sulla Terra e allo scioglimento della criosfera, ossia l'insieme dei ghiacci presenti sul nostro pianeta. Le dirette conseguenze di tutto questo sono: aumento delle temperature, innalzamento del livello dei mari ed eventi meteorologici estremi in tutto il mondo.
La grande rilevanza del bilancio energetico terrestre per la regolazione della temperatura superficiale è nota da almeno due secoli, ciononostante la nostra capacità di valutare tale squilibrio risulta in pericolo perché molti satelliti potrebbero essere smantellati.
Uno shock per gli scienziati
A metà degli anni 2000, lo squilibrio energetico registrato era stato in media di circa 0,6 watt per metro quadrato (W/m^2). Negli ultimi anni, invece, la media è stata di circa 1,3 W/m^2. Significa che il tasso attraverso cui l'energia viene accumulata vicino alla superficie del pianeta è raddoppiato. Constatare questo raddoppio è stato come uno shock per gli scienziati, perché i sofisticati modelli climatici a nostra disposizione non avevano previsto un cambiamento così ampio e rapido.
Anche un altro studio pubblicato sulla rivista scientifica Science aveva dimostrato che lo squilibrio energetico terrestre si è rafforzato tra il 2001 e il 2023, grazie ai dati raccolti dai satelliti. Lo studio aveva anche rivelato che i modelli a bassa sensibilità climatica non riescono a cogliere l'andamento di tale squilibrio. In generale, i modelli avevano spiegato metà del cambiamento che invece starebbe avvenendo.

La scoperta indica che il cambiamento climatico potrebbe addirittura accelerare nei prossimi anni. Ancor peggio, la nostra capacità di agire per contrastare il riscaldamento globale potrebbe essere compromessa a causa della mancanza di fondi e di volontà politica necessarie a mantenere in funzione gli strumenti di rilevamento, come i satelliti, soprattutto da parte degli Stati Uniti. (continua…)
https://www.rinnovabili.it/clima-e-ambiente/cambiamenti-climatici/calore-intrappolato-dalla-terra/
Rinnovabili - *Erminia Voccia, 30 Giugno 2025*

We've All Been Wrong: Phishing Training Doesn't Work
Teaching employees to detect malicious emails isn't really having an impact. What other options do organizations have?
A recent study suggests, contrary to popular belief, that most phishing awareness initiatives aren't having a material impact on employee cybersecurity.
One of the most widely repeated, least examined memes in the cybersecurity industry is that, even more than technical solutions, organizations can best secure themselves by teaching cyber awareness among their employees. Building a "human firewall," to protect an organization's otherwise "weakest link."
The diagnosis is sound. The overwhelming majority of cyberattacks do occur due to some form of human error: an unwisely clicked link, a weak password, etc. The cure — occasional cybersecurity training obligations for employees — is often regurgitated and accepted without scrutiny.
To test out how well we're building our human firewalls, a team of 10 researchers from the University of Chicago, the University of California San Diego (UCSD), and UCSD Health performed a study of unprecedented scale in the cybersecurity industry. Over an eight month period in 2023, they studied the effects of phishing training on 19,789 personnel at UCSD Health, a large healthcare organization. At this year's Black Hat USA event in Las Vegas, two of the researchers will be discussing their findings: to wit, in certain circumstances, online phishing training can have some effect on employees' ability to identify malicious emails, but more often the difference is miniscule, and it's occasionally even counterproductive.
"The big finding is that these standard, out-of-the-box industry trainings are not efficacious in preventing users from clicking on emails in the future," says Ariana Mirian, one of the co-authors and senior security researcher at Censys. She adds, though, that "there's a lot of nuance there."
The Research on Phishing Training
As Mirian explains, "The idea of prioritizing awareness was very much predicated on research itself. There were some studies in the 2000s and 2010s that explored this notion that teaching awareness is the path forward to protect users. There's so much psychology and cognitive science research that also says the same. So a lot of security professionals were bringing it into the security realm and saying, 'We just need to make users aware.'"
The intuitive sense behind the idea makes it extra compelling and may explain why it persists despite rigorous recent evidence to the contrary. (continua…)
https://www.darkreading.com/endpoint-security/phishing-training-doesnt-work
DARKREADING - *Nate Nelson - July 1, 2025*

La gestione della Protezione civile richiede un coordinamento a livello europeo - Uno studio sviluppato dall'Unione Europea ha messo in evidenza quanto siano differenti i comportamenti e le responsabilità in situazioni di emergenza nei vari paesi europei e la necessità di un coordinamento europeo, superando i soli ambiti nazionali.

L'Unione europea attualmente si trova davanti a una moltitudine di scenari di rischio, che solo pochi anni fa non erano nemmeno concepibili. Si pensi ad esempio allo scenario dell'attacco della Russia all'Ucraina, che dimostra come i responsabili della protezione civile, nei vari paesi europei, devono migliorare e rinforzare il proprio livello di preparazione, nel fronteggiare scenari di rischio di varia natura.
Inoltre, non dimentichiamo che l'Europa continua a fronteggiare le conseguenze dell'evento pandemico legato al COVID 19, che ha portato a significative perdite di vita umana e sconvolgimenti della vita dei cittadini.
A questi scenari, come se non bastassero, si aggiunge l'impatto del cambiamento climatico, che si manifesta con fenomeni naturali di varia natura, ma spesso tanto imprevisti quanto violenti.
Ecco perché, in questo contesto, la direzione generale per la protezione civile europea, parte della commissione europea, ha avviato uno studio per garantire che i vari paesi dell'unione europea siano sufficientemente preparati e coordinati, per fronteggiare scenari estremi.
Il meccanismo di protezione civile europea, che è stato fondato nel 2001, mira proprio a migliorare la prevenzione, preparazione e capacità di rispondere a disastri. Per dare un'idea dell'importanza di questo organismo, dalla sua fondazione sono stati ben 700 gli interventi di assistenza, che hanno visto il coinvolgimento di altri paesi europei. (continua…)
https://www.puntosicuro.it/security-C-125/la-gestione-della-protezione-civile-richiede-un-coordinamento-a-livello-europeo-AR-25520/
Punto Sicuro - *Adalberto Biasiotti, 07/07/2025*

Cybersecurity, Frattasi ACN: in Italia scontiamo anni di ritardo in reti e servizi robusti - "Non esiste nulla che oggi possa essere associato alla fragilità quanto la sicurezza informatica": così Bruno Frattasi, Direttore Generale ACN, è intervenuto durante l'evento organizzato da SPES Academy, Scuola di alta formazione, per la presentazione del libro "Governare le fragilità" di Bernardo G. Mattarella e Roberto Garofoli.
"Parlando del nostro Paese – ha proseguito il Direttore dell'ACN – abbiamo avuto una stagione non proprio felice dal punto di vista dell'investimento in sicurezza digitale e questo è accaduto sia nel settore pubblico che nel settore privato. Scontiamo anni di ritardo, lo dicono molti studi, sulla robustezza dei nostri apparati, delle nostre reti, dei nostri servizi e dei nostri sistemi".
Frattasi, ACN: ASL bersaglio di attacchi informatici perché scarsamente protette
"Oggi –ha evidenziato Frattasi – stiamo cercando di recuperare grazie a investimenti resi possibili sia dal PNRR sia da risorse nazionali, come ad esempio il fondo per l'attuazione della Strategia Nazionale di Cybersicurezza. Recentemente abbiamo cercato di concentrare l'attenzione su realtà meno protette nel nostro panorama amministrativo. Mi riferisco in particolare alle amministrazioni locali, in particolare alle ASL, spesso bersaglio di attacchi informatici perché poco protette e con numerosi servizi esternalizzati a società non sempre mature dal punto di vista della sicurezza informatica".
La valenza del dato della salute
"Il dato della salute, il dato inerente alla salute della persona, è uno tra i più appetibili che ci possono essere per le organizzazioni e le filiere criminali che operano nell'ambito del cyber – ha spiegato il Direttore. – Le minacce principali sono la distruzione dei dati informatici in caso di mancato pagamento del riscatto oppure la loro pubblicazione online, con conseguenti danni economici e reputazionali. A ciò si aggiunge la responsabilità legale: il soggetto colpito risponde anche di fronte al Garante per la protezione dei dati personali per violazioni della normativa nazionale".

https://www.snewsonline.com/cybersecurity-frattasi-acn-italia-scontiamo-anni-ritardo-reti-servizi-robusti/
S News *- Redazione - 10 Luglio 2025*

La Cina alla conquista dell'IA: così Pechino minaccia il primato Usa
La Cina sta avanzando rapidamente nell'intelligenza artificiale, con una strategia che include investimenti massicci e una forte regolamentazione dei dati. Il suo obiettivo è superare gli Stati Uniti in vari settori tecnologici entro il 2030
Negli ultimi anni, la Cina ha accelerato drasticamente nel campo dell'intelligenza artificiale (IA), portando avanti una strategia di sviluppo centralizzata, massicci investimenti e una regolamentazione flessibile sull'uso dei dati. Questo le ha permesso di avvicinarsi, e in alcuni casi superare, gli Stati Uniti in settori chiave dell'IA. Molteplici e fondamentali sono i fattori che hanno prodotto tale evoluzione nella crescita cinese nei settori tecnologici in cui Pechino eccelle, senza escludere le risposte statunitensi e le implicazioni geopolitiche di questa corsa tecnologica globale.
Indice degli argomenti

Il contesto strategico: la svolta cinese sull'IA
Nel luglio 2017, il Consiglio di Stato della Repubblica Popolare Cinese ha pubblicato il documento strategico intitolato "*New Generation Artificial Intelligence Development Plan*". Questo piano ha determinato una svolta epocale nella politica tecnologica cinese, delineando un percorso articolato in tre fasi:

- leadership tecnologica interna entro il 2020;
- sviluppo sistemico entro il 2025;
- primato globale entro il 2030.

Una pianificazione strategica così **definita** e basata su tappe da rispettare rigidamente, oltre al duro ruolo guida del governo di Pechino, hanno di fatto consentito ed accelerato l'integrazione dell'intelligenza artificiale nella visione economica e industrial, a lungo termine, del paese. Il 14º Piano Quinquennale (2021–2025) ha inoltre confermato l'IA quale tecnologia abilitante chiave per la modernizzazione dell'economia, delle infrastrutture e finanche della difesa nazionale. Il presidente Xi Jinping ha dichiarato in più occasioni che l'IA rappresenta il motore dell'innovazione globale e che il successo in questo settore sarà determinante per lo status geopolitico della Cina nel XXI secolo.
La Cina e l'IA in ambito militare: droni e sorveglianza avanzata
Una particolare attenzione è stata riservata all'utilizzo dell'IA in ambito militare. La Cina considera l'intelligenza artificiale come una tecnologia chiave per la modernizzazione militare, parte integrante della strategia "c*ivil-military fusion*" (CMF) promossa dal presidente Xi Jinping. Questo approccio mira a integrare i progressi civili, in particolare nel campo dell'IA, nelle applicazioni belliche e di difesa nazionale.
Uno degli ambiti più avanzati è quello dei droni autonomi. Il China Aerospace Science and Industry Corporation (CASIC) ha sviluppato sciami di droni capaci di coordinarsi in tempo reale utilizzando algoritmi

di intelligenza collettiva. Tali droni, se impiegati in battaglia, potrebbero saturare le difese aeree convenzionali grazie al numero e all'autonomia decisionale. (continua**…)**
https://www.agendadigitale.eu/mercati-digitali/la-cina-alla-conquista-dellia-cosi-pechino-minaccia-il-primato-usa/
Agenda Digitale *- Antonio Teti - 11 luglio 2025*

350M Cars, 1B Devices Exposed to 1-Click Bluetooth RCE

Mercedes, Skoda, and Volkswagen vehicles, as well as untold industrial, medical, mobile, and consumer devices, may be vulnerable to an attack chain called "PerfektBlue."

Four vulnerabilities in a popular Bluetooth implementation can be chained together to enable remote code execution (RCE) in untold millions of vehicles and miscellaneous devices.

"Blue SDK" is a Bluetooth protocol stack and software development kit (SDK). On May 17, 2024, researchers from PCA Cyber Security discovered a range of vulnerabilities in Blue SDK that, together, allowed them to remotely execute code in devices that rely on it for Bluetooth connectivity. They called their exploit chain "PerfektBlue."

The scope of affected systems is massive. The developer, OpenSynergy, proudly boasts on its homepage that Blue SDK — and RapidLaunch SDK, which is built on top of it and therefore also possibly vulnerable — has been shipped in 350 million cars. Those cars come from companies like Mercedes-Benz, Volkswagen, and Skoda, as well as a fourth known but unnamed company. Since Ford integrated Blue SDK into its Android-based in-vehicle infotainment (IVI) systems in November, Dark Reading has reached out to determine whether it too was exposed.

Aside from just cars, though, OpenSynergy claims that Blue SDK touches more than 1 billion embedded devices around the globe, including in the consumer, mobile, industrial, and medical industries.

The PerfektBlue Exploit

The researchers counted four bugs in Blue SDK, labeled CVE-2024-45431 through CVE-2024-45434. They vary in criticality, with the former receiving a "low" 3.5 out of 10 rating in the Common Vulnerability Scoring System, and the latter a "high" 8.0.

Like any Bluetooth hack, the one major hurdle in actually exploiting these vulnerabilities is physical proximity. An attacker would likely have to position themselves within around 10 meters of a target device in order to pair with it, and the device would have to comply. Because Blue SDK is merely a framework, different devices might block pairing, limit the number of pairing requests an attacker could attempt, or at least require a click to accept a pairing.

This is a point of contention between the researchers and Volkswagen. The car manufacturer told Bleeping Computer that the exploit relies on five highly specific conditions:

- The attacker is within a maximum distance of 5 to 7 meters from the vehicle.
- The vehicle's ignition must be switched on.
- The infotainment system must be in pairing mode — i.e., the vehicle user must be actively pairing a Bluetooth device.
- The vehicle user must actively approve the external Bluetooth access of the attacker on the screen.
- The attacker must remain within that 5- to 7-meter maximum distance in order to maintain access to the vehicle.

Mikhail Evdokimov, senior security researcher of PCA, clarified that some of these conditions are not accurate. (continua…)
https://www.darkreading.com/vulnerabilities-threats/350m-cars-1b-devices-1-click-bluetooth-rce
DARKREADING *- Nate Nelson, Contributing Writer* - July 11, 2025

Quando la resilienza funziona: più attacchi DDoS, ma impatto minore

Mostrano un netto miglioramento i dati dell'ACN sull'incidenza degli attacchi DDoS confrontati con i tempi di disservizio e la quantificazione dei danni. Ciò testimonia l'efficacia delle azioni di prevenzione e protezione messa in campo per aumentare la resilienza complessiva del sistema Italia

Senza voler sfidare nessuno bisogna riconoscere a 'Cesare quel che è di Cesare': **l'innalzamento nazionale del livello di resilienza, mostra una tendenza positiva che giustifica un cauto ottimismo**. È quanto si evince dai dati forniti da ACN direttamente alla nostra redazione lo scorso 15 luglio.

La strada intrapresa dalle maggiori organizzazioni italiane, complici le normative (**NIS2**, Legge 90, normative europee), i fondi del PNRR e le campagne di informazione e formazione, restituiscono gli effetti attesi: **una capacità migliorata nella prevenzione e una migliore reazione agli incidenti DDoS che si traduce in una migliore mitigazione, riduzione dei tempi di disservizio e minore entità dei danni**.

Come sempre nella sicurezza informatica sembra essere più importante la notizia della riuscita di un attacco, mentre l'efficacia delle azioni difensive raramente viene segnalata perché percepita e giudicata come scontata.

Tuttavia, è importante sottolineare il momento in cui si esce dall'emergenza e si entra in una fase di 'normale amministrazione' con un approccio strutturato ai rischi e una protezione preventiva in atto.

Indice degli argomenti

Dati sui DDoS ieri: emergenza e preoccupazione

Molti degli 'addetti ai lavori' della cyber security ricorderanno come, in corrispondenza dell'avvio del confitto russo-ucraino, si siano verificati sul territorio nazionale italiano **ondate di campagne di attacco di negazione distribuita del servizio** (Distributed Denial of Service, DDoS) che avevano richiesto un innalzamento dell'allerta nazionale a livello 'ALTO'.

Quegli stessi attacchi avevano causato disservizi ai siti governativi o a grandi organizzazioni, con risonanza nelle cronache giornaliere, preoccupazione diffusa, ed avevano richiesto al Cyber Security Incident Response Team (CSIRT) ACN l'**emissione di specifici bollettini informativi** e naturalmente l'attuazione di un supporto operativo per ogni entità colpita per riportare la situazione alla normalità.

Dati sui DDoS oggi: minori disservizi e danneggiamenti

Già nell'ultima edizione della **Relazione al Parlamento di ACN** si rendeva evidente, in tema attacchi DDoS, come dei "519 attacchi censiti effettuati da attivisti, solo il 15% aveva prodotto disservizi misurabili di carattere temporaneo (tipicamente circa un'ora di irraggiungibilità della risorsa attaccata), mentre nei restanti casi non sono stati rilevati impatti".

I dati forniti alla nostra redazione dall'ACN il 15 luglio evidenziano la crescita di incidenza degli attacchi DDoS ma anche minori disservizi.

In particolare, è stato osservato "**un aumento del' 77% nel 1° semestre 2025 con 598 attacchi rispetto ai 336 del 1° semestre 2024.** Tali campagne di hacktivism, molto intense tra dicembre 2024 e febbraio 2025, hanno subito una progressiva attenuazione nei mesi successivi, per poi ripresentarsi alla fine del semestre. (continua…)

https://www.cybersecurity360.it/outlook/quando-la-resilienza-funziona-piu-attacchi-ddos-ma-impatto-minore/
CYBERSECURITY360-*Alessia Valentini - 17 luglio 2025*

Phishing-as-a-Service (PhaaS): ora si integra con l'AI
Il fenomeno non è nuovo, ma la crescente diffusione di kit pronti all'uso, l'integrazione con strumenti di intelligenza artificiale e l'organizzazione strutturata delle piattaforme PhaaS ne stanno aumentando drasticamente l'efficacia e la diffusione
Si sta diffondendo, negli ultimi mesi, un fenomeno che abbassa drasticamente la soglia tecnica per entrare nel mondo del cybercrime: si tratta del cosiddetto **Phishing-as-a-Service (PhaaS)**, un modello a sottoscrizione che consente anche a utenti privi di competenze informatiche avanzate di lanciare campagne di phishing sofisticate e scalabili.
Il fenomeno non è nuovo, ma la crescente diffusione di kit pronti all'uso, **l'integrazione con strumenti di intelligenza artificiale** e l'organizzazione strutturata delle piattaforme PhaaS ne stanno aumentando drasticamente l'efficacia e la diffusione.
Indice degli argomenti

Phishing-as-a-Service: ora il PhaaS s'integra con l'AI
Il funzionamento è simile a quello delle legittime **piattaforme Software-as-a-Service (SaaS)**: l'utente paga una quota, ottiene accesso a un'interfaccia utente intuitiva, modelli di mail, portali di login fasulli e strumenti per la gestione della campagna.
L'obiettivo finale è ottenere **credenziali**, **dati bancari o informazioni sensibili** da rivendere nel mercato secondario o da sfruttare in prima persona.
Le statistiche più recenti del Federal Bureau of Investigation (FBI) indicano che nel solo 2023 sono stati registrati **quasi 300.000 casi di phishing e spoofing** (esattamente 298.878), superando il numero combinato di casi di estorsione e violazione dei dati personali.
Piattaforme con assistenza ai clienti
Queste piattaforme, oltre a fornire i tool tecnici, offrono anche assistenza clienti, aggiornamenti regolari per eludere i filtri antispam, e dashboard in tempo reale per monitorare l'esito delle campagne. Sono quindi **veri e propri ecosistemi criminali chiavi in mano, comparabili a startup illegali in piena regola**. (continua…)
https://www.cybersecurity360.it/nuove-minacce/phishing-as-a-service-phaas-ora-si-integra-con-lai/
CYBERSECURITY360 *– Luisa Franchina- Tommaso Diddi - 17 luglio 2025*

4 Chinese APTs Attack Taiwan's Semiconductor Industry
Chinese threat actors have turned to cyberattacks as a way to undermine and destabilize Taiwan's most important industrial sector.

New Chinese threat actors have been trying to use phishing as a means of breaching Taiwan's famed semiconductor industry.
Taiwan's semiconductor industry is one of the most geopolitically significant on the planet. Far beyond just earning income, it is a unique and presently irreplaceable supply chain cog to various global technologies. That makes Taiwan's prosperity — and by extension, the Chinese Communist Party's (CCP) aims to take over the island — of critical importance to countries besides itself, most notably the US.
More than ever before, China is now using cyberattacks as a weapon to undermine Taiwan's semiconductors and, by extension, Taiwan's national defense. Proofpoint researchers have identified three as yet unclassified advanced persistent threats (APT) targeting its chip industry in only the past few months, in addition to a fourth spotted late last year.
"Some of them are a little bit more novice, but we do see them develop over time," notes Proofpoint staff threat researcher Mark Kelly. Others, he says, have more specialized, custom capabilities.

Four Previously Undocumented APTs

In May and June, Taiwanese companies involved in semiconductor manufacturing, packaging, testing, and supply chain organizations received an email from a "graduate student." Using a Taiwanese university email address, the student was reaching out to recruitment and human resources (HR) personnel to ask for a job.
The emails contained either a PDF or a password-protected archive. Early on, the files concealed Cobalt Strike, then graduated to carry the Voldemort backdoor. Voldemort is a custom tool characterized by its odd way of using Google Sheets for command and control (C2). Though in the past it has only been used by APT41 (aka TA415, Double Dragon, Brass Typhoon), Proofpoint tracks this latest threat cluster as distinct from APT41, temporarily referring to it as "UNK_FistBump."
While UNK_FistBump was playing the role of grad student, in April and May, a threat actor referred to as "UNK_DropPitch" was masquerading as an imaginary investment firm. These attacks — which dropped a simple, custom backdoor called "HealthKick" — were aimed not at semiconductor companies themselves but at large investment banks.
The motive behind the emails wasn't financial. (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/4-chinese-apts-taiwan-semiconductor-industry
DARKREADING - *Nate Nelson - July 18, 2025*

Cos'è la Direttiva NIS 2 e perché è importante: ecco come adeguarsi

Come adeguarsi alla NIS2? E quali aziende sono coinvolte? Ecco tutto quello che bisogna sapere sulla direttiva che stabilisce nuovi standard di sicurezza per un'ampia platea di imprese.
La direttiva Nis2 stabilisce standard e regole sulla sicurezza di reti e sistemi informativi. Una normativa importante che coinvolge numerosi settori, ma che spesso risulta complessa ai non esperti e quindi le aziende possono incontrare difficoltà nella compliance. Come implementare la Nis2 nella propria impresa? Ecco tutto quello che bisogna sapere.
Indice degli argomenti

- Che cos'è la NIS2
  - Perché la direttiva NIS 2 è importante
- Chi deve rispettare la direttiva NIS 2
  - Obblighi e adempimenti previsti dalla NIS 2
- Come adeguarsi alla direttiva NIS 2
  - Conseguenze e sanzioni per chi non rispetta la NIS 2
  - Quando entra in vigore la NIS 2

  - Quali settori sono coinvolti dalla direttiva NIS 2
- Settori coinvolti dalla direttiva NIS 2
  - NIS2 settore energia
  - Settore sanitario e NIS2
  - NIS2 e settore trasporti
  - NIS2 per settore finanziario e bancario
  - Settore delle infrastrutture digitali e NIS2
  - Settore idrico e NIS2
  - Settore gestione rifiuti e NIS2
  - PA e NIS2 adempimenti

Che cos'è la NIS2

La direttiva NIS 2 (Network and Information Security 2) è la nuova **normativa europea in materia di cybersecurity** che aggiorna e sostituisce la precedente direttiva NIS del 2016. Entrata in vigore a gennaio 2023, la NIS 2 ha l'obiettivo di **migliorare la resilienza e la sicurezza delle reti e dei sistemi informativi** in tutta l'UE. Si tratta di un insieme di regole unificate a livello europeo per garantire un elevato livello comune di cybersicurezza, imponendo standard più elevati e misure più rigorose rispetto alla normativa precedente. In pratica, la direttiva richiede agli Stati membri di potenziare le proprie capacità di cybersecurity e introduce **obblighi di gestione del rischio e di notifica degli incidenti per un numero molto più ampio di settori critici** rispetto al passato. Questo significa che più organizzazioni, in diversi ambiti, sono tenute a adottare misure di sicurezza informatica adeguate e a cooperare a livello nazionale ed europeo per prevenire e gestire gli incidenti informatici.

Perché la direttiva NIS 2 è importante

La direttiva NIS 2 riveste un'importanza fondamentale perché nasce in risposta a una **crescente minaccia cyber** e ai potenziali gravi impatti degli attacchi informatici sulle nostre società. Negli ultimi anni l'Europa ha visto aumentare l'esposizione a cyber attacchi sofisticati, con conseguenze che vanno ben oltre il danno tecnico immediato: interruzione delle attività operative, compromissione di dati sensibili, pesanti danni reputazionali e perdite economiche o legali. I settori chiave dell'economia (energia, trasporti, sanità, finanza, ecc.) sono sempre più interconnessi e digitalizzati; quindi, un singolo incidente potrebbe avere effetti a cascata su servizi essenziali per i cittadini e le imprese. La NIS 2 è importante perché innalza il livello di sicurezza informatica in modo uniforme in tutti gli Stati membri, colmando le lacune della precedente direttiva: amplia il campo di applicazione a nuovi settori, introduce regole più chiare e poteri di vigilanza più forti, e rende **i vertici aziendali direttamente responsabili della cybersecurity**. Questa normativa aggiornata è considerata un pilastro per rafforzare la resilienza dell'Unione Europea contro i cyber rischi emergenti, proteggendo servizi essenziali e infrastrutture critiche da minacce sempre più sofisticate. (continua….)

https://www.agendadigitale.eu/cultura-digitale/cose-la-direttiva-nis-2-e-perche-e-importante-ecco-come-adeguarsi/

***AGENDA DIGITALE** - Tommaso Diddi - Luisa Franchina -18 luglio 2025*

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

Con questo numero la newsletter AIIC va in vacanza. Ci rivedremo a settembre.
Buone ferie dal Comitato Editoriale e dal Consiglio Direttivo AIIC!

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.

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

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 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.