



IL FOTOVOLTAICO ALL'ESAME DI CYBERSECURITY

LA FORTE CRESCITA DEL NUMERO DI IMPIANTI SOLARI, LA LORO DIGITALIZZAZIONE E LA DIPENDENZA DA PIATTAFORME CLOUD STANNO RENDENDO SEMPRE PIÙ CENTRALE IL TEMA DELLA SICUREZZA INFORMATICA. NON È SOLTANTO UNA QUESTIONE TECNOLOGICA, MA COINVOLGE LA CULTURA AZIENDALE, LA RESPONSABILITÀ LUNGO LA FILIERA E L'ADEGUAMENTO ALLE NORMATIVE. PER TUTELARE LE INSTALLAZIONI ESISTENTI E QUELLE DI NUOVA REALIZZAZIONE È NECESSARIO UN APPROCCIO STRUTTURATO, CONDIVISO E SOSTENUTO DA REGOLE CHIARE E STRUMENTI PER SUPPORTARE GLI INVESTIMENTI

DI ALDO CATTANEO

Per anni il fotovoltaico è stato percepito come un settore semplice, quasi "meccanico", lontano dalle complessità delle infrastrutture storicamente ritenute critiche a livello informatico. Oggi quella percezione non è più sostenibile. La crescita esponenziale del numero degli impianti, la loro digitalizzazione e la dipendenza da piattaforme cloud hanno trasformato il solare in una componente strategica del sistema elettrico europeo. E, allo stesso tempo, in un bersaglio sempre più esposto alle minacce informatiche.

Il report di SolarPower Europe dal titolo *Solutions for PV Cyber Risks to Grid Stability* analizza in profondità come la crescente diffusione del fotovoltaico stia trasformando il sistema elettrico europeo e, allo stesso tempo, introducendo nuove vulnerabilità informatiche. L'Europa sta passando da un modello basato su grandi centrali di produzione elettrica a una rete molto più distribuita, composta da milioni di piccoli impianti solari, spesso installati su tetti di abitazioni o di piccole imprese. Questa evoluzione aumenta la resilienza complessiva del sistema, perché riduce la dipendenza da pochi nodi critici, ma amplia enormemente la superficie d'attacco per potenziali cyber-minacce.

Gli attacchi informatici contro infrastrutture energetiche europee sono in forte aumento, come mostrano i dati citati nel report. Finora il settore fotovoltaico non è stato colpito da incidenti gravi,

ma la sua crescente importanza nel mix energetico europeo lo rende un bersaglio sempre più appetibile. Inoltre, la competizione di mercato spinge molti operatori a privilegiare il contenimento dei costi rispetto agli investimenti in sicurezza informatica, creando un contesto in cui la maturità cyber è molto eterogenea.

«La crescente digitalizzazione degli impianti fotovoltaici comporta inevitabilmente un aumento della superficie di esposizione ai rischi cyber», spiega Girolamo Di Francia, responsabile del Laboratorio sviluppo applicazioni digitali fotovoltaiche e sensoristiche di Enea. «Nel fotovoltaico, però, questa evoluzione presenta caratteristiche specifiche rispetto ad altre infrastrutture energetiche. Se in passato gli unici elementi connessi erano sostanzialmente gli inverter, oggi gli impianti sono dotati di una quantità sempre maggiore di sensori, utilizzati per monitorare in tempo reale le condizioni operative di tutti i componenti».

A questo si aggiunge un contesto geopolitico sempre più instabile. Gli attacchi informatici contro infrastrutture energetiche europee sono in aumento, e gli attori ostili guardano con crescente interesse ai sistemi distribuiti, spesso meno protetti rispetto alle grandi centrali tradizionali.

«Oggi tutti gli impianti fotovoltaici sono connessi alla rete e alle piattaforme cloud» conferma Averaldo Farri, division director di ZCS. «Questo aumenta

notevolmente l'esposizione al rischio cyber rispetto al passato, quando gli impianti erano meno digitalizzati».

PERICOLO PERCEPITO?

Anche per il ruolo sempre più strategico del fotovoltaico, la cyber sicurezza degli impianti sta progressivamente diventando un elemento attenzionato in fase di progettazione anche se è consigliabile evitare approcci allarmistici. «È giusto alzare l'attenzione sulla cybersecurity, ma non ha senso la caccia alle streghe contro i prodotti che per provenienza possono essere potenzialmente pericolosi», afferma Fulvio Ferrari, consigliere di Italia Solare. «Il punto è un altro: la sicurezza informatica non è più un tema accessorio, ma centrale. Oggi, se un'azienda supera una certa dimensione viene considerata soggetto rilevante e deve rispettare specifici obblighi normativi in materia di sicurezza». È giusto che chi lavora nell'energia, soprattutto su scala medio-grande, applichi queste regole. Fino a tre anni fa si faceva pochissimo in questo ambito. La direzione intrapresa oggi è corretta.

«Soprattutto da parte dei finanziatori e degli investitori nei grandi impianti c'è la percezione che quelle solari siano infrastrutture critiche», spiega Averaldo Farri di ZCS. «Negli ultimi mesi il tema è diventato molto più sentito, anche a seguito di attacchi mediaticamente rilevanti. Oggi la questione è particolarmente attenzionata in Europa e negli Stati Uniti, soprattutto per quanto riguarda la localizzazione e il controllo dei dati».

Come mettere in sicurezza un impianto fotovoltaico

- **Integrare** la **sicurezza informatica** già in **fase di progettazione**, evitando di considerarla un'aggiunta successiva.
- **Segmentare** e **difendere** le **reti di comunicazione** con strumenti adeguati, come firewall, VPN e sistemi di intrusion detection.

- **Limitare** e **tracciare** gli **accessi ai sistemi di supervisione** e monitoraggio, adottando quando possibile l'autenticazione a più fattori (MFA).
- **Garantire l'aggiornamento** costante di **firmware** e **software** per ridurre l'esposizione a vulnerabilità note.
- **Investire** nella **formazione** del **personale**, affinché conosca rischi, procedure corrette e buone pratiche di cybersicurezza.

SICUREZZA A DUE VELOCITÀ

Nel settore fotovoltaico si osserva una dinamica piuttosto chiara: l'attenzione alla sicurezza informatica tende a diminuire al calare della taglia dell'impianto. È massima nei progetti utility scale e nel segmento commerciale-industriale e spesso diventa marginale nel residenziale. Non si tratta tanto di una diversa natura del rischio, quanto di una diversa percezione e di differenti condizioni economiche e organizzative. Negli impianti di grande taglia il committente è spesso una multinazionale, un fondo infrastrutturale o una utility energetica. Parliamo di soggetti strutturati, con uffici IT, responsabili della compliance, procedure interne codificate e obblighi normativi sempre più stringenti. In questi contesti la cybersecurity è parte integrante del progetto fin dalle prime fasi: rientra nei capitoli tecnici, nelle due diligence dei finanziatori e nei requisiti richiesti per l'accesso al credito. La protezione delle reti di comunicazione, la segmentazione dei sistemi, l'adozione di standard riconosciuti e l'implementazione di protocolli di monitoraggio sicuro non sono considerati optional, ma elementi strutturali dell'investimento.

Scendendo di taglia cambia il profilo del decisore. Nel residenziale il committente è il proprietario di casa, la cui attenzione è comprensibilmente concentrata su costo complessivo, produzione attesa e tempo di rientro dell'investimento. La sicurezza informatica è spesso percepita come un tema distante, tecnico, poco tangibile rispetto ai benefici immediati dell'impianto. A questo si aggiunge un fattore economico: gli interventi necessari per allinearsi agli standard di cybersecurity - firewall dedicati, reti separate, sistemi di autenticazione avanzata, aggiornamenti certificati - hanno un'incidenza percentuale molto contenuta su un impianto da decine di megawatt, ma possono pesare in modo significativo su un impianto da pochi kilowatt. Di conseguenza, nel piccolo impianto tali misure tendono a essere viste come un costo aggiuntivo, mentre nel grande impianto sono parte fisiologica del budget. «C'è poi un altro tema: la cultura della sicurezza», afferma Fulvio Ferrari di Italia Solare. «Nei grandi impianti è ormai consolidata; negli impianti domestici e di piccola taglia molto meno. L'installatore spesso non ha competenze specifiche in cybersecurity e l'utente finale ne ha ancora meno. È difficile convincere il cliente a spendere 150 euro in più per un dispositivo di sicurezza quando non percepisce il rischio».

Dello stesso parere è Hector Rodriguez, fotovoltaic market manager di SMA Italia, che sottolinea: «La percezione del rischio cyber nel fotovoltaico sta cambiando, ma in modo lento e non uniforme. Mentre i grandi impianti utility scale vengono ormai considerati asset strategici - e quindi gestiti con maggiore attenzione alla sicurezza - i piccoli e medi impianti continuano spesso a essere percepiti come semplici pannelli sul tetto».

Il risultato è una sorta di squilibrio culturale e strutturale: gli impianti più grandi, potenzialmente più rilevanti sotto il profilo sistemico, sono anche quelli più presidiati dal punto di vista cyber; il vasto parco diffuso di piccoli impianti, invece, è meno strutturato e meno consapevole su questi temi. Non perché il

L'Energia del Futuro inizia da qui
Capacità di accumulo superiore a 1 MWh

Inverter ibrido WIT
+ accumulo AXE

Efficienza senza paragoni
per applicazioni C&I



Move forward WIT the future
GROWATT
ITALIA



rischio sia necessariamente maggiore o minore in assoluto, ma perché cambiano il contesto decisionale, la capacità organizzativa e l'impatto relativo dei costi di adeguamento. In altre parole, nell'utility scale la sicurezza informatica è ormai una componente intrinseca del progetto, mentre nel residenziale resta ancora, troppo spesso, una variabile accessoria.

INVERTER, ANELLO DEBOLE?

Tra tutti i componenti di un impianto fotovoltaico, gli inverter rappresentano il nodo più delicato. Sono dispositivi intelligenti, connessi, aggiornabili da remoto, capaci di influenzare direttamente la stabilità della rete. In molti casi, funzionano più come dispositivi IoT che come componenti industriali.

«L'inverter è di fatto il cervello dell'impianto fotovoltaico», spiega Hector Rodriguez di SMA Italia. «Converte l'energia prodotta dai moduli, coordina il funzionamento dei diversi componenti e gestisce le comunicazioni verso l'esterno. Proprio per questo rappresenta uno dei punti più critici dal punto di vista della cyber security».

Le caratteristiche che incidono maggiormente sulla sicurezza sono note: password predefinite o deboli, accessi remoti non regolamentati, firmware non aggiornati o non firmati digitalmente, comunicazioni non cifrate, dipendenza da server cloud situati fuori dall'Unione Europea. A ciò si aggiunge la possibilità, per un attaccante, di manipolare parametri critici come la potenza reattiva o la tensione, con effetti potenzialmente sistemici. Ma Fulvio Ferrari di Italia Solare ritiene che sistemi per mettere in sicurezza qualsiasi impianto, con qualsiasi inverter, esistono e sono efficaci. «Esistono sistemi che permettono di inibire accessi non autorizzati, utilizzare comunicazioni criptate e controllare in modo rigoroso le connessioni», ha dichiarato il portavoce di Italia Solare. «Tuttavia, la maggior parte degli attacchi informatici non si basa su tecnologie misteriose o super innovative, ma su errori umani: disattenzione, mancata attivazione di una protezione, clic su un link sospetto».

MINACCE INFORMATICHE E ALLA RETE

Le minacce cyber al fotovoltaico si manifestano su due livelli distinti. Da un lato ci sono gli attacchi ai singoli impianti, spesso opportunistici, che sfruttano configurazioni errate, portali esposti su Internet tramite port forwarding o accessi remoti non protetti.

«Diversi report pubblicati negli ultimi anni indicano che gli attacchi avvengono più frequentemente a livello di singolo impianto», sottolinea Hector Rodriguez di SMA Italia, «poiché tali dispositivi - molto più numerosi - risultano spesso esposti direttamente a Internet a causa di configurazioni deboli come password di default, firmware obsoleto, porte aperte, protocolli non cifrati».

Dall'altro lato, molto più preoccupante, si stanno moltiplicando gli attacchi alle piattaforme centralizzate di monitoraggio e gestione. Un portale cloud compromesso può consentire a un attaccante di controllare una numerica molto elevata di impianti. Lo sottolinea anche Averaldo Farri di ZCS: «Secondo la nostra esperienza, gli attacchi sono principalmente indirizzati alle piattaforme di monitoraggio centralizzate, perché colpirle consente potenzialmente di accedere a più impianti contemporaneamente».

Le tecniche utilizzate sono ormai note nel settore industriale: ransomware che bloccano la produzione, malware che alterano i protocolli non cifrati, attacchi Distributed Denial of Service DDoS che possono saturare i sistemi di comunicazione, impedendo l'accesso alle piattaforme di controllo e monitoraggio e compromettendo la continuità operativa che rendono indisponibili i servizi di monitoraggio, oppure compromissioni della supply chain che sfruttano manutenzione o provider cloud come vettori d'ingresso.

Di contro, come elemento di resilienza dell'ecosistema fotovoltaico, rispetto ad eventuali cyber attacchi Girolamo di Francia di Enea suggerisce: «La polverizzazione sul territorio delle centrali solari rende il sistema energetico intrinsecamente più resiliente. Il malfunzionamento o l'attacco a un singolo impianto non genera conseguenze drammatiche sull'intero sistema. Al contrario, la diffusione capillare degli impianti rende più difficile provocare danni sistemici su

HANNO DETTO



“NON È PIÙ POSSIBILE IGNORARE IL TEMA”

Fulvio Ferrari, consigliere di Italia Solare

«Se si lavora bene, i rischi diventano accettabili. Oggi l'asticella si è alzata moltissimo: esistono obblighi stringenti, con penali importanti, e non è più possibile ignorare il tema. Le aziende sono sempre più tenute a dotarsi di personale dedicato alla sicurezza informatica, perché è un aspetto sensibile in qualsiasi settore».



"PARTE FONDAMENTALE DELL'ARCHITETTURA STESSA DEL SISTEMA"

Averaldo Farri, division director di ZCS

«La cybersecurity deve essere integrata fin dalla fase di progettazione dell'impianto. Non può essere considerata un elemento accessorio o aggiuntivo in un secondo momento, ma deve far parte dell'architettura stessa del sistema. Adottare la sicurezza fin dalla fase progettuale è oggi essenziale per contenere in modo sistemico l'esposizione ai rischi».



“CRESCE LA CONSAPEVOLEZZA DEI RISCHI”

Hector Rodriguez, photovoltaic market manager di SMA Italia

«Oggi il rischio cyber viene sempre più integrato sia nella valutazione degli investimenti sia nella gestione degli asset fotovoltaici, grazie alla crescente consapevolezza che le minacce verso le infrastrutture energetiche sono in aumento. Tali minacce possono infatti compromettere anche la performance di produzione degli impianti».



“IMPIANTI DATATI PIÙ A RISCHIO”

Girolamo Di Francia, responsabile del Laboratorio sviluppo applicazioni digitali fotovoltaiche e sensoristiche di Enea

«Un tema particolarmente delicato riguarda gli impianti più datati. Molti di questi hanno dispositivi che utilizzano oggi software obsoleti e insicuri. In questi casi l'aggiornamento continuo è fondamentale, quando possibile, oppure diventa necessario pianificare la sostituzione dei componenti critici».

Perché il fotovoltaico è esposto ai rischi cyber?



1. Elevato livello di digitalizzazione

Gli impianti di nuova generazione integrano inverter connessi, sistemi Scada, interfacce HMI e piattaforme cloud per il monitoraggio e la manutenzione predittiva. Questa crescente interconnessione amplia notevolmente la superficie d'attacco, esponendo sia i dispositivi sia le infrastrutture di rete.

2. Dispositivi con protezioni limitate

In molti casi vengono impiegate apparecchiature con standard di sicurezza essenziali. Alcuni inverter, soprattutto di fascia economica, utilizzano credenziali predefinite o condivise. La mancata installazione di aggiornamenti firmware periodici aumenta ulteriormente il livello di rischio.

3. Mancanza di uniformità tecnologica

La coesistenza di soluzioni differenti - per marchi, protocolli e architetture - rende complesso adottare criteri di protezione omogenei. Ogni impianto presenta specificità che complicano integrazione, gestione e difesa.

4. Rilevanza strategica del settore

Il fotovoltaico è parte delle infrastrutture energetiche nazionali. Un attacco coordinato potrebbe avere effetti che vanno oltre il singolo impianto, con ripercussioni sulla stabilità della rete elettrica, come già evidenziato da episodi di blackout legati ad attacchi informatici in Europa.



larga scala, rafforzando la sicurezza energetica di un Paese anche dal punto di vista geopolitico».

CONSEGUENZE OPERATIVE ED ECONOMICHE

Le conseguenze di un attacco possono essere molto diverse, ma tutte potenzialmente gravi. Un impianto può essere spento, danneggiato o configurato in modo da operare fuori dai limiti di sicurezza. Un portafoglio di impianti può subire un fermo prolungato, con perdite economiche significative. Nei casi più estremi, un attacco coordinato può contribuire a destabilizzare la rete elettrica, generando blackout o disservizi diffusi. «Dal punto di vista economico, ciò si traduce in un impatto significativo», afferma Hector Rodriguez di SMA Italia, «oltre ai costi per la sostituzione dei componenti danneggiati, agli interventi di emergenza e ai tempi di fermo impianto, occorre considerare anche la mancata vendita di energia, la perdita di accesso agli incentivi e l'eventuale applicazione di penali contrattuali, ad esempio per mancate consegne previste nei PPA». Oltre ai danni diretti, ci sono quelli indiretti: perdita di fiducia degli investitori, aumento dei costi assicurativi, necessità di interventi di ripristino complessi, impatti sulla reputazione delle aziende.

«Le conseguenze di un attacco informatico», conferma Averaldo Farri di ZCS, «possono includere blocco dell'impianto da remoto, perdita di produzione, danni economici, sottrazione di dati strategici e impatti reputazionali».

RESPONSABILITÀ CONDIVISE

Per ridurre i rischi e aumentare la sicurezza informatica di un impianto fotovoltaico è necessario che più profili collaborino tra loro. La cyber security infatti non dipende da un solo attore. Il produttore dell'inverter deve garantire la sicurezza del firmware; l'installatore è responsabile della configurazione iniziale; il proprietario gestisce la rete locale; il provider cloud controlla i dati e gli accessi remoti.

«La sicurezza informatica di un impianto fotovoltaico è una responsabilità condivisa lungo l'intera filiera, poiché ogni fase del ciclo di vita introduce potenziali vulnerabilità», afferma Hector Rodriguez di SMA Italia. «Gli OEM devono garantire la security by design e integrare misure di protezione già in fase di sviluppo».

Questa frammentazione potrebbe creare però delle zone grigie in cui sembra che nessuno abbia una responsabilità piena, diretta e chiara. Le criticità emergono in tutte le fasi: progettazione, installazione e gestione operativa. Spesso la cybersecurity non viene considerata in fase di progetto, le configurazioni iniziali sono approssimative e la manutenzione non include controlli periodici.

NORMATIVE INSUFFICIENTI E SCARSA CHIAREZZA

Come anticipato, il rischio cyber sta iniziando a entrare nei processi di due diligence, ma non è ancora un elemento standardizzato. Si tratta di un approccio destinato a cambiare rapidamente, soprattutto alla luce delle nuove normative europee e dell'aumento degli attacchi. A proposito di normative, quelle europee (NIS2, Cyber Resilience Act, Network Code on Cybersecurity) rappresentano un passo avanti, ma non sono ancora pienamente adeguate al fotovoltaico distribuito. Non coprono gli impianti di piccola taglia, non regolano in modo specifico l'accesso remoto dei produttori e non definiscono requisiti minimi per le piattaforme cloud. Questa incertezza normativa influenza le scelte tecnologiche e progettuali, spingendo molti operatori a privilegiare soluzioni meno costose e meno sicure.

«Per i grandi impianti, normative come la NIS2 stanno già spingendo in questa direzione», afferma Fulvio Ferrari di Italia Solare. «Le aziende strutturate hanno obblighi di sicurezza che si estendono a tutti i loro asset, compresi gli impianti. Il problema restano gli impianti piccoli: oggi è difficile che chi realizza un piccolo impianto abbia un obbligo concreto che lo spinga a investire di più in cybersecurity. Non è ancora un tema percepito come prioritario, soprattutto dal punto di vista economico».

IL PROBLEMA DEI VECCHI IMPIANTI

Certamente per quanto riguarda le nuove installazioni si sta diffondendo la cultura della sicurezza informatica, per cui alcuni sistemi per prevenire attacchi informatici vengono presi in considerazione già in

fase di progettazione. Di contro esiste una numerica enorme di impianti datati. In passato certe precauzioni non si prendevano, anche perché non c'era la percezione del problema. Oggi il monitoraggio remoto è una pratica standard e consolidata, ma proprio per questo la superficie di attacco è aumentata.

«Sul grande parco di impianti già installati e potenzialmente insicuri è difficile intervenire per la messa in sicurezza, soprattutto in assenza di incentivi economici», spiega Fulvio Ferrari di Italia Solare. «Senza un obbligo normativo o un vantaggio economico concreto, difficilmente si procederà con aggiornamenti massivi. Forse avrebbe senso rendere obbligatori, in caso di revamping o repowering, anche aggiornamenti legati alla sicurezza informatica: ad esempio il cambio del router o l'adozione di specifiche protezioni di rete».

VERSO UN FOTOVOLTAICO "SECURE BY DESIGN"

Il futuro della sicurezza informatica nel fotovoltaico passa da un cambio di paradigma. La cyberse-

curity dovrà essere integrata fin dalla fase di progettazione degli impianti. Gli inverter del futuro saranno sempre più "secure by design", con controlli di accesso rigorosi, firmware firmati digitalmente, protocolli cifrati e architetture che limitano la possibilità di manipolazioni coordinate.

In definitiva, la tutela della rete energetica nazionale non può più essere delegata a iniziative isolate. È imperativo stabilire un ecosistema di sicurezza che sia chiaro nelle regole, incentivato sul piano fiscale e condiviso tra tutti gli stakeholder, al fine di blindare l'intero parco impiantistico contro vulnerabilità sempre più sofisticate. Il vero salto di qualità, tuttavia, deve essere culturale prima ancora che tecnologico: è auspicabile che la necessaria svolta normativa ed economica non giunga come una reazione tardiva a un'offensiva cibernetica di vasta scala, ma come il risultato di una lungimirante strategia di difesa preventiva. Proteggere il fotovoltaico oggi significa garantire la sovranità energetica di domani.



SAJ | **al-keeper**

Trasforma l'energia in valore con l'intelligenza Artificiale!

CHS2 e CM2: accumulo intelligente per ridurre i costi e valorizzare gli asset aziendali



Sicurezza



Continuità Operativa



Stabilità



Risparmio Reale



SAJ Italia

✉ italy@saj-electric.com

☎ +39 324 286 4300

🌐 it.saj-electric.com



SAJ