Uno scenario in cambiamento tra cyber security Act, direttiva NIS e Raccomandazioni EU per energy e cyber security

Ing. Luisa Franchina

INDICE

1. La cyber security nel settore energetico
2. Lo scenario normativo europeo
3. Le nuove Raccomandazioni EU in materia di cyber-energia
4. Le iniziative degli operatori dell'energia
5. Il contesto italiano e le strategie di intervento
6. Conclusioni

La cybersecurity nel settore energetico

Il settore dell'energia è caratterizzato da trend innovativi che ne stanno aumentando la potenziale esposizione ad attacchi cibernetici

Energie rinnovabili

Incremento del numero di impianti di generazione (parchi fotovoltatici, eolici, ecc.)

Prosumer model

Imprese industriali, attività commerciali, famiglie che ricoprono il duplice ruolo di generatori e consumatori di energia

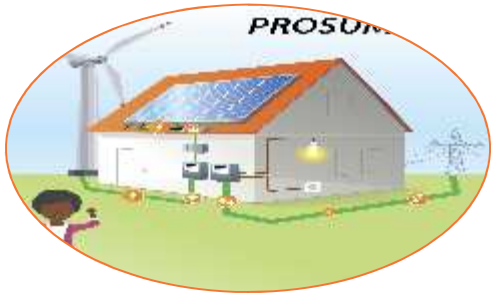
Digital Energy

Crescente uso di tecnologie ICT per gestire tutte le attività della catena del valore dei vari operatori della filiera

***Energy Cybersecurity Report 2018 - Osservatorio Energy Cybersecurity dell'Energy & Strategy Group, School of Management del Politecnico di Milano - https://www.infobuildenergia.it/Allegati/14066.pdf**

La cybersecurity nel settore energetico

Significativo numero di nuovi attori nel settore (tipicamente con scarsa esperienza e ridotta conoscenza dei rischi di natura «cyber»)



Smart Grid - crescita esponenziale del numero di attori, anche di piccola o piccolissima taglia, connessi alla rete (Player della generazione, TSO/DSO, Prosumer, Consumatori)

Connessione alla rete di sistemi e strutture inizialmente non concepite in ottica cybersecurity e dotati di software obsoleti e difficilmente aggiornabili

Aumento della potenziale superficie di attacco e del livello di vulnerabilità sistemica delle infrastrutture energetiche

***Energy Cybersecurity Report 2018 - Osservatorio Energy Cybersecurity dell'Energy & Strategy Group, School of Management del Politecnico di Milano - https://www.infobuildenergia.it/Allegati/14066.pdf**

Lo scenario normativo europeo

La Direttiva NIS del 6 Luglio 2016 stabilisce obblighi di sicurezza e di notifica per gli operatori dei settori che sono fondamentali per l'infrastruttura economica e sociale dei sistemi Paese (cosiddetti Operatori di Servizi Essenziali)

CRITERI DI IDENTIFICAZIONE - Articolo 5, Paragrafo 2

- un soggetto fornisce un servizio che è essenziale per il mantenimento di attività sociali e/o economiche fondamentali
- la fornitura di tale servizio dipende dalla rete e dai sistemi informativi
- un incidente avrebbe effetti negativi rilevanti sulla fornitura di tale servizio

Riesame e aggiornamento biennale dell'elenco degli operatori

↓

Trasmissione informazioni alla Commissione

*Direttiva UE 2016/1148 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=CS)

Lo scenario normativo europeo

Gli Operatori di servizi essenziali in ambito energetico

Energia elettrica

- Imprese elettriche
- Gestori del sistema di distribuzione (DSO)
- Gestori del sistema di trasmissione (TSO)

Petrolio

- Gestori di oleodotti
- Gestori di impianti di produzione, raffinazione, trattamento, deposito e trasporto di petrolio

Gas

- Imprese fornitrici
- Gestori del sistema di distribuzione (DSO)
- Gestori del sistema di trasmissione (TSO)
- Gestori dell'impianto di stoccaggio
- Gestori del sistema GNL
- Imprese di gas naturale
- Gestori di impianti di raffinazione e trattamento di gas naturale

***Direttiva (UE) 2016/ 1148 – Allegato II – Tipi di soggetti ai fini dell'articolo 4, punto 4 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32016L1148&from=CS**

Lo scenario normativo europeo

Il percorso tracciato con la Direttiva NIS in merito alla sicurezza delle reti e dei sistemi informativi viene integrato e rafforzato con il nuovo Cybersecurity Act.

Creazione di un quadro europeo per la certificazione della sicurezza cibernetica dei prodotti ICT e dei servizi digitali

- Armonizzazione delle condizioni e dei requisiti sostanziali per l'ottenimento delle certificazioni nell'ambito della cybersecurity
- Predisposizione di norme tecniche, criteri di valutazione e metodologie di prova comuni

Affermazione dei principi di cooperazione e sussidiarietà fra gli Stati membri

- «Per aumentare la cyberresilienza collettiva dell'Unione non saranno sufficienti le azioni individuali da parte degli Stati membri dell'UE e un approccio frammentario alla sicurezza informatica»
- Rafforzamento ruolo e competenze ENISA e valorizzazione Agenzie europee di settore (fra cui la ACER - Agenzia per la cooperazione fra i regolatori nazionali dell'energia)

*European Parliament legislative resolution of 12 March 2019 (http://www.europarl.europa.eu/doceo/document/TA-8-2019-0151_EN.pdf?redirect)

Le Raccomandazioni EU in materia di cyber-energia

Smart Grid e *Smart Device* sempre più interconnessi aumentano l'esposizione ad attacchi e incidenti informatici.
La Commissione europea raccomanda l'attuazione di una serie di misure operative volte al miglioramento della cybersecurity nel settore dell'energia.

Vengono individuate tre grandi sfide da affrontare in relazione a:

- Esigenze delle componenti dell'infrastruttura energetica in un contesto di *real time*
- Effetti a cascata
- Tecnologie preesistenti e tecnologie all'avanguardia

*Raccomandazione (Ue) 2019/553 della Commissione del 3 aprile 2019 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0553&from=EN)

Le Raccomandazioni EU in materia di cyber-energia

Le misure di cybersecurity devono essere in grado di adattarsi alle strutture del sistema energetico, che devono operare «in tempo reale», ossia eseguendo i comandi entro pochi millisecondi. Per assicurarsi che ciò avvenga, i gestori delle reti energetiche dovrebbero:

- Applicare le norme tecniche in materia di cybersecurity per le nuove installazioni; considerare misure di sicurezza fisica complementari per i vecchi impianti
- Attuare le norme tecniche per la comunicazione sicura in tempo reale non appena i prodotti diventano disponibili sul mercato
- Considerare le reti private per i sistemi di tele-protezione al fine di garantire il livello di qualità del servizio richiesto per gestire le contingenze in tempo reale
- Definire limiti temporali e vincoli di processo delle strutture energetiche al fine di poter applicare misure di cybersecurity o considerare altri metodi di protezione

*Raccomandazione (Ue) 2019/553 della Commissione del 3 aprile 2019 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0553&from=EN)

Le Raccomandazioni EU in materia di cyber-energia

Data l'interconnessione tra reti elettriche e gasdotti in Europa, un attacco cyber che dovesse causare indisponibilità o interruzioni in una parte del sistema energetico potrebbe innescare effetti a cascata di vasta portata in altre sue parti. Per far fronte a tali rischi, i gestori delle reti energetiche dovrebbero:

- Provvedere affinché i nuovi dispositivi, compresi i dispositivi *IoT*, abbiano e mantengano un livello di cyber security adeguato alla criticità del sito
- Tenere debitamente conto degli effetti cyber fisici al momento della definizione e della revisione periodica dei piani di continuità operativa
- Stabilire dei criteri di progettazione e un'architettura atti a garantire la resilienza delle reti

*Raccomandazione (Ue) 2019/553 della Commissione del 3 aprile 2019 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0553&from=EN)

Le Raccomandazioni EU in materia di cyber-energia

Nell'attuale sistema energetico coesistono due tipologie differenti di tecnologie:

- Tecnologie *legacy*, progettate senza tener conto della cybersecurity
- Tecnologie moderne, che riflettono lo stato dell'arte della digitalizzazione

Per evitare le possibili disfunzionalità derivanti da un simile scenario ibrido, i gestori delle reti energetiche dovrebbero:

- Effettuare un'analisi periodica dei rischi e delle vulnerabilità su tutti gli impianti *legacy;* aggiornare, quando possibile, sistemi hardware e software
- Collaborare con i fornitori di tecnologia per sostituire i sistemi *legacy* ogni volta in cui ciò dovesse apportare benefici in termini di sicurezza
- Adottare misure di prevenzione degli attacchi e predisporre un sistema di monitoraggio della sicurezza e di risposta e gestione degli incidenti
- Formulare i bandi delle gare di appalto privilegiando i requisiti di cybersecurity; chiarire le responsabilità del fornitore del servizio in caso di incidenti IT

*Raccomandazione (Ue) 2019/553 della Commissione del 3 aprile 2019 (https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32019H0553&from=EN)

Le iniziative degli operatori dell'energia

ENTSO (European Network of Transmission System Operators) è un organismo di cui fanno parte alcuni fra i più importanti operatori privati in ambito energetico, il quale si occupa, su input della EU, di elaborare standard e pratiche condivise per il settore dell'energia.

entsoe

MEMORANDUM OF UNDERSTANDING CYBERSECURITY

Quadro generale su regole, pratiche e standard condivisi nell'ambito della cybersecurity dei sistemi di trasmissione elettrica

ENCS

European Network for Cyber Security

ENTSO-E ha approvato, nel giugno 2018, il Common Grid Model Security Plan che definisce i requisiti di cybersecurity della piattaforma Operational Planning Data Environment (OPDE).

*https://www.entsoe.eu/Documents/Publications/ENTSO-E%20general%20publications/ENTSO-E_PowerFacts_2019.pdf?Web=1
*https://consultations.entsoe.eu/entso-e-general/annual-work-programme-2019/supporting_documents/I_entsoe_AWP_2019_09.pdf

Il contesto italiano e le strategie di intervento

Strategia nazionale per la sicurezza informatica in attuazione di direttive, regolamenti e raccomandazioni elaborate in ambito sovranazionale. Gli organi preposti all'attuazione di tale strategia sono:

DIS (Dipartimento per le informazioni sulla sicurezza)

organo governativo che vigila sulle infrastrutture critiche e sullo spazio cibernetico italiano

Nucleo Sicurezza Cibernetica (NSC)

composto da rappresentanti dei ministeri principali, delle agenzie di intelligence, del Dipartimento della protezione civile e dell'Agenzia per l'Italia digitale; organo ricondotto all'interno del DIS che si occupa di assicurare la risposta coordinata agli eventi cibernetici significativi per la sicurezza nazionale

OBIETTIVI

Identificazione di un perimetro nazionale di cybersecurity, al fine di proteggere i servizi la cui interruzione comprometterebbe la sicurezza nazionale

*https://www.wired.it/internet/regole/2019/02/13/sicurezza-informatica-italia-piano-hacker/?refresh_ce=

Il contesto italiano e le strategie di intervento

I punti principali di attuazione della strategia sono:

Individuazione di aziende pubbliche e private (operanti nei settori sanitario, energetico, dei trasporti, finanziario, ecc.) che possano essere classificate come **Operatori dei Servizi Essenziali (OSE)**

465 imprese già identificate dal DIS a dicembre 2018

OBIETTIVI

Innalzamento delle difese delle 465 aziende selezionate e comunicazione di una serie di linea guide cui le stesse dovranno uniformarsi

OBIETTIVI

Rafforzamento della resilienza cibernetica delle infrastrutture critiche del Paese e identificazione di nuovi schemi e processi di certificazione

Certificazione delle tecnologie informatiche per assicurarsi che rispettino gli standard nazionali ed europei.

Gestione del processo di certificazione affidata al Centro di Valutazione e Certificazione Nazionale (CVCN) da insediare al Ministero dello Sviluppo Economico

***https://www.wired.it/internet/regole/2019/02/13/sicurezza-informatica-italia-piano-hacker/?refresh_ce=**

Conclusioni

Per rispondere alle minacce di natura cibernetica, gli operatori della filiera energetica sono chiamati ad adottare specifici approcci operativi per la gestione della sicurezza.

Tutte le indicazioni regolamentari suggeriscono la messa a punto di un cybersecurity management system:

- *Risk analysis*
- *Identificazione delle contromisure adeguate*
- *Monitoraggio e miglioramento continuo*
- *Awareness e formazione*
- *Definizione di policy e guidelines*

Nella progettazione di tale sistema di gestione della cybersecurity, un ruolo importante è attribuito all'individuazione di standard procedurali nell'ambito della sicurezza OT (Operational Technology) delle reti energetiche e alla sensibilizzazione degli end-user in tema di rischi cibernetici legati allo svolgimento delle attività.

Grazie per l'Attenzione

Per ulteriori informazioni

AIIC
Ing. Luisa Franchina
Presidente AIIC / Partner Hermes Bay
blustarcacina@gmail.com