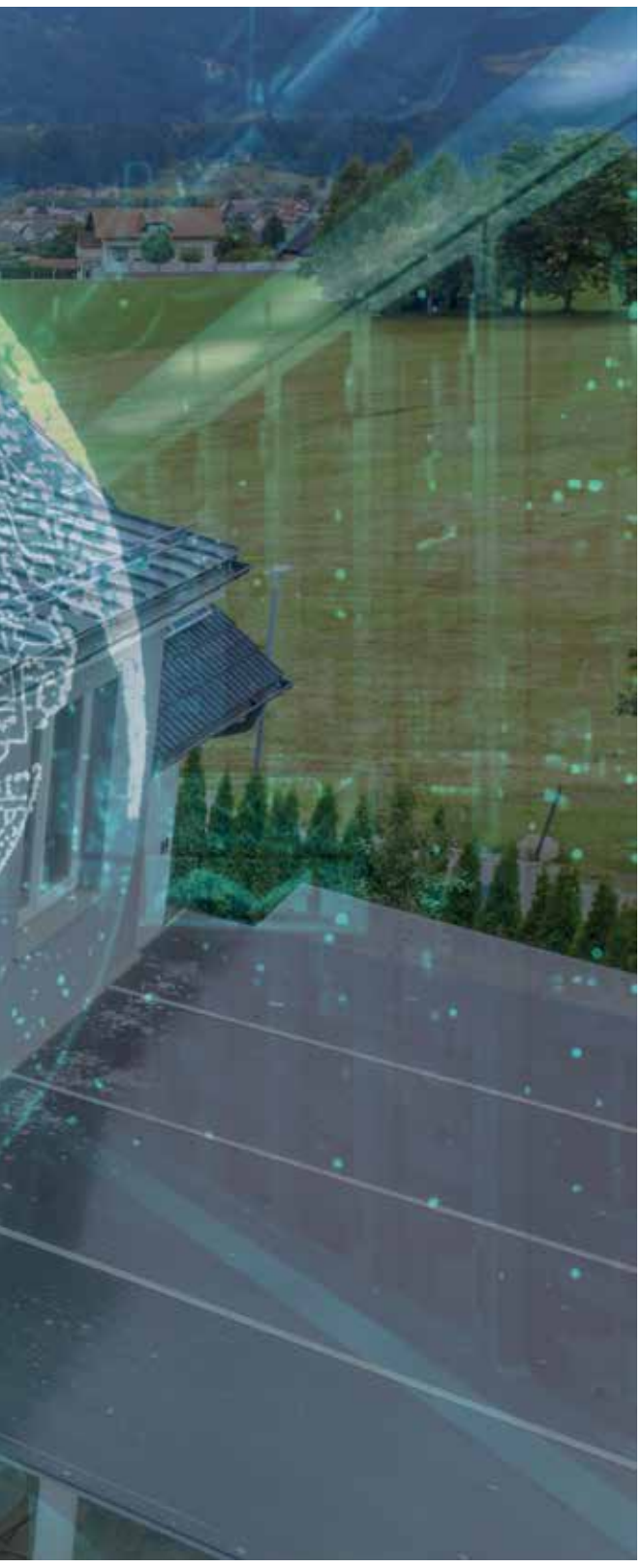
CYBERSECURITY UN ASPETTO PRIORITARIO PER IL FOTOVOLTAICO

LA CRESCENTE DIGITALIZZAZIONE DEGLI IMPIANTI FOTOVOLTAICI LI ESPONE A SEMPRE MAGGIORI MINACCE INFORMATICHE. LA CYBER SICUREZZA IN QUESTO SETTORE NON È SOLO UNA QUESTIONE TECNICA, È ANCHE UNA SFIDA CULTURALE, NORMATIVA E DI RESPONSABILITÀ DI TUTTI I SINGOLI ATTORI DELLA FILIERA. SERVE UN SISTEMA CHIARO, E CONDIVISO, CAPACE DI PROTEGGERE DALLE VULNERABILITÀ LE INSTALLAZIONI

DI ALDO **CATTANEO**

Negli ultimi anni, la digitalizzazione crescente del settore energetico ha reso gli impianti fotovoltaici sempre più soggetti a minacce informatiche. Queste infrastrutture, una volta considerate sistemi isolati con vita a sé, oggi comunicano in tempo reale con reti di monitoraggio, controllo e gestione, spesso accessibili via Internet: la cybersicurezza è diventata una priorità strategica, non solo per proteggere la produzione energetica ma anche per garantire la resilienza dell'intero sistema elettrico nazionale ed europeo.
«Gli impianti fotovoltaici oggi rappresentano una componente strategica del sistema energetico nazionale», spiega Marco Sandrini, CEO di Security Trust. «Parliamo di infrastrutture sempre più digitalizzate, connesse alla rete e gestite da sistemi intelligenti che se da un lato ne aumentano l'efficienza, dall'altro ne amplificano la superficie d'attacco». L'esposizione diretta su Internet di servizi interni come portali di monitoraggio o di configurazione, spesso raggiungibili attraverso tecniche di port-forwarding (procedura che permette di trasferire dati tra due dispositivi utilizzando una specifica porta di comunicazione), rappresenta un punto di ingresso facilmente sfruttabile. Inoltre la compromissione di fornitori esterni, come provider di servizi Cloud o portali utilizzati per il monitoraggio da remoto da terze parti, può avere conseguenze dirette sull'impianto a cui si collegano. Infine, l'uso di strumenti di accesso remoto come TeamViewer o AnyDesk direttamente sugli HMI o sistemi Scada, senza l'impiego di soluzioni sicure come VPN o JumpHost, espone l'impianto a rischi gravi.
«Oggi bisogna partire da un dato di fatto: un impianto fotovoltaico non è più connesso solo alla rete elettrica, ma è collegato anche a Internet», afferma Fulvio Ferrari, fondatore e application manager di Higeco More. «Questo vale sia per il monitoraggio in tempo reale - ormai presente su impianti di ogni dimensione - sia per la gestione dinamica della compravendita di energia, con tariffe variabili. Per impianti superiori al megawatt, inoltre, è previsto che il gestore di rete sia connesso direttamente all'impianto attraverso reti protette. La connessione però è presente anche su impianti di piccole dimensioni e rappresenta una potenziale vulnerabilità».
Lo scenario italiano del fotovoltaico è fortemente caratterizzato dalla diffusione di impianti residenziali installati diversi anni fa, in un'epoca in cui la protezione informatica non era una priorità e non c'era una particolare sensibilità su questo tema. In molti casi si utilizzavano semplici modem, spesso privi di password, in un contesto privo di normative specifiche che imponessero protocolli di sicurezza. La predominanza del segmento residenziale in Italia è un dato di fatto: al 31 maggio 2025 infatti risultavano connessi in Italia 1.935.509 impianti fotovoltaici, per una potenza complessiva di circa 38,5 GW. Di questi, 1,82 milioni (ovvero circa 94%)



sono impianti residenziali con potenza fino a 20 kW. È comunque vero che un impianto di qualsiasi dimensione, una volta connesso alla rete Internet, può diventare oggetto di attacchi informatici.
«Gli impianti fotovoltaici, specialmente quelli di grandi dimensioni sono sempre più integrati con tecnologie avanzate di monitoraggio, controllo e automazione, che li rendono vulnerabili a potenziali attacchi», afferma Gennaro Fiorenza, responsabile cybersecurity di Gridspertise. «Questi sistemi sono connessi a reti di comunicazione per trasmettere dati sulle prestazioni, lo stato operativo e altre informazioni cruciali. Tuttavia, questa interconnessione può esporre gli impianti a diverse minacce informatiche».

UN RISCHIO REALE

Gli attacchi al sistema energetico non sono più una minaccia teorica, anzi esistono già casi concreti: ad esempio, in Sudafrica, un grande impianto eolico è stato bloccato da hacker che hanno trafugato i dati e spento le pale eoliche, costringendo i proprietari a pagare un riscatto per riavviare la produzione e limitare le perdite economiche. I dati parlano di centinaia di attacchi ogni anno, su scala globale, al settore energetico.
«Con l'affermarsi dell'energia fotovoltaica come fonte cruciale di approvvigionamento energetico», afferma Uri Sadot, cybersecurity program director di SolarEdge, «sono emersi timori relativi agli attacchi informatici che possono interferire con la normale produzione di energia, insieme a dibattiti su come questi rischi dovrebbero e potrebbero essere

LE BEST PRACTICE PER PROTEGGERE UN IMPIANTO

- Mantenere aggiornati i firmware e i software dei dispositivi;
- Monitorare e controllare gli accessi ai sistemi di controllo e monitoraggio, preferibilmente con autenticazione multifattoriale (MFA);
- Proteggere le reti di comunicazione tramite firewall, VPN e sistemi di rilevamento delle intrusioni;
- Formare il personale aziendale con corsi specifici sulla cybersicurezza.

evitati. Incidenti recenti come il blackout in Spagna dimostrano chiaramente la necessità di poter contare su una rete elettrica affidabile e sicura. Negli ultimi anni, sui mercati europei è stato introdotto un numero crescente di dispositivi a basso costo con scarsi controlli di sicurezza informatica».
Secondo il rapporto Clusit pubblicato a marzo 2024, in Italia i cyber attacchi riusciti contro il settore energetico sono raddoppiati negli ultimi quattro anni, con il 90% dei casi classificati come di impatto "Critico" o "Alto". Inoltre, nel solo primo trimestre del 2024, il numero di incidenti nel settore Energy & Utilities è aumentato di oltre il 50% rispetto a tutto il 2023. I continenti più colpiti risultano essere Europa e America, dove si verifica l'80% dei casi analizzati. Al contrario, in Asia si è osservata una significativa diminuzione degli incidenti, mentre in Africa si è registrata una forte crescita.
«Gli impianti fotovoltaici sono sempre più esposti a rischi informatici», spiega Lorenzo Pavarino, tecnico informatico di Albasolar. «Malware e ransomware possono compromettere la produzione, mentre accessi non autorizzati e attacchi Distributed Denial of Service mettono a rischio dati e continuità operativa. Basta una falla in un componente per aprire la porta a vulnerabilità estese».

UN PROBLEMA DI RESPONSABILITÀ

La sicurezza informatica è una responsabilità condivisa che coinvolge diverse figure, sia interne che esterne all'organizzazione. «Al cuore dell'operatività troviamo IT manager, responsabili O&M, energy manager e professionisti DevOps», spiega Marco Sandrini di Security Trust, «che hanno il compito di gestire infrastrutture digitali, dispositivi di campo e controllare gli accessi ai sistemi. A loro si affiancano consulenti specializzati come esperti di cybersecurity, integratori OT/IT e Managed Security Service Provider, che forniscono servizi cruciali tra cui audit di sicurezza, monitoraggio continuo e protezione avanzata dalle minacce».
Anche i fornitori di tecnologia giocano un ruolo determinante, assicurando che le soluzioni proposte rispettino standard aggiornati e requisiti di sicurezza robusti.

HANNO DETTO

"SCEGLIERE UN PARTNER TECNICO ESPERTO IN CYBERSECURITY"

Lorenzo Pavarino, tecnico informatico di Albasolar

«Oggi, a differenza del passato, la scelta di un partner tecnologico deve tenere in forte considerazione anche l'affidabilità nella gestione della sicurezza informatica. È fondamentale valutare come vengono gestiti, protetti e controllati i dati e gli accessi agli impianti, poiché da questi aspetti dipende sempre più la continuità operativa e la resilienza dell'intera infrastruttura energetica».

"L'ETEROGENEITÀ DI SOLUZIONI RENDE DIFFICILE L'ADOZIONE DI MISURE DI DIFESA"

Marco Sandrini, CEO di Security Trust

«Gli impianti fotovoltaici oggi rappresentano una componente strategica del sistema energetico nazionale. Parliamo di infrastrutture sempre più digitalizzate, connesse alla rete e gestite da sistemi intelligenti che, se da un lato ne aumentano l'efficienza, dall'altro ne amplificano la superficie d'attacco. Spesso ci troviamo di fronte a dispositivi con firmware non aggiornati, configurazioni di sicurezza deboli o assenti, e un'eterogeneità di soluzioni che rendono difficile l'adozione di misure di difesa coerenti».

"GARANTIRE CHE SIANO STABILITI STANDARD SUFFICIENTI E OBBLIGATORI"

Uri Sadot, Cybersecurity program director di SolarEdge

«Riteniamo che ogni produttore abbia la responsabilità di creare soluzioni sicure, durevoli e protette a livello informatico fin dalla progettazione. Ad oggi, tuttavia, i produttori non sono obbligati da normative dedicate a soddisfare vari standard di sicurezza o cybersecurity. Pertanto, è responsabilità ultima dei governi e degli enti nazionali per l'energia elettrica (servizi pubblici e gestori di rete) garantire che siano stabiliti standard sufficienti e obbligatori».

"PORTARE LA CYBERSECURITY AL CENTRO DELLA PROGETTAZIONE DI UN IMPIANTO"

Fulvio Ferrari, fondatore e application manager di Higeco More

«È fondamentale portare la cybersecurity al centro della progettazione di un impianto. Certo, si tratta di un investimento aggiuntivo, ma il suo impatto economico è marginale rispetto al costo totale e può evitare problemi gravi in futuro. La sua implementazione va vista allo stesso modo dei sistemi di monitoraggio: nonostante abbiano un'incidenza economica, offrono un valore che non si può quantificare, in termini di continuità, efficienza e durata dell'impianto».

"TUTTI GLI ATTORI DELLA FILIERA DEVONO CONTRIBUIRE ALLA SICUREZZA"

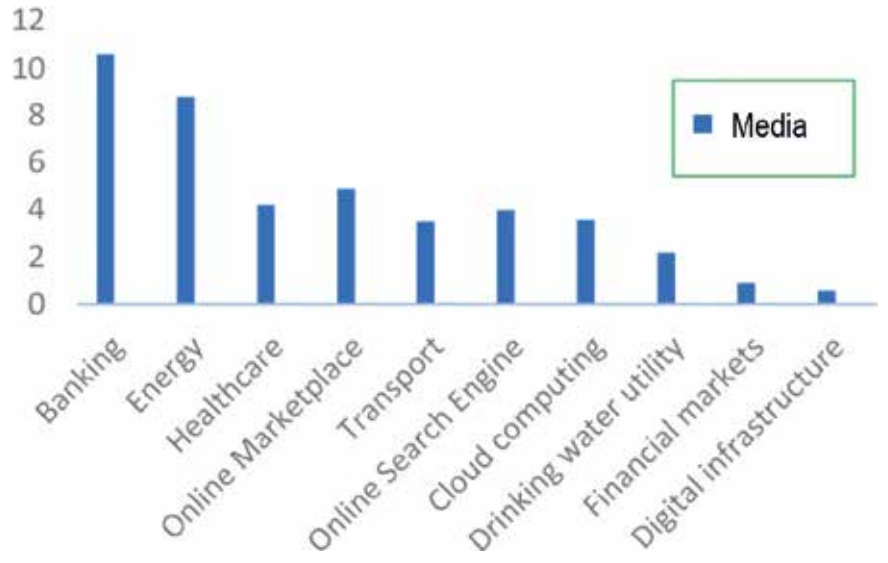
Gennaro Fiorenza, responsabile cybersecurity di Gridspertise

«La crescente digitalizzazione degli impianti fotovoltaici - connessi a Internet e gestiti da remoto - li rende esposti a cyberattacchi. La best practice più importante è l'approccio di "Security by Design", da applicare sin dalla fase di progettazione e per tutto il ciclo di vita, non solo per gli impianti fotovoltaici ma per tutti fornitori di soluzioni per le smart grid e i produttori di contatori intelligenti, consapevoli che i loro prodotti sono parte di infrastrutture cruciali».

«Un altro tema chiave è quello della responsabilità», sottolinea Fulvio Ferrari di Higeco More. «Chi deve garantire che un impianto sia conforme agli standard di sicurezza? Nei grandi impianti la questione è più chiara: le aziende dispongono di reparti dedicati alla sicurezza e di figure responsabili per ogni processo. Ma nei contesti medio-piccoli, che costituiscono la maggioranza in Italia, il quadro è ben più complesso. Le procedure sono numerose, spesso non standardizzate, e non è sempre evidente a chi competano. In assenza di un responsabile definito, il rischio è che nessuno si faccia carico dell'adeguamento e dell'aggiornamento dei sistemi, e che le vulnerabilità persistano».
Anche i produttori hanno la responsabilità di creare soluzioni sicure, durevoli e protette a livello informatico fin dalla progettazione.
«I produttori di componenti, siano essi inverter o altri device collegati alla rete ma anche i fornitori

Investimenti in sicurezza informatica per settore nel 2023 in milioni di euro

Quello dell'energia è uno dei settori con i più alti investimenti in sicurezza informatica a livello europeo, secondo solo a quello bancario



FONTE: "A SNAPSHOT OF CYBERSECURITY IN THE EU" EURELECTRIC POSITION PAPER

LE PRINCIPALI MINACCE

1 ACCESSI NON AUTORIZZATI
Portali di monitoraggio e configurazione esposti direttamente su Internet tramite tecniche di port-forwarding sono facili bersagli per attaccanti.

2 COMPROMISSIONE DI FORNITORI ESTERNI
Provider cloud e manutentori remoti possono rappresentare un punto d'ingresso per attacchi supply-chain.

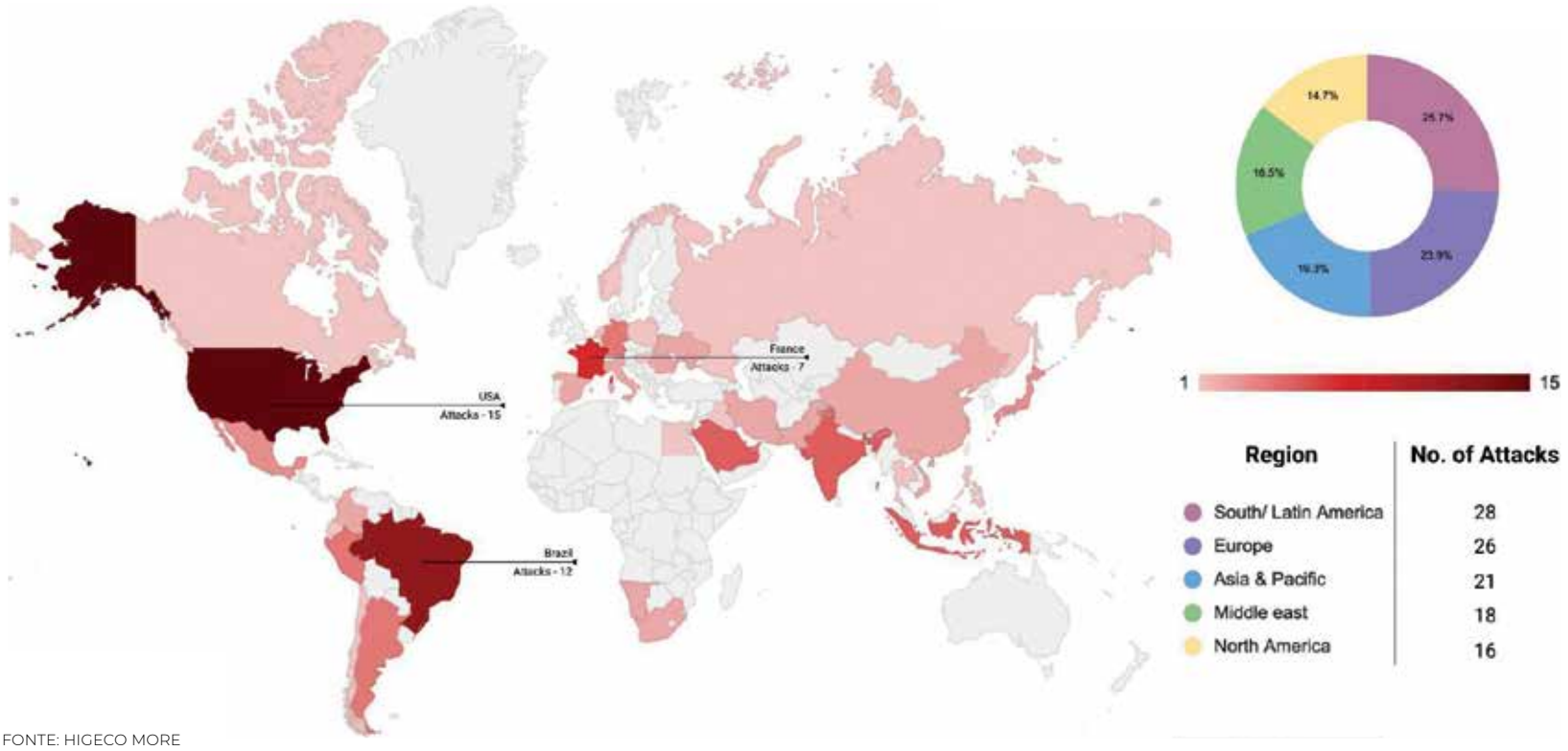
3 RANSOMWARE
L'attacco tramite ransomware su server Scada o gateway può causare l'interruzione della produzione e la perdita di dati strategici.

4 MALWARE E MANOMISSIONE DEI DATI
Gli attacchi più sofisticati mirano alla modifica dei protocolli di comunicazione OT non cifrati, alterando i dati energetici in transito.

5 DDOS
Attacchi Distributed Denial of Service possono rendere indisponibili i servizi di monitoraggio e controllo, bloccando la produzione energetica.

Attacchi informatici al settore energetico nel 2021

L'infografica evidenzia come nel 2021 la numerica degli attacchi informatici rilevati nel settore energetico in Europa fosse già rilevante anche rispetto le altre aree geografiche



FONTE: HIGECO MORE

di servizi, come i fornitori delle piattaforme di monitoraggio e controllo, devono garantire che i loro dispositivi siano "secured by design" e che ricevano supporto a lungo termine», spiega Gennaro Fiorenza di Gridspertise. «E qui entra in gioco il ruolo di Gridspertise che, lavorando a stretto contatto con gli operatori di rete, si occupa di proteggere l'intero sistema».

Gli enti pubblici e i legislatori a loro volta sono chiamati a definire norme e linee guida chiare e a esercitare attività di vigilanza. Nel caso di impianti aziendali, le aziende possono adottare diverse misure per proteggere le proprie reti interne da dispositivi non sicuri, come la scelta di fornitori affidabili, l'utilizzo di password complesse e la creazione di reti dedicate (Vlan) per l'impianto fotovoltaico. Nel caso dei campi e dei parchi fotovoltaici, ci sono molte misure che i proprietari possono adottare per ridurre il rischio di intrusioni informatiche, come la norma IEC 62443, l'utilizzo di firewall e connessioni VPN.

NORME, INCENTIVI E CULTURA

Il settore fotovoltaico nonostante la sua crescente rilevanza strategica è ancora privo, in particolare in Italia, di una normativa tecnica specifica per il settore fotovoltaico, che ne regoli in modo puntuale gli aspetti legati alla sicurezza, alla qualità e alla gestione operativa.

«A livello europeo, strumenti normativi come la Direttiva Nis2 e il Cyber Resilience Act», precisa Marco Sandrini di Security Trust, «stanno estendendo in modo chiaro e vincolante gli obblighi di cybersicurezza anche agli impianti alimentati da fonti rinnovabili, che sono ormai riconosciuti come parte integrante del sistema energetico nazionale. In questo contesto, riferimenti internazionali come la ISO/IEC 27001 - che definisce i requisiti per la protezione delle informazioni - e la IEC 62443 - focalizzata sulla sicurezza dei sistemi industriali e degli ambienti OT - rappresentano un supporto metodologico fondamentale per garantire un approccio strutturato, efficace e allineato alle migliori prassi globali».

Anche Uri Sadot di SolarEdge, conferma che «L'Europa ha già avviato alcuni primi passi con l'Articolo 3.3 della direttiva Red, e ha approvato la Nis 2 e il Cyber Resilience Act. Queste ultime due leggi sono in fase di implementazione da parte dei singoli stati membri e dovrebbero imporre requisiti più severi agli inverter fotovoltaici non sicuri». È parere diffuso quindi che la prima vera misura per garantire la sicurezza informatica degli impianti fotovoltaici sarebbe l'introduzione di una normativa specifica, che imponga l'adozione obbligatoria di sistemi di protezione su tutte le installazioni. Questo tipo di norma sarebbe sicuramente più facile da applicare agli impianti di nuova costruzione, ma la questione si complica quando si parla dei numerosissimi impianti residenziali già installati negli anni passati.

«In questi casi, il principale ostacolo è legato ai costi» spiega Fulvio Ferrari di Higeco More. «L'investimento necessario per implementare sistemi di cybersecurity dipende dal livello di protezione che si vuole raggiungere, che spesso non viene considerato prioritario. Per favorire l'aggiornamento e la messa in sicurezza di questi impianti obsoleti sarebbe necessario un intervento dello stato con incentivi specifici, in linea con ciò che è avvenuto in ambiti come quello dell'efficienza energetica degli edifici. In altre parole, se l'ammodernamento è strategico per la resilienza energetica del paese, allora deve essere sostenuto anche economicamente per poterne favorire la realizzazione su larga scala».

Paradossalmente, è proprio la vasta presenza di impianti non aggiornati che sembra costituire un freno all'introduzione di una norma retroattiva: se si obbligassero tutti i proprietari ad adeguare i propri impianti, servirebbero investimenti pubblici su larga scala. Una misura che, se non accompagnata da strumenti concreti, rischierebbe di restare sulla carta.

«Oggi, a differenza del passato, la scelta di un partner tecnologico deve tenere in forte considerazione anche l'affidabilità nella gestione della sicurezza informatica», spiega Lorenzo Pavarino di Albasolar. «È fondamentale valutare come vengono gestiti, protetti e controllati i dati e gli accessi agli impianti, poiché da questi aspetti dipende sempre più la continuità operativa e la resilienza dell'intera infrastruttura energetica».

Gennaro Fiorenza di Gridspertise aggiunge: «Quello della sicurezza informatica nel fotovoltaico è una combinazione tra aspetti normativi, culturali ed economici: normativi perché l'assenza di regole chiare e cogenti ha finora permesso una diffusione

Perché il FV è vulnerabile agli attacchi informatici?

1 Digitalizzazione e superficie d'attacco
Gli impianti fotovoltaici moderni sono dotati di dispositivi intelligenti, inverter connessi, sistemi Scada, HMI e piattaforme cloud per la manutenzione predittiva. Questo livello di digitalizzazione ha ampliato esponenzialmente la superficie d'attacco, rendendo vulnerabili sia i dispositivi che le reti a cui sono collegati.

2 Dispositivi non sicuri e firmware obsoleti
Molti impianti utilizzano dispositivi economici con livelli di sicurezza minimi. In particolare, gli inverter low-cost condividono spesso le stesse credenziali di accesso. L'assenza di aggiornamenti regolari dei firmware rappresenta un ulteriore punto debole.

3 Eterogeneità delle soluzioni
La varietà di soluzioni adottate rende difficile un approccio standardizzato alla cybersicurezza. Ogni impianto rappresenta un caso a sé, rendendo complesse l'integrazione e la protezione dei sistemi.

4 Considerazioni Strategiche
Il fotovoltaico è parte integrante delle infrastrutture critiche nazionali. Un attacco informatico ben orchestrato potrebbe compromettere non solo l'impianto ma anche l'intera rete elettrica, come dimostrano i blackout causati da attacchi mirati in Europa.

di impianti con standard di sicurezza non adeguati; culturali perché manca la consapevolezza del rischio. Molti proprietari di impianti e installatori infatti vedono la cybersecurity come un costo e un aggravio inutile, non come un investimento essenziale per la continuità operativa e la sicurezza del proprio asset e dell'intero sistema. Infine, è un problema economico perché l'implementazione di soluzioni di sicurezza ha un costo iniziale, che però deve essere visto come un'assicurazione contro danni potenzialmente catastrofici».

UN PASSO NECESSARIO

Proteggere le infrastrutture dalle minacce informatiche non è solo una necessità operativa, ma un imperativo per garantire l'affidabilità e la sostenibilità dell'energia pulita. Le direttive europee che riguardano il settore energetico richiedono l'implementazione di principi di risk management, business continuity e cybersecurity, adottando un approccio basato sul rischio e sulla resilienza. Guardando al futuro, sarà essenziale che le organizzazioni continuino a innovare e collaborare per rafforzare la sicurezza informatica e promuovere la resilienza delle infrastrutture critiche in Europa, senza dimenticare l'importanza di promuovere una formazione continua ed esercitazioni periodiche per consolidare la cultura della cyber resilience nel settore.
La sicurezza informatica nel fotovoltaico non è solo una questione tecnica: è anche una questione di cultura, normativa e responsabilità. Serve un sistema chiaro, incentivato e condiviso, capace di proteggere l'intero parco impiantistico dalle vulnerabilità, ed è auspicabile che una svolta normativa ed economica significativa in tema di sicurezza informatica non debba arrivare solo in seguito a un attacco cibernetico importante.