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. 1/ 2025** **gennaio 2025**

Cyber attacchi e non solo.

Nei giorni 11 e 13 gennaio 2025 un gruppo di siti istituzionali, alcune banche e aziende in Italia sono state oggetto di un attacco cyber da parte di un gruppo di hacker filorusso, denominato NoName057, che lo ha motivato come risposta al sostegno espresso dall'Italia all'Ucraina nell'incontro di Giorgia Meloni con Volodymyr Zelensky**.**

Il tipo di attacco è stato DDoS (Distributed Denial of Service) che mira a bloccare temporaneamente il servizio dei siti attaccati attraverso l'invio di un flusso continuo di richieste provenienti da una rete di computer compromessi.
Gli attacchi DDoS sono una categoria di difficile identificazione nelle fasi iniziali e di non semplice mitigazione quando sono in atto.

Secondo le notizie disponibili risultano essere stati attaccati: il Ministero della Difesa (Marina e Aeronautica), quello degli Esteri, quello delle Infrastrutture e dei Trasporti, la Consob, i Carabinieri. Sono stati anche compromessi i siti delle aziende di trasporto pubblico di Roma, Palermo e Genova, come pure i porti di Taranto e Trieste. Infine, sono stati bloccati i siti di Intesa San Paolo e Monte dei Paschi di Siena. Risulta anche che siano state attaccate alcune aziende.

"L'Italia dovrebbe iniziare ad aiutare se stessa e, prima di tutto, la sua sicurezza informatica" è stata la rivendicazione dei cyber criminali.

A parte il disagio degli utenti e il danno di immagine, ritengo che la rivendicazione del gruppo di hacker possa essere lo spunto per una maggiore presa di coscienza dello stato della nostra cybersicurezza per quanto riguarda i settori critici. Infatti, tutte le strutture coinvolte nell'attacco appartengono a tale ambito e le attività "ostili" si sono intensificate già da dopo l'inizio del conflitto in Ucraina (febbraio 2022) e hanno visto dei picchi anche in occasione dell'inasprirsi di altre tensioni internazionali.

L'Italia si è dotata di norme e strutture che definiscono e presidiano il perimetro nazionale di cybersicurezza e la strategia (legge 18 novembre 2019; n. 133; legge 4 agosto 2021, n. 109; DPCM 17 maggio 2022 e DPCM 8 luglio 2024); ha anche recepito le direttive europee per la cybersecurity (NIS2, DORA) e la resilienza dei settori critici (CER). Ma le norme per essere efficaci devono tradursi in azioni da parte delle decine di migliaia di entità, pubbliche e private, che appartengono ai settori considerati "critici" per il funzionamento del sistema paese.
Quindi nell'opera di rafforzamento della cybersicurezza e della resilienza delle infrastrutture critiche devono operare sia le amministrazioni pubbliche sia le imprese, entrambi con l'obiettivo di rafforzare le proprie difese.
Questa condivisione di intenti rappresenta un'opportunità unica di cooperazione tra pubblico e privato purché la si riesca a sviluppare, possibilmente, con un dialogo nel quale l'autorità pubblica non venga percepita come il controllore, troppo spesso "fiscale", dell'attuazione di norme "astruse ed inutili" che

ostacolano l'attività di impresa. Quindi la "postura" dell'amministrazione pubblica è fondamentale per veicolare il messaggio che la sicurezza è un processo e un risultato collettivo e non può limitarsi ad una conformità formale a norme e standard. Analogamente, diverse entità, pubbliche e private, dovranno far proprio un concetto di sicurezza che sia basato su azioni e misure concrete, derivate da un'analisi dei rischi, e non sia finalizzato alla sola conformità "cartacea" ad uno standard.

Questa evoluzione richiederà anche risorse economiche per l'acquisizione di strumenti tecnici e la formazione di specialisti, questi ultimi attualmente decisamente carenti rispetto alle esigenze. Se questo divario non verrà superato il nostro paese rischia di essere sempre più esposto al ripetersi di attacchi il cui costo complessivo sarà, purtroppo, molto superiore a quello necessario per difendersi. La prassi "dell'invarianza dei costi", diffusa nella P.A. nei periodi di difficoltà di bilancio, non è certo garanzia di raggiungimento degli obiettivi. Forse è il caso di ribadire, per l'ennesima volta, che la sicurezza non è un costo ma un investimento, ovviamente se ben impiegato.

Infine, è in pieno svolgimento la registrazione dei soggetti NIS2 presso il sito dell'ACN (Agenzia per la cybersicurezza nazionale), si tratta di alcune decine di migliaia di soggetti, pubblici e privati, appartenenti a settori critici. L'applicazione della NIS2 rappresenta un'opportunità unica per rafforzare complessivamente le infrastrutture del paese. All'ACN spetta un compito molto oneroso di impulso e coordinamento, iniziato con atteggiamento molto collaborativo e per il quale speriamo disponga di risorse adeguate, mentre alle entità pubbliche private è richiesto di acquisire la consapevolezza che la sicurezza richiede azioni e misure concrete e, quindi, impegno organizzativo ed economico.

Glauco Bertocchi

Laurea in Fisica all'Università di Roma "la Sapienza" Più di 40 anni di esperienza in IT e nella sicurezza acquisita all'interno di università e istituzioni nazionali. Attivo nella ricerca in ambito protezione e resilienza delle Infrastrutture critiche.
Certificato CISM, ISO 27001:2013/2022, CDPSE.
Vicepresidente del capitolo ISACA Roma, componente del CD di AIIC.

ATTIVITA' DELL'ASSOCIAZIONE

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

NEWS E AVVENIMENTI

NIS2: le sfide e come affrontarle - La Direttiva NIS2 è stata recepita con D.Lgs. n. 138/2024, pubblicato in Gazzetta Ufficiale il 1° ottobre 2024. Inaspettatamente siamo tra i primi in Europa.
Siamo certi che la normativa, comunemente chiamata NIS2, riguardi solo un numero ristretto di aziende?
Potrebbe sorprendere sapere che la fascia è assai più ampia di quel che si pensi. I fattori chiave che ne determinano l'appartenenza non sono solamente criticità, dimensioni, fatturato, settore di business, ma anche la contribuzione, in veste di fornitore strategico, alla sicurezza di chi ne fa parte: essere all'interno di una filiera impone la condivisione di obblighi con il capo-fila.
Conoscere detta norma, legata a tre macigni quali il D.Lgs. n.134/2024 (CER), il D.L. n. 105/2019 (PSNC) e, non ultimo, il GDPR, consente di prepararsi a quel fatidico momento assicurando un vantaggio competitivo difficile da scalfire nel breve-medio termine *(continua).*
https://www.snewsonline.com/nis2-sfide-come-affrontarle/
S News - *Cristhian Re - 17 Dicembre 2024*

La NIS 2 prende forma: tutti gli adempimenti per avviare il percorso di conformità - Con la pubblicazione da parte dell'Agenzia per la Cybersicurezza Nazionale della determina che dettaglia i primi aspetti concreti di implementazione della NIS 2 è formalmente iniziato, per le aziende, il percorso di conformità alla direttiva europea. Ecco tutto quello che c'è da sapere per non farsi trovare impreparati.
NIS 2 percorso di conformità
La determina pubblicata dall'Agenzia per la Cybersicurezza Nazionale dettaglia i primi aspetti concreti di implementazione della Direttiva NIS 2: quella sui termini, le modalità e i procedimenti di utilizzo e accesso alla piattaforma digitale.
Nello specifico, quest'ultima sarà uno dei principali strumenti di comunicazione tra l'Agenzia e i soggetti essenziali o importanti fin dalle primissime fasi di applicazione della normativa.
Infatti, tra le prime attività richieste alle aziende italiane vi è l'obbligo di registrarsi su tale piattaforma affinché l'ACN possa censire gli enti presenti sul territorio nazionale e individuare i soggetti essenziali e importanti.

Indice degli argomenti

(*continua…)*
https://www.cybersecurity360.it/legal/la-nis-2-prende-forma-tutti-gli-adempimenti-per-avviare-il-percorso-di-conformita
Cybersecurity360 - *Pierluigi Perri, Lucrezia Falciai - 19 dic 2024*

Supercalcolo, intelligenza artificiale e sostenibilità ambientale - L'IA può essere usata per migliorare l'efficienza e la Sostenibilità delle città e per salvaguardare l'ambiente naturale. Un progetto sul verde urbano e uno studio sugli impatti dei fenomeni meteorologici sulla produzione di energia elettrica.
Negli ultimi anni, l'intelligenza artificiale (IA) ha dimostrato un enorme potenziale in una moltitudine di settori, tra i quali uno dei più promettenti è sicuramente quello della gestione dell'ambiente naturale e urbano. Grazie alla capacità di analizzare grandi quantità di dati in tempo reale, l'IA può diventare uno strumento fondamentale per prevenire disastri ambientali, monitorare il cambiamento climatico e ottimizzare l'utilizzo delle risorse naturali.
Una delle applicazioni dell'intelligenza artificiale in questo ambito è la creazione di digital twin delle città, modelli virtuali che riproducono fedelmente lo sviluppo e le dinamiche urbane, con un approccio che sta rivoluzionando il modo in cui monitoriamo e gestiamo lo spazio pubblico. Oltre a permettere di tenere traccia delle modifiche strutturali, facilitando una gestione più sostenibile delle città, i gemelli digitali aiutano anche i decisori a prevedere l'effetto delle possibili scelte, fornendo simulazioni reali degli impatti delle modifiche proposte. In campo ambientale, l'IA può predire con grande precisione eventi come frane, inondazioni e incendi, permettendo così di intervenire tempestivamente e prevenire danni ingenti. Monitorando l'utilizzo delle risorse, come l'acqua e l'energia, l'IA può ottimizzare i consumi, riducendo sprechi e contribuendo alla sostenibilità a lungo termine. Allo stesso tempo, grazie agli algoritmi specifici, si possono analizzare immagini satellitari o da droni per rilevare cambiamenti nel territorio, come deforestazioni illegali, espansioni urbane incontrollate e altre attività umane che possono compromettere l'equilibrio ambientale. (continua…)
https://www.puntosicuro.it/sostenibilita-C-149/supercalcolo-intelligenza-artificiale-sostenibilita-ambientale-AR-24899
Punto Sicuro - *Redazione - 19/12/2024*

Hackers Are Hot for Water Utilities
The US water sector suffered a stream of cyberattacks over the past year-and-a-half from a mix of cybercriminals, hacktivists, and nation-state hacking teams. Here's how the industry and ICS/OT security experts are working to better secure vulnerable drinking and wastewater utilities.
The unprecedented wave of high-profile cyberattacks on US water utilities over the past year has just kept flowing.
In one incident, pro-Iranian hackers penetrated a Pittsburgh-area water utility's PLC and defaced the touchscreen with an anti-Israel message, forcing the utility to revert to manual control of its water pressure-regulation system. A water and wastewater operator for 500 North American communities temporarily severed connections between its IT and OT networks after ransomware infiltrated some

back-end systems and exposed its customers' personal data. Customer-facing websites and the telecommunications network at the US's largest regulated water utility went dark after an October cyberattack.

Those were just some of the more chilling stories that have recently sparked fear over the security and physical safety of drinking water and wastewater systems. The cyberattacks have spurred warnings and security guidelines from the Cybersecurity and Infrastructure Security Agency (CISA), the White House, the FBI and the Office of the Director of National Intelligence (ODNI), the Environmental Protection Agency (EPA), and the Water ISAC (Information Sharing and Analysis Center).

Most of the attacks landed on the softest of targets, small water utilities without security expertise and resources, in mainly opportunistic attacks. Meanwhile, cyberattacks on large utilities like Veolia and American Water hit IT, not OT, systems — none of which actually disrupted water services. Overall, the cyberattacks on water appeared to be mainly about "poking around and eroding confidence," says Gus Serino, president of I&C Secure and a former process control engineer for the Massachusetts Water Resources Authority.

The race is now on to secure the water sector — especially the smaller more vulnerable utilities — from further cyberattacks. Many larger water utilities already have been "stepping up their game" in securing their OT networks, and others started building out their security infrastructures years ago, notes Dale Peterson, president of ICS/OT security consultancy Digital Bond. "My first client in 2000 was a water utility," he recalls. "Some [large utilities] have been working on this for a very long time." (continua…)

https://www.darkreading.com/ics-ot-security/hackers-hot-water-utilities

DARKREADING- *Kelly Jackson Higgins- December 27, 2024*

BIG U e i piani anti-alluvione: cosa insegnano i progetti di resilienza climatica per Lower Manhattan - Dal masterplan di BIG U di alcuni anni fa alle realizzazioni dei giorni nostri: la difesa di Lower Manhattan dagli eventi estremi e dall'innalzamento delle acque prosegue. Nasce un nuovo paesaggio urbano fatto di paratie mobili, muri anti-inondazione, parchi sopraelevati e pavimentazioni permeabili, in cui la vista e l'accesso al lungomare è garantito.

Piani anti-alluvione per Lower Manhattan: un esempio concreto di convivenza con gli effetti della crisi climatica

Il primo articolo dedicato ai piani anti-alluvione per Lower Manhattan (Ingenio del 9 settembre 2024) si chiudeva con una presa d'atto, di come cioè questo importante distretto di New York rappresenti un esempio concreto di convivenza con gli effetti della crisi climatica e, in particolare, con il fenomeno sempre più frequente, imprevedibile e disastroso delle alluvioni e dell'innalzamento delle acque degli Oceani.

Nonostante se ne sia parlato molto e in diverse occasioni, è il caso di ricordare come e quando nella Grande Mela è iniziata questa lotta contro il tempo e gli eventi estremi.

La visione di BIG U

L'inizio della svolta ci fu nel 2012, subito dopo il disastroso passaggio su New York e sulla costa atlantica dell'uragano Sandy; un passaggio che segno uno spartiacque: da lì in poi ci fu una pronta e decisa reazione delle istituzioni locali e federali e della società civile, quest'ultima organizzata attorno al cartello Rebuild by Design. Furono loro infatti a imprimere una svolta per un futuro resiliente di New York e di Lower Manhattan.

Con la Hurricane Sandy Competition di quegli anni, fu il progetto BIG U, sviluppato dallo studio danese Bjarke Ingels Group , a vincere il concorso internazionale per difendere Lower Manhattan dagli eventi alluvionali estremi. Con i progettisti di BIG lavorarono importanti studi internazionali di architettura,

ingegneria e del paesaggio come One Architecture, Starr Whitehouse, James Lima Planning + Development, Green Shield Ecology, AEA Consulting, Level Agency for Infrastructure, Arcadis, Buro Happold.
Nel corso degli anni, l'idea ha lasciato il posto al progetto (ai progetti) e alla realizzazione di infrastrutture anti-inondazione, capaci abbracciare più zone di Manhattan e coinvolgere più istituzioni governative e locali. *(continua)*
https://www.ingenio-web.it/articoli/big-u-e-i-piani-anti-alluvione-cosa-insegnano-i-progetti-di-resilienza-climatica-per-lower-manhattan
Ingenio - *Pietro Mezzi – 7 gennaio 2025*

Starlink e sicurezza nelle telecomunicazioni Italiane: le sfide da affrontare
La costellazione di satelliti in orbita bassa gestita da SpaceX rappresenta un sistema innovativo, ma il confronto con altre tecnologie terrestri e marittime richiede un'analisi approfondita in termini di sicurezza, resilienza e funzionalità. L'elemento di sicurezza rappresenta, però, una questione delicata
La recente attenzione verso l'integrazione di Starlink nei sistemi di comunicazione strategica italiana pone diverse domande di natura tecnica e funzionale.
La costellazione di satelliti in orbita bassa gestita da SpaceX rappresenta un sistema innovativo rispetto alle infrastrutture satellitari più tradizionali, ma il confronto con altre tecnologie terrestri e marittime richiede un'analisi approfondita in termini di sicurezza, resilienza e funzionalità.
Indice degli argomenti

Come si potrebbe integrare Starlink in un ecosistema più ampio
Telespazio, una joint venture tra Leonardo (67%) e Thales (33%), è uno dei principali operatori mondiali nel campo delle soluzioni e dei servizi satellitari. Con il recente accordo con SpaceX, prevede di integrare Starlink nella propria rete globale di connettività ibrida, che combina soluzioni satellitari e terrestri per garantire comunicazioni affidabili e resilienti con copertura globale.
Questa collaborazione rappresenta un esempio concreto di come Starlink possa essere integrato in un ecosistema più ampio per offrire vantaggi significativi in termini di flessibilità e resilienza.
Esaminando il contesto marittimo, è evidente come i sistemi satellitari rappresentino una soluzione imprescindibile per le comunicazioni. In mare aperto, dove le reti terrestri sono completamente assenti, la connettività satellitare è l'unica opzione praticabile.
In questo ambito, Starlink si distingue grazie alla sua architettura basata su una costellazione di migliaia di satelliti in orbita bassa (LEO), che garantisce una copertura più capillare e una latenza significativamente inferiore rispetto ai satelliti geostazionari tradizionali.
Inoltre, la maggiore densità della rete riduce il rischio di interruzioni nel servizio.
I satelliti LEO di Starlink offrono latenze significativamente inferiori rispetto ai satelliti GEO, che operano a circa 36.000 km di altezza. La distanza più ridotta dei satelliti LEO, tipicamente tra i 300 e i 1.200 km dalla Terra, consente una trasmissione di dati più rapida, con latenze che possono scendere sotto i 20 millisecondi.

Questa caratteristica rende il sistema particolarmente adatto per applicazioni che richiedono comunicazioni in tempo reale: in confronto, i satelliti GEO possono presentare latenze superiori ai 600 millisecondi.
Tuttavia, l'elemento di sicurezza rappresenta una questione delicata. Dal punto di vista della sicurezza cibernetica, Starlink introduce alcuni miglioramenti rispetto ai tradizionali sistemi satellitari commerciali, ma resta distante dagli standard dei sistemi militari.
Starlink e il fattore sicurezza
Starlink utilizza crittografia avanzata per proteggere i dati in transito. Il protocollo è basato su standard moderni, come AES (Advanced Encryption Standard), che garantiscono la sicurezza delle comunicazioni contro intercettazioni non autorizzate. (continua…)
https://www.cybersecurity360.it/cybersecurity-nazionale/starlink-e-sicurezza-nelle-telecomunicazioni-italiane-le-sfide-da-affrontare/
***Cybersecurity360** - Luisa Franchina, Tommaso Diddi - 9 gen 2025*

Chinese APT Group Is Ransacking Japan's Secrets
Since 2019, MirrorFace has been stealing information from myriad Japanese organizations to gain leverage over Japan in the event of hostilities between the two countries, experts said.
The National Police Agency and the National Center of Incident Readiness and Strategy for Cybersecurity warned Japanese organizations of a sophisticated Chinese state-backed cyber-espionage effort called "MirrorFace" to steal technology and national security secrets.
Japanese authorities said the advanced persistent threat group (APT) MirrorFace has been operating since 2019.
"By publicizing the modus operandi of 'MirrorFace' cyberattacks, the purpose of this alert is to make targeted organizations, business operators, and individuals aware of the threats they face in cyberspace and to encourage them to take appropriate security measures to prevent the damage caused by cyberattacks from spreading and to prevent damage from occurring in the first place," read a statement from Japanese police.
MirrorFace Cyberattacks Against Japan
Japanese law enforcement identified three types of MirrorFace attacks. The earliest and most enduring tactic used by MirrorFace to steal Japanese secrets was an elaborate phishing campaign between 2019 and 2023 aimed at delivering malware to the country's think tanks, governments, and politicians, according to the warning issued by Japan's National Police Agency and translated to English.
In 2023, MirrorFace pivoted to finding vulnerabilities in network devices across healthcare, manufacturing, information and communications, education, and aerospace, the police continued. MirrorFace exploited vulnerabilities in devices that included Fortinet FortiOS and FortiProxy (CVE-2023-28461), Citrix ADC (CVE-2023-27997,) and Citrix Gateway (CVE-2023-3519).
Another phishing campaign began around June 2024 and used basic phishing tactics against the media, think tanks, and Japanese politicians, according to police. And from February 2023 to October 2023, the group was observed exploiting an SQL injection in an external public server to gain access to Japanese organizations. (continua…)
https://www.darkreading.com/cyberattacks-data-breaches/chinese-apt-group-ransacking-japans-secrets
***Dark Reading** - Becky Bracken - January 10, 2025*

NIS2, adeguarsi è difficile ma possibile: ecco una guida

L'implementazione della direttiva NIS2 pone sfide significative per le piccole e medie imprese italiane, soprattutto riguardo i collegamenti societari e gli obblighi di sicurezza. Un'analisi delle complessità e delle soluzioni proposte

La stagione dell'attuazione della **direttiva europea NIS2** è iniziata ufficialmente.

Questa, come nel sentimento comune di giuristi e tecnici, rappresenta una modifica più che significativa dell'approccio alla gestione della sicurezza delle informazioni, per più ragioni, non ultima delle quali, **l'impressionante estensione del suo ambito di applicazione** che va ben oltre la semplice elencazione dei soggetti appartenenti a settori ad alta criticità, "altri settori critici", amministrazioni centrali, regionali, locali o altre tipologie di cui agli allegati al decreto di recepimento, con un potenziale espansivo la cui reale dimensione sarà misurabile solo al completamento del processo di autodichiarazione.

Nell'apprezzare lo sforzo comunicativo dell'Agenzia per la Cybersicurezza Nazionale, che mette in secondo piano l'aspetto del processo repressivo e sanzionatorio rispetto alla promozione della partecipazione attiva, è stato però evidenziato che **il processo di attuazione degli obiettivi della Direttiva non può risolversi soltanto in un ossequio formale al sistema di gestione della sicurezza** – quella che si definisce comunemente "security di carta" o "law security", ma richiede invece uno sforzo sostanziale per la definizione di obiettivi concreti e sostenibili di sicurezza delle singole realtà, che si trasforma in un processo di sicurezza collettiva o, se si preferisce, di sicurezza nazionale.

Indice degli argomenti

Responsabilità e obblighi delle imprese sotto la INS2

Tralasciando gli aspetti più strettamente legati alla tecnica dei sistemi di gestione della sicurezza delle informazioni, è necessario **svolgere qualche riflessione preliminare su questioni che attengono al processo di responsabilizzazione delle imprese** e delle pubbliche amministrazioni, oggi accomunate in un obiettivo giuridicamente rilevante di protezione di interessi che trascendono ampiamente la dimensione della singola organizzazione e definiscono una vera e propria "posizione di garanzia" qualificata, che comporta conseguenze di non poco conto.

Sulla **responsabilità degli "Organi di amministrazione e direttivi"** di cui all'art. 23 del Decreto legislativo 138/2024 sarà necessario un approfondimento specifico in altro articolo. In questa sede ci si preferisce soffermarsi su un aspetto diverso e, se si vuole, più pratico, che riguarda sia la più prossima scadenza del regime di autodichiarazione sulla piattaforma messa a disposizione da ACN, sia alcune considerazioni di natura più strettamente giuridica, sulla qualificazione di quella "posizione di garanzia" cui si è precedentemente accennato. (continua..)

https://www.agendadigitale.eu/sicurezza/imprese-e-nis2-guida-alla-nuova-normativa/

AgendaDigitale **-** *Francesco Di Maio - 14 gen 2025*

Starlink, ecco i punti che fanno la differenza in Italia

Analisi del fenomeno Starlink nel panorama delle telecomunicazioni: dalla rivoluzione tecnologica alle dinamiche di mercato. Come le costellazioni satellitari ridefiniscono il futuro della connettività globale
Il 2025 delle telecomunicazioni italiane inizia con le polemiche sul ruolo di **Elon Musk** e uno dei suoi progetti industriali, **Starlink**, la costellazione di satelliti a bassa quota.
Come la maggior parte dei progetti di Musk, anche Starlink è una soluzione molto innovativa che si distingue dagli altri servizi satellitari per la combinazione di tecnologie e architetture di rete avanzate.
Indice degli argomenti

L'innovazione della soluzione Starlink: facciamo chiarezza
Va innanzitutto premesso come ci sia un po' di confusione sul tema dell'innovazione della soluzione Starlink, che ha almeno **due declinazioni**: la prima riguarda in generale le **performance** dei servizi di **connettività** a banda ultralarga; la seconda attiene invece alla **sicurezza delle comunicazioni**.
Nel seguito ci concentreremo sul primo aspetto, mentre per il secondo rimandiamo a successivi approfondimenti e alle possibili **considerazioni di natura geopolitica**, anche in considerazione dei vincoli che prevedono le autorizzazioni dell'Federal Communications Commission (FCC) in situazioni di emergenza e di sicurezza nazionale.
Starlink, un cambio di paradigma nella connettività satellitare
Innanzitutto, Starlink rappresenta un **cambiamento di paradigma** nella connettività satellitare. Grazie all'uso di **satelliti LEO, laser inter-satellite, antenne avanzate e un'architettura di rete scalabile**, Starlink riesce a fornire servizi a banda **ultralarga con bassa latenza**, superando le limitazioni dei tradizionali servizi satellitari geostazionari.
In modo molto schematico, la tabella seguente riassume le principali caratteristiche di una costellazione **Low Orbit Satellite (LEO)**, come Starlink, rispetto alla tradizionale soluzione Geostationary Satellite (GEO), ad esempio Eutelsat VHTS (Very High Throughput Satellite).(continua…)
https://www.agendadigitale.eu/infrastrutture/starlink-tra-mito-e-realta-innovazione-e-scenari-geopolitici/
AgendaDigitale - Cristoforo Morandini - 14 gen 2025

As tensions mount with China, Taiwan sees surge in cyberattacks
In 2024, the Taiwanese government saw the daily average of attempted attacks by China double to 2.4 million, with a focus on government targets and telecommunications firms.
Using phishing emails and zero-day exploits, China's cyber-operations groups targeted Taiwanese organizations — including government agencies, telecommunications firms, and transportation — with significantly higher volumes of attacks in 2024.

On average, Taiwan saw more than 2.4 million attack attempts per day, double the 1.2 million average daily attacks in 2023, with the vast majority of activity targeting the Taiwanese government, according to an annual analysis published by Taiwan's National Security Bureau (NSB). Like many other countries, Taiwan has also detected a surge in attacks targeting its telecommunications sector, with the number of security events rising by more than sixfold, the analysis stated.
"China has continued to intensify its cyberattacks against Taiwan," the NSB stated in the report. "By applying diverse hacking techniques, China has conducted reconnaissance, set cyber ambushes, and stolen data through hacking operations targeting Taiwan's government, CI [critical infrastructure] and key private enterprises."
China has become increasingly aggressive in its cyber operations. Government-backed groups in the country have compromised telecommunications networks in the US, stolen information from Southeast Asia and Africa, and targeted individuals in India with SMS phishing attacks. China-based groups, specifically, have branched out into a variety of different areas, going beyond cyber espionage.
To date, very few countermeasures have been effective at restraining China in cyberspace, says Jon Clay, vice president of threat intelligence at cybersecurity firm Trend Micro. (continua…)
https://www.darkreading.com/cyber-risk/as-tensions-with-china-mount-taiwan-sees-surge-in-cyberattacks
DARKREADING - *Robert Lemos- January 15, 2025*

Cybersicurezza: Linee guida funzioni criptografiche - Un prezioso documento pubblicato dall'agenzia per la cybersicurezza nazionale (ACN) fornisce le indicazioni per orientarsi tra gli algoritmi crittografici, che permettono di proteggere le comunicazioni nel mondo digitale in maniera sicura ed efficiente.
L'agenzia per la cybersicurezza nazionale ACN ha cominciato a pubblicare preziosi documenti, che permettono di tenere aggiornati gli esperti di sicurezza informatica su tecniche di attacco e tecniche di difesa. Presentiamo oggi le "Linee guida funzioni criptografiche", un manuale dedicato all'illustrazione delle funzioni criptografiche
Il documento, pubblicato nel luglio 2024, contiene un'introduzione al tema della criptografia, aggiornata alla data della pubblicazione. Il documento si preoccupa di segnalare ai lettori che la rapida evoluzione delle tecniche di attacco e difesa può rendere opportuno un frequente aggiornamento di questo documento.
Il documento passa in rassegna, in termini facilmente comprensibili, i concetti base della criptografia, cominciando dalla criptografia alfabetica dei tempi degli antichi romani, sino alle moderne tecniche di protezione, applicabili a documenti digitalizzati.
Di particolare interesse il capitolo dedicato alle tecniche di attacco, che comportano uso di computer quantistici. Al proposito, i nostri lettori sono stati costantemente informati circa il fatto che i computer quantistici possono rappresentare, allo stesso tempo, sia uno strumento di difesa, sia uno strumento di attacco. Il computer quantistico è uno strumento di difesa, quando può essere utilizzato per mettere a punto algoritmi crittografici difficilmente violabili, mentre diventa uno strumento di attacco, quando le sue potentissime capacità di calcolo vengono utilizzate per tentare di violare un algoritmo criptografico.
(continua)
https://www.puntosicuro.it/sicurezza-informatica-C-90/cybersicurezza-linee-guida-funzioni-criptografiche-AR-24995/
Punto Sicuro - *Adalberto Biasiotti- 15 gennaio 2025*

Qualcuno vuole sabotare i treni italiani? Perché non possiamo escluderlo

Fs denuncia "circostanze altamente sospette" dopo l'ennesimo incidente sulla rete ferroviaria e presenta un esposto alla Digos. Nel mirino guasti e ritardi in orari critici, che potrebbero rientrare in una strategia di sabotaggio. L'ipotesi di attore statuale dietro gli attacchi fisici e informatici

Attacchi fisici, a "bassa tecnologia" ma con mezzi professionali. E attacchi informatici, con le centrali mandate in tilt. Sono le evidenze, piuttosto circostanziate, al centro dell'esposto denuncia presentato dal Gruppo Fs alla luce "dell'ennesimo incidente anomalo sulla rete". È quanto spiegano a *Formiche.net* fonti investigative.

Stamattina, il Gruppo Fs ha annunciato l'esposto denuncia dopo i ritardi di questi giorni, parlando di "circostanze altamente sospette". Gli orari in cui si sono verificati "alcuni problemi (non può essere un caso che si tratti di quelli più complicati per la circolazione ferroviaria, con ricadute pesanti su tutta la rete), il tipo di guasti e la loro frequenza stanno destando più di qualche interrogativo", si legge in una nota della società. L'incartamento è stato trasmesso poi dai denuncianti alla Digos della Questura capitolina che poi invierà nei prossimi giorni una informativa alla Procura di Roma. Questa, dopo aver stabilito la competenza territoriale, lo invierà alle procure competenti che potrebbero essere quelle di Firenze e Arezzo.

Il ministero delle Infrastrutture ha preso "atto con estrema attenzione dell'iniziativa del gruppo Fs che ha deciso di presentare alle autorità un esposto alla luce di troppi episodi sospetti che hanno avuto ricadute sulla circolazione ferroviaria", si legge in una nota. (continua…)

https://formiche.net/2025/01/ferrovie-esposto-denuncia-sabotaggi/#content

***Formiche** - Gabriele Carrer - 15/01/2025*

Adattamento climatico: a Copenhagen il parco urbano contro le bombe d'acqua - Da alcuni anni nella capitale danese, l'Enghaveparken, un'area verde di 35mila metri quadrati, in caso di forti piogge viene utilizzata come vasca di raccolta delle acque piovane dell'intero bacino idrografico del quartiere di Vesterbro. E questo senza perdere i suoi caratteri storici e la sua multifunzionalità. Il progetto è di Tredje Natur.

Il progetto di riqualificazione di Enghaveparken a Copenhagen ha trasformato il parco storico in un bacino di gestione delle acque piovane, integrando soluzioni per affrontare eventi climatici estremi e promuovendo sostenibilità e biodiversità.

Il progetto di Enghaveparken che raccontiamo in queste pagine non è recentissimo. La conclusione dei lavori di riqualificazione e rifunzionalizzazione risale infatti ad alcuni anni orsono, al 2019 per la precisione.

È interessante tornare a parlarne per due ordini di ragioni. Il primo motivo consiste nella sua riqualificazione e nel mantenimento della sua funzione originaria di area verde. Enghaveparken è infatti un parco storico, in un quartiere semi-centrale della capitale danese, capace di offrire verde e ristoro agli abitanti della zona.

La seconda motivazione risiede invece nella possibilità di essere trasformato a contenitore delle acque piovane in eccesso in occasione di eventi estremi, come quello avvenuto pochi anni prima, quando l'alluvione del 2014 colpì Copenhagen e mise sott'acqua molti quartieri della città, a dimostrazione della capacità della capitale di mettere in pratica azioni concrete di adattamento al cambiamento climatico.

Da alcuni anni quindi lo storico parco Enghaveparken, con i suoi 35mila metri quadrati di superficie, è diventato il più grande progetto climatico di Copenaghen. Il bacino idrico che è stato appositamente creato, che vale più di 22mila metri cubi di portata, risponde all'esigenza di gestire, assieme ad altre soluzioni, le future sfide idriche della capitale danese. *(continua…)*

https://www.ingenio-web.it/articoli/adattamento-climatico-a-copenhagen-il-parco-urbano-contro-le-bombe-d-acqua/
Ingenio - *Pietro Mezzi - 16.01.2025*

Gli hacker cinesi stanno ridisegnando il campo di battaglia cyber: ecco come
Recenti incidenti evidenziano la natura trasformativa delle ambizioni di hacking della Cina. Attraverso campagne come Volt Typhoon e Salt Typhoon, Pechino sta dimostrando una capacità di preposizionamento e sabotaggio senza precedenti, mirata a destabilizzare gli Usa in caso di conflitto.
Focus sull'escalation degli hacker cinesi
Gli **hacker cinesi** stanno utilizzando strategie avanzate per **infiltrarsi nelle infrastrutture critiche e nelle telecomunicazioni degli Stati Uniti**, mettendo a rischio la sicurezza nazionale e civile.
Attraverso campagne come **Volt Typhoon** e **Salt Typhoon**, Pechino sta dimostrando una **capacità di preposizionamento e sabotaggio senza precedenti**, mirata a **destabilizzare gli USA in caso di conflitto**.
Questa escalation **evidenzia** le vulnerabilità sistemiche delle reti americane e la necessità di una risposta coordinata tra pubblico e privato.
Indice degli argomenti

La minaccia degli hacker cinesi e le ambizioni di Pechino
Le rivelazioni sulle sofisticate operazioni di hacking della Cina hanno segnato una svolta decisiva nella narrazione della cyber security globale.
Gli eventi svelati durante un incontro riservato alla Casa Bianca nell'autunno del 2023, in cui il consigliere per la sicurezza nazionale del presidente Biden, Jake Sullivan, si è rivolto ai principali dirigenti delle telecomunicazioni e della tecnologia, servono come un forte **promemoria dell'intensificarsi delle minacce nel campo digitale**.
Il messaggio allarmante di Sullivan rivelava che **gli hacker cinesi avevano ottenuto la capacità di compromettere a piacimento infrastrutture critiche statunitensi**, tra cui porti, reti elettriche e altri sistemi vitali, tramite l'infiltrazione simultanea e segreta nelle reti di telecomunicazione.
Questi incidenti evidenziano **la natura trasformativa delle ambizioni di hacking della Cina**.
Storicamente noti per il **furto di segreti aziendali e dati sensibili**, gli hacker cinesi si sono trasformati in una f**orza formidabile in prima linea nei conflitti geopolitici**. I loro obiettivi strategici includono ora **la prevenzione e la neutralizzazione delle capacità di proiezione di potenza** degli Stati Uniti per alterare gli equilibri in un eventuale conflitto. (continua..)
https://www.cybersecurity360.it/nuove-minacce/gli-hacker-cinesi-stanno-ridisegnando-il-campo-dibattaglia-cyber-ecco-come/
Cybersecurity360 - *Tommaso Diddi - 16 gen 2025*

NOTIZIE D'INTERESSE:

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

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*

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.