QUOTIDIANO ENERGIA

**ROMA**, 26 settembre 2018 Ricerca - Sistema energetico

# Cybersecurity, la spinta normativa e il ruolo della ricerca

## L'importanza di equiparare i livelli di sicurezza in una filiera elettrica in continua evoluzione, tra digitalizzazione, rinnovabili e prosumer

di G. Dondossola*

Che le reti elettriche siano vulnerabili e possano subire i danni degli attacchi informatici ormai è un rischio accertato. Il blackout avvenuto a dicembre 2015 in Ucraina che ha coinvolto tre società di distribuzione provocando il distacco di 27 stazioni elettriche disalimentando 230.000 utenze per diverse ore ha segnato la storia del crimine informatico verso le utility elettriche. Come evidenziato dall'analisi del caso di attacco reale, l'azione malevola verso i sistemi OT (Operational Technology) veniva veicolata da azioni malevole verso i sistemi IT (Information Technology) della rete corporate aziendale.

I big player concordano sul fatto che la cybersecurity è una dimensione irrinunciabile per il business dell'energia e il welfare della nazione, che necessita cooperazione tra operatori energetici, fornitori di prodotti e di servizi digitali. Per i grandi operatori il metodo è tracciato: occorre procedere con la classificazione degli asset, la scelta delle misure di sicurezza organizzative e tecniche commisurate al livello di rischio, le richieste di conformità agli standard di cybersecurity e di certificazione verso i fornitori di prodotti e servizi.

A livello istituzionale, la Strategia energetica nazionale (Sen) fa riferimento allo schema nazionale di cybersecurity, partendo dal decreto della presidenza del Consiglio dei ministri (Dpcm Gentiloni del 17 febbraio 2017) che ne definisce l'architettura e i ruoli delle istituzioni preposte alla sua implementazione in collaborazione con i fornitori dei servizi essenziali. Il decreto Gentiloni ha anche promosso la costituzione di un Centro di Valutazione e Certificazione Nazionale (Cvcn) per la verifica dell'affidabilità della componentistica ICT utilizzata nelle infrastrutture critiche e strategiche.

In tema di regolamentazione della cybersecurity per il settore energia il riferimento è il recente decreto legislativo n. 65, entrato in vigore il 24 giugno 2018, il quale costituisce l'attuazione italiana della direttiva europea Nis (EU 2016/1148) sulla sicurezza delle reti e dei sistemi digitali, praticamente gemella della Gdpr, ossia della regolamentazione sulla

protezione dei dati sensibili, la cui entrata in vigore non è certamente passata inosservata a nessuno di noi.

Un primo fondamentale provvedimento stabilito dal D.Lgs è che entro il 9 novembre 2018 dovranno essere identificati tutti i fornitori di servizi essenziali, quali quelli energetici, soggetti agli obblighi in materia di sicurezza e notifica degli incidenti indicati dall'articolo 14, e alle relative sanzioni amministrative in caso di inadempienza di cui all'articolo 21. Il decreto stabilisce che tali obblighi non si applicano alle micro imprese e alle piccole imprese che in base alla definizione contenuta nella raccomandazione della Commissione europea n.2003/361/CE, sono tutte quelle imprese che occupano meno di 50 persone e realizzano un fatturato annuo o un totale di bilancio annuo non superiori a 10 milioni di euro.

Quali e quanti produttori di energia, prosumer o aggregatori rientreranno nella categoria piccola impresa esente dagli obblighi di cybersecurity imposti dal decreto?

Ma soprattutto che impatto provocherebbe un eventuale incidente cyber in termini di megawatt non forniti al sistema elettrico o di carico non assorbito?

Quanti e quali utenti subirebbero un disservizio prolungato a causa di un attacco sufficientemente distribuito in termini di superficie cyber? Si consideri ad esempio un sistema elettrico decentralizzato la cui architettura ICT è riportata in Figura 1.

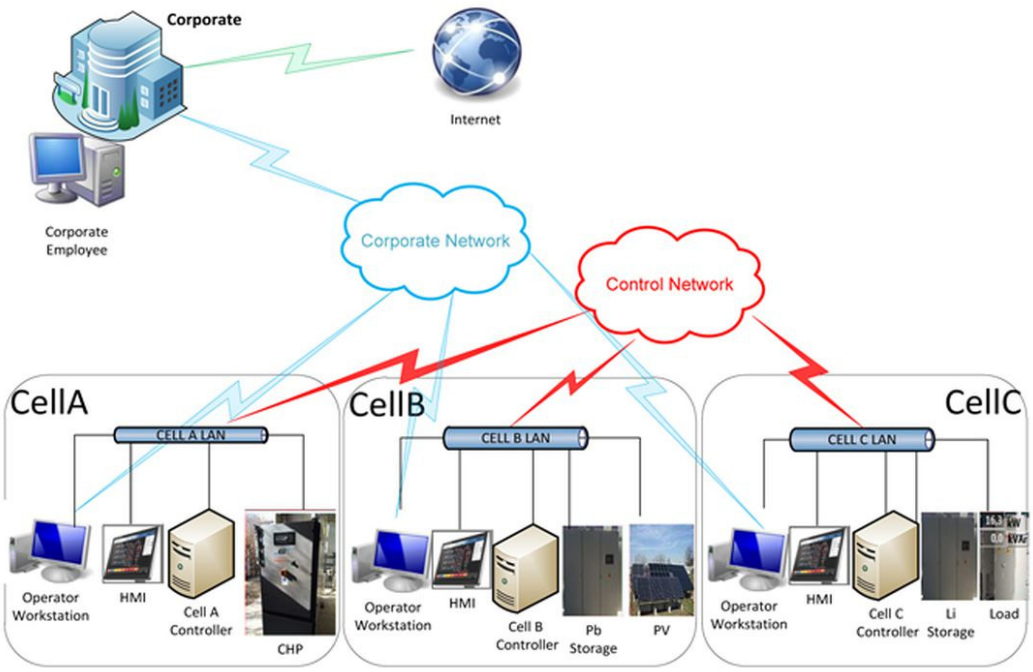


***Figura 1 – Architettura ICT di un sistema elettrico decentralizzato***

Riguardo alla possibilità che questi sistemi subiscano gli effetti di un attacco cyber (Figura 2), se guardiamo alla casistica delle vulnerabilità note, possiamo rilevare dati inquietanti: i risultati estraibili dai motori di ricerca rilevano che diversi impianti sono piuttosto esposti, visibili e controllabili da Internet senza alcun grado di protezione.

La strada per l'attaccante è praticamente tracciata.

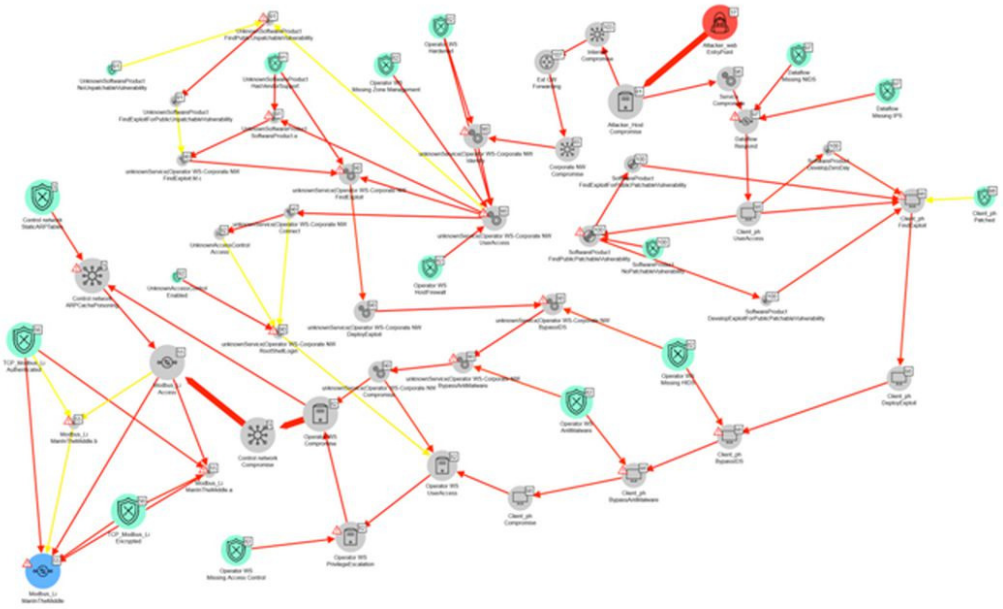

***Figura 2 – Grafo degli attacchi cyber relativi all'architettura riportata in Figura 1***

Si ravvisa una disparità di livello di sicurezza tra i sistemi di controllo dell'infrastruttura elettrica e quelli degli impianti di potenziali fornitori di servizi di flessibilità. E' più che plausibile supporre che il livello di maturità in termini di sicurezza di questi impianti sia molto inferiore al livello medio utilizzato per la gestione dei rischi cyber dagli operatori di rete.

Per questo motivo si sta ponendo un'attenzione specifica alla cybersecurity dei titolari di questi impianti.

A livello italiano, la norma CEI 0-16, attualmente in corso di sviluppo, che definisce le regole tecniche per la connessione di utenti attivi alle reti in alta e media tensione, recepisce gli standard di cybersecurity più recenti e prevede la messa in sicurezza delle comunicazioni tra il controllore dell'impianto e i soggetti esterni che vi possono accedere da remoto, ad esempio un soggetto aggregatore.

La norma CEI 0-16 nasce come specifica per i controllori centrali di impianti di generazione o di sistemi di accumulo, ma in prospettiva è prevedibile una sua evoluzione che la renda

applicabile anche ai cosiddetti carichi flessibili e ai consumatori che sono anche produttori, perché dotati ad esempio di impianti di co-generazione o di sistemi di accumulo. La normativa per la partecipazione della domanda ai nuovi mercati prevede che anche questi interlocutori siano soggetti a vincoli di cybersecurity per le comunicazioni verso gli operatori di rete o gli aggregatori.

La stessa Sen, nel capitolo dedicato alla cybersecurity, sottolinea come prima linea di azione la necessità di svolgere attività di ricerca e sviluppo e vede Rse coinvolta in primo piano nello svolgimento del programma finanziato dal fondo della Ricerca di Sistema, e finalizzata a produrre strumenti di valutazione dei rischi e misure di sicurezza idonee all'esercizio di sistemi energetici eterogenei sia dal punto di vista elettrico che digitale. In Figura 3 è mostrato il laboratorio di cybersecurity di Rse ed in Figura 4 il relativo “word cloud”.

Il piano della ricerca nel settore elettrico affronta aspetti di cybersecurity negli scenari energetici futuri, che comprendono impianti di generazione da fonti rinnovabili, aggregatori, prosumer, valutando la resilienza dei nuovi schemi di controllo, l’integrazione di nuove tecnologie e standard di cybersecurity per fornire una risposta adeguata ad eventuali nuove minacce.

Il piano di ricerca affronta le sfide di cybersecurity dei sistemi elettrici sviluppando strumenti per accelerare l’innovazione tecnologica richiesta agli operatori energetici, ai fornitori di servizi digitali e di telecomunicazione.

Gli asset del piano di ricerca includono strumenti per la specifica e la valutazione della sicurezza informatica, piattaforme sperimentali IT/OT per la sicurezza end-to-end delle comunicazioni su tecnologie di rete eterogenee, sistemi di monitoraggio della sicurezza in tempo reale e rilevamento delle anomalie, funzioni di cyber-resilienza integrate in scenari di controllo elettrico.

Un contributo fondamentale del piano di ricerca è relativo all’evoluzione degli standard per le comunicazioni del settore energetico, alla loro implementazione e certificazione in prodotti e soluzioni IT/OT/IoT, competenze di cui possono avvalersi anche i regolatori dell'energia e i responsabili politici a livello europeo e nazionale.

***Figura 3 – Laboratorio di cybersecurity di RSE***

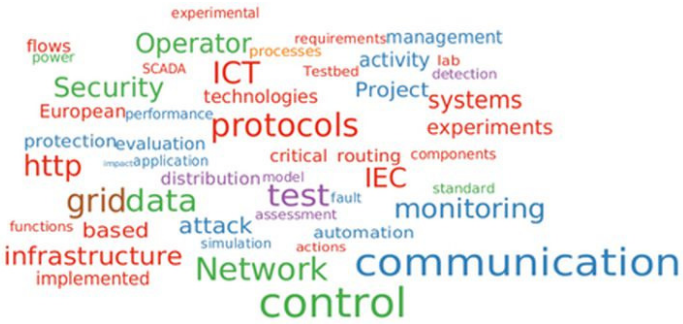


***Figura 4 - Word cloud del laboratorio di cybersecurity di RSE***

***Dipartimento Tecnologie di Trasmissione e Distribuzione**
**Rubrica a cura di Claudia Imposimato**

TUTTI I DIRITTI RISERVATI. È VIETATA LA DIFFUSIONE E RIPRODUZIONE TOTALE O PARZIALE IN QUALUNQUE FORMATO.
Privacy policy (GDPR)
www.quotidianoenergia.it