

Cyberattacchi, agenzia Ue: â??Potrebbero colpire anche elettrodomestici e routerâ?•

Descrizione

default watermark

(Adnkronos) â?? Dopo i recenti attacchi cyber ai frigoriferi industriali dei supermercati, i dispositivi domestici potrebbero essere i prossimi obiettivi. Questo lâ??allarme, lanciato oggi, martedÃ¬ 10 novembre, allâ??Afp dal Juhan Lepassaar, direttore esecutivo dellâ??agenzia di cybersicurezza dellâ??Ue, Enisa, secondo cui lâ??Unione dovrebbe investire di piÃ¹ per contrastare le minacce informatiche crescenti.

Lepassaar non ha voluto commentare direttamente lâ??attribuzione della Francia, secondo cui dietro allâ??ondata di attacchi contro i frigoriferi di ottobre ci sarebbe lâ??Iran, ma ha affermato che â??attori allineati allo Statoâ?• cinesi, iraniani, nordcoreani e russi sono noti per prendere di mira lâ??Europa. â??La sicurezza non dovrebbe e non puÃ² essere un ripensamento. Oggi sono stati i frigoriferi, domani potrebbero essere i router, dopodomani potrebbero essere gli elettrodomestici e cosÃ¬ viaâ?•, ha detto nel corso di unâ??intervista a Bruxelles.

La valutazione delle minacce a livello comunitario conferma che il livello di rischio cyber per lâ??Ue rimane elevato. Nonostante la preparazione nella cybersicurezza dellâ??Unione sia migliorata, lâ??intero ecosistema attraversa una fase di profonda mutazione. Eâ?? quanto si legge nellâ??EU Cybersecurity Index sviluppato dallâ??Enisa, lâ??Agenzia Ue per la cybersecurity.

Lâ??Enisa ha valutato il grado di maturitÃ delle capacitÃ e delle risorse di cybersicurezza negli Stati membri. Il punteggio medio complessivo dellâ??Indice Ue per il 2026 si attesta a 71,53 punti su una scala da 0 a 100. La maggior parte degli Stati membri ha raggiunto un livello di postura maturo o superiore, procedendo in linea con lâ??obiettivo di garantire uno standard elevato e condiviso di cybersicurezza in tutta lâ??Unione. Intanto perÃ² lâ??ecosistema che quegli stessi Paesi deve affrontare sta cambiando, potenziato dallâ??Ai. Le attivitÃ di intrusione si sono mantenute intense e diversificate nel 2025 e nel 2026, a fronte di uno scenario di minaccia sempre piÃ¹ complesso, dice il report.

Lâ??ideologia si conferma il principale motore degli incidenti cyber, le tensioni geopolitiche continuano a plasmare le operazioni ostili, le attivitÃ a scopo di lucro mantengono un impatto rilevante e gli

hacktivist continuano a dominare i volumi complessivi degli attacchi. Parallelamente, lâ??Ai agisce da moltiplicatore delle capacitÃ sia offensive sia difensive, mentre lâ??evoluzione dei modelli di Ai sta accelerando lâ??individuazione e lo sfruttamento delle vulnerabilitÃ , si legge nel report dellâ??Enisa.

Lâ??executive director dellâ??Enisa, Juhan Lepassaar, ha dichiarato che â??le sfide persistono e i recenti sviluppi â?? non solo nei modelli di Ai di frontiera, ma anche negli incidenti informatici che hanno colpito i sistemi di refrigerazione in tutta lâ??Ue â?? evidenziano lacune operative e la necessitÃ di un coordinamento e di una condivisione tempestiva delle informazioni. Ã? fondamentale consolidare una consapevolezza situazionale comune e accrescere lâ??allineamento delle policy nei settori critici. Sono stati compiuti progressi, ma ora dobbiamo partire da queste basi per aggiornare le nostre strategie e affrontare uno scenario di cybersicurezza sempre piÃ¹ complessoâ?•.

La maggioranza degli Stati membri ha raggiunto un livello di postura maturo o avanzato nellâ??attuazione delle policy a livello nazionale (66,72 punti), si legge nel report. Quasi tutti gli Stati membri dichiarano di aver conseguito un livello avanzato nella gestione delle supply chain dei propri soggetti essenziali e importanti (89,91 punti), mentre la maturitÃ dei Computer security incident response team (Csirt) risulta consolidata (54,76 punti), sebbene permangano disomogeneitÃ tra gli Stati membri. Lâ??integrazione della cybersicurezza nei percorsi di istruzione, in particolare a livello primario e secondario, presenta ulteriori margini di miglioramento (73,59 punti nellâ??istruzione superiore, 55,44 punti nellâ??istruzione primaria e secondaria). Gli ecosistemi di certificazione nazionali appaiono divisi tra contesti maturi e meno maturi, con gli Stati membri distribuiti agli estremi della scala di valutazione (55,56 punti). La maggior parte degli Stati membri ha raggiunto una postura avanzata sul fronte delle prioritÃ e delle iniziative di Ricerca e sviluppo (R&s) in ambito cybersecurity (79,24 punti), evidenziando una crescente coerenza nel panorama della Ricerca e innovazione.

default watermark

Il Rapporto traccia cinque direttrici chiave per il futuro dellâ??Unione, sulla base delle quali sono state elaborate le raccomandazioni di policy: concentrarsi sullâ??armonizzazione degli aspetti transfrontalieri e inter-normativi, affinchÃ© i soggetti che operano in piÃ¹ Stati membri possano contare su un contesto coerente, funzionale e integrato; adottare una capacitÃ operativa integrata in caso di crisi; rafforzare la preparazione e la resilienza delle infrastrutture critiche anche se nel rapporto la maturitÃ della cybersicurezza nei settori critici mostra un miglioramento costante. ma i progressi restano disomogenei e le realtÃ operative settoriali non sono uniformi e lâ??Ai rischia di amplificare il divario di esposizione al rischio.

Inoltre i rischi legati alle catene di fornitura e le dipendenze transfrontaliere assumono una rilevanza crescente, con implicazioni che vanno ben oltre la dimensione puramente tecnica. Dal 2024, la maggior parte degli Stati membri ha compiuto progressi nella maturitÃ delle policy di divulgazione delle vulnerabilitÃ , e il numero di Paesi dotati di una policy nazionale di Cvd (Coordinated vulnerability disclosure) Ã¨ salito da 7 a 17. Lâ??Ai ha inciso profondamente sulla gestione delle vulnerabilitÃ , industrializzandone lâ??individuazione e imponendo un potenziamento delle capacitÃ di risposta. Lâ??Enisa ricorda che il Global cybersecurity outlook 2025 del World economic forum evidenzia un ampliamento dello skill gap in ambito cyber, cresciuto dellâ??8% rispetto al 2024.

In questo contesto, il panorama delle policy di cybersicurezza dellâ??Ue Ã¨ caratterizzato da tendenze convergenti. Lâ??Unione nel suo complesso avanza nellâ??attuazione delle principali normative di settore, in particolare la Direttiva Nis2, il Cyber resilience act e il Cyber solidarity act. Nondimeno, le dinamiche transfrontaliere e le intersezioni tra diversi quadri normativi stanno assumendo un peso sempre maggiore, spingendo verso sforzi di semplificazione e ricalibrazione legislativa. Al contempo, si osserva come il quadro geopolitico e gli sviluppi tecnologici abbiano innescato il varo o lâ??aggiornamento di diverse iniziative, tra cui la proposta per il Cybersecurity act 2 e il recente Piano dâ??azione dellâ??Ue su cybersicurezza e Ai.

â??

internazionale/esteri

webinfo@adnkronos.com (Web Info)

Categoria

1. Comunicati

default watermark

Tag

1. Ultimora

Data di creazione
Novembre 10, 2026
Autore
redazione