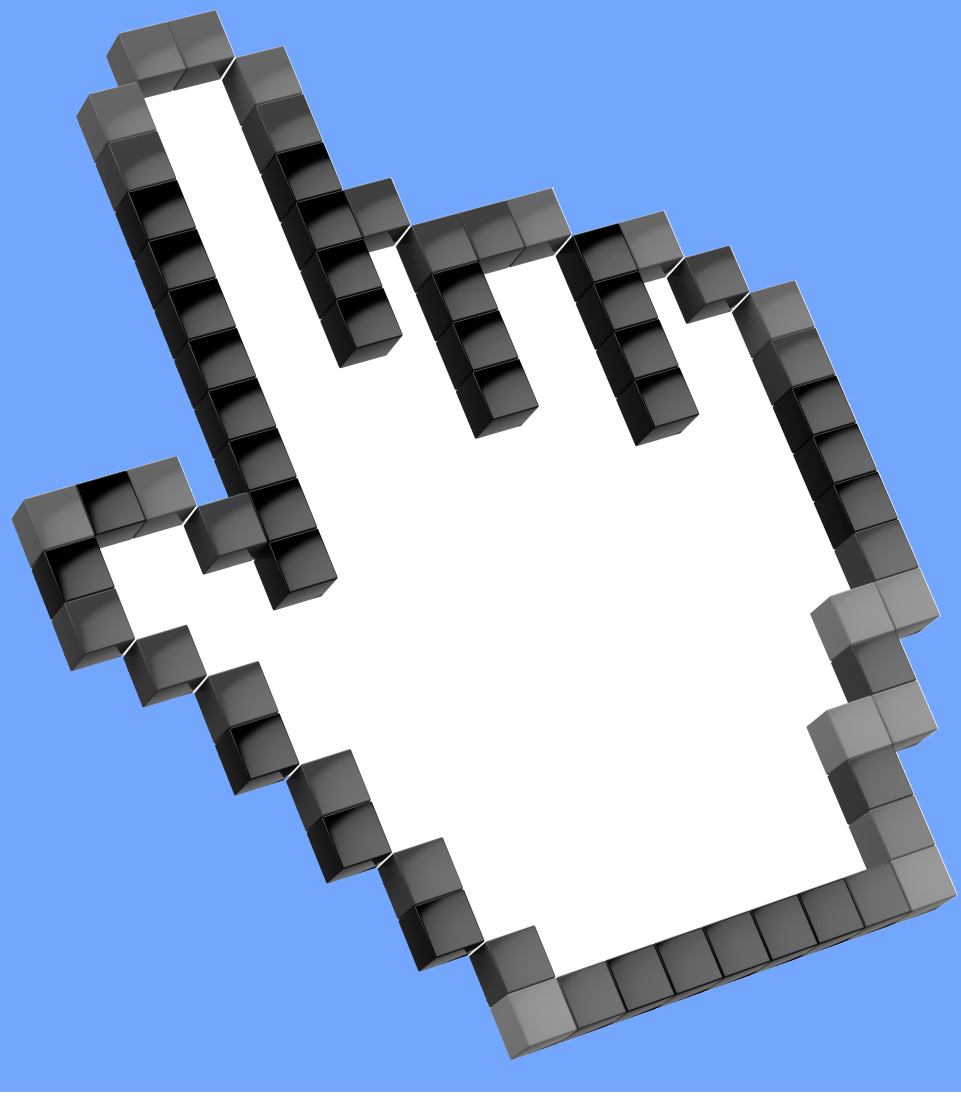
Cyber Security Energia

Un fattore di forte impatto sul valore economico di utility ed energy company



ENERGIAMEDIA

Energia Media

Energia Media è un'agenzia di comunicazione e relazioni che opera, principalmente, nei settori energy, utility e smart city.
Sviluppa strategie comunicative, facilita le relazioni, elabora contenuti e informazione.
Sostiene le aziende migliorandone il posizionamento e creando occasioni di business. Affianca associazioni e istituzioni in programmi di comunicazione pensati per aumentare la reputazione nei confronti dei propri stakeholder.
Energia Media nasce nel 2013, a Milano, dall'esperienza maturata da un gruppo di persone in oltre vent'anni di lavoro nel campo dell'informazione, delle relazioni e della consulenza strategica nei settori energy e utility.

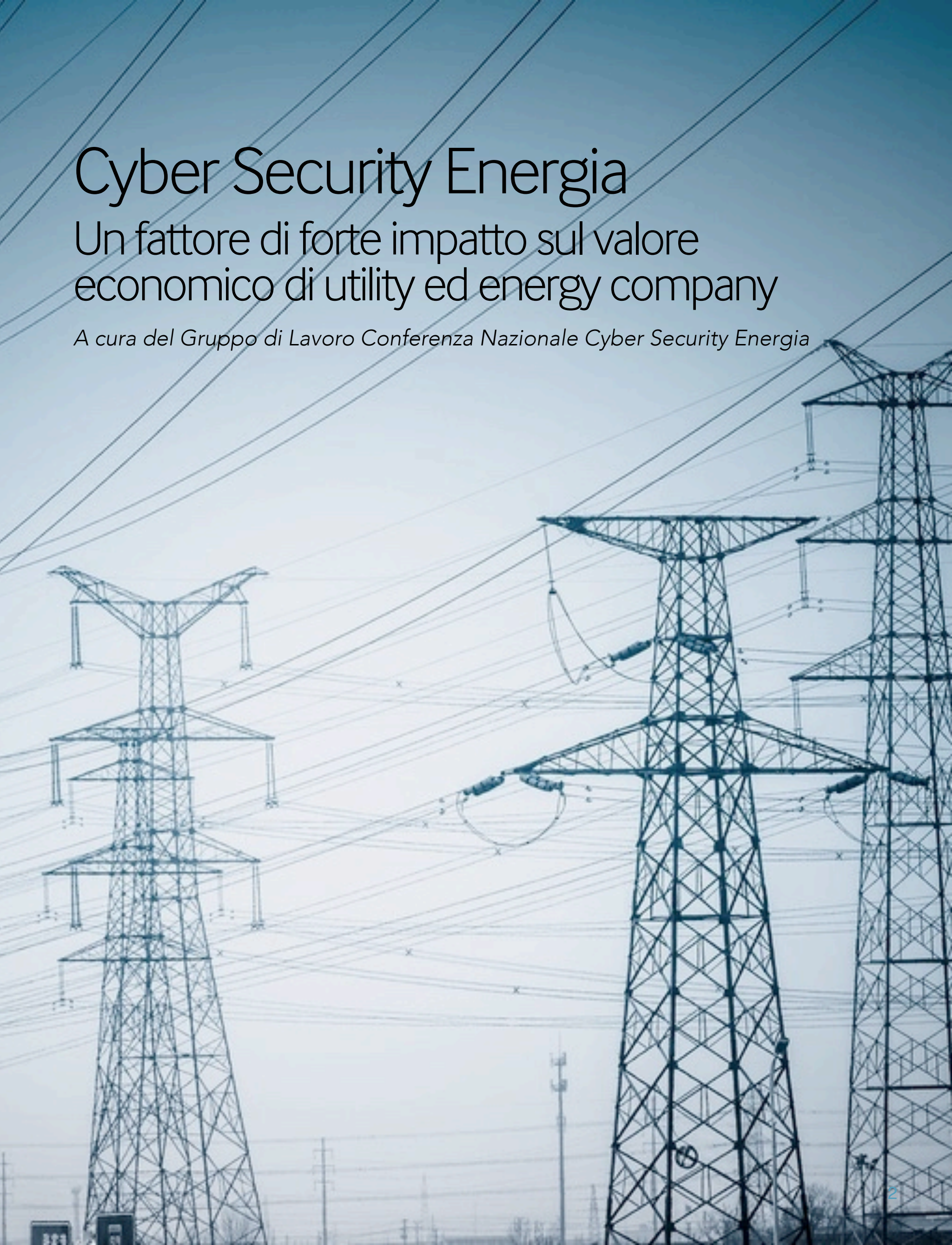
Tutte le immagini e fotografia presenti in questo Paper sono state regolarmente acquistate su banche dati. Nel caso in cui l'autore ritenga che siano state violate le regole di copyright, è pregato di segnalarlo al seguente indirizzo:
comunicazione@energiamedia.it

©Energia Media - gennaio 2016

Cyber Security Energia

Un fattore di forte impatto sul valore economico di utility ed energy company

A cura del Gruppo di Lavoro Conferenza Nazionale Cyber Security Energia



Nota introduttiva

Dopo la 2ª Conferenza Nazionale Cyber Security Energia (CSE), svoltasi a Roma il 24 settembre 2015, il Ministero dello Sviluppo Economico ha incoraggiato il Gruppo di Lavoro (GdL CSE) - costituitosi grazie all'iniziativa di Energia Media - nel proseguire in modo intenso con l'attività di divulgazione e di scambio di esperienze tra società fornitrici di tecnologie e servizi, utility ed energy company.

Ad oggi, sul tema in oggetto, si registrano enormi vuoti culturali e normativi che dovranno essere colmati da un'azione formativa e informativa pensata ad hoc per uno fra i segmenti più strategici per il Paese. A questa carenza si aggiunge una diffusa sottovalutazione del rischio derivante dalla scarsa considerazione per la sicurezza informatica dei sistemi.

La cyber security impatterà sempre di più sul valore economico delle società, sullo svolgimento delle rispettive attività e sui comportamenti di ogni membro dell'organizzazione aziendale. Il fatto che, a partire da gennaio 2016, Moody's aggiungerà la sicurezza informatica fra i criteri di valutazione per l'assegnazione dei rating alle imprese (e così sarà per i singoli Stati) rafforza la correttezza di questa previsione.

La sicurezza informatica passa, dunque, dall'essere una questione di esclusiva o quasi pertinenza dei settori IT a un tema di primaria rilevanza per il top management delle aziende, dal CFO al marketing manager fino al CEO.

Domande aperte totalmente irrisolte

Ad oggi, quant'è - pienamente - compreso il valore dei dati? Esiste un controllo sul flusso di dati iniettati (e ricavati) sulle reti elettriche, gas, acqua? C'è certezza della loro qualità? E come sono gestiti quelli rilevati da smart meter abilitati - tra l'altro - a tracciare i consumi delle famiglie?
È davvero chiaro, poi, quale sia l'impatto della cyber security sulle smart city, con dati che viaggiano su power line? Quanto se ne ha piena e reale consapevolezza? Come viene valorizzato l'ambito "infrastrutture critiche" (la cui definizione peraltro è diversa da una nazione all'altra e ogni direttiva rimanda al legislatore locale)?
Inoltre, in termini di analisi dei dati di vendita tra competitor, si è certi della qualità e della sicurezza degli stessi? Si tratta di dati che impattano sulle strategie di marketing e commerciali; un ambito che riguarda - tra le altre - le società di vendita d'energia.
Domande che presuppongono un'attenzione particolare alla cyber security ma alle quali oggi - in moltissimi casi - non viene data risposta; nemmeno da parte delle società quotate in borsa, la cui sensibilità al tema dovrebbe essere naturale, scontata. Per esempio, tutte le imprese del settore idrico utilizzano sistemi di tipo SCADA, che generano *big data*, e che necessitano di strumenti per gestire dati di cui non conoscono appieno il significato.
Inoltre, esistono enormi vuoti normativi, che vanno anche a interessare ambiti come i trasporti, l'internet industrial, il concetto di fabbrica 4.0 e l'IoT in genere. È sufficiente pensare a quanto le tecnologie di telecontrollo e telecomunicazioni possano contribuire a una gestione ottimale delle future smart city per comprendere l'im-

portanza di mettere in sicurezza i dati relativi a quell'ambito. Generalmente, la rilevanza della sicurezza informatica viene compresa appieno solamente quando questa viene a mancare, durante le situazioni di crisi. A ciò si aggiunge una mancanza di chiarezza nei ruoli, in special modo sulle figure professionali che all'interno delle organizzazioni dovrebbero occuparsi del tema cyber security. In questo senso l'interesse mostrato dalle utility è marginale. Un incrocio ragionato dei dati - declinato per energia, acqua, illuminazione, trasporti, ecc. - potrebbe favorire una governance complessiva in grado di dare orientamenti, fare politiche, fornire indirizzi, dare direttive.
È fondamentale, tuttavia, poter disporre di una misura sicura e incontestabile; solamente con meter certificati si avranno dati corretti. L'analisi dei dati rimane la base concreta - tecnologicamente e culturalmente possibile - su cui operare a più livelli in termini decisionali. Quando gli operatori tecnologici propongono assestment sui temi della cyber security in ambito telecontrollo delle reti o per l'automazione industriale nella maggioranza dei casi vengono ignorati, dimostrando ancora una volta l'ampia sottovalutazione dei rischi corsi da parte dei vertici aziendali. Gli stessi progetti di cyber security non vengono attuati, rimanendo per lo più delle volte su carta. Alla sottovalutazione del rischio è possibile aggiungere la scarsa comunicazione tra CSO, CEO e CFO sui temi della sicurezza. In questo senso elemento chiave per un cambiamento potrebbe essere il già menzionato criterio di sicurezza informatica introdotto da Moody's per l'assegnazione dei rating. Gli indicatori valoriali nel controllo di gestione delle società (come il brand o le professionalità dei propri addetti, per i quali esistono standard europei) e il supply chain management, dovrebbero ormai comprendere la cyber security. In definitiva si può affermare che il panorama del settore energy & utility registri molti parallelismi con il mondo degli istituti di credito di 15-20 anni fa, cioè prima che venissero intraprese decise azioni di modernizzazione nella gestione. Efficientare le infrastrutture è un obbligo, magari anche con la creazione di un CERT Industry realizzato sull'esempio statunitense dell'ICS-CERT (The Industrial Control Systems Cyber Emergency Response Team), che in parallelo veda nascere dei servizi consortili per le imprese.

Gli obiettivi del Gruppo di Lavoro CSE

Ci si è posti l'obiettivo di fare da trait d'union tra istituzioni e aziende, e tra imprese tecnologiche, energy company e utility. I ministeri dello Sviluppo Economico (tra cui il diparti-

mento degli approvvigionamenti energetici diretto dall'ingegner Gilberto Dialuce), delle Telecomunicazioni, della Difesa, l'ISCOM, hanno l'esigenza di meglio comprendere cosa le aziende stiano facendo a fronte del CERT Nazionale, anche in funzione del lavoro che verrà svolto all'interno del Tavolo di coordinamento costituitosi presso il Ministero dello Sviluppo Economico (Mise).

Portare all'attenzione best practice, per arrivare alla definizione di regole comportamentali condivise, è quanto mai urgente, soprattutto laddove si parli - come in questo caso - di interdipendenze, di vasi comunicanti tra tematiche diverse, di sistemi di sistemi. Ugualmente urgente è dare un contributo anche per la produzione di bozze normative armonizzate a livello internazionale.

Il nostro sistema di governo delle utility sconta un difetto di programmazione. Ad esempio, in Italia non si vede traccia di un analogo piano di investimenti sulle perdite nel settore idrico al pari di quello realizzato nel Regno Unito (con obiettivi quinquennali a cui dovranno obbligatoriamente sottostare le 16 utility locali). Il percorso intrapreso dell'Autorità per l'energia elettrica il gas e il servizio idrico (Aeegsi) favorirà investimenti in innovazione sull'acqua nei prossimi anni, anche in funzione del processo di aggregazione tra imprese che il settore dovrà affrontare. In entrambi i casi, sia dunque che si parli di Regno Unito o Italia, si va incontro a un processo di non ritorno verso una piena convergenza tra servizi pubblici locali qualsiasi essi siano (acqua, energia, trasporti, rifiuti, ecc.) e IT, con una conseguente centralità del tema cyber security. La sicurezza dei sistemi idrici - per rimanere sull'esempio di prima - risulta ampiamente sottovalutata, e si è già potuto riscontrare come spesso proprio il carattere interministeriale di alcune tematiche faccia morire ogni possibile introduzione di nuove regole.

Il Gruppo di Lavoro e la Conferenza Nazionale CSE - iniziative favorite da Energia Media - possono aiutare l'introduzione di "pilota" che le aziende tecnologiche si candidano a sostenere e a implementare; con una visibilità anche su eventuali bandi europei adatti al coinvolgimento di Piccolo Medie Imprese (PMI). Ci si propone di supportare il nuovo Framework Nazionale per la Cyber Security che verrà presentato a Roma il 4 febbraio 2016 (www.cybersecurityframework.it), un tavolo permanente tra vendor, produttori, associazioni che da circa un anno già collaborano allo sviluppo del framework per definire il panorama sulla sicurezza informatica. L'obiettivo è fornire il prima possibile uno strumento agile e di facile utilizzo soprattutto per le PMI: 20 regole con semplici indicazioni da seguire per rendere più consapevole del tema tutto il settore (utility comprese).

Come far sì che le PMI trovino le risorse economiche necessarie per affrontare la questione cyber security? Serve probabilmente un meccanismo di pena/incentivo: "ti allacci alla rete per fare business solo se dimostri di esser sicuro". Un concetto qualitativo da introdurre nelle gare d'appalto a prova del fatto che la cyber security sia indice di qualità del servizio (si pensi al settore gas e alle concessioni 2016).
Mise, Aeegsi, Terna, Snam, sono gli abituali interlocutori di Energia Media in diversi ambiti e ancor più dovranno esserlo per il Gruppo di Lavoro CSE.
Terna, per esempio, dovrà implementare la cyber security per ogni RTU (Remote Terminal Unit), sicurezza informatica che dovrebbe entrare nel codice di rete approvato dall'Aeegsi. Un'azienda che sa come organizzarsi, cosa può o non può fare chi si allaccia alla rete; come muoversi all'interno del meccanismo "merit order", con premi e penalità sulle interruzioni. E in modo analogo dovrebbe agire Snam per il settore gas.
Anche istituzioni locali quali le Regioni italiane andranno adeguatamente sensibilizzate sulla questione della qualità dei servizi pubblici da mettere in relazione con la cyber security.
Il Gruppo di Lavoro CSE agirà nei confronti delle istituzioni il cui obbligo - ormai non più procrastinabile - dovrebbe essere quello di muoversi sul tema con grande determinazione.

Italia, infrastrutture energetiche e sicurezza informatica

Le grandi reti nazionali di elettricità (Terna) e gas naturale (Snam) e la logistica petrolifera (Eni) percorrono la penisola italiana sia lungo le linee di costa sia all'interno, collegando il proprio sud e quello Mediterraneo con il Centro Europa. Le reti continentali sono poi collegate con le grandi isole, Sardegna e Sicilia, estese circa 50.000 km2 rispetto ai 275.000 km del resto del Paese.

La lunghezza della Rete nazionale di trasmissione dell'elettricità è di 65.000 km; 500 le stazioni di smistamento. A questa rete sono allacciati 137 distributori locali in media e bassa tensione, che servono 37 milioni di punti di prelievo di elettricità. Alle reti di distribuzione, estese 1 milione e 250 mila km, sono anche collegati centinaia di migliaia di piccoli impianti fotovoltaici ed eolici. In pochissimi anni il sistema di produzione elettrica, basato su poche centinaia di centrali, ha superato le 800 mila unità produttive. Tutte queste reti e punti di prelievo e immissione sono tra loro collegati con sistemi di trasmissione dati.

Nel settore del gas naturale, utilizzato non solo per il riscaldamento delle abitazioni e per l'industria, ma anche per la produzione di elettricità, il solo gasdotto dall'Algeria è lungo ben 1.830 km dalla costa tunisina al principale centro di smistamento in Valle Padana (Minerbio). La rete nazionale è lunga 34.600 km, cui sono collegati 230 distributori locali che riforniscono 23 milioni di clienti attraverso una rete di 256.000 km. Della rete fanno parte anche 6.323 cabine e più di 95.000 gruppi di riduzione finale. I gasdotti che alimentano l'Italia da Olanda, Russia, Libia e Algeria sono 4 e 3 i rigassificatori, supportati nella loro funzione da 10 stoccaggi geologici.

Nell'ambito della filiera petrolifera e petrolchimica, i porti sedi di impianti costieri sono 40, i depositi di GPL (gas di petrolio liquefatto) 15, con circa 100 distributori, i depositi chimici 13, quelli di oli minerali 36 gestiti da una trentina di società. Le raffinerie, oggi solo costiere, sono 10 e gli stabilimenti petrolchimici 8, operati da circa 50 soggetti. Le basi logistiche, dalle quali i prodotti vengono inviati ai vari punti di consumo, sono 41. Circa 20.000 le stazioni di servizio di distribuzione dei carburanti raggiunte da autobotti e container ferroviari. Sono 6 gli oleodotti internazionali (con Svizzera, Austria e Slovenia) e una ventina quelli interni che collegano principalmente gli stabilimenti tra loro.

L'innovazione tecnologica necessita sicurezza

L'Italia è stato il primo Paese al mondo ad introdurre, a partire dal 2000 per il settore elettrico, i contatori elettronici con il servizio di telelettura gestito su reti di TLC. Processo analogo è stato avviato per i contatori del gas naturale, mentre buona parte delle stazioni di servizio carburanti sono collegate in rete per il pagamento tramite POS.

L'intera rete elettrica nazionale in alta, media e bassa tensione è sottoposta ad una intensa attività di ricerca e di innovazione tecnologica volta allo sviluppo di "smart grid" e "smart city" che prevedono un ampio utilizzo di tecnologie IoT (internet of thing), introduzione della nuova generazione di "smart meter" e domotica basata sul telecontrollo anche da dispositivi mobili. Sono in fase di realizzazione analoghi processi di introduzione di "smart meter" nel settore del gas naturale e in prospettiva dei contatori dell'acqua. L'integrazione delle reti, per ora a livello progettuale, riguarda anche quella fissa di TLC.

Questo processo di innovazione tecnologica, finalizzato anche all'attivazione di politiche di gestione attiva della domanda, è fortemente supportato dall'Autorità nazionale di regolazione di elettricità, gas e acqua, con particolare attenzione alla corretta gestione delle innovazioni relative agli "smart meter", alle "smart grid" e "smart city".
Riconosciuto che il principale ruolo nel settore della cyber security energetica deriva dalla regolazione internazionale e nazionale e dall'interesse proprio dei principali operatori, la 2ª Conferenza Nazionale Cyber Security Energia ha messo in luce la sempre maggiore esigenza di collaborazione con i soggetti intermedi - circa 500 - , operatori della distribuzione (elettricità, gas, petrolio, acqua) cui spetterebbe anche il compito di educare il vasto pubblico, per un servizio o l'altro o per tutti, propri clienti.

FOCUS
1/2016 - CYBER SECURITY ENERGIA

Energia Media
Milano / Roma
comunicazione@energiamedia.it
www.energiamedia.it