Istituto nazionale di test per la cibersicurezza

COMUNICATO STAMPA
Rapporto di sintesi sulla cibersicurezza degli impianti fotovoltaici

Impianti fotovoltaici di importanza sistemica: l'NTC presenta un'analisi approfondita della cibersicurezza con raccomandazioni concrete

Zugo, 17 settembre 2026 – Gli impianti fotovoltaici sono diventati di importanza sistemica per l'approvvigionamento elettrico svizzero. Alla fine del 2025 in Svizzera erano installati circa 338'000 impianti fotovoltaici allacciati alla rete. In questo contesto l'Istituto nazionale di test per la cibersicurezza NTC ha verificato di propria iniziativa sistemi molto diffusi in Svizzera. Complessivamente sono stati sottoposti a un'analisi approfondita sette inverter e quattro sistemi di gestione dell'energia. Sono stati così identificati oltre 50 rilievi, tra cui sette critici e sei elevati. I rilievi sono stati segnalati ai produttori in via confidenziale. La maggior parte ha reagito rapidamente, mentre per alcuni prodotti l'eliminazione delle vulnerabilità è ancora in corso.

Risultati dell'analisi di sicurezza e schemi di rischio principali

Per valutare il livello di sicurezza della tecnica fotovoltaica diffusa in Svizzera, nell'arco di un anno l'NTC ha sottoposto undici prodotti a un'analisi tecnica di sicurezza completa: sette inverter e quattro sistemi di gestione dell'energia di otto produttori in totale, tra cui i fornitori che determinano il mercato.

Complessivamente le verifiche hanno portato alla luce oltre 50 rilievi, sette dei quali critici e altri sei elevati. Cinque degli undici prodotti presentavano almeno un rilievo elevato o critico. In quattro prodotti l'NTC ha ottenuto il controllo completo del dispositivo, in parte introducendo codice di programma estraneo, in parte attraverso un accesso di manutenzione del produttore protetto in modo insufficiente.

Sono emersi quattro schemi ricorrenti: carenze nell'autenticazione e nel controllo degli accessi, ad esempio password predefinite; accessi di manutenzione non sicuri con credenziali identiche per l'intero parco di dispositivi; cifratura assente o debole delle interfacce locali; nonché interfacce non disattivabili. In quasi tutti gli inverter verificati era possibile modificare, attraverso l'interfaccia di comando locale e senza alcuna autenticazione, quanta potenza l'impianto immette in rete, fino a zero.

Il livello di sicurezza dei singoli prodotti non è peraltro peggiore di quello di altri dispositivi connessi molto diffusi che l'NTC ha già verificato. Non sono emersi indizi di backdoor inserite intenzionalmente e la maggior parte dei produttori ha reagito rapidamente alle vulnerabilità segnalate. Ciò che distingue gli impianti solari da altri dispositivi connessi non è la qualità dei prodotti, bensì il loro ruolo: nel loro insieme sono di importanza sistemica per la rete elettrica. Nelle giornate soleggiate, a mezzogiorno, coprono regolarmente oltre la metà del consumo istantaneo di elettricità.

Determinante per la rilevanza di un rilievo per la rete elettrica non è la sua sola gravità, bensì la sua portata. Il singolo impianto solare sul tetto di un'abitazione o di un edificio commerciale resta irrilevante per la rete elettrica: se si guasta o viene manipolato, ciò non cambia nulla nel sistema complessivo. Diventa un rischio il fatto che molti di questi impianti sono collegati ai cloud dei produttori e per questa via vengono riforniti ad esempio degli aggiornamenti del firmware. Sei dei rilievi agiscono attraverso una simile istanza centrale su un intero parco di dispositivi e quindi potenzialmente su migliaia di impianti contemporaneamente. «Non è la sola gravità di una vulnerabilità a renderla pericolosa, bensì la sua portata», afferma Tobias Castagna, responsabile degli esperti di test presso l'NTC. «Negli impianti fotovoltaici un singolo rilievo in un componente centrale può riguardare migliaia di impianti contemporaneamente, ecco perché servono contromisure mirate, ma realizzabili».

Raccomandazioni per la riduzione dei rischi

L'NTC ha comunicato i rilievi ai produttori interessati già prima della pubblicazione del rapporto. Molti hanno reagito immediatamente e hanno già chiuso le falle.

Sulla base delle conoscenze acquisite con questa indagine, l'NTC ha formulato per cinque gruppi di destinatari raccomandazioni su misure per ridurre i ciberrischi negli impianti fotovoltaici:

- **Gestori di impianti di piccole dimensioni**: scelta di un fornitore affermato, conferma di password individuali al momento della consegna e chiarimento contrattuale della competenza per gli aggiornamenti;
- **Gestori di impianti più grandi:** inventario delle interfacce e degli accessi remoti, separazione dal resto della rete nonché requisiti di sicurezza nei bandi di concorso;
- **Aziende installatrici:** credenziali individuali per ogni impianto, nessuna raggiungibilità diretta da Internet, separazione dal resto della rete e una consegna documentata;
- **Produttori:** la sicurezza come principio costruttivo, credenziali individuali, aggiornamenti del firmware firmati, accessi di manutenzione limitati nel tempo e revocabili nonché un blocco di fabbrica del controllo a distanza rilevante per la rete elettrica, revocabile soltanto in loco;
- **Politica e autorità:** requisiti minimi per l'immissione in commercio di inverter e sistemi di gestione dell'energia, requisiti di sicurezza come condizione per l'allacciamento alla rete nonché una competenza designata per il rischio che nasce dalla somma degli impianti di piccole dimensioni.

Una soluzione semplice e completa non esiste; tutti gli approcci hanno vantaggi e svantaggi, e queste raccomandazioni non coprono l'intera gamma delle misure possibili. Ma ogni misura qui indicata che viene attuata accresce la cibersicurezza.

L'indagine è avvenuta su iniziativa dell'Istituto nazionale di test per la cibersicurezza NTC, che ha fornito anche il team di test e una parte sostanziale dei mezzi finanziari. L'indagine è stata sostenuta finanziariamente da SvizzeraEnergia. Diverse organizzazioni, in prevalenza del settore energetico, hanno messo a disposizione dispositivi di test e hanno partecipato ai costi.

L'NTC ringrazia tutte le organizzazioni coinvolte e SvizzeraEnergia per il loro sostegno. Per garantire l'indipendenza dei risultati, né i produttori né le organizzazioni di sostegno hanno influito sulla selezione, sulla portata della verifica o sui risultati; i produttori sono stati contattati soltanto nell'ambito della segnalazione confidenziale per l'eliminazione delle vulnerabilità.

Rapporto di sintesi fotovoltaico

Contatto per i media:
Andreas W. Kaelin, Direttore Esecutivo
+41 41 317 00 11, andreas.kaelin@ntc.swiss

Sull'Istituto nazionale di test per la cibersicurezza NTC
L'Istituto nazionale di test per la cibersicurezza NTC contribuisce alla sicurezza e alla sovranità digitale della Svizzera, individuando in modo proattivo le vulnerabilità critiche dei prodotti digitali e i rischi delle nuove tecnologie digitali e sostenendone la mitigazione. Quale associazione senza scopo di lucro con sede a Zugo, l'NTC opera secondo i principi di indipendenza e oggettività. L'NTC verifica di propria iniziativa prodotti e applicazioni digitali che in Svizzera non vengono verificati a sufficienza, pur essendo di grande importanza per l'economia e la società. Allo stesso modo l'NTC esegue verifiche di cibersicurezza su incarico di gestori di infrastrutture critiche e di autorità. https://it.ntc.swiss