Elementi essenziali e gestione della sicurezza informatica (settore energetico)

CSP001

Argomento 7/10: Sicurezza dei dati e privacy by design (SDPbd) per il settore energetico

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Introduction to SDPbd

Introduzione alla SDPbd

Sicurezza dei dati e privacy by design (SDPbd)

- La sicurezza dei dati e la privacy by design (SDPbd) è un approccio proattivo che integra misure di sicurezza dei dati e privacy nella progettazione e nel funzionamento dei sistemi energetici sin dall'inizio.
- Scopo: l'obiettivo principale di SDPbd è proteggere i dati energetici sensibili, comprese le informazioni personali e i dati operativi, garantendo al contempo la conformità alle normative sulla privacy dei dati e alle linee guida sulla sicurezza informatica nel settore energetico.
- Importanza: integrando misure di sicurezza e privacy nella fase di progettazione, SDPbd contribuisce a ridurre al minimo il rischio di violazioni dei dati e della privacy, rafforzando in ultima analisi la fiducia nei sistemi energetici.

Security and Privacy by Design

Sicurezza e privacy fin dalla progettazione

Come implementarla?

- Implementare misure di sicurezza dei dati robuste per salvaguardare i dati sensibili relativi all'energia.
- Utilizzare tecniche di crittografia per proteggere i dati inattivi e in transito, garantendone la riservatezza.
- Utilizza controlli di accesso e autorizzazioni basate sui ruoli per limitare l'accesso non autorizzato ai dati sensibili.
- Implementare mascheramento dei dati per anonimizzare informazioni mascheramento per informazioni identificabili (PII) e dati operativi, preservando la privacy.
- Un esempio di implementazione della privacy by design nel settore energetico è lo sviluppo di contatori intelligenti con funzionalità di privacy integrate. Questi contatori raccolgono dati sul consumo energetico preservando la privacy degli utenti grazie all'anonimizzazione delle informazioni di identificazione personale e alla trasmissione sicura dei dati.

Privacy and Threat Intelligence

Privacy e intelligence sulle minacce

Importanza della privacy nell'intelligence sulle minacce

- Le aziende energetiche collaborano attraverso i Centri di condivisione e analisi delle informazioni (ISAC) per condividere le informazioni sulle minacce. Tuttavia, devono garantire che le informazioni sensibili sulle vulnerabilità delle infrastrutture critiche siano rese anonime o condivise in modo selettivo per impedire agli avversari di sfruttare i punti deboli.
- Strategie per la protezione della privacy nella condivisione delle informazioni sulle minacce: un'azienda energetica che partecipa a un ISAC condivide indicatori di minaccia relativi a malware che prendono di mira i sistemi SCADA, ma rende anonimi i dettagli specifici sulla propria infrastruttura per impedire l'identificazione da parte degli autori delle minacce.

Privacy and Threat Intelligence

Apprendimento federato e privacy

Apprendimento federato nel settore energetico

- Un'azienda energetica desidera migliorare il proprio sistema di manutenzione predittiva per le turbine eoliche. Anziché centralizzare i dati di tutte le turbine, il che potrebbe compromettere informazioni operative sensibili, l'azienda adotta un approccio di apprendimento federato in cui i modelli vengono addestrati localmente su ciascuna turbina e solo gli aggiornamenti aggregati dei modelli vengono condivisi con il server centrale.
- Vantaggi dell'apprendimento federato nella tutela della privacy: utilizzando l'apprendimento federato, un'azienda energetica può addestrare modelli di IA per prevedere la domanda di elettricità in diverse regioni senza accedere ai dati dei singoli clienti, preservando la privacy dei consumatori e beneficiando comunque di previsioni accurate della domanda.
- Applicazione dell'apprendimento federato nei modelli di IA del settore energetico: un operatore di rete intelligente sfrutta l'apprendimento federato per analizzare i dati in tempo reale provenienti dai sensori distribuiti nella sua infrastruttura di rete, al fine di rilevare anomalie e prevedere le esigenze di manutenzione senza trasmettere letture sensibili dei sensori sulla rete, garantendo la privacy e la sicurezza dei dati.

Conformità alle normative e alle linee guida

Conformità normativa e considerazioni di dominio

- Garantire la conformità alle normative pertinenti in materia di privacy dei dati, come il Regolamento generale sulla protezione dei dati (GDPR), il California Consumer Privacy Act (CCPA) e le linee guida sulla sicurezza informatica nel settore energetico, come il Cybersecurity Framework del National Institute of Standards and Technology (NIST) e la norma 62443 della Commissione Elettrotecnica Internazionale (IEC).
- Stabilire un quadro di governance completo in materia di sicurezza informatica per le organizzazioni energetiche al fine di gestire efficacemente i rischi di sicurezza informatica.
- Definire ruoli e responsabilità, politiche e procedure per la gestione della sicurezza informatica all'interno dell'organizzazione.
- Designare un responsabile della sicurezza informatica o un team incaricato di supervisionare e gestire le iniziative di sicurezza informatica all'interno dell'organizzazione.
- Selezionare esperti di sicurezza informatica con competenze nel settore energetico, compresa la conoscenza di protocolli specifici per l'energia come Modbus e DNP3, per affrontare in modo efficace le sfide di sicurezza informatica specifiche del settore.

Grazie

Relatore: Stylianos Karagiannis (PDMFC, Portogallo) Si prega di

inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com