Cybersicurezza dei sistemi energetici

La cybersicurezza dei sistemi energetici rappresenta oggi una delle priorità globali più urgenti, soprattutto considerando l'importanza di queste infrastrutture per il buon funzionamento delle società moderne. L'energia alimenta non solo le abitazioni e le imprese, ma anche infrastrutture vitali come i trasporti, gli ospedali e i servizi pubblici, che sono essenziali per la vita quotidiana. Proteggere i sistemi energetici da potenziali attacchi informatici è quindi fondamentale non solo per garantire il corretto funzionamento delle economie moderne, ma anche per preservare la stabilità sociale, economica e politica delle nazioni.

DOI 10.12910/EAI2025-022

di Maria Valenti, Giovanna Adinolfi, Roberto Ciavarella Laboratorio smart grid e reti energetiche - Massimo Celino, Divisione per lo Sviluppo di Sistemi per l'Informatica e l'ICT - ENEA

La cybersicurezza dei sistemi energetici rappresenta oggi una delle priorità globali più urgenti, soprattutto considerando l'importanza delle infrastrutture energetiche per il buon funzionamento delle società moderne. L'energia alimenta non solo le abitazioni e le imprese, ma anche infrastrutture vitali come i trasporti, gli ospedali e i servizi pubblici, che sono essenziali per la vita quotidiana. Proteggere i sistemi energetici da potenziali attacchi informatici è quindi fondamentale non solo per garantire il corretto funzionamento delle economie moderne, ma anche per preservare la stabilità sociale, economica e politica delle nazioni. Inoltre, la protezione di queste infrastrutture è cruciale per tutelare la sicurezza dei cittadini e prevenire danni derivanti da interruzioni o disastri tecnologici.

Il processo di digitalizzazione del settore energetico ha portato senza dubbio a numerosi benefici, migliorando l'efficienza e la gestione dei sistemi, ma ha anche aperto nuovi orizzonti per i cybercriminali, ampliando le possibili superfici di attacco. La progressiva integrazione di quote sempre maggiori di energie rinnovabili, come anche la crescente adozione di tecnologie digitali avanzate nelle reti elettriche, rappresenta uno strumento fondamentale per la transizione energetica. Tuttavia, questa evoluzione determina una maggiore vulnerabilità agli attacchi informatici, che sono ormai un rischio concreto e tangibile. **Dal rapporto CLUSIT (Associazione Italiana per la Sicurezza Informatica) 2024 il numero di attacchi andati a buon fine in Italia nel settore Energy & Utilities è raddoppiato tra il 2018 e il 2022. Nei primi tre mesi del 2024 si sono registrati oltre la metà degli incidenti dell'intero 2023. La principale tecnica di attacco è stata il malware utilizzata in circa il 60% degli attacchi nel 2023 e il 96% nel 2024. La presenza di vulnerabilità ha rappresentato il "punto di ingresso" per l'attacco nel 13% dei casi nel 2022 e nell'11% nel 2023**.

Garantire una transizione energetica sostenibile e sicura

La crescente integrazione di energie rinnovabili e l'adozione di tecnologie digitali avanzate nelle reti elettriche rappresentano un pilastro fondamentale della transizione energetica. Tuttavia, questi sviluppi comportano anche un aumento della vulnerabilità agli attacchi informatici, un rischio ormai concreto e tangibile. **Sebbene il settore energetico sia attualmente coinvolto solo nel 4% degli attacchi cyber, la digitalizzazione crescente delle infrastrutture potrebbe amplificare l'esposizione a minacce sempre più sofisticate**.

È quindi fondamentale progettare e sviluppare soluzioni avanzate e sicure, garantendo una transizione energetica non solo sostenibile, ma anche resiliente sotto il profilo della protezione informatica. Gli attacchi informatici contro i sistemi energetici, infatti, potrebbero avere conseguenze rilevanti, come blackout di portata estesa, che potrebbero causerebbero non solo disservizi ma anche danni economici significativi. Oltre agli impatti diretti, gli attacchi cibernetici potrebbero anche danneggiare fisicamente gli impianti e le infrastrutture, aumentando notevolmente i costi di riparazione e sostituzione. Le aziende potrebbero subire gravi perdite a causa dell'interruzione delle loro attività, e a livello geopolitico,

un attacco riuscito potrebbe minare la fiducia pubblica e istituzionale, creando instabilità in un contesto già complesso.

Furto e manipolazione dei dati

Un ulteriore rischio cruciale riguarda il furto e la manipolazione dei dati. I moderni sistemi energetici sono dotati di tecnologie che raccolgono enormi quantità di dati, il cui obiettivo è ottimizzare la produzione e distribuzione dell'energia, anche massimizzando l'uso delle fonti rinnovabili. Tuttavia, l'integrità di questi dati è essenziale per prendere decisioni operative corrette. Un cyberattacco che comprometta l'affidabilità delle informazioni potrebbe portare a scelte errate nella gestione delle risorse energetiche o alla perdita di dati sensibili, con ripercussioni sulla sicurezza e sull'efficienza dei sistemi.
Un esempio emblematico della gravità di questi rischi è rappresentato dagli attacchi cibernetici alle reti elettriche subiti dall'Ucraina nell'ultimo decennio (2015, 2016, 2022). Nel 2016, un attacco condotto con il malware Industroyer One causò un blackout, lasciando un quinto della popolazione senza energia per ore. Questo malware, progettato per colpire i sistemi di controllo industriale, è stato attribuito al GRU, l'intelligence militare russa, dall'alleanza Five Eyes (alleanza di intelligence composta da Stati Uniti, Regno Unito, Canada, Australia e Nuova Zelanda). Nel 2022, un nuovo attacco mirato a spegnere la rete elettrica ucraina, questa volta con Industroyer2, evoluzione del precedente malware, è stato sventato, evitando che due milioni di persone rimanessero senza energia. Questi episodi evidenziano come **gli attacchi informatici contro le infrastrutture critiche siano diventati potenziali armi di guerra. L'Unione Europea ha riconosciuto l'urgenza di affrontare tali minacce e ha adottato misure significative per rafforzare la cybersicurezza dei sistemi energetici. Tra le iniziative principali vi sono la Direttiva NIS (Network and Information Security) del 2016 e il suo aggiornamento NIS2 del 2020. Questi strumenti normativi impongono obblighi stringenti agli operatori di infrastrutture critiche, tra cui il settore energetico, per migliorare la sicurezza delle reti e dei sistemi di informazione.**
Parallelamente, l'UE ha sviluppato una Strategia per la Cybersecurity che prevede investimenti significativi per aumentare la resilienza cibernetica del settore energetico. La creazione dell'European Cybersecurity Industrial, Technology and Research Competence Centre è un esempio concreto di questa strategia: il centro coordina attività di ricerca e sviluppo per rafforzare le difese contro le minacce informatiche. Inoltre, attraverso l'Agenzia dell'Unione europea per la cybersicurezza (ENISA), vengono promosse linee guida, buone pratiche e misure proattive come la segmentazione delle reti, sistemi di monitoraggio avanzati e formazione del personale.

L'integrazione della cybersicurezza nelle politiche climatiche ed energetiche

Un aspetto cruciale dell'approccio europeo è l'integrazione della cybersicurezza nelle politiche climatiche ed energetiche. Programmi come Horizon Europe finanziano progetti che richiedono lo sviluppo di soluzioni e prodotti avanzati che combinino l'innovazione tecnologica nel settore energetico con la sicurezza cibernetica, nell'obiettivo generale di promuovere una **transizione energetica cybersicura**.
Anche l'Italia ha assunto un ruolo attivo nella sfida della cybersicurezza, avviando numerose iniziative finalizzate a garantire la cyber-resilienza dei propri sistemi energetici. Nel 2021, ad esempio, è stata istituita **l'Agenzia per la Cybersicurezza Nazionale** (ACN), un organismo fondamentale per il coordinamento delle attività di prevenzione e risposta agli attacchi informatici. L'ACN dedica particolare attenzione alla protezione delle infrastrutture critiche, consolidando così un approccio integrato e lungimirante nella difesa delle risorse strategiche del Paese. Consapevole dell'importanza di proteggere le infrastrutture energetiche, considerate risorse critiche vulnerabili a possibili attacchi informatici, **la legislazione italiana pone particolare attenzione alle sfide di cybersicurezza legate all'evoluzione dei sistemi energetici.**
Un esempio significativo di questo impegno è il più recente aggiornamento del Piano Nazionale Integrato per l'Energia e il Clima (PNIEC). Obiettivo principale del PNIEC è garantire la transizione verso un sistema energetico sostenibile, decarbonizzato, sicuro e competitivo, in linea con gli impegni europei per la riduzione delle emissioni di gas serra e il raggiungimento degli obiettivi climatici. Il PNIEC punta a promuovere l'efficienza energetica, l'adozione di fonti di energia rinnovabile e la digitalizzazione delle infrastrutture energetiche, favorendo un'economia a basse emissioni di carbonio, assicurando al contempo la sicurezza e la resilienza delle reti energetiche. Tale Piano cita, in maniera esplicita, il tema della cybersicurezza applicata ai sistemi energetici, evidenziando come la crescente digitalizzazione e interconnessione dei sistemi energetici accrescano la vulnerabilità a minacce informatiche.
Il PNIEC sottolinea, perciò, la necessità di adottare tecnologie e protocolli avanzati per prevenire, rilevare e contrastare efficacemente gli at-

tacchi, rafforzando allo stesso tempo la resilienza delle infrastrutture energetiche, in modo da garantire la continuità operativa anche in caso di incidenti così da ridurre al minimo le conseguenze sulle forniture. **Parallelamente, si dà grande importanza alla collaborazione, sia a livello nazionale che europeo, con l'obiettivo di sviluppare strategie condivise, scambiare informazioni e adottare le migliori pratiche in materia di difesa cibernetica. Queste azioni sono pienamente coerenti con la Strategia Nazionale di Cybersicurezza 2022-2026, che prevede 82 interventi mirati a rafforzare la sicurezza cibernetica del Paese entro il 2026**.

L'impegno della ricerca per la cybersicurezza dei sistemi energetici

Ancora in linea con gli obiettivi di promuovere una transizione energetica cybersicura per il nostro Paese, a partire dal Piano Triennale 2022-2024, il programma nazionale della Ricerca di Sistema elettrico [1], promosso dal MASE (Ministero dell'Ambiente e della Sicurezza Energetica), ha integrato tra i suoi progetti un'iniziativa strategica dedicata alla sicurezza cibernetica dei sistemi energetici. Il progetto 2.1 "Cybersecurity dei Sistemi Energetici" [2], in particolare, è un progetto integrato che coinvolge tre enti di ricerca – RSE (Ricerca sul Sistema Energetico), ENEA (Agenzia Nazionale per le nuove tecnologie, l'energia e lo sviluppo economico sostenibile) e CNR (Consiglio Nazionale delle Ricerche) – e numerose università italiane, che lavorano con l'obiettivo comune di contribuire al raggiungimento della priorità "Digitalizzazione ed evoluzione delle reti" dell'Accordo di Programma 2022-2024.

Il progetto, conclusosi a dicembre 2024, ha consentito di progettare e implementare studi, strumenti e metodologie, con un livello di sviluppo tecnologico pari a TRL 4, finalizzati a: garantire la sicurezza delle tecnologie per le comunicazioni nei sistemi energetici; preservare la resilienza del sistema elettrico a fronte di attacchi cyber; sfruttare l'intelligenza artificiale per il rilevamento di anomalie cyber in infrastrutture energetiche. **Il progetto continuerà all'interno del Piano Triennale 2025-2027, con l'obiettivo di consolidare e migliorare il livello di sviluppo tecnologico raggiunto nel precedente triennio. L'intento è quello di introdurre progressivamente soluzioni sempre più avanzate e pronte per l'industrializzazione**.

[1] *Il programma nazionale della Ricerca di Sistema elettrico sostiene attività di ricerca e sviluppo di rilevante interesse generale per il sistema elettrico e si estende anche a settori correlati, con ricadute dirette sul settore energetico.*

[2] *https://www.ricercasistemaelettrico.enea.it/accordo-di-programma-mase-enea-2022-2024/digitalizzazione-ed-evoluzione-delle-reti/progetto-integrato-cyber-security-dei-sistemi-energetici.html*