Elementi essenziali e gestione della sicurezza informatica (settore energetico)

CSP001

Argomento 8/10: Governance della sicurezza informatica per le organizzazioni energetiche

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Governance della sicurezza informatica

Introduzione

- La governance della sicurezza informatica si riferisce al quadro e ai processi stabiliti all'interno di un'organizzazione per gestire e mitigare efficacemente i rischi legati alla sicurezza informatica.
- La governance della sicurezza informatica è fondamentale per le organizzazioni energetiche al fine di proteggere le infrastrutture critiche, i dati sensibili e garantire l'affidabilità e la resilienza dei sistemi energetici.
- Stabilire un quadro di governance della sicurezza informatica completo e su misura per alle esigenze e alle sfide specifiche delle organizzazioni energetiche.
- Condurre regolarmente valutazioni e audit dei rischi di sicurezza informatica per identificare, valutare e dare priorità ai rischi di sicurezza informatica all'interno dell'organizzazione.
- Valutare l'efficacia dei controlli esistenti e identificare le lacune o le vulnerabilità che potrebbero rappresentare una minaccia per i sistemi energetici.
- La creazione di un solido quadro di governance della sicurezza informatica migliora la posizione di sicurezza dell'organizzazione garantendo una gestione proattiva dei rischi e la conformità agli standard e alle normative del settore.

Valutazione dei rischi

Introduzione

La valutazione dei rischi è un processo sistematico di identificazione, analisi e valutazione dei potenziali rischi o minacce che potrebbero influire su un'organizzazione o un sistema.

1. Identificare risorse: Critiche energia infrastrutture vulnerabili alle minacce informatiche.
2. Valutare le vulnerabilità: valutare i punti deboli nel software, nell'hardware, nelle configurazioni di rete e nei processi operativi.
3. Determinare minacce: Identificare potenziali minacce minacce e le loro capacità.
4. Valutare le conseguenze: valutare i potenziali impatti degli attacchi informatici sulle operazioni energetiche, sulla sicurezza e sull'affidabilità.
5. Calcolare il rischio: quantificare la probabilità e l'impatto dei rischi identificati.
6. Mitigazione e gestione dei rischi: sviluppare strategie per mitigare e gestire i rischi.
7. Monitoraggio e revisione: monitorare continuamente le minacce emergenti e rivedere le misure di mitigazione dei rischi.

Risk Assessment

Identificare le risorse

Componenti critici delle infrastrutture energetiche

- Modbus: protocollo di comunicazione ampiamente utilizzato nei sistemi di controllo industriale (ICS) per i sistemi di supervisione, controllo e acquisizione dati (SCADA). È comunemente utilizzato negli impianti di generazione e distribuzione di energia elettrica.
- DNP3 (Distributed Network Protocol): un altro protocollo utilizzato nei sistemi SCADA, in particolare nel settore dell'energia elettrica, per la comunicazione tra stazioni master e unità terminali remote (RTU).
- Sistemi di controllo e sistemi SCADA: sistemi di controllo centralizzati utilizzati per monitorare e controllare i processi industriali, compresa la produzione e la distribuzione di energia.
- Data center: strutture che ospitano server, dispositivi di archiviazione e apparecchiature di rete per la gestione dei dati e delle applicazioni relativi all'energia.
- Reti aziendali: infrastruttura IT utilizzata per funzioni amministrative, tra cui posta elettronica, condivisione di file e applicazioni aziendali.

Assess Vulnerabilities and Threats

Valutare le vulnerabilità - Determinare le minacce

Valutare i punti deboli del software, dell'hardware e dei processi operativi

- Vulnerabilità nelle implementazioni Modbus e DNP3 (ad esempio, mancanza di autenticazione, comunicazione non crittografata).
- Versioni obsolete di software e firmware nei sistemi di controllo.
- Controlli di accesso inadeguati e password deboli.
- Architetture di rete vulnerabili con segmentazione insufficiente.
- Mancanza di consapevolezza e formazione in materia di sicurezza informatica migliori pratiche.
- Minacce esterne: soggetti malintenzionati che prendono di mira le infrastrutture energetiche per ottenere guadagni finanziari, causare interruzioni o sabotaggi.
- Attori statali che conducono attività di spionaggio informatico o lanciano attacchi informatici per scopi politici o strategici.
- Minacce interne: dipendenti, appaltatori o fornitori terzi che hanno accesso a sistemi e informazioni critici.

Valutare le conseguenze

Valutare i potenziali impatti degli attacchi informatici

- Interruzione dell'approvvigionamento energetico con conseguenti perdite economiche e potenziali blackout.
- Compromissione della sicurezza del personale e del pubblico a causa di guasti operativi
  .
- Danni ambientali danni rilasci causati da o guasti rilasci incontrollati nei sistemi di monitoraggio.
- Danno alla reputazione e perdita di fiducia dei clienti nel fornitore di energia.

Quantificare la probabilità e l'impatto dei rischi identificati:

- Metriche di probabilità: basate su dati storici, informazioni sulle minacce e valutazioni delle vulnerabilità.
- Metriche di impatto: impatto finanziario, tempi di inattività operativa, rischi per la sicurezza, sanzioni per non conformità normativa.
- Valutazione del rischio: utilizzo di una matrice o formula di rischio per calcolare il livello di rischio complessivo in base alla probabilità e ai punteggi di impatto.

Mitigazione e gestione dei rischi

Mitigare e gestire i rischi

- Implementare controlli di sicurezza informatica: firewall, sistemi di rilevamento/prevenzione delle intrusioni (IDS/IPS), protezione degli endpoint, patch di sicurezza.
- Migliorare i controlli di accesso: meccanismi di autenticazione forte, accesso con privilegi minimi, controlli di accesso basati sui ruoli (RBAC).
- Condurre regolarmente valutazioni della vulnerabilità e test di penetrazione.
- Sviluppare e implementare piani di risposta agli incidenti e di continuità operativa.
- Fornire continua consapevolezza formazione formazione in materia di migliori migliori pratiche.

Monitoraggio continuo delle minacce emergenti e revisione delle misure di mitigazione dei rischi

.

- Implementare strumenti e tecnologie di monitoraggio delle minacce in tempo reale per Modbus, DNP3 e altre risorse critiche. Rivedere e aggiornare regolarmente i controlli di sicurezza informatica e i piani di risposta agli incidenti.
- Condurre analisi post-incidente per identificare le lezioni apprese e migliorare la resilienza.

Grazie

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

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