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 2026 | **n. 9/ 2026** | **ottobre 2026**

Quando si fermano i camion

Per circa dieci giorni, a ottobre, la protesta degli autotrasportatori contro il caro carburante ha bloccato strade, caselli, porti e depositi di carburante in diverse regioni del Sud. Non entriamo nel merito della vertenza, ci interessano le conseguenze sul funzionamento delle infrastrutture.

Gli effetti si sono visti in pochi giorni. In Campania, Sicilia, Puglia, Calabria e Molise i supermercati hanno esaurito prima i prodotti freschi e poi, in alcune zone, anche beni di base. Molti distributori sono rimasti senza carburante e alcuni aeroporti del Sud hanno avuto problemi di approvvigionamento di jet fuel. Ci sono state difficoltà per i collegamenti con le isole minori e allarmi per i trasporti sanitari. Il blocco della raffineria di Taranto, legato a un'altra vertenza, ha aggravato il quadro.

Da questa vicenda emergono quattro elementi utili per chi si occupa di resilienza.

L'anello debole era fuori dal perimetro. Le imprese di autotrasporto merci non rientrano tra i soggetti della direttiva CER né della NIS2. Nel trasporto stradale le norme riguardano le autorità stradali e gli operatori dei sistemi di trasporto intelligenti. Nella filiera alimentare riguardano la distribuzione all'ingrosso e la produzione industriale. Grossisti, industria e raffinerie potevano funzionare, ma senza camion i loro servizi non arrivavano a destinazione. La resilienza dei soggetti critici dipende quindi anche da operatori su cui le norme non impongono obblighi. Le valutazioni del rischio devono tenerne conto esplicitamente.

Pochi nodi bastano. Non è stato necessario fermare tutti i camion. Sono bastati presidi in punti precisi: svincoli autostradali, accessi ai porti, depositi e raffinerie. Questi punti di strozzatura sono noti e vanno mappati con la stessa cura riservata agli asset dei soggetti critici.

I flussi sono ripartiti con strumenti di ordine pubblico. Scorte di polizia ai depositi, precettazione, rimozione dei presidi. Non risulta che abbiano avuto un ruolo i piani di continuità degli operatori. È una cosa da tenere presente mentre i soggetti critici scrivono i loro piani di resilienza.

La fine del blocco non è la fine della crisi**.** Secondo le associazioni del commercio, per tornare alla normalità serve circa una settimana dopo la rimozione dei presidi. I tempi di ripristino vanno valutati con la stessa attenzione dei tempi di tenuta.

I soggetti critici individuati a luglio hanno dieci mesi dalla notifica per adeguarsi agli obblighi CER. Per i soggetti NIS iscritti nel 2025, il 31 ottobre scade il termine per le misure di sicurezza di base. Questa crisi offre un caso concreto su cui verificare le valutazioni del rischio.

Maria Beatrice Versaci
Intelligence Senior Analyst presso Hermes Bay srl.

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

ATTIVITA' DELL'ASSOCIAZIONE

WEBINAR AiNTS _ AIIC

Il mese prossimo **AiNTS** – *Associazione Italiana Non-Technical Skills* e **AIIC** – *Associazione Italiana esperti in Infrastrutture Critiche* vi attendono insieme per un nuovo webinar.
Segnatevi la data: **giovedì 19 novembre dalle ore 18:00 alle ore 19:30**, si parlerà di fattori umani e intelligenza artificiale nelle infrastrutture critiche, di sensibilità ai segnali deboli e molto altro.
Presto maggiori dettagli sui nostri canali, seguiteci per rimanere aggiornati!

WEBINAR AIIC su RETI ELETTRICHE

Stiamo programmando, per il mese di dicembre, un webinar sulle reti elettriche con un docente di prestigio. Vi terremo informati.

GRUPPO DI LAVORO AIIC

Vi ricordiamo che è attivo il Gruppo di Lavoro AIIC su ***"Artificial Intelligence for Critical Infrastructure Resilience in an Underwater Environment"***, coordinato da Sandro Bologna. Possono contribuire alla stesura del rapporto tutti i soci AIIC, semplicemente contattando il coordinatore del GdL s.bologna@infrastrutturecritiche.it

RINNOVO ASSOCIATIVO ANNO 2027

Il 31 dicembre 2026 scadrà 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 2027".
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.

Il Consiglio Direttivo di AIIC ha deciso una facilitazione per chi si iscriverà come nuovo socio: a partire dal mese di ottobre 2026, pagando la relativa quota sociale, il nuovo socio avrà diritto a vedere la propria iscrizione valida fino a tutto l'anno 2027.

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

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.

SITO WEB AIIC – FONTE UFFICIALE DELL'ASSOCIAZIONE

Vi ricordiamo che il sito web www.infrastrutturecritiche.it rappresenta la **fonte ufficiale dell'Associazione Italiana esperti in Infrastrutture Critiche**: è accessibile a tutti, e contiene tutte le informazioni necessarie per un corretto svolgimento della vita associativa. 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.

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

Zero trust per l'IoT: come proteggere una superficie d'attacco sempre più estesa - In Italia sono attivi 175 milioni di oggetti connessi. Sensori, telecamere e apparati industriali ampliano la superficie d'attacco e spesso sfuggono ai controlli tradizionali. Lo zero trust consente di limitarne accessi e comunicazioni, ma richiede inventario, identità affidabili e collaborazione tra IT, cybersecurity e OT. Le best practice
Sensori industriali, telecamere, contatori intelligenti, apparati medicali e sistemi per la gestione degli edifici sono spesso progettati per lavorare per anni, con capacità di elaborazione limitate e procedure

di aggiornamento poco trasparenti. Una combinazione che rende l'Internet of Things uno dei punti più difficili da governare per CIO e CISO. Il modello zero trust permette di ridurre l'esposizione, a condizione di adattarlo ai vincoli operativi dell'IoT e di non considerarlo un prodotto da installare.
In Italia sono attivi 175 milioni di oggetti connessi, circa tre per abitante. Il mercato IoT ha raggiunto nel 2025 un valore di 10,9 miliardi di euro, in crescita del 12% rispetto all'anno precedente. Il 71% delle grandi aziende manifatturiere e il 59% di quelle medie hanno già avviato almeno un progetto Industrial IoT. Utility, auto connesse, smart building e fabbriche concentrano una parte consistente degli investimenti, secondo l'Osservatorio Internet of Things del Politecnico di Milano.
La stessa espansione moltiplica gli oggetti da censire, configurare, aggiornare e sorvegliare. Ogni dispositivo introduce software, credenziali, protocolli e dipendenze da servizi esterni. Compromettere un sensore può alterare un dato, mentre prendere il controllo di un attuatore può incidere sulla produzione, sulla sicurezza di un impianto o sulla continuità di un servizio.
È su questa superficie frammentata che lo zero trust trova una delle applicazioni più concrete. La domanda da porre a ogni connessione cambia: invece di presumere affidabile un dispositivo perché si trova nella rete aziendale, occorre verificarne identità, stato e comportamento, concedendogli soltanto le comunicazioni necessarie alla funzione assegnata.
Indice degli argomenti
Le debolezze ricorrenti della sicurezza IoT
Come lo zero trust riduce il rischio IoT
I limiti dello zero trust negli ambienti IoT
Le migliori pratiche per implementare lo zero trust nell'IoT
1. Partire da inventario e dipendenze
2. Classificare per rischio e impatto
3. Disegnare i flussi consentiti
4. Usare identità forti dove possibile
5. Segmentare per funzione, non soltanto per sede
6. Governare accessi remoti e fornitori
7. Integrare il comportamento nelle decisioni
8. Misurare copertura ed efficacia
Dal rischio tecnico alla responsabilità di filiera
(continua…)
https://www.zerounoweb.it/iot/zero-trust-per-liot-come-proteggere-una-superficie-dattacco-sempre-piu-estesa/
ZeroUno Web - *Gianluca Ferrari, 27 ago 2026*

Cyber Resilience Act, al via gli obblighi di notifica dell'articolo 14 - Dall'11 settembre i fabbricanti dovranno segnalare entro 24 ore vulnerabilità attivamente sfruttate e incidenti gravi. Il Cyber Resilience Act impone nuovi processi, responsabilità lungo la catena di fornitura e sanzioni fino a 15 milioni di euro
L'11 settembre 2026 è una data chiave per l'applicazione del Cyber Resilience Act, il Regolamento (UE) 2024/2847 in vigore dal 2024. L'articolo 14 rende subito operativi i primi, severi obblighi di segnalazione: da questa data i fabbricanti di prodotti con elementi digitali dovranno segnalare le vulnerabilità attivamente sfruttate e gli incidenti gravi con impatto sulla sicurezza del prodotto, secondo tempistiche stringenti.
Il regolamento è entrato in vigore il 10 dicembre 2024 e avrà piena applicazione dall'11 dicembre 2027, ma alcune disposizioni sono state anticipate. L'11 giugno 2026 è entrato in applicazione il capo relativo

alla notifica degli organismi di valutazione della conformità; dall'11 settembre scattano invece gli obblighi di comunicazione dell'articolo 14. Quando una vulnerabilità viene sfruttata in un prodotto distribuito su larga scala, la rapidità con cui l'informazione circola può diventare parte della risposta all'incidente.

Indice degli argomenti

Obblighi di segnalazione Cyber Resilience Act: cosa prevede l'articolo 14
Single Reporting Platform ENISA e notifiche ai CSIRT
Prodotti digitali, componenti e catena di fornitura
Sanzioni CRA e rischi operativi per le imprese
Linee guida e piena applicazione del Cyber Resilience Act

Obblighi di segnalazione Cyber Resilience Act: cosa prevede l'articolo 14

Il CRA non impone di segnalare ogni vulnerabilità scoperta nel codice. L'articolo 14 riguarda le vulnerabilità attivamente sfruttate contenute nel prodotto con elementi digitali e gli incidenti gravi che hanno un impatto sulla sicurezza del prodotto. Una falla individuata durante un test o un'attività di ricerca, senza elementi che mostrino un suo sfruttamento effettivo, non determina quindi automaticamente una notifica. Se emergono invece evidenze che la vulnerabilità è stata utilizzata da un attore malevolo, il fabbricante deve attivare la procedura senza indebito ritardo e comunque entro i termini stabiliti. (continua)

https://www.agendadigitale.eu/sicurezza/cyber-resilience-act-al-via-gli-obblighi-di-notifica-dellarticolo-14/

Agenda Digitale - *Tommaso Diddi, Luisa Franchina - 10 set 2026*

AI e infrastrutture: il vero salto non è nel calcolo, ma in una memoria tecnica interrogabile - *L'AI nelle infrastrutture può diventare una memoria tecnica interrogabile capace di collegare progetti, ispezioni, monitoraggi e decisioni. Per ponti, viadotti e gallerie il valore non è sostituire l'ingegnere, ma ricostruire informazioni disperse, segnalare incoerenze e supportare la gestione del rischio.*

L'intelligenza artificiale applicata alle infrastrutture è uno strato cognitivo che legge e collega capitolati, relazioni, modelli di calcolo, schede di ispezione e dati di monitoraggio lungo il ciclo di vita dell'opera. Risolve la frammentazione informativa: segnala parametri discordanti fra revisioni e ricostruisce la storia di ponti e gallerie con archivi lacunosi. Si applica a progettazione, classificazione del rischio (D.M. 204/2022) e manutenzione, con un'adozione in quattro livelli. INGENIO pubblica l'analisi di Marano e Chiaia (Politecnico di Torino), con limiti attuali e obblighi di AI Act e legge 132/2025.

L'intelligenza artificiale può trasformare la filiera delle infrastrutture perché opera in modo trasversale rispetto alle singole applicazioni: progettazione, analisi dei rischi, diagnostica, consolidamento, manutenzione e adempimenti normativi.

Può leggere e mettere in relazione capitolati, relazioni, elaborati grafici, modelli di calcolo, schede di ispezione, dati di monitoraggio e corrispondenza, mantenendo la continuità informativa lungo l'intero ciclo di vita dell'opera.

Il valore principale non risiede nell'automazione di un singolo calcolo, ma nella capacità di costruire una memoria tecnica interrogabile, riconoscere incongruenze e anticipare criticità: un'esigenza particolarmente acuta per ponti, viadotti e gallerie esistenti, la cui storia documentale è spesso lacunosa.

Per ottenere questo risultato servono un'introduzione progressiva, dati organizzati, tracciabilità, consapevolezza dei limiti attuali della tecnologia e una responsabilità professionale chiaramente affidata all'uomo, come oggi richiede anche la legge.

(continua)
https://www.ingenio-web.it/articoli/intelligenza-artificiale-ponti-viadotti-gallerie-memoria-tecnica/
Ingenio *- Bernardino Chiaia | Giuseppe Carlo Marano, 22 settembre 2026*

RED IV, quanto sarà ambiziosa la nuova direttiva per le rinnovabili? - Il documento di lavoro trapelato da Bruxelles insiste su uno scenario centrale che stima una capacità rinnovabile che copra il 65–70% dei consumi. Per l'idrogeno rinnovabile viene indicato un target di consumo indicativo a livello UE pari a 8 Mt.
RED IV, quanto sarà ambiziosa la nuova direttiva per le rinnovabili?
Indice dei contenuti
Verso la nuova Direttiva Rinnovabili 2040 (RED IV)
La spinta degli Stati membri verso una maggiore flessibilità energetica
Gli scenari di sviluppo per le fonti rinnovabili al 2040
La revisione degli obiettivi per idrogeno e biocarburanti
Verso la nuova Direttiva Rinnovabili 2040 (RED IV)
Con la tenuta del Green Deal sempre più incerta, immaginare il percorso di decarbonizzazione europeo post 2030 appare arduo. Tuttavia le norme comunitarie che disciplinano la strategia energetica del Blocco sono agli sgoccioli e la Commissione si trova oggi fra le mani il delicato compito di definire i target UE per il 2040. Obiettivi che confluiranno nella prossima Direttiva sulle energie rinnovabili RED IV da pubblicare entro la fine del 2026.
Il provvedimento avrà il compito di allineare l'ambizione energetica agli obiettivi riduzione delle emissioni di CO2 entro la stessa data (-90% rispetto al 1990), ma con qualche sfida in più rispetto al passato.
La spinta degli Stati membri verso una maggiore flessibilità energetica
Perché qualche sfida in più? Perché 15 Stati membri tra cui l'Italia e i Paesi dell'Alleanza Nucleare capitanati dalla Francia, stanno da tempo facendo pressioni per allentare l'ambizione che ha caratterizzato le diverse revisioni e modifiche dell'originale Direttiva sulle energie rinnovabili del 2009. La richiesta primaria del gruppo? "Un quadro energetico flessibile [...] che promuova l'uso di tutte le fonti energetiche a basse emissioni di carbonio" che, tradotto in termini spiccioli, significa una sola cosa: ogni Paese dovrebbe decidere in maniera autonoma, senza vincoli e senza una miriade di sotto – obiettivi settoriali.
(continua)
https://www.rinnovabili.it/energia/eolico/red-iv-ambiziosa-direttiva-rinnovabili/
Rinnovabili - *Stefania Del Bianco, 22 Settembre 2026*

Attacchi russi coi droni, perché il Mediterraneo è considerato a rischio - Un rapporto attribuito alla CIA e riportato da El Mundo segnala possibili attacchi russi con droni nel Mediterraneo contro Italia, Francia e Spagna. Il governo italiano smentisce l'allarme, mentre Bruxelles e diversi analisti richiamano l'attenzione sulla minaccia ibrida
Il Mediterraneo sarebbe il prossimo obiettivo della Russia. È quanto dichiarato da un rapporto della CIA riportato dalla testata spagnola El Mundo, secondo cui i Paesi dell'Europa del Sud, in particolare Francia, Spagna e Italia, sarebbero a rischio attacco russo.
L'attacco di cui la CIA ci sta mettendo in guardia, sfrutterebbe un particolare tipo di drone, il Gerbera, lanciato da container trasportati su navi mercantili sotto la veste di traffico commerciale ordinario.
Indice degli argomenti

Il drone Gerbera e il possibile uso dal mare
Le reazioni dei vertici europei
La distanza geografica non implica maggiore sicurezza
I precedenti dei droni russi in Europa

Il drone Gerbera e il possibile uso dal mare

Si tratta di un drone russo economico e piccolo di dimensioni, due metri di lunghezza, 18 chili di peso, ma con grande autonomia, circa 600 chilometri che riesce a percorrere a quasi 160 km/h e che trasporta dai quattro ai cinque chili di esplosivo.

La scelta di questo tipo di strumento risiederebbe nella volontà di effettuare un attacco più simbolico che di distruzione di massa, come la chiusura temporanea di un porto o di un aeroporto, un incendio, il danneggiamento di strutture esposte, con il solo obiettivo di dimostrare al mondo che la Russia può avere accesso a qualsiasi passaggio terrestre.

Inoltre, strumenti così piccoli permettono a una nave mercantile di trasportarne diversi e catapultarli con molta meno difficoltà rispetto a droni notevolmente più grandi. Da una distanza di 200 o 300 chilometri dalla costa, il volo durerebbe approssimativamente tra un'ora e un quarto e due ore, a seconda della velocità effettiva.. (continua…)

https://www.agendadigitale.eu/sicurezza/attacchi-russi-coi-droni-perche-il-mediterraneo-e-considerato-a-rischio/

Agenda Digitale *- Marco Santarelli - 24 set 2026*

Rinnovabili contro il caro-gas: l'analisi EEA su prezzi e stabilità - Il report EEA evidenzia come l'elettricità verde sia il miglior scudo economico contro le oscillazioni del gas: i dati sui risparmi in Europa, le stime al 2030 e le azioni necessarie su reti, stoccaggi ed elettrificazione.

L'Agenzia Europea dell'Ambiente (EEA) ha pubblicato un briefing strategico che analizza il ruolo dell'elettricità da fonti rinnovabili (FER) nel proteggere l'economia europea dalle continue oscillazioni dei prezzi del gas naturale: " Renewable electricity: best buffer against gas price volatility".

Il documento dimostra con dati quantitativi come la transizione energetica non sia soltanto una priorità climatica ed ecologica, ma rappresenti una fondamentale garanzia di stabilità finanziaria, competitività industriale e sovranità strategica per l'Unione Europea.

1. Il contesto: la persistente vulnerabilità fossile dell'Europa

L'analisi dell'EEA prende le mosse dall'elevata dipendenza dell'Unione Europea dalle importazioni di combustibili fossili dall'estero: la UE importa infatti circa l'85% del gas naturale e oltre il 97% dei prodotti petroliferi consumati al suo interno.

Questa marcata dipendenza espone costantemente il mercato interno a shock esterni, tensioni geopolitiche e strozzature nelle catene di approvvigionamento globale. L'instabilità dei mercati internazionali del gas si traduce immediatamente in un impatto sui prezzi all'ingrosso dell'energia elettrica, a causa del meccanismo del prezzo marginale (marginal pricing) che regola il mercato elettrico europeo. (continua…)

https://www.puntosicuro.it/sostenibilita-C-149/rinnovabili-contro-il-caro-gas-l-analisi-eea-su-prezzi-ed-stabilita-AR-26757/

Punto Sicuro *– Redazione, 29/09/2026*

I giovedì di TopForGrowth - L'Associazione TOPForGrowth annuncia un nuovo ciclo degli incontri *"I giovedì di TOPForGrowth"*, dedicato a un tema di grande attualità e crescente importanza per imprese, professionisti, istituzioni e cittadini: *REGOLE E RESPONSABILITÀ: L'AI IN PRATICA - Gestire i rischi, tutelare le persone, abilitare l'innovazione.*

L'intelligenza artificiale sta entrando rapidamente nei processi delle organizzazioni e nella vita quotidiana. Non ci chiediamo più soltanto che cosa possa fare l'AI, ma anche quali regole dobbiamo rispettare, quali responsabilità dobbiamo assumerci e come adottare queste tecnologie in modo consapevole, sicuro e sostenibile.
Gli incontri sono aperti anche a chi non fa parte dell'associazione.
Per informazioni: info@topforgrowth.it
Qui di seguito il calendario degli incontri.
Dal 22 ottobre al 17 dicembre 2026 – Ogni giovedì alle ore 18:00, online.
Il collegamento è: https://meet.google.com/asi-zzha-ppr

22 ottobre – AI Act, Omnibus e Legge 132: ruoli, classificazione e obblighi
Cristina Turconi
Il quadro normativo europeo e italiano, i ruoli di fornitori e utilizzatori, i livelli di rischio e i principali obblighi.

29 ottobre – Quali regole si applicano alla mia organizzazione?
Alberto Caruso de Carolis
Come orientarsi tra AI Act, GDPR, NIS2 e altri obblighi, individuando il perimetro normativo rilevante per la propria organizzazione.

5 novembre – Digitalizzazione dei processi e AI: verso la semplificazione degli adempimenti
Luca Tufarelli, con Maria Lilia La Porta
Come digitalizzazione e AI possono contribuire a rendere più semplici, coerenti ed efficienti i processi di gestione degli adempimenti.

12 novembre – AI Risk Management in un'azienda consolidata: il caso Technis Blu
Massimo Lacidogna, con Vittorio Della Rossa
Una testimonianza concreta su governance, gestione dei rischi, sistemi aziendali, controlli e responsabilità nell'introduzione dell'AI.

19 novembre – AI Risk Management in una startup
Matteo Bertezzolo
Come affrontare rischi, responsabilità e requisiti normativi fin dalle prime fasi di sviluppo di un prodotto o servizio basato sull'AI.

26 novembre – AI nella scuola: opportunità, responsabilità e rischi
Manuela Bianchi
L'impatto dell'AI sull'apprendimento, sul ruolo degli insegnanti, sulla valutazione e sulla tutela degli studenti.

3 dicembre – Dati, privacy e AI
Stefania Discepoli,
Protezione dei dati personali, riservatezza, condivisione delle informazioni e responsabilità nell'utilizzo dei sistemi AI.

10 dicembre – Cybersecurity e resilienza digitale
Pierfrancesco Poce, con Gianluca Borghesan
Le implicazioni dell'AI per la sicurezza informatica, la resilienza delle organizzazioni e il rapporto con normative quali NIS2 e DORA.

17 dicembre – Tavola rotonda: dalla normativa al piano d'azione
Moderatore: Carlo Mario Poli, con il contributo dei relatori del ciclo
Un confronto conclusivo per collegare i temi affrontati e identificare priorità, responsabilità e possibili percorsi operativi.

EU Grocers Pay a Steep Price for Unpatched Fridge Firmware

Hundreds of stores lost millions of euros because they hired third parties to manage the outdated OT firmware running their cooling systems.

Hundreds of French grocers lost tens, if not hundreds of millions of euros this week from cyberattacks that manipulated their refrigeration systems.

Overnight on Monday, hackers broke into commercial refrigeration system controllers at major French grocery chains. They converted refrigerators, freezers, and cold storage rooms into heating units, raising their temperatures up to 50 degrees Celsius (over 120 degrees Fahrenheit), completely spoiling all of the food they contained, and reportedly even causing some small fires. The threat actor's identity and motives are unclear.

Refrigeration controllers allow grocers to set and monitor their fridge temperatures remotely, 24/7. It follows, then, that store owners could've been alerted to, or manually discovered, the fact that something was amiss. To prevent that from happening, French sources report that the attackers extended their targeted systems' defrost cycles — where freezers intentionally melt accumulated frost and ice — so that the heating looked like routine maintenance.

According to the companies' own reports, the attacks impacted somewhere north of 700 grocery and retail stores, all on the same night. An analyst for French cybersecurity company Sekoia told Reuters that Spain, Portugal, Poland, Germany, and Belgium had also been affected, and a major supermarket chain in the Netherlands shut its systems down as a precaution, according to the AP. Just one French chain, Intermarché, reported tens of millions of euros in losses.

Worst of all, experts point out that the attacks were almost certainly avoidable with standard cyber hygiene.

What Caused Freezers to Burn?

Initial reports suggested that Monday's attacks traced back to refrigeration controllers from Danish manufacturer Danfoss. Danfoss has a large footprint in supermarket and food retail control solutions, with more than 50,000 installations of its technology worldwide, according to its website.

On Aug. 9, cybersecurity researchers from Claroty's Team82 disclosed three vulnerabilities in Danfoss' AK-SM 800A platform. The issues — assigned CVE-2025-41450, CVE-2025-41451, and CVE-2025-41452 — allowed attackers to perform remote code execution (RCE) or denial-of-service (DoS) against enterprise refrigeration fleets. Danfoss patched the vulnerabilities but counted on customers to update their systems themselves.

In a statement to Reuters, Danfoss pinned the blame on customers running outdated firmware, writing that it "long advised customers to keep supported systems updated with the latest firmware and to migrate legacy systems to current-generation solutions." (continua…)

https://www.darkreading.com/ics-ot-security/eu-grocers-unpatched-fridge-firmware

DarkReading - *Nate Nelson, - October 15, 2026*

AI Takes Control of Robotic Arm in 16 Minutes Flat

Most OT devices at utilities, factories, and elsewhere have been deployed for a decade or more, but operators need to get agile and deploy new cyber defenses.

Frontier AI models targeting operational technology (OT) environments, from utilities to factories and beyond, could compromise the network and take control of devices in minutes, according to a fresh round of in-the-lab testing.

Conducted by Booz Allen, the government and military contractor, the tests found that in a typical OT environment, commercial AI models could identify misconfigured devices and work their way through multiple layers of networks to take physical action, the company stated in an October report. In one

case, the model was able to take control of and move a robotic arm in an attack that lasted only 16 minutes.

The researchers were not surprised that the AI models succeeded, but how quickly they could find a pathway into the operational side of the network was the top-line finding, says Kyle Miller, vice president of infrastructure cybersecurity at Booz Allen.

"I've been doing OT security my whole career, and whether we like it or not, we live a little bit by security through obscurity — we believe that an attacker needs to [be sophisticated] to get into an OT environment and understand it well enough to be able to manipulate things and cause a kinetic outcome," he tells Dark Reading. "This frontier model testing shows that AI knocks down a lot of those barriers."

While cyberattackers and nation-state operatives are quick to experiment with AI — with near-autonomous AI attacks becoming more common — AI-assisted attacks on OT networks are relatively rare. In early 2026, a small hacking group gained access to at least nine Mexican agencies assisted by AI, yet they failed to gain access to the OT network of a local water and drainage utility.

The adversary combined two commercial models that had little to no OT-specific knowledge, but which quickly highlighted the system as a high-value target and researched methods of gaining access, says Jay Deen, associate principal adversary hunter at OT cybersecurity firm Dragos, which reported the incident.

"What stood out ... was not that AI introduced new or particularly sophisticated techniques, but that it significantly reduced the expertise and time needed to carry out a large-scale intrusion," he says, adding that "the AI got close enough to identify and actively develop a path toward the OT environment, but there is no evidence the adversary actually crossed into the control network."

A Decades-Long Life Cycle, Minutes to Compromise

In Booz Allen's testing, the AI models managed to get further, and successfully achieved all of its eight test objectives, from mapping the environment to finding security vulnerabilities to compromising a SCADA system, according to the firm's report. While the effort was fast, if the model did not require human-in-the-loop approval, it likely would have taken half the time, says Booz Allen's Miller.

"That 16-minute time window was the time it took for the models to get from the perimeter firewall through the IT network, into the OT network, and cause a kinetic outcome — so actually energize an output on one of the controllers in the OT environment," he says.

In the initial runs, Booz Allen left in some unpatched vulnerabilities, so the attack time did not include the time to research and develop exploits for zero-day vulnerabilities, he says. (continua…)

https://www.darkreading.com/ics-ot-security/ai-takes-control-robotic-arm-16-minutes

DarkReading - *Robert Lemos, -October 16, 2026*

EY Cyber Barometer

Sicurezza cyber, la filiera resta il punto debole delle imprese

L'EY Cyber Barometer 2025 misura la maturità cyber delle imprese italiane e individua nella supply chain il fronte più fragile. Controlli di base diffusi, divari tra settori e verifiche ancora deboli mostrano perché continuità operativa, fornitori e capacità di ripristino devono entrare nelle decisioni aziendali

Pensiamo a cosa succede quando un fornitore si ferma o quando il ripristino deve rispettare i tempi promessi ai clienti: è lì che si misura davvero la **sicurezza di un'impresa**. Ed è proprio su questo terreno che l'EY Cyber Barometer 2025 porta il suo contributo al dibattito italiano, collegando la **maturità dei controlli alla continuità dei servizi**. Questa seconda edizione analizza oltre 300 società italiane sottoposte a financial audit, contro le oltre 100 del biennio precedente.

Indice degli argomenti

- EY Cyber Barometer 2025 e maturità cyber delle imprese italiane
- Come si misurano i livelli di maturità cyber aziendale
- La filiera frena la maturità cyber delle imprese italiane
  - Il disallineamento tra criticità e maturità
  - La filiera come rischio operativo
- Settori e dimensioni dividono la cybersicurezza delle aziende italiane
  - Il divario tra piccole, medie e grandi imprese
- Investimenti e incidenti nel quadro cyber delle imprese italiane
  - Gli eventi cyber e il rischio di propagazione
- Dalle evidenze alla resilienza cyber delle filiere italiane
  - Le evidenze necessarie al management
  - La resilienza della filiera come leva competitiva

EY Cyber Barometer 2025 e maturità cyber delle imprese italiane

L'analisi si articola in **otto domini**, costruiti in coerenza con la direttiva NIS 2: rischio, incidenti, continuità operativa, reti, cifratura, persone e asset, verifica dell'efficacia e fornitori. Ciascun dominio viene valutato su una **scala da zero a cinque**, che considera quanto i presidi sono formalizzati e attuati, quali evidenze operative esistono e se i risultati vengono misurati.

Nell'aggregare i punteggi si tiene conto anche del profilo di rischio dei singoli settori. È importante chiarirlo subito: il Barometer non è una certificazione di conformità, ma un **benchmark pensato per aiutare le aziende a orientare le proprie decisioni**.

Come si misurano i livelli di maturità cyber aziendale

Che cosa ci dicono i numeri? Il modello di valutazione adotta una **scala di maturità da 0 a 5**, articolata in cinque livelli progressivi. A ciascun intervallo di score corrisponde un diverso grado di maturità, da Initial (0–1), caratterizzato da presidi limitati, non strutturati e prevalentemente ad hoc, fino a Optimized (4–5), che identifica un modello pienamente strutturato, con processi uniformi e integrati, una governance efficace e un monitoraggio continuo.

I livelli intermedi, **Managed (1–2), Defined (2–3) e Quantitatively Managed (3–4)**, rappresentano una progressiva evoluzione delle capacità, delle tecnologie, della formalizzazione dei processi e dei meccanismi di governance. All'aumentare dello score aumenta quindi il livello di strutturazione, diffusione e consolidamento dei presidi all'interno dell'organizzazione.

La filiera frena la maturità cyber delle imprese italiane

Le **medie degli otto domini oscillano tra 2,39 e 3,02 su cinque**. Il risultato migliore riguarda la gestione delle persone, controllo degli accessi e asset, con 3,02; seguono reti e sistemi a 2,75 e gestione degli incidenti a 2,62. Una buona notizia: i controlli di base sono ormai diffusi nel campione.

Il quadro cambia però quando guardiamo alla **sicurezza della catena di approvvigionamento**, che scende a 2,39. Le procedure per verificare l'efficacia delle misure si fermano a 2,48, mentre continuità operativa e gestione delle crisi arrivano a 2,54. Il messaggio è chiaro: **avere una policy non basta a garantire che funzioni nel momento della crisi**.

Il disallineamento tra criticità e maturità

I numeri diventano ancora più utili se li leggiamo in base alla criticità. Nella fascia di massima priorità, il **Tier 1**, il rapporto colloca analisi del rischio, incidenti, continuità operativa e sicurezza della filiera, e proprio quest'ultima registra il punteggio più basso.

Il report parla di **«disallineamento sistemico tra criticità e livelli di maturità»**: in altre parole, gli ambiti da cui dipende la tenuta del servizio non ottengono, nel complesso, punteggi più alti degli altri. Per decidere da dove partire, quindi, non basta misurare il divario nei controlli: occorre chiedersi anche quale impatto potrebbe avere sul business.

La filiera come rischio operativo

Facciamo un esempio. Una azienda manufatturiera può proteggere bene la propria rete e restare comunque esposto al **software di un terzo o a una piattaforma logistica condivisa**.
Per questo il Barometer richiama l'importanza di **valutare i fornitori**, definire clausole contrattuali adeguate, monitorarli, avviare azioni correttive e conoscere anche i **subfornitori**. È un lavoro di squadra, che chiama in causa sicurezza, acquisti, funzione legale e operations. L'**articolo 21 della NIS 2** include sia la sicurezza della catena di approvvigionamento sia la verifica dell'efficacia dei controlli, e la ricerca ci mostra quanto impegno organizzativo richieda tradurre questi principi nella pratica.
Settori e dimensioni dividono la cybersicurezza delle aziende italiane
Anche tra i settori il panorama è tutt'altro che uniforme. Nella vista aggregata, la **gestione dei servizi TIC per altre imprese raggiunge 3,34** e i fornitori di servizi digitali 3,28. In fondo alla graduatoria del campione troviamo invece la gestione dei rifiuti, con 1,80, e la fabbricazione di beni intermedi, con 1,70. Le ragioni si possono intuire: per chi opera nel digitale, garantire la disponibilità del servizio e rispondere alle verifiche dei clienti fa parte del lavoro di ogni giorno, mentre nell'industria entrano in gioco anche impianti, tecnologie operative e **filiere più stratificate**. Il rapporto propone queste chiavi di lettura, senza attribuire i punteggi a un'unica causa. (continua…)
https://www.agendadigitale.eu/sicurezza/sicurezza-cyber-la-filiera-resta-il-punto-debole-delle-imprese/
AgendaDigitale *-Davide Benevolo- 22 ott 2026*

Mille siti Web da proteggere in poche ore: dentro la crisi di PHP
Due vulnerabilità critiche di PHP hanno costretto organizzazioni e università a sospendere servizi, aggiornare migliaia di siti e gestire sistemi legacy senza patch. L'esperienza dell'Università di Pisa mostra come AI, esecuzione di codice remoto e carenza di risorse stiano trasformando le crisi di sicurezza in una nuova normalità
Dopo soli sei mesi di allarmismo e di commenti sul potenziale impatto dell'AI sulla sicurezza globale dei sistemi digitali è arrivata la prima crisi globale dovuta all'impiego dell'AI in termini di sicurezza, e come tutti ormai sappiamo **due vulnerabilità di PHP** hanno impattato quello che si stima essere il 70% circa del Web.
La maggior parte delle organizzazioni a livello globale hanno reagito all'annuncio sospendendo i propri servizi Web e provvedendo all'aggiornamento, ma siamo pronti a fronteggiare questo nuovo tipo di crisi? Non credo di avere ricette magiche, ma posso sicuramente raccontare **la mia personale esperienza nella gestione della crisi presso l'Università di Pisa**.
Indice degli argomenti

- Vulnerabilità PHP e il tam tam della crisi globale
  - Il rischio dell'esecuzione di codice remoto
  - Procedure interne e comunicazione sugli hack generati dall'AI
- CMS e sistemi legacy davanti alle falle di PHP
  - Versioni obsolete e patch non disponibili
  - La risposta operativa dell'Università di Pisa
- Le lezioni delle vulnerabilità PHP per la sicurezza IT
  - Sistemi legacy e siti storici da spegnere
- Nuove falle in PHP: perché è solo l'inizio

Vulnerabilità PHP e il tam tam della crisi globale
Come tutte le organizzazioni e soprattutto quelle che sono impegnate nella piena **attuazione della direttiva NIS 2** in qualità di soggetto importante, il personale tecnico dell'Università monitora costantemente i vari siti con aggiornamenti di varia natura, partendo ovviamente da una valutazione supportata dall'AI dell'impatto sui nostri sistemi di ciascuna CVE rilasciata.

Le CVE sono però sempre più numerose e quando un'organizzazione gestisce migliaia di apparati e decine se non centinaia di tecnologie differenti si trova rapidamente nel quadrante in cui deve valutare **elevati numeri di vulnerabilità e i relativi impatti** per decidere una priorità nell'aggiornamento dei sistemi.

Ma quando un software alla base di molti servizi Web come PHP annuncia **una vulnerabilità critica che consente l'esecuzione di codice remoto** in server Web senza neanche essere autenticati allora la notizia non arriva da una CVE, ti telefonano in tanti dicendo "bisogna aggiornare".

Improvvisamente la tua giornata cambia corso e cominci a seguire le normali procedure in una situazione di crisi: fai l'assessment della superficie di potenziale impatto, decidi se il rischio è tale da giustificare **il fermo di più di mille siti Web** della tua organizzazione, e soprattutto valuti le potenziali remediation.

Il rischio dell'esecuzione di codice remoto

Ho vissuto numerose situazioni di crisi negli ultimi anni, ma questa era la mia seconda crisi globale (la precedente era stata nel febbraio 2022 con la vulnerabilità di log4j) e soprattutto **il rischio di esecuzione di codice remoto via Web** è tra le peggiori notizie che si possano ricevere perché il Web è largamente aperto a Internet offrendo un vettore di attacco enorme.

Procedure interne e comunicazione sugli hack generati dall'AI

La gestione della crisi è stata anche un'occasione per rivedere le **procedure interne in materia di cybersecurity**, sia dal punto di vista decisionale che poi nella comunicazione con l'utenza. Dopo pochi minuti è stato più che evidente che era opportuno non prendere rischi soprattutto per la confusione che imperava sulla disponibilità di **hack generati da AI** e che sembrava avrebbero compromesso il Web nell'arco di poche ore (spoiler: successivamente si è scoperto che la maggior parte di questi hack semplicemente non funzionavano e le due vulnerabilità erano molto più difficili da sfruttare da quanto la comunicazione globale lasciasse intendere).

Le notizie sul sito di PHP non erano particolarmente rassicuranti e anche i sommari delle vulnerabilità rendevano difficile comprendere se fossero direttamente utilizzabili e in che condizioni. Non sorprende quindi che tutti abbiano considerato l'opzione di spegnere ed aggiornare anche se **la PHP Foundation** informava che le versioni di PHP 8.1 e precedenti non avrebbero ricevuto aggiornamenti dalla fondazione.

CMS e sistemi legacy davanti alle falle di PHP

La valutazione di impatto è un'attività che deve essere svolta tempestivamente in una situazione di crisi, e quando l'impatto non è direttamente collegato ad un sistema in uso ma bensì al runtime su cui questo si basa è un'attività difficile da condurre.

Non stupisce quindi che la reazione globale sia stata **spegnere e aggiornare** per non prendersi rischi inutili.

In effetti come si giudica se **un CMS popolare come Wordpress** (o uno dei suoi plugin) sia effettivamente esposto ad una vulnerabilità di PHP? La semplice valutazione avrebbe richiesto ore o giorni che nessuno si poteva permettere. È il prezzo da pagare per l'uso di framework che un tempo si comprendevano ma oggi sono divenuti troppo complessi da conoscere per effettuare valutazioni specifiche. (continua…)

https://www.agendadigitale.eu/sicurezza/mille-siti-web-da-proteggere-in-poche-ore-dentro-la-crisi-di-php/

AgendaDigitale - *Antonio Cisternino - 26 ott 2026*

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	Silvano Bari Glauco Bertocchi Maria Beatrice Versaci *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.