

17.03.22

La sicurezza informatica nell'energia: rischi e opportunità della generazione distribuita

Video intervista a Giovanna Dondossola, leading scientist di Rse e responsabile del progetto integrato "Cybersecurity per sistemi energetici".



Ascolta il podcast dell'intervista:

<https://www.qualenergia.it/pro/articoli/sicurezza-informatica-energia-rischi-opportunita-generazione-distribuita/>

Nonostante oggi le **tecnologie per la sicurezza informatica** applicata al settore energetico siano sufficientemente **mature** per garantire un livello di protezione adeguato, sono aumentate parallelamente anche le tipologie di codici malevoli che possono insinuarsi nei sistemi, sfruttandone le vulnerabilità.

17.03.22

Abbiamo parlato di questi temi con la dottoressa **Giovanna Dondossola**, Leading scientist di **Rse** e responsabile del progetto integrato “*Cybersecurity per sistemi energetici*” (video e audio in basso), facendo il punto sullo stato attuale delle tecnologie per la cybersecurity del settore energetico, soprattutto alla luce della sempre maggiore diffusione della generazione distribuita da fonti rinnovabili.

La prospettiva di un **sistema energetico decentralizzato e interconnesso**, composto da un numero crescente di reti di **prosumer** che autoproducono gran parte dell’energia di cui hanno bisogno con fonti rinnovabili e che condividono questa energia anche all’interno di comunità energetiche o offrono servizi di stabilità alla rete, rappresenta sia un **rischio** che un’**opportunità** per la sicurezza del sistema elettrico nel suo complesso (vedi dal min. 29 del video).

Nel corso dell’intervista abbiamo analizzato i **rischi** e le **modalità** con cui spesso avvengono questi attacchi, con **conseguenze** che riguardano sia la **fornitura di energia** che la protezione dei dati sensibili degli utenti, esposti anche tramite le **reti domestiche** attraverso le apparecchiature per la gestione dei carichi e il monitoraggio degli impianti Fer.

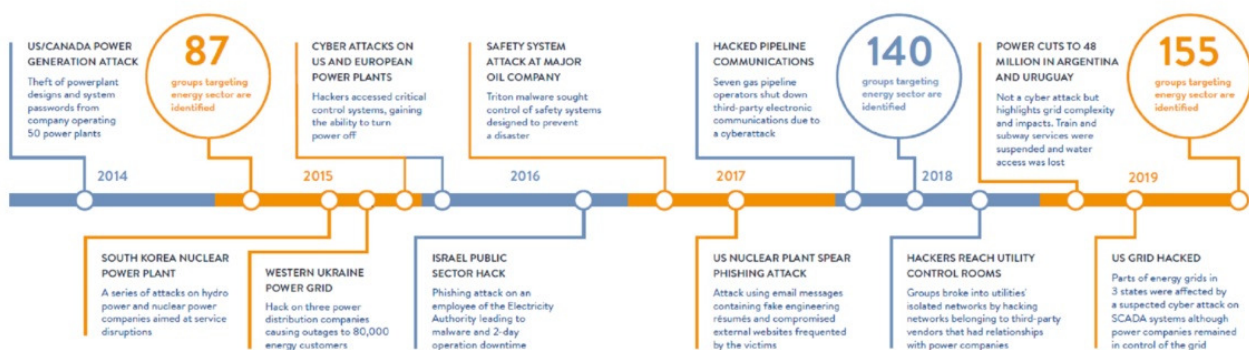
Nell’ottica di un aumento della generazione distribuita, ci spiega Giovanna Dondossola, un **maggior numero di prosumer** comporterà la crescita dell’estensione della superficie energetica digitale interconnessa (e quindi attaccabile), facendo **salire la probabilità di cyber attack**.

Ma se ogni elemento della catena fosse protetto da un’infrastruttura di sicurezza informatica adeguata, la **generazione decentralizzata** potrebbe garantire una **maggiore sicurezza del sistema nazionale**, permettendo di isolare le aree di rete “infettate”.

Questo però è **solo uno scenario ipotetico** e da analizzare in prospettiva, che andrà sperimentato quando realtà come ad esempio le comunità energetiche usciranno dalla fase “pionieristica” in cui sono ora nel nostro Paese.

Attacchi sempre più diffusi

I dati sugli attacchi informatici alle infrastrutture sono riservati e non divulgabili, ma da quanto si evince dai rapporti sugli episodi avvenuti a livello internazionale negli ultimi anni, il **trend** generale è in **aumento** (si veda il grafico elaborato dal World Energy Council).



17.03.22

Già nel 2018 RSE segnalava in un dossier che i principali rischi da affrontare in questo ambito fossero sostanzialmente legati al processo di **digitalizzazione delle infrastrutture**, richiesto dalla **transizione energetica** che caratterizzerà anche il prossimo decennio.

La società del Gestore dei Servizi Energetici si riferisce, in particolare, ai sistemi riguardanti l'esercizio degli impianti, come le **stazioni elettriche** o gli **impianti di generazione** e di carico che comprendono **impianti di grossa taglia** e risorse energetiche distribuite connesse in media e bassa tensione, in particolare risorse di generazione da fonti rinnovabili, infrastrutture di ricarica e di accumulo dei veicoli elettrici caratterizzate da un profilo elettrico imprevedibile dovuto alla mobilità dei veicoli, **sistemi di gestione flessibile della domanda** o che forniscono all'operatore di rete servizi necessari a garantire la sicurezza dell'intero sistema elettrico, funzionali anche alla gestione in sicurezza di un sistema energetico sostenibile.

Di seguito una classificazione – fornita da ENISA (l'Agenzia Europea sulla cybersecurity) – dei principali tipi di attacco informatico che possono interessare anche il settore energetico, colpendo *in primis* le **imprese** che operano in questo settore per **compromettere il funzionamento dei sistemi energetici**:

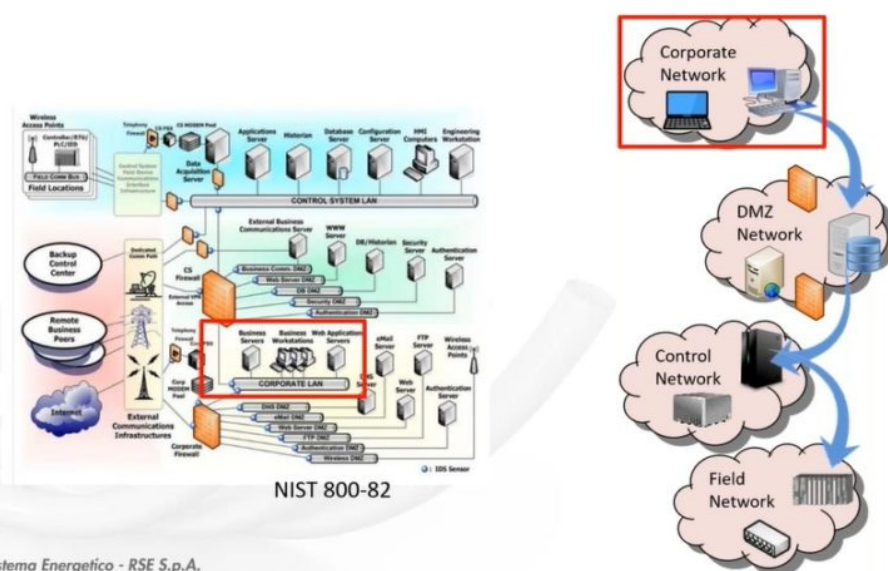
Figure 1: ENISA Threat Landscape 2021 - Prime threats



L'azione "malevola" verso i sistemi OT (Operational Technology) – spiega Dondossola – spesso viene veicolata da un'**intrusione iniziale in una rete informatica aziendale** e, attraverso le connessioni di rete, il contagio si sviluppa nell'infrastruttura di controllo del sistema elettrico.

17.03.22

PROCESSI DI ATTACCO



Ricerca sul Sistema Energetico - RSE S.p.A.

A livello nazionale – ci spiega la Leading scientist di RSE – è importante quindi implementare dei sistemi di monitoraggio della sicurezza che permettano di intercettare le minacce e di bloccarle prima che possano insinuarsi nella rete energetica e comprometterne il funzionamento, **come nel caso “Blackenergy” in Ucraina**, che nel 2015 ha coinvolto tre società di distribuzione, provocando il distacco di 27 stazioni elettriche, disalimentando 230.000 utenze per diverse ore. Un evento che ha segnato la storia del crimine informatico verso le utility elettriche.

A **livello domestico**, c'è invece un lavoro su più livelli da portare avanti. Partendo da una sensibilizzazione degli utenti che già in fase di acquisto possono richiedere maggiori informazioni sui livelli di sicurezza garantiti dagli apparecchi e che possono poi curarsi di impostare password adeguate e, quando possibile, richiedere la doppia autenticazione per l'accesso ai dispositivi.

È inoltre fondamentale – ha concluso la dottoressa Dondossola – che per questi apparecchi sia garantito un **aggiornamento automatico e remoto** perché possano sempre essere in grado di filtrare e bloccare i modi di attacco più recenti.