La cybersecurity dei sistemi energetici

6 dicembre 2024

Auditorium GSE, viale Maresciallo Pilsudski 92, Roma

Nel contesto socio-economico attuale, caratterizzato da un ruolo sempre più rilevante delle tecnologie digitali nell'erogazione dei servizi pubblici e privati, la cybersecurity assume una posizione strategica in quanto essenziale per la stabilità degli equilibri nazionali e globali. Lo sviluppo e l'adozione di misure di cybersecurity adeguate al livello di rischio per la fornitura di servizi energetici sempre più interconnessi è una priorità riconosciuta dalle strategie di sviluppo e innovazione tecnologica del sistema Paese, finalizzate a garantire un livello di maturità tecnologica allineato ai target di cybersecurity Europei e nazionali.

Con il coinvolgimento degli enti affidatari della Ricerca di Sistema (Piano Triennale di Ricerca 2022-2024), RSE, ENEA e CNR, il Workshop presenta i risultati del Progetto Integrato *Cybersecurity dei Sistemi Energetici* (https://www.rse-web.it/progetti/progetto-integrato-cyber-security-dei-sistemi-energetici/) finalizzati alla sperimentazione delle tecnologie di cybersecurity più mature in casi applicativi significativi per la transizione energetica e allo studio e valutazione di tecnologie e piattaforme innovative.

Programma

9:00 Registrazione partecipanti

9:30 Benvenuto e saluti istituzionali

9:40 *Sessione 1 Rischi cyber, Regolazione, Standard e Tecnologie Innovative di Cybersecurity*

11:45 *Sessione 2 Tecnologie di cybersecurity e resilienza infrastrutture energetiche*

12:30 Pausa pranzo

13:30 *Sessione 2 Tecnologie di cybersecurity e resilienza infrastrutture energetiche (cont.)*

14:30 *Sessione 3 Ruolo dell'Intelligenza Artificiale nella cybersecurity della transizione energetica*

15:15 Pausa caffè

15:30 *Sessione 3 Ruolo dell'Intelligenza Artificiale nella cybersecurity della transizione energetica (cont.)*

17:00 Conclusioni e ringraziamenti

Per partecipare si prega di registrarsi al seguente link.

Nel seguito l'Agenda con il dettaglio degli interventi.

Agenda	Affidatario	Relatore	Ora
Benvenuto e saluti istituzionali			9.30-9.40
Sessione 1 Rischi cyber, Regolazione, Standard e Tecnologie Innovative di Cybersecurity			
Regolazione energetica, standard di cybersecurity, innovazione	RSE	G. Dondossola	9.40-10.00
Standard IEC 62351: crittografia delle comunicazioni basate su PKI centralizzata per il controllo di risorse energetiche distribuite - valutazioni di prestazioni	RSE	M.G. Todeschini	10.00-10.15
Dispositivi IoT: autenticazione tramite PKI distribuita basata su tecnologia Blockchain ed instaurazione di canali sicuri per lo scambio di informazioni	RSE-FUB	N. Cardamone	10.15-10.30
Tecnologie quantistiche per la cybersecurity dei sistemi energetici	ENEA-UniPD	P. Villoresi	10.30-10:45
Apparati di protezione elettrica e cibernetica delle reti e microreti elettriche	ENEA	G. Adinolfi	10.45-11.00
Il 'cavo crittato': comunicazione sicura basata su primitive crittografiche implementate in logica programmabile	ENEA-UniRM1	P. Tommasino	11.00-11.15
Architetture di misura distribuite e interfacce di comunicazione per microreti resilienti alle minacce cyber basate sulla Power Line Communication (PLC)	CNR	G. Tinè	11.15-11.30
Soluzioni innovative per la trasmissione dati su microreti resilienti alle minacce cyber basate sulla tecnologia Power Line Communication (PLC)	CNR-UniPA	G. Artale	11.30-11.45
Sessione 2 Tecnologie di cybersecurity e resilienza infrastrutture energetiche			
Valutazioni di conformità cybersecurity di comunicazioni IoT per il controllo di una microrete energetica	RSE	M.G. Todeschini	11.45-12.00
Gestione di chiavi e certificati digitali per infrastrutture di ricarica di veicoli elettrici	RSE	E. Corniani	12.00-12.15
Test di cybersecurity su reti di comunicazione 5G	RSE-FUB	L. Sagratella	12.15-12.30
Pausa Pranzo			12.30-13.30
Sessione 2 Tecnologie di cybersecurity e resilienza infrastrutture energetiche (cont.)			
StuxTwin: simulazione di un attacco tipo Stuxnet tramite digital twin	CNR-IMT	G. Costa	13.30-13.45
Gestione dinamica del rischio	CNR	A. Yautsiukhin	13.45-14.00
Procedure di autorizzazione per un'architettura sicura di monitoraggio e controllo distribuito che integri sistemi di autorizzazione in sistemi distribuiti di generazione, accumulo di energia e produzione di idrogeno	CNR	G. Brunaccini	14.00-14.15
Tecniche e meccanismi decentralizzati post-quantum per l'autenticazione e l'autorizzazione nei sistemi di generazione, accumulo di energia e produzione di idrogeno	CNR-UniME	F. Longo	14.15-14.30
Sessione 3 Ruolo dell'Intelligenza Artificiale nella cybersecurity della transizione energetica			
Controllo proattivo di minacce cyber per infrastrutture energetiche che connettono risorse di generazione	RSE	R. Terruggia	14.30-14:45
SecuriDN: uno strumento per la modellazione della cyber kill chain funzionale al rilevamento di anomalie	RSE-UniPO	L. Egidi	14.45-15.00
Metodologie e algoritmi di Intelligenza Artificiale per il rilevamento di attacchi alle infrastrutture di ricarica per veicoli elettrici	RSE	A. Maldarella	15.00-15.15
Pausa caffè			15.15-15.30
Sessione 3 Ruolo dell'Intelligenza Artificiale nella cybersecurity della transizione energetica (cont.)			
Piattaforma per la cybersicurezza	ENEA	M. Celino	15.30-15.45
Un approccio di apprendimento non supervisionato per il rilevamento di anomalie nella rete ENEA	ENEA-UniRM3	T. Caiazzi	15.45-16.00
Metodi di Machine Learning supervisionato e non supervisionato per l'analisi del traffico di rete	ENEA-UniBA	G. Lorusso	16.00-16.15
Modelli di Machine Learning per la detezione di cyber-attacchi in sistemi energetici attraverso l'analisi statistica del dato misurato su nodi cyber-fisici	ENEA	S. De Vito	16.15-16.30
Rilevazione di Minacce a Smart Grids tramite Algoritmi di Meta-Learning	CNR-UniFI	A. Bondavalli	16.30-16.45
Classificazione dei malware via explainable AI	CNR	G. Ciaramella	16.45-17.00
Conclusioni e ringraziamenti			17.00