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. 2/ 2025** **febbraio 2025**

Cybersecurity 2024-2025

Il 2024 ha rappresentato un anno di svolta per la sicurezza informatica, con un aumento significativo delle minacce e una crescente consapevolezza della necessità di rafforzare le difese digitali. Secondo il Rapporto Clusit 2024, gli attacchi informatici gravi sono aumentati del 23% nel primo semestre rispetto allo stesso periodo dell'anno precedente, con una media di nove attacchi al giorno.

Il settore delle infrastrutture critiche ha subito attacchi mirati con conseguenze rilevanti. Per la loro rilevanza strategica, le IC sono infatti obiettivi sensibili, nel mirino sia di criminali comuni che di attori statali. Il settore sanitario ha visto un aumento del 60% degli attacchi ransomware rispetto al 2023, con conseguenti ritardi nelle cure mediche e rischi per i pazienti

Il ransomware ha continuato a essere una delle minacce più pericolose. Secondo un rapporto di Sangfor Technologies, il 65% delle organizzazioni finanziarie ha subito almeno un attacco ransomware nel corso dell'anno. Inoltre, un'analisi di Chainalysis ha evidenziato che nel 2024 sono stati pagati riscatti per un totale di oltre 1 miliardo di dollari, dimostrando come il fenomeno continui a generare profitti per i cybercriminali.

Il phishing ha raggiunto livelli di sofisticazione sempre più elevati grazie all'uso dell'intelligenza artificiale, rendendo più difficile per le vittime distinguere i messaggi fraudolenti da quelli legittimi. Un'indagine condotta da Proofpoint ha rilevato che il 45% delle aziende ha subito almeno un attacco di spear phishing avanzato nel 2024, con una crescita del 30% rispetto all'anno precedente. Inoltre, l'adozione del modello Zero Trust ha continuato a crescere, con analisi di Gartner che stimano un'implementazione del modello nel 60% delle grandi aziende entro il 2025.

Guardando al futuro, l'espansione dei dispositivi IoT rappresenterà una nuova sfida per la sicurezza informatica, con un numero crescente di punti di accesso potenzialmente vulnerabili. Secondo stime di IDC, entro il 2025 ci saranno oltre 41 miliardi di dispositivi IoT connessi a livello globale, aumentando esponenzialmente la superficie d'attacco per i criminali informatici. I deepfake sono sempre più utilizzati per frodi e disinformazione, con il 66% delle aziende che ritiene che questa tecnologia possa rappresentare una minaccia seria per la sicurezza aziendale, secondo un'indagine condotta da McAfee.

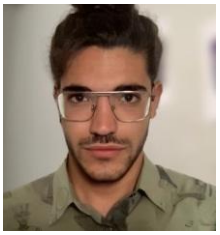
A testimonianza di una crescente consapevolezza del problema, gli investimenti in cybersecurity hanno raggiunto cifre record, con oltre 220 miliardi di dollari spesi a livello globale. Un segnale incoraggiante che indica una chiara presa di coscienza dell'importanza strategica della sicurezza informatica, sia nel settore pubblico che in quello privato.

Il 2025 si preannuncia quindi come un anno in cui la cybersecurity sarà chiamata a integrarsi ancor più profondamente nelle strategie aziendali e nelle politiche governative. Per affrontare queste minacce,

saranno necessarie strategie avanzate, simulazioni continue di attacchi e una stretta collaborazione tra settore pubblico e privato.

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.



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

ATTIVITA' DELL'ASSOCIAZIONE

RINNOVO ASSOCIATIVO ANNO 2025

Il 31 dicembre 2024 è scaduto il periodo associativo. Invitiamo pertanto i signori soci a rinnovare per tempo l'iscrizione alla nostra associazione versando il relativo contributo.
La quota per il rinnovo individuale è di euro 50 e può essere versata con bonifico sul conto corrente presso Banca Intesa Business, IBAN IT17B0306909606100000114955, intestato a AIIC Associazione Italiana esperti in Infrastrutture Critiche, indicando come causale "rinnovo socio ordinario nome e cognome anno 2025".
Le quote e le modalità di rinnovo per i soci collettivi sono contenute nel sito AIIC www.infrastrutturecritiche.it. La nostra segreteria è a disposizione, per ogni informazione, alla mail segreteria@infrastrutturecritiche.it.

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

PUBBLICAZIONE DI ARTICOLI DA PARTE DI SOCI E PARTECIPAZIONE AD EVENTI

Ricordiamo ai soci che nella pubblicazione di un articolo o di un libro **non è possibile** firmarsi qualificandosi come "Associazione Italiana esperti in Infrastrutture Critiche", in quanto solo chi ha la rappresentanza legale dell'Associazione può esprimersi a nome AIIC.

La stessa regola vale anche se si partecipa ad un evento in qualità di organizzatore, relatore o chairman.

La possibilità di pubblicare o partecipare ad eventi a nome AIIC deve essere approvata dal Consiglio Direttivo dell'Associazione su richiesta del socio che, pertanto, è pregato di contattare il CD con ragionevole anticipo.

È invece raccomandato indicare, nel proprio profilo professionale, l'appartenenza ad AIIC, Associazione Italiana esperti in Infrastrutture Critiche, in qualità di socio.

NUOVO SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Ricordiamo che è attivo il nuovo sito dell'Associazione Italiana Esperti in Infrastrutture Critiche.
L'indirizzo è sempre **www.infrastrutturecritiche.it** ma il sito è stato completamente rinnovato, sia nelle veste grafica che nei contenuti e nelle funzioni a disposizione.
Vi invitiamo a consultarlo e anche a farci pervenire le vostre osservazioni: i vostri suggerimenti sono sempre preziosi e ci aiutano a migliorare il prodotto.

Vi ricordiamo inoltre che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'associazione**, accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa.

COLLABORAZIONE ALLE ATTIVITA' AIIC

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

NEWS E AVVENIMENTI

Il sistema elettrico italiano in cifre. Nel 2024 rinnovabili da record - Lo scorso anno le fonti rinnovabili hanno coperto il 41,2 per cento della domanda elettrica. Merito anche dei 6.795 MW fotovoltaici aggiunti alla rete alla generazione idroelettrica
Indice dei contenuti
Il rapporto mensile di Terna sul sistema elettrico italiano
La produzione elettrica da FER in Italia

Le nuove installazioni rinnovabili
Il rapporto mensile di Terna sul sistema elettrico italiano
Anche per il sistema elettrico italiano è arrivato quel momento dell'anno dedicato ai consuntivi. Terna, il gestore della rete di trasmissione, ha pubblicato stamane il suo report aggiornato a dicembre 2024, tirando le somme su domanda, offerta e prezzi per l'energia elettrica per tutto l'anno appena concluso.
I dati, per chi ha seguito da vicino le diverse pubblicazioni mensili, non rappresentano una sorpresa. Il 2024 si conferma infatti come l'anno record per le fonti energetiche rinnovabili (FER) italiane, annullando la distanza dalle fossili nazionali lato consumi.
Stando alle rilevazioni di Terna, infatti, le green energy hanno registrato il dato più alto di sempre di copertura della domanda. Parliamo di ben il 41,2% del totale (nel 2023 era del 37,1%), lasciando ai carburanti fossili e alle importazioni rispettivamente una quota del 42,5% e del 16,3%.
(continua…)
https://www.rinnovabili.it/energia/infrastrutture/sistema-elettrico-italiano-cifre-rinnovabili/
Rinnovabili.it - *La Redazione•16 Gennaio 2025*

Mirai Botnet Spinoffs Unleash Global Wave of DDoS Attacks
Two separate campaigns are targeting flaws in various IoT devices globally, with the goal of compromising them and propagating malware worldwide.
Separate spinoffs of the infamous Mirai botnet are responsible for a fresh wave of distributed denial-of-service (DDoS) attacks globally. One is exploiting specific vulnerabilities in Internet of Things (IoT) devices to establish "expansive" botnet networks, while the other has been targeting organizations in North America, Europe, and Asia with DDoS attacks since the end of 2024, researchers have found.
An ongoing operation within Mirai dubbed "Murdoc_Botnet" (which began in July and has more than 1,300 active IPs) is targeting Avtech cameras and Huawei HG532 routers, researchers from Qualys revealed in a report posted today.
The researchers uncovered more than 100 distinct sets of servers associated with the Murdoc botnet, "each tasked with deciphering its activities and establishing communication with one of the compromised IPs implicated in this ongoing campaign," Qualys lead security researcher Shilpesh Trivedi wrote in the post.
Meanwhile, a botnet that comprises malware variants derived from both Mirai and Bashlite is exploiting security flaws and weak credentials in IoT devices in DDoS attacks spanning the globe, according to separate research from Trend Micro. "The malware infiltrates the device by exploiting RCE vulnerabilities or weak passwords, then executes a download script on the infected host," the researchers said.
The two campaigns demonstrate the ongoing impact of Mirai, a botnet that has spawned myriad variants since its source code was leaked in 2016 and which remains a significant security threat 10+ years after first appearing on the cyberattack scene. (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/mirai-botnet-spinoffs-global-wave-ddos-attacks
DarkReading - *Elizabeth Montalbano - January 21, 2025*

Le campagne di disinformazione russa eludono gli sforzi di Meta per bloccarle
Le sfide poste dalla disinformazione russa rappresentano un banco di prova per l'intero ecosistema digitale, richiedendo soluzioni innovative e una cooperazione senza precedenti. Ecco come queste operazioni hanno aggirato l'impegno di Meta, sfruttando lacune nei meccanismi di moderazione attualmente in uso, e come mitigano il fenomeno le principali piattaforme

Negli ultimi anni, si è osservata una crescita esponenziale delle campagne mirate a manipolare l'opinione pubblica attraverso piattaforme digitali, sfruttando vulnerabilità tecnologiche e psicologiche. Tra le piattaforme maggiormente colpite si annovera Meta, il colosso tecnologico che gestisce Facebook, Instagram e WhatsApp, il cui vasto bacino di utenti globali lo rende un obiettivo privilegiato.
Ecco come le campagne di disinformazione russa eludono gli sforzi di Meta per bloccarle.

Indice degli argomenti

La disinformazione russa ha eluso i tentativi di blocco da parte di Meta

Si consideri il contesto globale in cui operano i soggetti impegnati nella disinformazione. Gli attori statali (e non) che orchestrano queste campagne mirano a **generare divisioni sociali e a manipolare il discorso pubblico**, sfruttando le vulnerabilità intrinseche delle piattaforme digitali.
Meta, in quanto una delle realtà più influenti nel panorama tecnologico globale, rappresenta un **obiettivo privilegiato per tali operazioni**, con milioni di utenti distribuiti in ogni parte del mondo.
Le recenti **modifiche** alle regole sui contenuti di Meta, che **hanno rimosso alcune restrizioni automatiche**, sollevano **dubbi sull'efficacia delle politiche aziendali nel rispettare normative come il** Digital Services Act dell'Unione **Europea**.

Il caso della Social Design Agency

Un **caso emblematico** è rappresentato dalle **attività della Social Design Agency**, un'organizzazione russa oggetto di sanzioni internazionali per il suo ruolo nella diffusione di campagne di disinformazione.
Questa organizzazione è riuscita a pubblicare **oltre 8.000 inserzioni politiche che hanno affrontato temi di grande attualità come la guerra in Ucraina e la sicurezza internazionale**, con l'obiettivo di plasmare le percezioni degli utenti. (continua…)
Https://www.cybersecurity360.it/cybersecurity-nazionale/le-campagne-di-disinformazione-russa-eludono-gli-sforzi-di-meta-per-bloccarle/
CyberSecurity360 -*Luisa Franchina; Tommaso Diddi - 23 gen 2025*

Sanità sicura e resiliente, pietra angolare per l'Europa: i report di ACN e Commissione UE

Fra le infrastrutture critiche digitali oggetto di attacchi informatici, il settore sanitario ha un triste primato: risulta essere il più colpito e quello dove si registra la maggiore entità dei danni. Uno scenario ben fotografato dal report ACN e sul quale interviene il piano d'azione europeo. Ecco tutti i dettagli
Il **consolidamento della sicurezza informatica degli ospedali e degli operatori sanitari** può contare su un **piano d'azione di livello europeo**: il "Piano d'azione europeo sulla sicurezza informatica degli ospedali e degli operatori sanitari" pubblicato lo scorso 15 gennaio dalla Commissione Europea.
Si tratta della prima iniziativa specifica verticale di settore, che punta a **implementare le molteplici misure di sicurezza informatica previste dall'UE** indicate dalle norme di sicurezza europea.
In Italia, **un primo studio sulla sicurezza del settore sanitario** è stato pubblicato da ACN, con evidenze di attacchi e raccomandazioni a livello di singola organizzazione.
Il piano europeo presenta, invece, un **approccio coordinato e di "sistema" per la prevenzione e contrasto delle crisi di sicurezza nell'itero settore sanitario**.

Indice degli argomenti

- **Il settore sanitario è sotto attacco**
- **Sanità sicura e resiliente: i report di ACN e Commissione UE**
- **Sanità: attacchi in Italia e contromisure da ACN**
    - Contromisure proposte da ACN
- **Il piano europeo per il settore sanitario**

Il settore sanitario è sotto attacco

Fra le infrastrutture critiche digitali oggetto di attacchi informatici, **il settore sanitario ha un triste primato**: risulta essere il più colpito e quello dove si registra la maggiore entità dei danni.

I dati sono quelli che emergono dal report ACN dal titolo "La minaccia cibernetica al settore sanitario" che fotografa un andamento degli attacchi dal 2022 al 2024, periodo nel quale sono stati osservati sul territorio italiano una media di "2,6 eventi cyber malevoli al mese ai danni di strutture sanitarie, dei quali la metà circa ha dato luogo a "incidenti".

Ma gli attacchi al settore sanitario dilagano in tutta Europa, tanto che gli Stati membri hanno segnalato 309 incidenti significativi di sicurezza informatica che hanno interessato il settore sanitario nel 2023, più che in qualsiasi altro settore critico (fonte: **EU report**).

Per questo motivo, arriva in soccorso proprio la UE con il piano d'azione per la messa in sicurezza di ospedali e operatori sanitari che punta proprio a un **deciso miglioramento della postura di sicurezza di tutto il settore sanitario** per ottimizzare il rilevamento delle minacce, la preparazione e della risposta alle crisi nel settore sanitario.

Le indicazioni di progressiva attuazione fra il 2025 e il 2026 coinvolgono strumenti, servizi e formazione. (continua…)

Https://www.cybersecurity360.it/cybersecurity-nazionale/sanita-sicura-e-resiliente-pietra-angolare-per-leuropa-i-report-di-acn-e-commissione-ue/

CyberSecurity360 -*Alessia Valentini - 23 gen 2025*

Intelligenza blu per le aree marino-costiere - L'utilizzo dell'intelligenza artificiale e del machine learning per l'analisi dei big data offre soluzioni promettenti per la gestione integrata dei rischi in campo ambientale.

Nell'era dei big data, la produzione e sviluppo di informazioni sta crescendo quotidianamente a un ritmo esponenziale, aumentando in volume, velocità e varietà, trasformando settori chiave, inclusi quelli ambientali legati alla gestione e utilizzo degli ecosistemi marino-costieri. Attraverso satelliti, telerilevamento aereo, stazioni di monitoraggio, navi e boe, i dati ambientali vengono raccolti in modo continuo, fornendo elementi essenziali per una gestione efficace delle risorse marine e per interventi di protezione costiera. Questi dati non solo supportano la tutela ambientale, ma alimentano anche lo sviluppo di attività economiche come la pesca e il turismo, contribuendo alla crescita sostenibile delle economie costiere.

Gestione dei rischi e uso del machine learning

Gli ecosistemi marini e costieri, che includono habitat fondamentali come barriere coralline, mangrovie e praterie di fanerogame, sono sempre più minacciati dal cambiamento climatico e dalle attività antropiche. Il riscaldamento globale sta alterando le tendenze di temperatura e i livelli di ossigeno dei mari, intensificando gli eventi meteorologici estremi e aumentando i rischi per diversi sistemi e settori. Questi cambiamenti minacciano gli ecosistemi marini nella loro capacità di fornire servizi ecosistemici, fra i quali la regolazione del clima, la protezione dall'erosione costiera, la conservazione della biodiversità e la produzione alimentare. Di fronte a tale minaccia, la gestione dei rischi rappresenta una sfida cruciale per la comunità scientifica. Tale sfida è resa ancora più ardua dalla complessità di questi

ecosistemi e delle loro dinamiche, che rendono difficile identificare gli impatti e le aree critiche, nonché comprendere le sinergie tra le diverse pressioni, con effetti potenzialmente negativi sia sul breve sia sul lungo termine. Per affrontare queste sfide, è fondamentale sfruttare al meglio le informazioni disponibili e, in questo contesto, l'analisi dei big data mediante tecniche innovative legate all'intelligenza artificiale (IA), come il machine learning (Ml), stanno emergendo come soluzioni promettenti.
(*continua…)*
https://www.puntosicuro.it/ambiente-C-94/intelligenza-blu-per-le-aree-marino-costiere-AR-24902
Punto Sicuro - *Redazione - 23/01/2025*

Prevenzione sismica: questa sconosciuta - Il tema della prevenzione sismica in Italia richiede un'attenzione urgente. L'articolo analizza le criticità del patrimonio edilizio esistente, evidenziando le lacune normative e proponendo soluzioni come incentivi fiscali, assicurazioni obbligatorie e l'istituzione di un'Anagrafe del Costruito per una gestione più efficace e sicura della sicurezza sismica.
Lo scorso 12 dicembre, si è svolta a Roma la Settima Giornata Nazionale della Prevenzione Sismica (7GNPS), promossa da Fondazione Inarcassa, Consiglio Nazionale Ingegneri e Consiglio Nazionale Architetti Pianificatori Paesaggisti e Conservatori, del cui Comitato Tecnico-Scientifico ho l'onore di far parte sin dalla prima edizione.
L'iniziativa, che vuole essere una "grande occasione di confronto tra i rappresentanti delle istituzioni e gli esperti in materia, per discutere e analizzare le proposte in ambito scientifico, tecnologico e fiscale finalizzate alla messa in sicurezza del patrimonio edilizio", ha visto la presenza di rappresentanti di istituzioni politiche e di ricerca, nonché la partecipazione a distanza di migliaia di tecnici.
Con l'occasione si vuole fare il punto sulla situazione della sicurezza sismica in Italia, analizzando quanto fatto negli ultimi anni e riprendendo alcune proposte.
Imparare dal passato
Sbagliando s'impara: se guardiamo quello che succede nel nostro paese (e, in verità, anche in altri) con riferimento alle catastrofi naturali, questo famoso motto appare senz'altro falso.
Come ben noto, dopo un terremoto, i media dedicano gran parte del loro spazio all'evento: le varie TV ci mostrano immagini che già abbiamo visto, i giornali e i siti web pubblicano fotografie identiche a quelle che abbiamo già nel cassetto. Nonostante ciò, credendo nel *repetita iuvant*, rispondiamo alla pressione dei media evidenziando gli errori di progettazione e/o di realizzazione riscontrati, parlando di tecniche di costruzione, di adeguamento e miglioramento sismico, cioè di prevenzione.
(continua)
https://www.ingenio-web.it/articoli/prevenzione-sismica-questa-sconosciuta
Ingenio - *Paolo Clemente – 28.01.2025*

Attacchi cyber contro la Pa: come funziona la difesa del Polo Strategico Nazionale
Nell'ultimo trimestre, il Polo Strategico Nazionale (PSN) ha rilevato un'impennata di attacchi cyber rivolti alle pubbliche amministrazioni, sempre più presenti sul cloud. La situazione, invisibile al pubblico, viene gestita dal team di sicurezza del PSN, in particolare da Leonardo. Ecco come affronta la sfida, con quali tecnologie e finalità

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

Il **Polo Strategico Nazionale (PSN)** sta affrontando un'impennata di attività a difesa dagli attacchi informatici, con un crescente numero di **pubbliche amministrazioni** che **migrano i propri servizi sul cloud**.
La struttura, che punta a garantire la **sovranità del dato e la sicurezza digitale**, ha gestito numerosi attacchi informatici negli ultimi mesi, prevenendo danni e garantendo la continuità operativa dei servizi pubblici digitalizzati.

Indice degli argomenti

Polo Strategico Nazionale (PSN): come opera

Negli ultimi due o tre mesi, il PSN ha rilevato un aumento significativo degli attacchi cyber rivolti alle pubbliche amministrazioni che utilizzano i suoi servizi. La situazione non è visibile al pubblico, ma viene gestita quotidianamente dal team di sicurezza del Polo, in particolare da Leonardo, che ha la responsabilità della cyber sicurezza Questo incremento delle minacce informatiche evidenzia l'importanza di infrastrutture sicure per garantire la continuità operativa dei servizi essenziali della PA.
Il PSN, nato per colmare il gap infrastrutturale e garantire la sovranità digitale italiana, si configura come un progetto cruciale nel panorama della trasformazione digitale della PA.
La sua realizzazione è stata motivata dall'**esigenza di superare la frammentazione e la scarsa certificazione di molti data center pubblici,** fornendo un'**infrastruttura centralizzata e altamente sicura**. Con l'obiettivo di digitalizzare la PA, il PSN si pone anche come **baluardo nella protezione dei dati critici e strategici**.

La sovranità tecnologica

Dal punto di vista tecnologico, il **PSN** utilizza **data center certificati e tecnologie avanzate** per fornire **servizi cloud sicuri**.
L'infrastruttura sfrutta tecnologie di **virtualizzazione avanzata**, sistemi di **ridondanza geografica** per garantire la **continuità operativa** e piattaforme di **containerizzazione** per una gestione più efficiente delle risorse computazionali.
Tuttavia, **la dipendenza dell'Europa da produttori extra-UE per microchip, server e software**, pone delle **sfide in termini di sovranità tecnologica**. Sebbene **i servizi erogati dal PSN siano ospitati in data center italiani**, le tecnologie impiegate provengono spesso da aziende statunitensi o asiatiche.
Ciò significa che, mentre l'infrastruttura fisica rimane sotto controllo nazionale, la **componente tecnologica presenta elementi di interdipendenza con l'estero**.

Oltre 470 le PA migrate al cloud del Polo Strategico Nazionale

Attualmente, **oltre 470 pubbliche amministrazioni hanno scelto di migrare al cloud del PSN**. Di queste, più di 450 hanno già avviato il processo di migrazione, circa **320** hanno completato almeno un passaggio di servizio e più della metà ha completato **l'intero processo di migrazione**.
Particolarmente significativo è il coinvolgimento di **oltre 130 ospedali e ASL**, un settore in cui la sicurezza informatica e la protezione dei dati sensibili sono cruciali. (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/polo-strategico-nazionale-a-difesa-cloud-pa/

CyberSecurity360 -*Luisa Franchina; Tommaso Diddi - 30 gen 2025*

Attuazione Direttiva (UE) 2022/2557 CER sulla resilienza dei soggetti critici: implicazioni per le imprese di sicurezza privata in Italia - La Direttiva (UE) 2022/2557 CER del Parlamento Europeo e del Consiglio relativa alla resilienza dei soggetti critici e che abroga la direttiva 2008/114/CE del Consiglio, adottata il 14 dicembre 2022, rappresenta un significativo avanzamento nel quadro normativo europeo per garantire la resilienza dei soggetti critici, ovvero quegli enti pubblici e privati che erogano servizi essenziali per il funzionamento delle società e delle economie moderne. L'Italia ha recepito questa Direttiva attraverso il Decreto Legislativo 134/2024, che mira a rafforzare la protezione delle infrastrutture critiche e a garantire la continuità operativa in caso di minacce fisiche, naturali o antropiche.
Il Decreto Legislativo 134/2024 definisce una serie di obblighi e misure che i soggetti critici e le autorità competenti devono adottare per migliorare la loro resilienza. Tra questi, spiccano
la predisposizione di strategie nazionali,
l'istituzione di un Comitato Interministeriale per la Resilienza (CIR) e
l'adozione di strumenti di valutazione del rischio a livello nazionale e settoriale.
Questi elementi costituiscono il fulcro dell'adattamento italiano alla Direttiva CER (Critical Entities Resilience), evidenziando un impegno verso un approccio integrato e coordinato alla protezione delle infrastrutture critiche.
La Direttiva si inserisce in un contesto più ampio di regolamentazione europea, integrandosi con la Direttiva (UE) NIS2 2022/20025, focalizzata sulla cybersicurezza, e con il Regolamento Delegato (UE) 2023/2450, che stabilisce un elenco di servizi essenziali per i soggetti critici. Mentre la Direttiva CER si concentra sulla resilienza fisica e operativa dei soggetti critici, la NIS2 si occupa della sicurezza dei sistemi informatici che supportano tali entità. Questo approccio integrato riflette l'interdipendenza tra sicurezza fisica e digitale, evidenziata da crescenti minacce ibride e transfrontaliere.
(continua).
https://www.snewsonline.com/attuazione-direttiva-ue-2022-2557-cer-resilienza-soggetti-critici-implicazioni-imprese-sicurezza-privata-italia/
S News - *di Maria Cristina Urbano - 3 Febbraio 2025*

Agencies Sound Alarm on Patient Monitors With Hardcoded Backdoor
CISA and the FDA are warning that Contec CMS8000 and Epsimed MN-120 patient monitors are open to meddling and data theft; Claroty Team82 flagged the vulnerability as an avoidable insecure design issue.
Last week, the Cybersecurity and Infrastructure Security Agency (CISA), alongside the US Food and Drug Administration (FDA), raised an alert for Contec CMS8000 and Epsimed MN-120 healthcare monitors, warning they potentially put patients at risk once connected to the Internet, due to a malicious, hidden backdoor embedded into the devices. But security researchers say the issue isn't actually intentional malware but, rather, just insecure design.
The devices continuously monitor patient vital signs, such as heart rate, blood oxygen saturation, temperature, respiration rate, and more. CISA and the FDA reported findings for three cybersecurity risks in the gear thanks to the "backdoor": an unauthorized user could remotely control a monitor and cause it to function in an unintended manner; attackers could compromise the device and pivot to a network; and an attacker could exfiltrate the data that the monitor collects.

From a patient health perspective, if an attacker were able to manipulate the information the monitor gives patients, that could prevent them from realizing that there's something wrong. Though they reported no known cybersecurity incidents, deaths, or injuries related to the findings, the FDA still provided recommendations for patients and caregivers: talking to healthcare providers about evaluating their patient monitoring device and following certain steps if it does rely on an Internet connection. (continua…)
https://www.darkreading.com/vulnerabilities-threats/agencies-sound-alarm-patient-monitors-hardcoded-backdoor
DarkReading - *Kristina Beek - February 6, 2025*

Massive brute force attack uses 2.8 million IPs to target VPN devices
A large-scale brute force password attack using almost 2.8 million IP addresses is underway, attempting to guess the credentials for a wide range of networking devices, including those from Palo Alto Networks, Ivanti, and SonicWall.
A brute force attack is when threat actors attempt to repeatedly log into an account or device using many usernames and passwords until the correct combination is found. Once they have access to the correct credentials, the threat actors can then use them to hijack a device or gain access to a network.
According to the threat monitoring platform The Shadowserver Foundation, a brute force attack has been ongoing since last month, employing almost 2.8 million source IP addresses daily to perform these attacks.
Most of these (1.1 million) are from Brazil, followed by Turkey, Russia, Argentina, Morocco, and Mexico, but there's generally a very large number of countries of origin participating in the activity.
These are edge security devices like firewalls, VPNs, gateways, and other security appliances, often exposed to the internet to facilitate remote access.
The devices conducting these attacks are mostly MikroTik, Huawei, Cisco, Boa, and ZTE routers and IoTs, which are commonly compromised by large malware botnets.
In a statement to BleepingComputer, The Shadowserver Foundation confirmed that the activity has been ongoing for a while but recently increased to a much larger scale.
ShadowServer also said that the attacking IP addresses are spread across many networks and Autonomous Systems and are likely a botnet or some operation associated with residential proxy networks.
Residential proxies are IP addresses assigned to consumer customers of Internet Service Providers (ISPs), making them highly sought after for use in cybercrime, scraping, geo-restriction bypasses, ad verification, sneaker/ticket scalping, and more.
These proxies route internet traffic through residential networks, making it appear that the user is a regular home user rather than a bot, data scraper, or hacker. (continua…)
https://www.bleepingcomputer.com/news/security/massive-brute-force-attack-uses-28-million-ips-to-target-vpn-devices/?is=0b8f2776946dfb918b4bb1b43d6713cbf6a927ebd5e2184a38ea2f92df6f9da9
BleepingComputer *- Bill Toulas -February 8, 2025*

High performance computing (Hpc) nei data center: a che punto siamo
La tecnologia high performance computing nei data center permette di usufruire di un'enorme potenza di calcolo per gestire grandi quantità di dati: vediamo i vantaggi e le applicazioni
Gli **HPC data center**, offrono un'enorme potenza di calcolo per elaborare grandi volumi di dati, ma richiedono un'attenta gestione delle sfide operative e tecnologiche per sfruttarne le potenzialità, **sempre prestando attenzione al tema della sostenibilità**. Vediamo la situazione.

Indice degli argomenti

Cosa è un HPC e cosa sono gli HPC data center

HPC (High Performance Computing) si riferisce all'uso di risorse di elaborazione aggregate e tecniche di elaborazione simultanea per eseguire programmi avanzati e risolvere complessi **problemi di elaborazione**, oltre a garantire prestazioni migliori rispetto ad un singolo computer o server. Ciò può essere fatto in loco, nel cloud o in modalità ibrida. È doveroso evidenziare che i sistemi HPC sono progettati per funzionare alla massima velocità operativa per applicazioni che richiedono un'immensa potenza di elaborazione.

Un HPC data center ha processori potenti, un'elevata densità di server e grandi requisiti di raffreddamento. È stato sviluppato appositamente per gestire questa enorme capacità di potenza. Inoltre, oggi, molti HPC data center sono collegati a grandi aziende private e pubbliche che necessitano di "supercomputer" con molta potenza di calcolo che **sono utilizzati per simulazioni**, per ricerche e per altre elaborazioni di dati. Ancora, un HPC data center utilizza enormi quantità di energia per alimentare processori potenti, server ad alta densità e tecnologie di raffreddamento avanzate.

Vantaggi degli HPC data center

I moderni HPC data center, se da un lato possono facilitare attività complesse e ad alta intensità di elaborazione – consentendo un ampio margine per la scalabilità e per la gestione dei costi **in termini di gestione di hardware, di software, di rete, di storage e di sistemi**, oltre che garantire l'affidabilità, l'efficienza e la disponibilità – dall'altro lato comportano sfide che devono essere gestite. In particolare, ci sono alcuni aspetti da considerare.

Prestazioni migliorate

I sistemi HPC migliorano significativamente le prestazioni dei data center, consentendo loro di elaborare grandi set di dati e calcoli complessi in minuti o ore rispetto alle settimane o ai mesi di un normale sistema di elaborazione. Ciò è fondamentale per applicazioni e servizi di aziende che operano nell'ambito dell'intelligenza artificiale, della ricerca scientifica e dell'analisi dei big data.

Scalabilità

Gli HPC data center sono progettati per espandersi in modo flessibile, soddisfacendo le crescenti richieste, senza compromettere le prestazioni. Inoltre, grazie ai servizi cloud, è possibile accedere all'HPC da qualsiasi parte del mondo, offrendo una disponibilità globale e una maggiore efficienza operativa (continua…).

https://www.agendadigitale.eu/cittadinanza-digitale/data-management/hpc-high-performance-computing-nei-data-center-potenzialita-e-sfide-future/

AgendaDigitale *- Federica Maria Rita Livelli - 13 feb 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

NOTIZIE D'INTERESSE:

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

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

RIFERIMENTI DELL'ASSOCIAZIONE

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

Per maggiori informazioni sull'Associazione inviare una mail a

segreteria@infrastrutturecritiche.it

o visitate il sito

www.infrastrutturecritiche.it

ATTENZIONE

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

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

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

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

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.