Obiettivi Formativi

Conoscenze

- Comprendere l'interconnessione tra IA, sicurezza delle reti e privacy
- Conoscere i principali protocolli di sicurezza e crittografia
- Identificare le vulnerabilità nelle reti moderne
- Comprendere il ruolo dei big data nell'evoluzione delle reti

Competenze Tecniche

- Analizzare il traffico di rete in ottica sicurezza
- Valutare l'impatto delle tecnologie IA sulla gestione delle reti
- Implementare soluzioni base di sicurezza
- Comprendere i meccanismi di protezione della privacy

Competenze di Cittadinanza

- Sviluppare consapevolezza sulla sicurezza digitale
- Comprendere l'importanza della privacy online
- Valutare criticamente l'uso di tecnologie IA nelle reti
- Partecipare attivamente al dibattito su sicurezza e privacy

Contenuti della Lezione

Parte 1: Sicurezza delle Reti Moderne (45 minuti)

1. Evoluzione delle Minacce
    - Da attacchi manuali a minacce automatizzate
    - Ruolo dell'IA negli attacchi moderni
    - Zero-day exploits e vulnerabilità emergenti
2. Tecnologie di Protezione
    - Firewall next-generation
    - IDS/IPS basati su IA
    - Analisi comportamentale
3. Collegamenti col Programma
    - Protocolli di sicurezza (HTTPS, SSL/TLS)
    - VPN e tunneling
    - Crittografia simmetrica e asimmetrica

Parte 2: Privacy e Protezione Dati (45 minuti)

1. GDPR e Normative
   - Principi fondamentali
   - Diritti degli utenti
   - Responsabilità dei gestori di rete
2. Privacy by Design
   - Implementazione nei protocolli di rete
   - Tecniche di anonimizzazione
   - Data minimization
3. Collegamenti col Programma
   - Protocolli di comunicazione sicura
   - Gestione delle identità digitali
   - Log management e privacy

Parte 3: IA nelle Reti (30 minuti)

1. Network Intelligence
   - SDN (Software Defined Networking)
   - Ottimizzazione automatica
   - Prevenzione delle intrusioni
2. Casi d'Uso
   - Load balancing intelligente
   - Quality of Service adattivo
   - Manutenzione predittiva
3. Collegamenti col Programma
   - Protocolli di routing
   - Gestione della congestione
   - Monitoring di rete

Parte 4: Laboratorio Pratico (2 ore)

Attività: "Security and Privacy by Design Challenge"

Metodologia Didattica

- Lezione interattiva con esempi pratici
- Analisi di casi reali
- Esercitazioni pratiche
- Discussioni guidate

Assignment: "Secure Network Design Challenge"

Obiettivo

Progettare una rete aziendale sicura che integri tecnologie IA per la protezione dei dati e della privacy, considerando gli aspetti etici e normativi.

Struttura del Progetto

1. Organizzazione (gruppi di 3-4 studenti)
   Ogni gruppo rappresenta un team di consulenti IT che deve:
   - Analizzare i requisiti di un'azienda
   - Progettare l'infrastruttura di rete
   - Implementare misure di sicurezza
   - Considerare aspetti di privacy
2. Scenario Aziendale (esempi)
   - Startup con smart working
   - Ospedale con dati sensibili
   - Scuola con e-learning
   - Azienda retail con e-commerce

Requisiti Tecnici del Progetto

1. Architettura di Rete
   - Topologia e segmentazione
   - Posizionamento dei firewall
   - DMZ e zone di sicurezza
   - Configurazione VPN
2. Implementazione Sicurezza
   - Protocolli di crittografia
   - Sistemi di autenticazione
   - IDS/IPS
   - Log management
3. Privacy e Compliance
   - Mappatura dati sensibili
   - Procedure GDPR
   - Data retention policy
   - Incident response plan
4. Integrazione IA
   - Analisi del traffico
   - Rilevamento anomalie
   - Automazione sicurezza
   - Ottimizzazione prestazioni

Deliverable

1. Documentazione Tecnica
    - Schema della rete
    - Specifiche dei sistemi
    - Configurazioni di sicurezza
    - Politiche di privacy
2. Presentazione Business
    - Analisi costi/benefici
    - Timeline implementazione
    - Valutazione rischi
    - Piano di formazione
3. Demo/Simulazione
    - Proof of concept
    - Test di sicurezza
    - Scenari di attacco
    - Procedure di recovery

Criteri di Valutazione

1. Competenze Tecniche (30%)
    - Correttezza architetturale
    - Completezza misure sicurezza
    - Efficacia soluzioni proposte
    - Integrazione tecnologie
2. Conformità e Privacy (25%)
    - Rispetto GDPR
    - Protezione dati
    - Gestione consensi
    - Documentazione
3. Innovazione e IA (25%)
    - Uso tecnologie avanzate
    - Automazione
    - Scalabilità
    - Originalità soluzioni
4. Presentazione (20%)
    - Chiarezza espositiva
    - Qualità documentazione
    - Gestione domande
    - Lavoro di squadra

Timeline

- Settimana 1: Design e architettura
- Settimana 2: Implementazione e test
- Settimana 3: Documentazione e presentazione

Risorse e Strumenti

Software e Tool

- Packet Tracer/GNS3
- Wireshark
- Security testing tools
- Strumenti di documentazione

Materiali Didattici

- Template documentazione
- Esempi configurazioni
- Guide best practice
- Case studies

Estensioni e Approfondimenti

Workshop Tecnici

1. Analisi del Traffico
    - Cattura pacchetti
    - Identificazione anomalie
    - Pattern recognition
2. Sicurezza Attiva
    - Penetration testing
    - Vulnerability assessment
    - Incident response
3. Privacy in Pratica
    - Data mapping
    - Impact assessment
    - Breach notification

Collegamenti Interdisciplinari

- Matematica: crittografia e algoritmi
- Inglese: documentazione tecnica

- Diritto: normative e compliance

Valutazione Finale

- Progetto di gruppo (60%)
- Partecipazione workshop (20%)
- Relazione individuale (20%)

Note per il Docente

Punti Chiave

- Enfatizzare collegamenti pratici
- Promuovere pensiero critico
- Incoraggiare creatività
- Mantenere rilevanza tecnica

Possibili Estensioni

- Collaborazioni con aziende
- Certificazioni sicurezza
- Competizioni CTF
- Progetti open source

Adattamenti

- Modificare complessità scenari
- Aggiungere requisiti specifici
- Personalizzare timeline
- Integrare tecnologie emergenti