Cybersecurity in campo energetico

Paolo Maccarrone, direttore scientifico dell'Osservatorio Energy Cybersecurity dell'Energy&Strategy Group

La digitalizzazione è un fenomeno pervasivo e inarrestabile che sta modificando in modo epocale interi settori economici, generando processi di innovazione più o meno radicale di processi e prodotti, abilitando nuove funzionalità e servizi, dando luogo a business model e scenari competitivi inediti. Come sempre accade nel caso di cambiamenti del contesto, si creano opportunità, ma anche rischi, come quelli derivanti dalle minacce che arrivano dal cyberspazio, ovvero dal dominio virtuale costituito da tutti i device, gli apparati e le reti ICT.

Ciò vale anche per il settore energetico: la filiera elettrica, in particolare, è caratterizzata da trasformazioni estremamente rilevanti, in buona parte derivanti dall'introduzione di tecnologie digitali per la gestione delle diverse attività ai vari stadi della filiera, dalla produzione alla trasmissione, alla distribuzione, al consumo: si pensi al telecontrollo e al telemonitoraggio, all'ottimizzazione dei cicli di produzione dell'energia, alle smart grid, ai modelli di predictive maintenance resi possibili dall'analisi di grandi moli di dati (grazie anche all'artificial intelligence) e all'ottimizzazione dei consumi energetici (per gli end-user).

Questi trend evolutivi hanno comportato una crescente interconnessione digitale relativa agli impianti di produzione e agli apparati di rete (elettrica), esponendo tali asset a minacce ben note negli ambienti IT, ma ancora praticamente sconosciute nell'ambito dell'Operation Technology (OT). Non di rado, infatti, il funzionamento degli impianti e degli apparati di rete si basa su sistemi operativi e protocolli di comunicazione abbastanza "datati", che garantiscono grande affidabilità in un ambiente isolato e protetto, ma che risultano facilmente aggredibili se messi in contatto col mondo esterno.

Nel caso di attacchi cyber agli apparati di rete, si può giungere alla temporanea indisponibilità di una delle infrastrutture critiche del Paese, se non addirittura al danneggiamento fisico degli apparati stessi, con conseguenze potenzial-

mente drammatiche, soprattutto in caso di attacchi legati a cyber warfare, cioè ad opera di altre nazioni. A questo riguardo, è significativo quanto accaduto in Ucraina nel dicembre 2015, quando un attacco di natura cibernetica portò al blocco di un consistente numero di sottostazioni di tre società di distribuzione, con conseguente black-out che lasciò senza energia elettrica per diverse ore più di 230.000 utenti. Inoltre, lo sviluppo della generazione distribuita e delle fonti rinnovabili – che hanno raggiunto in Italia i 53 GW, coprendo nel 2017 il 36,2% della produzione annua e in crescita stimata al 60% entro il 2030 (Strategia Elettrica Nazionale) – ha determinato l'ingresso di numerosi nuovi operatori, molti dei quali con scarsa o nulla esperienza nel settore, e, conseguentemente, con una scarsa consapevolezza dei rischi di natura cibernetica in ambito energetico. Questi due fattori - l'incremento del numero di operatori, e quindi di soggetti target per gli attaccanti, e la loro relativa inesperienza - potrebbero combinarsi in modo decisamente pericoloso, determinando fenomeni di instabilità della rete elettrica nazionale, soprattutto nel caso di attacchi "distribuiti".

Da qui la decisione di attivare un Osservatorio sull'Energy Cybersecurity focalizzato sulla sicurezza industriale. Nel primo report, in particolare, abbiamo puntato l'attenzione sui rischi e i potenziali impatti per il sistema elettrico italiano e per le imprese operanti nella filiera, e sulla cultura delle industrie italiane nei confronti della Cybersecurity OT. Con riferimento al primo punto, oltre ad analizzare i potenziali impatti, operativi ed economici, per i vari operatori ai diversi stadi della filiera, abbiamo realizzato anche delle simulazioni per verificare il rischio «di sistema», ovvero la possibilità di mettere in crisi la stabilità della rete elettrica nazionale o comunque di costringere a sostenere extra-costi significativi per il ribilanciamento tra domanda e offerta.

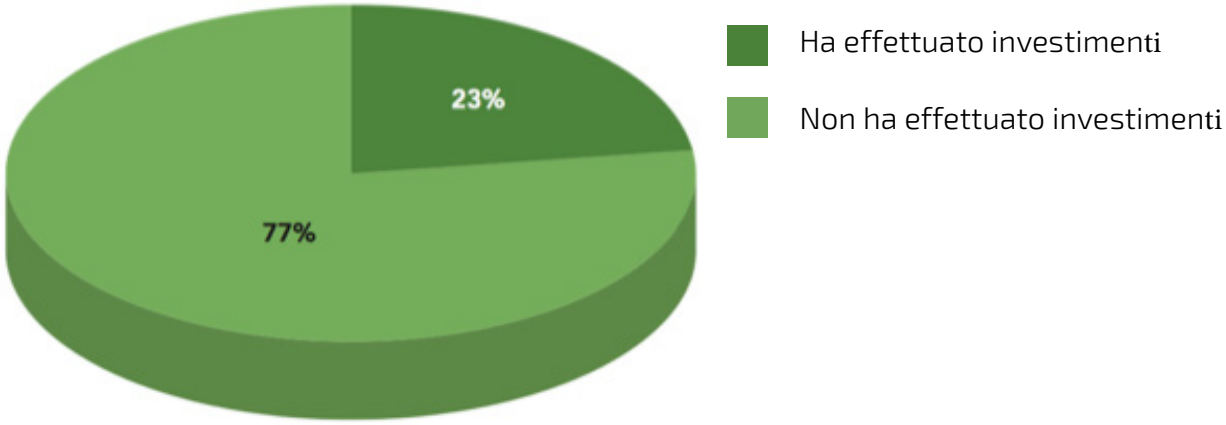
In particolare, le analisi hanno mostrato come un attacco volto a generare un black–out attraverso un "distacco" di una potenza pari almeno a 3 GW (soglia oltre la quale aumenta notevolmente il rischio di instabilità della rete) dovrebbe interessare contemporaneamente il 12,7% della potenza installata relativa agli impianti eolici e fotovoltaici. Un valore non così elevato, soprattutto tenendo presente l'aumento della capacità installata di queste due fonti.

Esaminando invece gli extra-costi generati da un attacco cyber agli impianti di produzione eolica e fotovoltaica, è possibile osservare come un'interruzione dell'erogazione di potenza che coinvolga il 50% della capacità installata, per il 10% delle ore medie annue di funzionamento, determini un aumento dei costi per la comunità pari a 264 milioni di euro, a causa della maggiore necessità di far ricorso al Mercato dei Servizi di Dispacciamento (MSD).

L'ultima parte del report si è focalizzata sugli end-user di natura industriale, con l'obiettivo di verificare il grado di diffusione della cultura relativa alla cybersecurity in ambito OT. Il quadro che ne emerge non è molto rassicurante: le imprese, infatti, sono consapevoli della necessità di gestire adeguatamente anche questi temi, alla luce della maggiore digitalizzazione introdotta all'interno dei processi produttivi, ma al momento li considerano ancora strategicamente poco rilevanti.

Infatti, i processi adottati nella gestione della Cybersecurity OT risultano ancora in media scarsamente strutturati, determinando un'incapacità da parte delle aziende di identificare le minacce (risk analysis) a carico degli impianti produttivi e le loro

probabilità di accadimento. Questo comporta una tendenza a non effettuare investimenti specifici in questo ambito, come dimostra il grafico sottostante:



Le imprese non solo non effettuano investimenti specifici volti a migliorare la sicurezza cyber degli impianti produttivi, ma nella maggior parte dei casi non considerano nemmeno le performance in ambito Cybersecurity come un driver fondamentale nella scelta di un nuovo impianto produttivo e del relativo fornitore (vedi grafico).

Il quadro non migliora se analizziamo i prosumer, ovvero le imprese industriali che hanno installato anche impianti per la produzione dell'energia elettrica. Pure in questo caso la consapevolezza delle minacce provenienti dal cyberspazio è estremamente ridotta, così come la percezione dei possibili impatti sulle attività "core".

CONCLUSIONI

E' evidente la necessità per le aziende del comparto di dotarsi di un adeguato sistema di governance della cybersecurity, ovvero di un insieme di soluzioni tecnologiche e organizzative in grado di garantire un adeguato livello di protezione da questo tipo di minacce. Le misure da adottare sono molto diverse, a seconda che si tratti di protezione delle apparecchiature e dei sistemi già installati o, al contrario, di nuovi asset. In particolare, nel primo caso è fondamentale non andare a interferire eccessivamente con l'operatività, in quanto nell'ambito delle operations la disponibilità delle risorse (e quindi dei dati necessari per il funzionamento degli apparati) è di fondamentale importanza e"domina" gli altri due requisiti tipici della sicurezza informatica, ovvero integrità e riservatezza.

Questo comporta lo sviluppo di approcci diversi rispetto a quelli tradizionalmente in uso in ambito IT, in cui invece l'integrità e la riservatezza dei dati sono prioritari. Per quanto riguarda i nuovi asset, invece, è fondamentale agire in ottica "design for security", adottando specifici criteri di progettazione dell'apparato/impianto e dei suoi componenti che tengano conto anche dei valori target delle prestazioni di sicurezza, lungo tutta la vita utile dell'asset.

In tale ambito un ruolo fondamentale spetta agli standard, che infatti stanno vivendo una fase di grande sviluppo. Come sempre in simili casi, è nato il dibattito sull'opportunità o meno di rendere obbligatoria l'adozione di almeno alcuni di tali standard. Un tema delicato, in quanto l'efficacia dell'intervento normativo dipende dalla "snellezza" dei processi necessari per ottenere la compliance: un'eccessiva focalizzazione sugli aspetti formali potrebbe rendere troppo lungo e oneroso il processo di omologazione dei nuovi prodotti, con il conseguente rischio di ostacolare o comunque rallentare l'innovazione. Inoltre, si rischierebbe probabilmente di danneggiare le PMI, tipicamente non strutturate per sopportare carichi di lavoro troppo elevati su questo tipo di attività.