DOSSIERSE

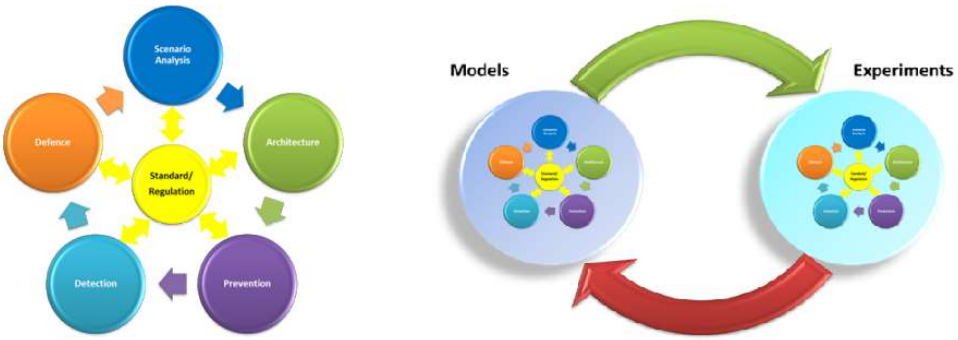
10/2019 Cybersecurity nella transizione energetica e digitale

SINTESI

Il grande pubblico ha conosciuto i pericolosi effetti di attacchi informatici alle reti elettriche nel dicembre del 2015. Durante il conflitto fra Ucraina e Russia un gruppo di hacker violò i sistemi di controllo della rete elettrica nella regione occidentale ucraina Ivano-Frankivsk e attraverso l'uso di malware portò al distacco di oltre 230.000 utenze. Quell'attacco informatico, organizzato in modo da ritardare le risposte dei clienti e dell'assistenza tecnica delle società energetiche, fu un chiaro monito dei rischi legati alla mancanza di azioni di prevenzione e di sicurezza nei sistemi informatici di gestione delle reti energetiche.
Proprio di questo si occupa la cyber security, la disciplina che studia come limitare i rischi che attacchi di questo tipo possono portare all'approvvigionamento energetico e alle gestione dei dati degli utenti.

Se da un lato la digitalizzazione delle reti porta con sé benefici, in termini di servizi e prestazioni, a questi fanno da contraltare i rischi in termini di sicurezza dell'operatività messa maggiormente a rischio proprio dall'impiego di tecnologie digitali.
Oggi i requisiti di autenticazione, autorizzazione, integrità e tracciabilità delle operazioni nelle reti informatiche si basano principalmente su algoritmi crittografici e richiedono sistemi di gestione di chiavi e certificati elettronici. I requisiti di disponibilità sono invece principalmente gestiti mediante tecniche di segregazione delle reti, sistemi di controllo del traffico (firewall), protezioni antivirus e tecniche di ingegneria dei sistemi per la gestione della ridondanza. Complementari alle misure di prevenzione della sicurezza, sono le pratiche di monitoraggio della sicurezza basate sull'utilizzo di sistemi per il rilevamento delle intrusioni e per la gestione degli eventi di sicurezza.
I quesiti aperti riguardano l'impatto provocato da un eventuale incidente cyber in termini di megawatt non forniti al sistema elettrico o di carico non assorbito. E ancora quanti e quali utenti subirebbero un disservizio prolungato a causa di un attacco sufficientemente distribuito in termini di superficie cyber.

Per dare risposte a queste domande RSE svolge attività di ricerca, finanziate dal Fondo per la Ricerca di Sistema, in questo ambito strategico e fondamentale per il Paese. Progetti che riguardano la sicurezza delle infrastrutture esistenti, ma soprattutto, gli scenari energetici futuri, l'interazione fra i sistemi informatici (IT) e quelli di operation (OT) e la necessità di renderli interoperabili, l'utilizzo di piattaforme aperte basate su tecnologie IoT (Internet of Things) e servizi edge e cloud.
La stessa SEN sottolinea la necessità di attività di ricerca e sviluppo sulla cybersecurity per produrre strumenti di valutazione dei rischi e misure di sicurezza idonee all'esercizio di sistemi energetici eterogenei sia dal punto di vista elettrico sia digitale.



Il framework di analisi della resilienza dei sistemi cyber-fisici

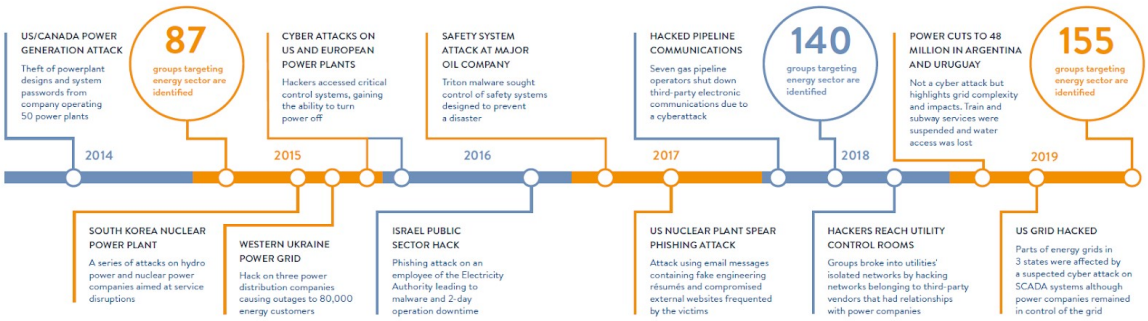
Dalle analisi svolte da RSE si evince una certa disparità fra i livelli di sicurezza dei sistemi di controllo dell'infrastruttura elettrica e quelli degli impianti di potenziali fornitori di servizi di flessibilità. Si può supporre quindi che la maturità, in termini di sicurezza cyber, degli impianti di generazione distribuita attualmente connessi alla rete di distribuzione sia inferiore al livello medio utilizzato per la gestione dei rischi dagli operatori di rete. In linea con le direttive europee, secondo ARERA è necessario inserire nei regolamenti nazionali livelli di sicurezza cyber relativi allo scambio dati con i nuovi impianti, ma anche con gli impianti, di potenza superiore a 1 MW, già connessi alla rete di MT.
RSE prende in considerazione schemi di rete con una massiccia presenza di impianti di generazione da fonti rinnovabili, aggregatori, prosumer e sviluppa sistemi di valutazione della resilienza dei nuovi schemi di controllo, che integrano nuove tecnologie e standard di cybersecurity per fornire una risposta adeguata all'evoluzione delle minacce.

Un ulteriore campo di azione delle ricerche di RSE è riferito allo sviluppo di modelli di simulazione e piattaforme evolute di raccolta e analisi di dati rilevanti per la cyber security basate sull'applicazione di tecniche di machine e deep learning. Queste consentono di comprendere il comportamento dei sistemi di controllo e di valutare software prototipali per il monitoraggio della sicurezza in tempo reale e il rilevamento tempestivo di anomalie.
Le funzioni di detection consentono di sviluppare strategie di recovery che RSE integra a scopo dimostrativo in scenari di controllo elettrico.

I risultati della ricerca RSE sono destinati a operatori energetici, a sviluppatori di prodotti hardware e software e a fornitori di servizi digitali e di telecomunicazione per consentire un'accelerazione del processo di innovazione tecnologica richiesta dalla transizione energetica. Il percorso di collaborazione avviato da RSE con le principali imprese nazionali ha reso possibile l'adozione di principi e pratiche derivate dalle analisi e dalla sperimentazione, in un ciclo sinergico tra innovazione industriale e risultati della ricerca, tenendo conto degli opportuni feedback. Un lavoro fondamentale per poter contribuire alla sicurezza di un sistema nel perimetro della sicurezza nazionale sempre più spesso oggetto dell'attenzione di soggetti potenzialmente in grado di attaccarlo.

Nel 2019 il rapporto "Cyber challenges to the energy transition" del World Energy Council ha identificato nel mondo 155 gruppi potenzialmente pericolosi per la sicurezza digitale del

sistema energetico, rispetto agli 87 di inizio 2015. Una tendenza che fa riflettere sulla necessità di potenziare gli sforzi della ricerca e le azioni di salvaguardia della sicurezza delle infrastrutture energetiche.



Gli incidenti informatici aumentano sia in frequenza che in impatto

Fonte: www.dossierse.it