PIANO TRIENNALE DI REALIZZAZIONE 2022-24 - RICERCA DI SISTEMA ELETTRICO NAZIONALE
Progetti di ricerca di cui all'art. 10 comma 2, lettera a) del decreto 26 gennaio 2000

AFFIDATARIO ENEA

Tema 2.1 – Cybersecurity dei sistemi energetici

Durata: 36 Mesi

Semestre n. 5 – Periodo attività: 01/01/2024 – 30/06/2024

ABSTRACT ATTIVITA' SEMESTRALE:

Il presente documento descrive le attività di ricerca del progetto “Cybersecurity dei sistemi energetici” svolte da ENEA e dai propri co-beneficiari durante il quinto semestre di progetto.

Le attività di ricerca hanno riguardato le seguenti Linee di Attività:

- ENEA (affidatario del progetto) per LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5;
- UniPD-QTech (cobeneficiario del progetto) per LA1.7 e LA1.8;
- UNINA-FISICA (cobeneficiario del progetto) per LA1.9 e LA1.10;
- ROMA1-DIET (cobeneficiario del progetto) per la LA1.11;
- ROMA3-DICITA (cobeneficiario del progetto) per LA3.9;
- UNIBA (cobeneficiario del progetto) per LA3.10;
- DIG-UNISANNIO (cobeneficiario del progetto) per LA3.12.

AFFIDATARIO / COBENEFICIARIO	SINTESI DELLE ATTIVITÀ DI RICERCA SVOLTE E DEI RISULTATI CONSEGUITI
ENEA	<p>Nell'ambito del presente semestre, ENEA ha condotto attività di ricerca relativamente alle seguenti linee di attività: LA1.6, LA2.7, LA3.4, LA3.7; LA3.8; LA3.13; LA4.5.</p> <p>La Linea di Attività LA1.6 “Valutazione della cyber-vulnerabilità di microreti elettriche dotate di apparati e tecnologie di comunicazione, monitoraggio, gestione e test degli interventi mitigativi” si è concentrata sull'analisi delle cybervulnerabilità dei dispositivi e delle tecnologie di comunicazione, monitoraggio e gestione integrati nelle microreti elettriche.</p> <p>Per valutare tali vulnerabilità dal punto di vista della cybersecurity, è stato deciso di condurre penetration test (PET) su dispositivi commerciali presenti nella rete ENEA. Nel corso del quinto semestre è stata quindi svolta un'approfondita analisi bibliografica finalizzata all'individuazione del metodo più efficace per l'esecuzione dei test. Al termine di questa fase, è stato selezionato il software NMAP (Network Mapper), implementato sulla distribuzione Kali Linux.</p>

Successivamente, sono stati individuati i dispositivi da sottoporre a test. In particolare, la scelta è ricaduta su dispositivi comunemente impiegati nelle reti elettriche, sia lato generazione e carico (come inverter fotovoltaici e pompe di calore), sia lato controllo e misura da remoto (come prese intelligenti WiFi, stazioni meteo smart per uso domestico e smart meter). Per conferire un carattere di generalità all'attività di ricerca, sono stati selezionati dispositivi di tipo commerciale. Nel semestre successivo, per ciascun apparato selezionato, verranno eseguiti test di penetrazione, analizzati i risultati ottenuti e formulate proposte di azioni mitigative.

In aggiunta alle attività precedentemente descritte, nel quinto semestre si è proceduto all'acquisizione, installazione e collaudo delle apparecchiature QKD (Quantum Key Distribution). Tali dispositivi sono stati impiegati nell'ambito della Linea di Attività LA2.7, dove sono stati integrati nel prototipo di sistema di protezione sviluppato da ENEA.

Per ciò che concerne la **LA2.7 "Implementazione di uno schema di protezione e sviluppo di un prototipo per la mitigazione degli effetti connessi ai cyber-attacchi in ottica di incremento della cyber-resilienza delle reti e delle microreti elettriche"**, nel presente semestre è stato portato a termine lo sviluppo del dispositivo di protezione per reti e microreti elettriche in presenza di mezzo trasmissivo in fibra ottica (CYPROBER) in base all'architettura definita nella LA2.2.

Inoltre, sono state definite le logiche di controllo del suddetto apparato a fronte di guasti di mera natura elettrica, di mera natura cibernetica e guasti ibridi (elettrici e cibernetici).

Infine, una campagna di simulazioni è stata condotta per la verifica delle logiche proposte. Tale fase è risultata propedeutica alla fase di prototipazione del dispositivo di protezione.

Nel successivo semestre verranno eseguiti i test per la validazione sperimentale del prototipo.

Con riferimento alla **LA 3.4 "Implementazione di una infrastruttura di calcolo a basso consumo per il controllo informatico delle reti elettriche intelligenti cyber-resilienti"**, nel quinto semestre sono proseguite le seguenti attività di installazione e configurazione parzialmente avviate nel precedente semestre:

- Installazione e Migrazione dei Firewall Palo Alto: si tratta degli elementi di sicurezza perimetrale di ultima generazione che garantiscono un più elevato grado di sicurezza al traffico della rete di ENEA Casaccia e di ENEA Portici.
- Installazione e configurazione Server di Calcolo e Storage SuperMicro: L'attività ha permesso la loro corretta installazione, configurazione e integrazione con la rete di produzione ENEA, garantendo la piena operatività e la comunicazione con gli altri sistemi dell'infrastruttura.
- Installazione e configurazione dei sensori/attuatori: i sensori/attuatori sono stati installati e configurati per comunicare con la rete di produzione di Casaccia su una VLAN dedicata.

- Installazione di server Kali Linux: utili alla generazione, anche se in maniera controllata, di un traffico malevolo che si sovrappone a quello normalmente presente sulla rete ENEA.
- Installazione di un Webserver: il webserver apache è stato installato e configurato al fine di simulare la reazione di un server web che riceve traffico malevolo.
- Configurazione DarkTrace per comunicare con Elasticsearch: la soluzione Darktrace, già ampiamente utilizzata in ENEA per la segnalazione di eventi anomali, ha svolto nell'ambito del progetto l'elemento chiave che ha permesso di collezionare i dati per poi trasferirli nel formato opportuno ad Elasticsearch. In questa fase sono state portate a termine le procedure di anonimizzazione dei dati per permetterne la condivisione, con i co-beneficiari di progetto, garantendo il rispetto delle normative relative alla privacy.

In aggiunta alle precedenti attività, al fine di effettuare dei test sul corretto funzionamento dell'infrastruttura di calcolo in presenza di attacchi malevoli e al fine di generare un dataset utile all'addestramento degli algoritmi di Machine Learning, sono stati simulati, grazie ad i tool disponibili su Kali Linux, attacchi informatici rivolti ai sensori e ad un webserver.

Nel successivo semestre le attività proseguiranno con l'installazione e configurazione di un nodo Elasticsearch e la definizione del framework privacy

Le attività della **LA3.7 "Realizzazione e implementazione su un caso d'uso di una piattaforma di stream analytics e implementazione delle logiche di training e inference dei modelli di Machine Learning e Artificial Intelligence su acceleratori di varia natura (FPGA/GPU)"** sono state focalizzate, nel semestre, sulla creazione di diversi componenti di data analytics capaci di elaborare il flusso di eventi, proveniente dal componente di stream processing basato su Apache Kafka precedentemente predisposto, utilizzando algoritmi di machine learning e di intelligenza artificiale sviluppati dai partner di progetto per alcuni casi d'uso.

L'attività proseguirà nel semestre successivo con l'individuazione di una dashboard con un'interfaccia di gestione facile ed intuitiva per la gestione dei singoli componenti e la loro scalabilità e replicabilità.

Nell'ambito della **LA3.8 "Test dell'infrastruttura di calcolo a basso consumo per il controllo informatico smart di reti cyber-resilienti"** il quinto semestre è stato focalizzato sulla finalizzazione dei test-case preliminari relativi alla rilevazione di intrusioni nei sistemi informatici.

Grazie agli strumenti di generazione di traffico malevolo, sono stati simulati attacchi (es. Slowloris Denial of Service, attacchi forza bruta) per addestrare algoritmi di Machine Learning capaci di identificare anomalie operative.

I dati pseudo-anonimizzati sono stati usati per addestrare modelli di ML successivamente implementati per analisi in tempo reale del traffico di rete.

L'attività proseguirà nel semestre successivo con l'implementazione di procedure per misurare le bande di comunicazione e le latenze nel server di calcolo.

	<p>La linea di attività LA3.13 “Validazione ed integrazione in piattaforma di un toolset di rivelazione attacchi nel contesto delle microreti elettriche” si è posta come obiettivo la progettazione e la validazione di un prototipo di sistema di Adversarial Training per la risposta automatica e la resilienza in contesti operativi reali. Più nello specifico, a seguito dello studio preliminare dell’infrastruttura da monitorare, condotto nel semestre precedente, nel quinto semestre sono state svolte le seguenti attività: i) progettazione della componentistica (script) per la ricezione dei dati rilevanti tramite protocollo MQTT; ii) progettazione della componentistica per l’esecuzione degli script di rilevazione all’interno della piattaforma sviluppata da ICT ENEA.</p> <p>L’attività proseguirà nel semestre successivo con la validazione dei componenti progettati, al fine di verificarne l’efficacia e l’integrazione nel sistema complessivo.</p> <p>La LA4.5 “Attività di diffusione II SAL” ha come obiettivo la divulgazione dei risultati di progetto conseguiti da ENEA e dai relativi co-beneficiari. Nel quinto semestre precedente, ENEA e i propri co-beneficiari hanno avviato un insieme di attività preparatorie finalizzate alla partecipazione agli eventi di disseminazione scientifica previsti nel sesto semestre. Tali attività hanno riguardato la pianificazione dei contenuti, la selezione dei contributi tecnico-scientifici e la coordinazione tra i partner per garantire una comunicazione integrata e rappresentativa del progetto. In particolare, sono stati predisposti gli interventi per il <i>Cybersecurity Day</i> organizzato dal CNR (ottobre 2024), per la conferenza <i>NanoInnovation 2024</i> (settembre 2024) e per il workshop <i>“La cybersecurity dei sistemi energetici”</i> presso il GSE (dicembre 2024). In parallelo, sono proseguite le attività di disseminazione scientifica attraverso la pubblicazione di articoli e la partecipazione ai tavoli tecnici di settore.</p>
<p>UniPD-QTech</p>	<p>Nel periodo di riferimento, UniPD-QTech è stata impegnata nelle attività LA1.7 e LA1.8.</p> <p>Con riferimento alla LA1.7 “Definizione e implementazione sperimentale di un protocollo quantistico di autenticazione di un comando a distanza con l’obiettivo di incremento della cyber-sicurezza delle reti energetiche”, nel semestre in esame le attività dei ricercatori UniPD-QTech si sono inizialmente concentrate sull’analisi delle vulnerabilità dei protocolli Modbus e IEC 61850. È stato studiato il loro funzionamento, evidenziando le principali carenze in termini di sicurezza, tra cui la mancanza di supporto nativo alla crittografia.</p> <p>Alla luce di queste criticità, si è optato per un’architettura che incapsula i dati all’interno di un protocollo criptato, sfruttando chiavi simmetriche generate tramite Quantum Key Distribution (QKD). Questo approccio ha permesso di garantire l’autenticazione e la protezione dei comandi trasmessi.</p> <p>Successivamente, è stata avviata la configurazione degli encryptor, dispositivi deputati alla cifratura e decifratura dei comandi mediante chiavi quantistiche. Gli encryptor sono stati installati sia lato client che lato server, assicurando che ogni comando a distanza fosse trasmesso in modo sicuro e autenticato, e risultasse non alterabile da attori malevoli.</p>

	<p>Durante l'implementazione, è stata inoltre esplorata la possibilità di ridurre il numero di dispositivi QKD necessari, condividendo le chiavi tra più nodi all'interno di un'area sicura. Questo approccio ha consentito un'ottimizzazione delle risorse senza compromettere la sicurezza. Tuttavia, è emerso che il rate di generazione delle chiavi potrebbe rappresentare un limite in reti ad alto traffico. Per affrontare questa sfida, sono stati condotti diversi test volti a bilanciare il compromesso tra sicurezza e prestazioni.</p> <p>Nel semestre successivo, verranno eseguiti test pratici con il sistema IDQ Clavis XGR, finalizzati alla verifica della soglia di Quantum Bit Error Rate (QBER).</p> <p>Per quanto riguarda la LA1.8 "Individuazione dei modelli di rete QKD appropriati per servire le necessità più rilevanti per le architetture di sistemi energetici", nel semestre in esame, a valle dei risultati ottenuti dall'analisi delle diverse topologie delle reti e microreti di distribuzione dell'energia elettrica condotta nel semestre precedente, l'attività si è concentrata sulla progettazione di una rete QKD integrata con un sistema dedicato di gestione delle chiavi (Key Management System).</p> <p>La rete è stata progettata con l'obiettivo di ottimizzare la sicurezza delle infrastrutture elettriche, garantendo la distribuzione sicura delle chiavi crittografiche in ambienti multiterminali. L'approccio adottato ha previsto l'impiego di più coppie di dispositivi QKD per supportare il traffico generato dalla rete e assicurare comunicazioni protette tra i nodi.</p> <p>Un aspetto centrale dell'attività ha riguardato lo studio delle prestazioni della rete, con particolare attenzione al numero ottimale di dispositivi QKD necessari per mantenere un elevato livello di sicurezza senza compromettere le prestazioni. Sono state condotte simulazioni in diversi scenari di traffico, analizzando il Secret Key Rate in funzione del Quantum Bit Error Rate (QBER). I risultati hanno evidenziato che un singolo dispositivo QKD può gestire fino a 50 terminali con un carico dati moderato; per configurazioni più complesse, è necessario ricorrere a più unità.</p> <p>Per la gestione delle chiavi, è stata adottata un'architettura basata su "stanze sicure", in cui più dispositivi condividono un unico sistema QKD, ottimizzando così le risorse disponibili.</p> <p>Nel prossimo semestre, l'attività si concentrerà sull'integrazione di protocolli QKD multiterminali, con l'obiettivo di superare le limitazioni dell'attuale configurazione point-to-point e migliorare ulteriormente la scalabilità e la resilienza della rete.</p>
<p>UNINA-FISICA</p>	<p>Nel periodo di riferimento, UNINA-FISICA è stata impegnata nelle attività relative a LA1.9 e LA1.10.</p> <p>Con riferimento alla LA1.9 "Progettazione e sviluppo di schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning", nel semestre in esame, sulla base delle conoscenze acquisite durante il quarto semestre, è stato avviato lo sviluppo di algoritmi efficienti per l'apprendimento di risorse quantistiche. In</p>

	<p>particolare, sono stati progettati due algoritmi avanzati per l'apprendimento della classe, completamente generale, dei <i>t-doped stabilizer states</i>.</p> <p>Nel successivo semestre, le attività proseguiranno con il completamento dello sviluppo degli algoritmi, con l'obiettivo di integrarli nei modelli di comunicazione quantistica sicura per rafforzare la resilienza delle infrastrutture elettriche.</p> <p>Per ciò che concerne la LA1.10 "Emulazione e test degli schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning, nel presente semestre, i ricercatori UNINA-FISICA hanno avviato la fase di testing sperimentale degli schemi di cyber difesa delle reti elettriche tramite Quantum Secure Direct Communication assistita da Quantum Machine Learning messi a punto. Nello specifico, sono state eseguite misure di Stabilizer Entropy (magic) utilizzando il prototipo di computer quantistico superconduttivo dell'Università di Napoli.</p> <p>Nel successivo semestre verranno analizzati i risultati delle misure sperimentali.</p>
<p>ROMA1-DIET</p>	<p>Nel periodo di riferimento, ROMA1-DIET è stata impegnata nelle attività relative alla LA1.11.</p> <p>Per ciò che concerne la LA1.11 "Implementazione efficiente su logiche programmabili di primitive crittografiche per la sintesi di funzioni di cifratura a flusso e autenticazione", nel semestre in esame, i ricercatori di ROMA1-DIET si sono dedicati all'analisi della letteratura scientifica per valutare i requisiti degli algoritmi di cifratura più adatti alle esigenze di una smart grid. Parallelamente, è stata elaborata una tabella comparativa contenente le principali figure di merito da considerare per confrontare le prestazioni degli algoritmi, come efficienza computazionale, robustezza contro attacchi, scalabilità e compatibilità con le infrastrutture energetiche.</p> <p>Nel successivo semestre l'attività sarà focalizzata sulla valutazione delle prestazioni e la selezione degli algoritmi di cifratura da implementare in logica programmabile.</p>
<p>ROMA3-DICITA</p>	<p>Nel periodo di riferimento, ROMA3-DICITA è stata impegnata nelle attività relative alla LA3.9.</p> <p>Per ciò che concerne la LA3.9 "Progettazione e implementazione di un sistema di raccolta, conservazione e analisi di flussi di dati per la cybersicurezza delle reti di sensori", nel presente semestre sono state svolte le seguenti attività:</p> <ul style="list-style-type: none"> • Raccolta dati: sono stati raccolti dati reali sul traffico di rete ENEA utilizzando Darktrace, una piattaforma che impiega algoritmi di intelligenza artificiale per il monitoraggio della rete. I dati sono stati suddivisi in record grezzi e avvisi generati dall'intelligenza artificiale. I dati sono stati acquisiti e conservati tramite Elasticsearch, un motore distribuito di gestione dei dati basato su Apache Lucene. Elasticsearch memorizza i dati come documenti JSON organizzati in indici che

	<p>agiscono come contenitori logici e strutturati per i dati. I documenti sono indicizzati tramite un motore full-text che consente ricerche rapide e flessibili basate su testo libero.</p> <ul style="list-style-type: none"> • Etichettatura dei dati: I record grezzi sono stati etichettati manualmente confrontandoli con gli alert di Darktrace e con i parametri degli attacchi simulati. Questo processo ha comportato il confronto tra le due sorgenti di dati e la verifica della presenza di una corrispondenza all'interno dell'intervallo di tempo. • Pre-elaborazione dei dati: Sono state utilizzate diverse tecniche per trasformare i dati grezzi in un formato adatto all'addestramento del modello autoencoder. Tra queste, la selezione delle feature, concentrandosi su attributi rilevanti, i codici di stato e le informazioni di autenticazione. È stata eseguita l'imputazione dei dati, sostituendo i valori numerici mancanti con la media e i valori categorici con i più frequenti nelle rispettive colonne. Le caratteristiche categoriche sono state convertite in formato numerico utilizzando la codifica one-hot. Infine, le caratteristiche numeriche sono state normalizzate utilizzando il Min-Max Scaling per garantire che tutte le caratteristiche fossero comparabili. <p>Nel successivo semestre l'attività proseguirà con lo sviluppo del modello e la valutazione delle prestazioni.</p>
<p>UNIBA</p>	<p>Nel periodo di riferimento, UNIBA è stata impegnata nelle attività relative alla LA3.10.</p> <p>Per quanto riguarda la LA3.10 "Sviluppo e implementazione di metodi di Machine Learning supervisionati e non supervisionati per lo studio delle anomalie", nel semestre in esame i ricercatori UNIBA si sono concentrati sull'esplorazione e sull'organizzazione dei dati messi a disposizione da ENEA. I dati analizzati provengono dai registri di connessione generati dal software Darktrace, e il numero di connessioni giornaliere varia in modo significativo. In media, ciascun registro di traffico giornaliero occupa oltre 100 GB di spazio di archiviazione, rendendo necessarie strategie di gestione e analisi efficienti. Poiché i modelli di machine learning supervisionati richiedono dati etichettati per la fase di addestramento, il secondo step ha previsto, con il supporto del personale ENEA, la simulazione di attacchi informatici. Questi attacchi sono stati inseriti nei registri in modo da poter essere facilmente identificati e correttamente etichettati.</p> <p>Nel prossimo semestre verranno sviluppati modelli di machine learning sia supervisionati che non supervisionati, finalizzati all'analisi dei dati di traffico e all'individuazione automatica di anomalie.</p>
<p>DIG-UNISANNIO</p>	<p>Nel periodo di riferimento, DIG-UNISANNIO è stata impegnata nelle attività relative alla LA3.12.</p> <p>Per quanto riguarda la LA3.12 "Sviluppo e confronto prestazionale di algoritmi di rilevamento stocastico di cyber-attacchi nel contesto delle"</p>

microreti elettriche”, nel semestre in esame le attività si sono concentrate, a seguito di un’approfondita analisi delle tecniche di rilevamento delle anomalie basate su algoritmi di apprendimento automatico (Machine Learning), sull’individuazione dell’approccio più adatto alle peculiarità delle microreti elettriche, tenendo conto della natura dei dati e delle caratteristiche operative delle Smart Grid.

In particolare, gli algoritmi non supervisionati si sono rivelati particolarmente efficaci per l’anomaly detection in ambienti dinamici come le Smart Grid, dove il comportamento normale della rete può variare nel tempo e i dati relativi agli attacchi possono essere assenti o difficilmente identificabili. Tra le tecniche esplorate, il clustering si è dimostrato utile per suddividere i dati in gruppi omogenei e rilevare deviazioni significative, potenzialmente indicative di anomalie o malfunzionamenti. In questo contesto, l’algoritmo DBSCAN si è distinto per la sua capacità di individuare pattern complessi e gestire efficacemente dati rumorosi e outlier, aspetti cruciali per il monitoraggio delle microreti elettriche.

Nel prossimo semestre verranno valutate le prestazioni dell’algoritmo selezionato, con l’obiettivo di verificarne l’efficacia in scenari realistici e di definirne i limiti operativi.