WEC Italia e le Utility italiane insieme per la Cyber Security Energia

La digitalizzazione dei servizi e delle informazioni, pur permettendo una forte accelerazione delle economie dei Paesi più avanzati, ha determinato un parallelo incremento delle vulnerabilità delle infrastrutture che si avvalgono di supporti digitali. Il pericolo di furto, manomissione e compromissione dei dati nello spazio cibernetico ha evidenziato la necessità di mettere in sicurezza le attività in esso condotte. Il tema della cyber security ha dunque assunto nel tempo un ruolo di estrema rilevanza, soprattutto con riferimento alla protezione di infrastrutture considerate critiche, in quanto fornitrici di servizi pubblici essenziali, quali energia elettrica, gas e acqua.

Nonostante l'impegno profuso dalle principali organizzazioni nazionali, la minaccia Cyber non può essere contrastata attraverso singole iniziative, ma ha bisogno di una risposta a livello di Sistema Paese. È necessario quindi muoversi con un approccio organico che garantisca livelli standard minimi di sicurezza, a favore dell'interoperabilità delle soluzioni e della maturazione complessiva del settore dei servizi pubblici locali e di quello energetico in particolare, facendo uso del recente Framework Nazionale per la Cyber Security e considerando le necessità di *compliance* indicate dall'UE (Direttiva Network and Information Security - Nis), alle quali i Paesi membri dovranno attenersi in breve tempo.

La condivisione di esigenze, esperienze e buone pratiche tra istituzioni, regolatori, Energy Company, Utility e fornitori di tecnologie e servizi è necessaria per la messa in sicurezza contro i rischi cyber che minacciano il settore energetico nazionale.

La Conferenza Nazionale Cyber Security Energia (Conferenza CSE), iniziativa fondata da Energia Media in collaborazione con WEC Italia (Comitato Nazionale Italiano del Consiglio Mondiale dell'Energia), con la sua terza edizione 2016 ha avviato una collaborazione strategica con Utilitalia, la Federazione che associa circa 500 Utility del settore elettrico, gas, acqua e ambiente, per facilitare ulteriormente il dialogo tra Istituzioni competenti sulla sicurezza informatica, Energy companies, Aziende della consulenza, vendor di tecnologie e soluzioni per la cyber security, Istituti di ricerca e mondo delle Utility italiane.

A livello globale i **rischi** legati alla **Cyber Security** sono in continuo **aumento** in termini di **numerosità, impatto** e **sofisticatezza** degli **attacchi**.

Attacchi informatici contro infrastrutture energetiche possono potenzialmente **attraversare la dimensione Cyber e invadere il mondo fisico**, nel caso in cui venga compromessa l'operatività di un asset energetico.

Le grandi infrastrutture energetiche centralizzate sono asset particolarmente a rischio a causa del **potenziale "effetto domino"** che un attacco contro raffinerie di petrolio, impianti nucleari, centrali termoelettriche potrebbe causare.

Gli energy Leader hanno ormai acquisito consapevolezza sul fatto che gli **attacchi informatici** rappresentano una **minaccia concreta per l'operatività di un'Azienda**. Entro il 2018 l'industria oil&gas da sola potrebbe arrivare a spendere ogni anno circa **1,87 miliardi di dollari** per la sicurezza informatica.

Considerati questi elementi di contesto, WEC Italia e Utilitalia con il presente documento di sintesi si propongono di portare all'attenzione delle Istituzioni competenti le principali istanze a cui gli Stakeholders nazionali della cyber security energia dovranno dare risposte e soluzioni nei prossimi anni.

1. Il **rischio Cyber** non deve essere considerato semplicemente come una minaccia IT, ma come un fattore che **riguarda l'operatività di tutta l'Azienda**. La sua gestione richiede quindi un **approccio intersettoriale** che coinvolga tutti i livelli aziendali, dalla governance ai team operativi;

2. Per contrastare i rischi cyber deve essere adottato un **approccio sistemico** che riguardi **tutta la filiera di approvvigionamento energetico**, così da limitare anche i possibili effetti a cascata che potrebbero essere causati da un guasto lungo la supply chain;

3. La sempre maggiore **interconnessione e digitalizzazione del settore energetico** (inclusi smart grids, dispositivi e device per la domotica e Internet of Things) favorisce il processo di **efficientamento del settore nel suo complesso**, ma genera al contempo un **incremento delle vulnerabilità** alle quali si è esposti e aumenta la complessità della gestione dei rischi informatici. I **fornitori di tecnologie** possono giocare un ruolo fondamentale nel favorire la protezione delle infrastrutture energetiche contro le minacce Cyber. I vendor dovranno, quindi, assicurare di fornire tecnologie che incorporino **standard di sicurezza** nei prodotti immessi sul mercato;

4. Il successo di molti attacchi informatici spesso dipende da **errori umani** dovuti a una **scarsa consapevolezza** circa i rischi informatici con i quali ci si deve confrontare. La **formazione del personale** sulle potenziali vulnerabilità informatiche alle quali è esposta l'Azienda dovrebbe essere parte integrante della **strategia sulla sicurezza informatica** di ogni Operatore;

5. Le Compagnie energetiche possono affrontare il rischio cyber secondo due tipologie di intervento complementari che riguardano:

    - **Misure tecniche:** implementazione di tecnologie per la protezione dei sistemi hardware e software, limitazione dell'accesso ai data center e adozione di standard procedurali;
    - **Formazione del personale:** favorire lo sviluppo di una cultura cyber tra e a tutti i livelli delle organizzazioni.

6. Anche se le Aziende sono sempre più consapevoli dei rischi in ambito cyber, si registra ancora una **scarsa condivisione delle informazioni** tra gli Operatori industriali e di settore su esperienze e buone pratiche adottate in casi di attacchi informatici. Un maggiore **scambio di informazioni** permetterebbe di **comprendere** meglio il potenziale **impatto** che i **rischi informatici** hanno sia sulle Compagnie energetiche sia sul settore energetico nel suo complesso;

7. Una maggiore **collaborazione tra istituzioni governative e private** può aiutare a ottenere una comprensione più ampia dei potenziali impatti dei cyber-attack. Appare necessario rafforzare la **cooperazione** per garantire la sicurezza informatica dei sistemi energetici;

8. La **diffusione di informazioni** sugli incidenti, la **condivisione delle migliori pratiche** e l'introduzione di **standard di sicurezza informatica internazionali** sono elementi chiave per affrontare la sfida posta dal cyber crime;

9. Le **istituzioni governative** hanno un **ruolo chiave** nel **supportare le Aziende** nel proteggersi **contro i rischi informatici**, potendo: predisporre **Framework nazionali** con norme e regolamenti specifici; favorire la **condivisione di informazioni**; stimolare la **cooperazione internazionale** in materia di strutture di sicurezza informatica;

10. Esistono **meccanismi di assicurazione** contro i rischi Cyber che possono aiutare le aziende a compensare/mitigare alcune delle potenziali perdite finanziarie derivanti da un cyber-attacco. Tuttavia, la mancanza di dati storici consistenti relativi a un rischio emergente e in continua evoluzione come quello cyber, fa si che il **mercato assicurativo cyber** sia ancora **poco maturo**. L'utilizzo di questi meccanismi di per sé può però essere vantaggioso, in quanto fa sì che le Aziende si confrontino con le proprie vulnerabilità informatiche.

Il contributo acquisito da Esperti provenienti da Istituzioni, Imprese, Consulenti, Fornitori di tecnologie, Università e Istituti di ricerca ha evidenziato le "best practice" sulla governance aziendale della sicurezza informatica, oggetto anche dei dibattiti della terza edizione della Conferenza Nazionale CSE a cui hanno partecipato Istituzioni e soggetti del mondo della ricerca con i rappresentanti del Ministero Sviluppo Economico, dell'ISCOM, dell'Autorità per l'energia elettrica il gas e il settore idrico, di Acquirente Unico S.p.A., del Joint Research Centre e di Ricerca sul Sistema Energetico S.p.A.

WEC Italia e Utilitalia auspicano una forte azione delle Istituzioni nazionali e Comunitarie volta alla evidenziazione del ruolo strategico della Cyber Security nel settore dell'Energia e al sostegno delle iniziative che le Utility dovranno mettere in campo; si impegnano a diffondere presso le Imprese associate la sensibilità verso tali temi della sicurezza informatica, in stretto coordinamento con le Istituzioni deputate.

Utilitalia
Piazza Cola di Rienzo, 80A
00192 - Roma
T 06 94 52 82 10-20
F 06 94 52 82 00

WEC Italia
Via Mosca, 32
00142 - Roma
T 06 51606091
F 06 51885135