Elementi essenziali e gestione della sicurezza informatica per il settore energetico

Argomento 1: Condotta etica e professionalità nel campo della sicurezza informatica

PRESENTAZIONE DI:
Paresh Rathod
Laurea University of Applied Sciences, Finlandia

Ringraziamenti

- Finanziato dall'Unione Europea. Le opinioni e i pareri espressi sono tuttavia esclusivamente quelli dell'autore/degli autori e non riflettono necessariamente quelli dell'Unione Europea o dell'HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili per essi.
- Accordo di progetto n. 101083594

Funded by the European Union

CyberSecPro

Importanza della professionalità e della condotta etica nella sicurezza informatica nel settore energetico

Nel campo della sicurezza informatica energetica, è fondamentale mantenere i più elevati standard di professionalità e condotta etica. In quanto infrastrutture critiche, i sistemi energetici sono un obiettivo primario per le minacce informatiche, rendendo essenziale il rispetto dei principi di riservatezza, integrità e disponibilità. Il mancato rispetto di tali principi potrebbe avere gravi conseguenze, tra cui potenziali interruzioni dell'approvvigionamento energetico, perdite finanziarie e persino implicazioni per la sicurezza nazionale.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Incontra i tuoi formatori

Paresh Rathod

Specializzato in formazione sulla sicurezza informatica e responsabile tematico RDI presso Laurea, Finlandia. Apporta un bagaglio di conoscenze nel campo della tecnologia e della formazione.

Pasi Kämppi

Specializzato in formazione sulla sicurezza informatica e coordinatore dei corsi di laurea presso Laurea, Finlandia. Apporta un bagaglio di conoscenze nel campo delle infrastrutture di rete e della formazione

Ricardo Lugo

Specializzato in aspetti umani della formazione sulla sicurezza informatica e ricercatore post-dottorato e senior presso TalTech, Accademia marittima estone.

Kitty Kioskli

Specializzata negli aspetti umani della formazione sulla sicurezza informatica, è amministratore delegato e cofondatrice di trustilio BV, Paesi Bassi. Ha conseguito un dottorato di ricerca in psicologia della salute presso il King's College di Londra.

Principi etici alla base delle pratiche di sicurezza informatica e della condotta professionale

1 Integrità

I professionisti della sicurezza informatica devono mantenere l'integrità dei dati e dei sistemi garantendone l'accuratezza, la completezza e l'autenticità. Ciò comporta l'implementazione di controlli rigorosi, lo svolgimento di audit regolari e l'adesione alle migliori pratiche del settore per prevenire l'accesso non autorizzato, la modifica o la distruzione di informazioni sensibili.

2 Riservatezza

La protezione delle informazioni sensibili è una responsabilità fondamentale nella sicurezza informatica.
I professionisti devono salvaguardare la riservatezza dei dati implementando sistemi di crittografia robusti, controlli di accesso e procedure di gestione dei dati. Ciò garantisce che le informazioni sensibili rimangano accessibili solo alle persone autorizzate, proteggendo la privacy degli individui e delle organizzazioni.

3 Disponibilità

Le misure di sicurezza informatica devono garantire la disponibilità dei sistemi e dei dati quando necessario agli utenti autorizzati. Ciò comporta l'implementazione di ridondanza, meccanismi di failover e piani di risposta agli incidenti per ridurre al minimo i tempi di inattività e garantire la continuità operativa in caso di attacchi informatici o guasti del sistema.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Il ruolo fondamentale dell'etica

Salvaguardia delle infrastrutture critiche

Il settore energetico è una componente fondamentale delle infrastrutture di una nazione, in quanto fornisce energia alle abitazioni, alle imprese e ai servizi essenziali.
I professionisti della sicurezza informatica hanno l'enorme responsabilità di proteggere questi sistemi da attacchi dannosi, che potrebbero potenzialmente interrompere l'approvvigionamento energetico e causare gravi disagi.

Mantenere la fiducia del pubblico

La fiducia del pubblico nel settore energetico è essenziale per il suo funzionamento e la sua crescita continui. Aderendo ai principi etici, i professionisti della sicurezza informatica possono contribuire a mantenere questa fiducia, garantendo che gli interessi del pubblico siano prioritari e che la sua privacy e sicurezza siano protette.

Mantenere l'integrità professionale

I professionisti della sicurezza informatica nel settore energetico devono mantenere i più elevati standard di integrità professionale. Ciò include il mantenimento della riservatezza, il rispetto dei diritti di proprietà intellettuale e l'evitare conflitti di interesse che potrebbero compromettere la loro obiettività e imparzialità.

Divulgazione professionale responsabile e pratiche etiche

1

Identificare le vulnerabilità

I professionisti della sicurezza informatica hanno la responsabilità di identificare e segnalare le vulnerabilità nei sistemi energetici. Questo processo deve essere condotto in modo etico e professionale, senza sfruttare o danneggiare i sistemi oggetto di indagine.

2

Divulgazione responsabile

Una volta identificate le vulnerabilità, è necessario seguire pratiche di divulgazione responsabile. Ciò comporta la notifica alle parti interessate, come i proprietari o i fornitori dei sistemi, e la concessione loro di tempo sufficiente per risolvere le vulnerabilità prima di divulgare pubblicamente le informazioni.

3

Rimedio collaborativo

I professionisti della sicurezza informatica dovrebbero collaborare con le parti interessate per sviluppare e attuare strategie di rimedio efficaci. Questo processo dovrebbe essere guidato da principi etici, garantendo che gli interessi di tutte le parti coinvolte, compreso il pubblico, siano presi in considerazione.

CSP0
Pares a USA, Finlandia

Attuazione di linee guida e politiche etiche

1

Stabilire politiche chiare

Le organizzazioni energetiche dovrebbero stabilire politiche chiare e complete che definiscano linee guida etiche per le pratiche di sicurezza informatica. Tali politiche dovrebbero essere regolarmente riviste e aggiornate per riflettere i cambiamenti nelle normative, negli standard di settore e nelle minacce emergenti.

2

Fornire formazione e sensibilizzazione

È necessario condurre regolarmente programmi di formazione e sensibilizzazione per garantire che tutti i professionisti della sicurezza informatica e le parti interessate all'interno dell'organizzazione abbiano familiarità con le linee guida e le politiche etiche. Ciò contribuisce a promuovere una cultura di condotta etica e rafforza l'importanza di pratiche responsabili.

3

Monitorare e garantire la conformità

Le organizzazioni dovrebbero implementare meccanismi per monitorare e garantire il rispetto delle linee guida e delle politiche etiche. Ciò può comportare lo svolgimento di audit, l'implementazione di programmi di protezione degli informatori e la definizione di conseguenze chiare in caso di violazioni.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Evitare i conflitti di interesse

Interessi personali vs. interessi professionali

I professionisti della sicurezza informatica devono essere vigili nell'identificare ed evitare situazioni in cui i loro interessi personali potrebbero entrare in conflitto con le loro responsabilità professionali. Ciò include interessi finanziari, relazioni personali o qualsiasi altra circostanza che potrebbe potenzialmente influenzare la loro obiettività o compromettere la loro condotta etica.

Trasparenza e divulgazione

In situazioni in cui esiste un potenziale conflitto di interessi, i professionisti devono agire con trasparenza e comunicare il conflitto alle parti interessate. Ciò consente di adottare misure adeguate per mitigare il rischio e mantenere l'integrità etica.

Ricusazione e supervisione etica

Quando un conflitto di interessi non può essere risolto o gestito in modo adeguato, i professionisti della sicurezza informatica dovrebbero ricusarsi dalla situazione.
Le organizzazioni dovrebbero inoltre istituire comitati o processi di supervisione etica per esaminare e affrontare potenziali conflitti di interesse.

CSP001_C_E-ARGOMENTO-1:
Paresh Rathod, Laurea USA, Finlandia

Segnalazione di incidenti di sicurezza

1

Identificazione tempestiva

I professionisti della sicurezza informatica devono essere vigili nell'identificare tempestivamente potenziali incidenti o violazioni della sicurezza all'interno dei sistemi energetici. Ciò comporta il monitoraggio continuo dei sistemi alla ricerca di attività sospette, l'analisi dei registri e l'indagine sulle anomalie.

2

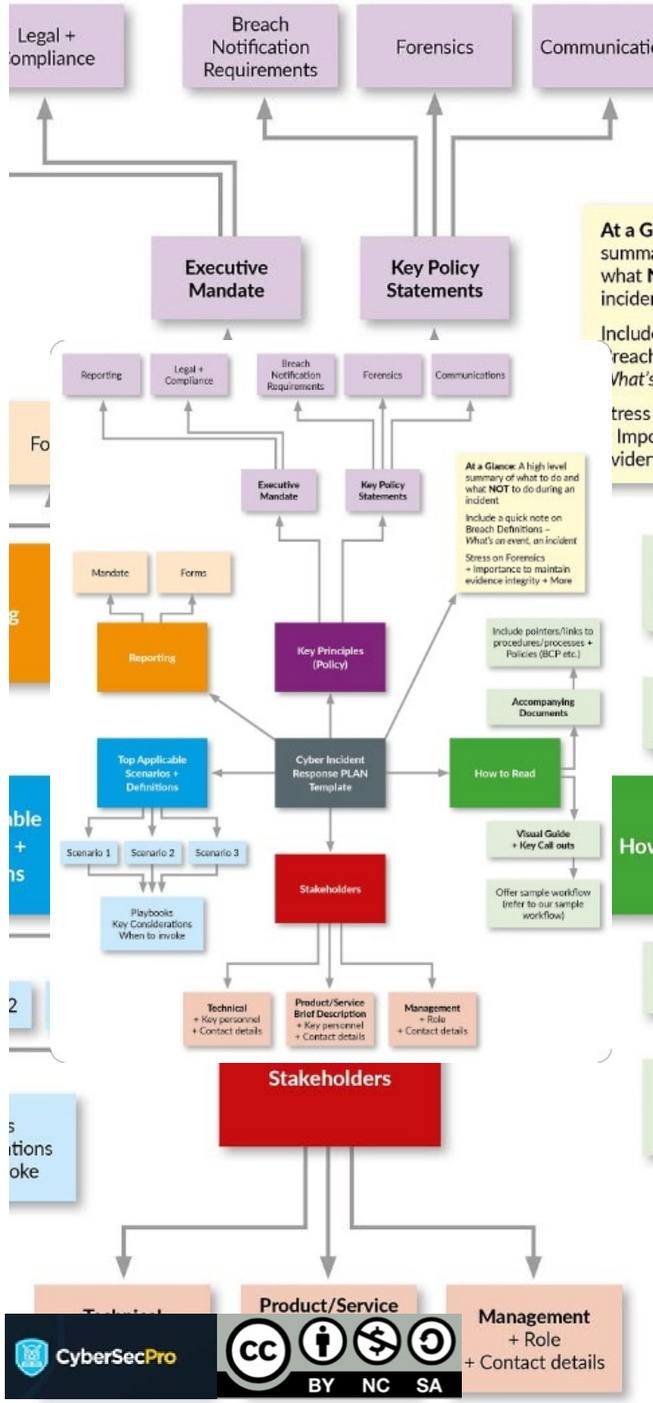
Segnalazione tempestiva

Una volta identificato un incidente di sicurezza, è necessario segnalarlo tempestivamente attraverso i canali e le procedure stabiliti. La segnalazione tempestiva è fondamentale per mitigare i potenziali danni, contenere l'incidente e avviare misure di risposta adeguate.

3

Documentazione completa

È necessario conservare una documentazione dettagliata dell'incidente di sicurezza, comprese le informazioni sulla natura dell'incidente, i sistemi interessati, il potenziale impatto e le azioni intraprese. Questa documentazione costituisce una risorsa preziosa per le indagini, la risoluzione dei problemi e la prevenzione di incidenti futuri.



CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Mantenere la riservatezza nella sicurezza informatica nel settore energetico

Classificazione dei dati

Le organizzazioni energetiche dovrebbero implementare solidi sistemi di classificazione dei dati per identificare e categorizzare le informazioni sensibili in base al loro livello di riservatezza. Ciò consente l'implementazione di controlli di sicurezza e restrizioni di accesso adeguati.

Controlli di accesso

L'accesso alle informazioni riservate dovrebbe essere limitato in base ai principi del privilegio minimo e della necessità di sapere. Ciò comporta l'implementazione di solidi meccanismi di autenticazione, controlli di accesso basati sui ruoli e revisioni periodiche dei privilegi di accesso.

Procedure di trattamento dei dati

È necessario stabilire procedure chiare per la gestione, l'archiviazione, la trasmissione e lo smaltimento sicuri dei dati riservati. Ciò include l'uso della crittografia, canali di comunicazione sicuri e il rigoroso rispetto delle politiche di conservazione e distruzione dei dati.

Sensibilizzazione e formazione

I professionisti della sicurezza informatica e le parti interessate dovrebbero seguire regolarmente programmi di formazione e sensibilizzazione per rafforzare l'importanza di mantenere la riservatezza e gestire correttamente le informazioni sensibili.

Integrità nei sistemi energetici

Controlli di accesso

L'implementazione di controlli di accesso robusti è fondamentale per mantenere l'integrità dei sistemi energetici. Ciò include meccanismi di autenticazione avanzati, restrizioni di accesso basate sui ruoli e audit regolari per impedire accessi e modifiche non autorizzati.

Pratiche di codifica sicure

L'adesione a pratiche di codifica sicure è essenziale per lo sviluppo e il mantenimento di sistemi energetici integri. Ciò comporta il rispetto delle migliori pratiche del settore, la conduzione di revisioni del codice e l'implementazione di standard di codifica sicuri per prevenire vulnerabilità e garantire l'affidabilità dei sistemi.

Audit e monitoraggio regolari

È necessario condurre audit regolari e un monitoraggio continuo dei sistemi energetici per individuare e risolvere eventuali problemi di integrità. Ciò include il monitoraggio di modifiche non autorizzate, la conduzione di valutazioni di vulnerabilità e l'implementazione di sistemi di rilevamento e prevenzione delle intrusioni.

Meccanismi di backup e ripristino

È necessario implementare solidi meccanismi di backup e ripristino per garantire l'integrità dei sistemi energetici in caso di incidenti di sicurezza o guasti del sistema. Ciò comporta il mantenimento di backup ridondanti, il collaudo delle procedure di ripristino e l'implementazione di piani di ripristino di emergenza.

Disponibilità dei sistemi energetici

Misura	Descrizione
Ridondanza	Implementazione di sistemi e componenti ridondanti per garantire la continuità delle operazioni in caso di guasti o attacchi.
Bilanciamento del carico	Distribuzione dei carichi di lavoro su più sistemi per prevenire il sovraccarico e garantire un utilizzo efficiente delle risorse.
Meccanismi di failover	Creazione di meccanismi di failover automatizzati per passare senza soluzione di continuità a sistemi o componenti di backup in caso di guasti.
Risposta agli incidenti	Sviluppo e verifica di piani di risposta agli incidenti per individuare, reagire e ripristinare rapidamente la situazione in caso di incidenti di sicurezza che potrebbero influire sulla disponibilità del sistema.
Continuità operativa	Implementazione di strategie e piani di continuità operativa per garantire la disponibilità di sistemi e servizi energetici critici durante e dopo eventi dirompenti.

Considerazioni etiche nella ricerca sulla sicurezza informatica nel settore energetico

Sperimentazione responsabile

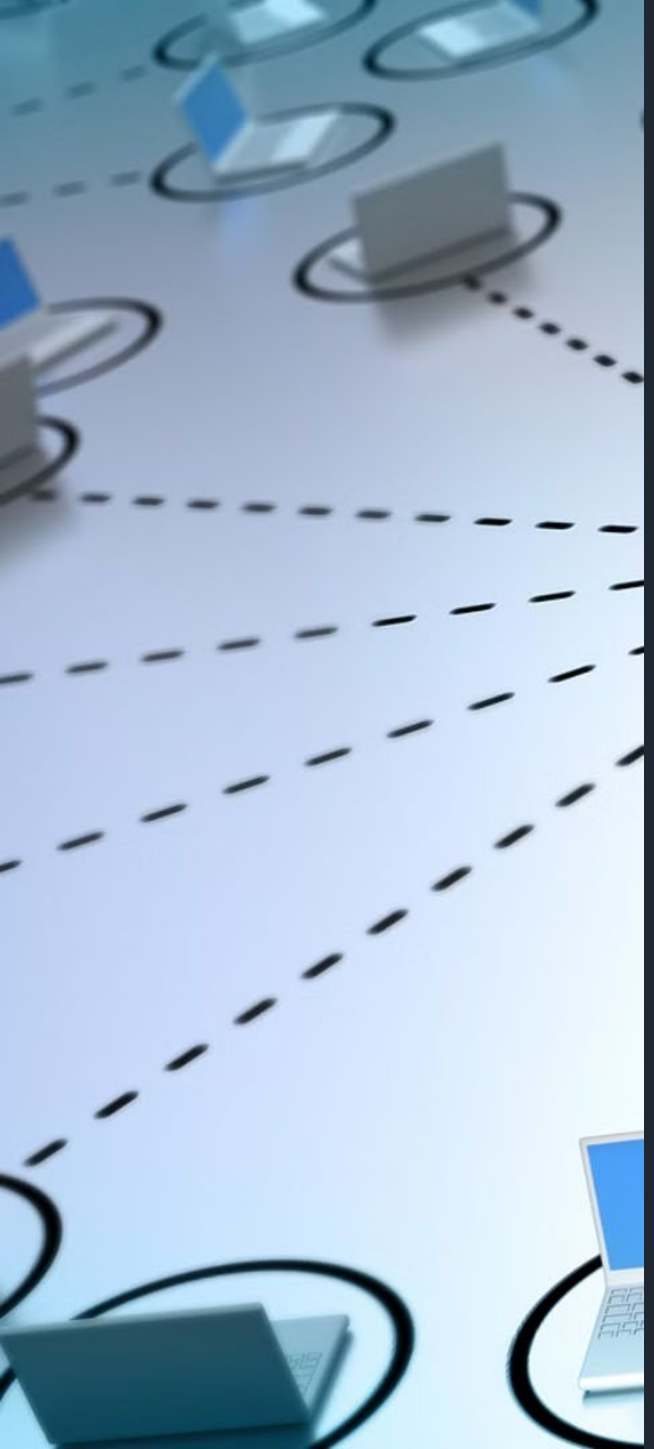
La ricerca sulla sicurezza informatica che coinvolge i sistemi energetici deve essere condotta in modo responsabile e controllato, assicurando che non vengano causati danni ai sistemi operativi o alle infrastrutture critiche. Ciò può comportare l'utilizzo di ambienti di prova isolati, simulazioni o l'ottenimento delle autorizzazioni e dei permessi adeguati.

Ricerca a duplice uso

I ricercatori devono essere consapevoli della potenziale natura a duplice uso del loro lavoro, in cui i risultati o le tecniche potrebbero essere utilizzati in modo improprio per scopi dannosi. È necessario predisporre adeguate misure di salvaguardia e considerazioni etiche per prevenire l'uso improprio dei risultati della ricerca.

Privacy e protezione dei dati

La ricerca sui sistemi energetici può comportare la raccolta e l'analisi di dati sensibili. È necessario adottare misure adeguate per proteggere la privacy e la riservatezza di qualsiasi informazione personale o sensibile, nel rispetto delle normative e delle linee guida etiche pertinenti.



Collaborazione e condivisione delle informazioni

1

Stabilire un rapporto di fiducia

Una collaborazione efficace e la condivisione delle informazioni nella sicurezza informatica energetica richiedono la creazione di un clima di fiducia tra le parti interessate. Ciò comporta la costruzione di relazioni, il rispetto dei principi etici e la dimostrazione di un impegno a proteggere le informazioni sensibili e le risorse condivise.

2

Definire i protocolli

È necessario stabilire protocolli e procedure chiari per regolamentare la condivisione di informazioni e intelligence relative alle minacce e agli incidenti di sicurezza informatica. Tali protocolli dovrebbero affrontare questioni quali la riservatezza, il trattamento dei dati e la protezione delle informazioni sensibili.

3

Promuovere le partnership

Promuovere partnership e collaborazioni tra organizzazioni energetiche, agenzie governative ed esperti di sicurezza informatica è fondamentale per migliorare la difesa collettiva contro le minacce informatiche. Ciò consente la condivisione delle migliori pratiche, delle informazioni sulle minacce e lo sviluppo di strategie di risposta coordinate.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Hacking etico e test di penetrazione

1 Ambito di applicazione e autorizzazione

Le attività di ethical hacking e penetration testing devono essere condotte entro un ambito chiaramente definito e con la debita autorizzazione delle parti interessate. Ciò garantisce che le attività siano concentrate su obiettivi legittimi e non causino inavvertitamente danni o violino leggi o regolamenti.

2 Divulgazione e segnalazione

Qualsiasi vulnerabilità o debolezza della sicurezza identificata durante l'hacking etico o i test di penetrazione deve essere comunicata in modo responsabile alle parti interessate. Ciò consente di porre rimedio e mitigare tempestivamente i potenziali rischi, nel rispetto dei principi etici e delle migliori pratiche.

3 Gestione sicura dei dati

Nel corso dell'hacking etico o dei test di penetrazione, i professionisti della sicurezza informatica possono avere accesso a dati o sistemi sensibili. È fondamentale gestire questi dati in modo sicuro, mantenere la riservatezza e garantire l'adozione di misure di protezione adeguate per impedire l'accesso non autorizzato o uso improprio.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Minacce interne e condotta etica

1

Consapevolezza e formazione dei dipendenti

Le organizzazioni dovrebbero implementare programmi completi di sensibilizzazione e formazione per educare i dipendenti sulle minacce interne, la condotta etica e l'importanza della sicurezza informatica. Ciò contribuisce a creare una cultura della sicurezza e riduce il rischio di attività interne involontarie o dolose.

2

Controlli di accesso e monitoraggio

L'implementazione di controlli di accesso robusti, principi di privilegio minimo e monitoraggio continuo delle attività degli utenti può aiutare a rilevare e mitigare potenziali minacce interne. Ciò include il monitoraggio di comportamenti sospetti, tentativi di accesso non autorizzati e sottrazione di dati.

3

Protezione degli informatori

Le organizzazioni dovrebbero stabilire politiche e procedure di protezione degli informatori per incoraggiare la segnalazione di attività non etiche o illegali relative alla sicurezza informatica. Ciò crea un ambiente di fiducia e responsabilità, proteggendo al contempo coloro che segnalano potenziali minacce o violazioni.

4

Risposta agli incidenti e indagini

È necessario predisporre procedure chiare per rispondere e indagare su potenziali minacce interne. Ciò include piani di risposta agli incidenti, capacità di analisi forense e collaborazione con le forze dell'ordine, se necessario.

Sfide etiche nella sicurezza informatica nel settore energetico

Privacy e sicurezza dei dati

Le aziende energetiche raccolgono e archiviano grandi quantità di dati sensibili, tra cui informazioni sui clienti, dati operativi e dettagli sulle infrastrutture critiche.
I professionisti della sicurezza informatica devono garantire che questi dati siano protetti da accessi non autorizzati, uso improprio o divulgazione.

Equilibrio tra sicurezza e accessibilità

Sebbene misure di sicurezza robuste siano essenziali, devono essere bilanciate con la necessità del personale autorizzato di accedere ai sistemi e ai dati in modo tempestivo. Controlli eccessivamente restrittivi possono ostacolare l'efficienza operativa e potenzialmente mettere a rischio vite umane in situazioni di emergenza.

Divulgazione delle vulnerabilità

I professionisti della sicurezza informatica possono scoprire vulnerabilità critiche nei sistemi o nei software utilizzati nel settore energetico. Devono affrontare il dilemma etico se rendere pubbliche tali vulnerabilità, che potrebbero potenzialmente aiutare malintenzionati, o collaborare in privato con fornitori e organizzazioni per risolvere i problemi.

Sviluppare una cultura etica

1

Impegno della leadership

La promozione di una cultura etica nella sicurezza informatica nel settore energetico inizia con un forte impegno da parte della leadership. I dirigenti e l'alta dirigenza devono dare l'esempio, dimostrando dedizione alla condotta etica e dandole la priorità insieme agli obiettivi aziendali.

2

Politiche e formazione complete

Le organizzazioni dovrebbero sviluppare e implementare politiche e procedure complete che delineino il comportamento etico previsto e forniscano indicazioni su come affrontare i dilemmi etici. Dovrebbero essere condotti regolarmente programmi di formazione e sensibilizzazione per garantire che tutti i dipendenti, compresi i professionisti della sicurezza informatica, abbiano familiarità con queste politiche e comprendano le loro responsabilità.

3

Comunicazione aperta e segnalazione

È fondamentale creare un ambiente in cui i dipendenti si sentano a proprio agio nel sollevare questioni etiche e segnalare potenziali violazioni. Le organizzazioni dovrebbero stabilire canali di segnalazione chiari e garantire che le questioni siano affrontate tempestivamente e senza ritorsioni.

4

Monitoraggio e miglioramento continui

La condotta etica dovrebbe essere costantemente monitorata e valutata, con processi in atto per identificare le aree di miglioramento. Audit regolari, valutazioni dei rischi e meccanismi di feedback possono aiutare le organizzazioni a stare al passo con le sfide etiche emergenti e a mantenere una forte cultura etica.

Considerazioni normative e legali

Regolamentazione/Legge	Descrizione
Standard per la protezione delle infrastrutture critiche (CIP)	Questi standard, sviluppati dalla North American Electric Reliability Corporation (NERC), stabiliscono i requisiti per la protezione delle infrastrutture critiche, compresi i controlli di sicurezza informatica e le pratiche di gestione dei rischi.
Leggi sulla privacy dei dati	Diverse leggi sulla privacy dei dati, come il Regolamento generale sulla protezione dei dati (GDPR) e il California Consumer Privacy Act (CCPA), regolano la raccolta, l'utilizzo e la protezione dei dati personali, comprese le informazioni sui clienti detenute dalle aziende energetiche.
Leggi sulla condivisione delle informazioni relative alla sicurezza informatica	Leggi come il Cybersecurity Information Sharing Act (CISA) incoraggiano la condivisione di informazioni sulle minacce alla sicurezza informatica tra il governo e il settore privato, comprese le aziende energetiche, al fine di migliorare la preparazione e la risposta complessive.
Leggi sul controllo delle esportazioni	Le normative che regolano l'esportazione di tecnologie sensibili, compresi alcuni strumenti e tecniche di sicurezza informatica, possono applicarsi alle aziende energetiche che operano a livello internazionale o che collaborano con entità straniere.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Gestione dei rischi di terze parti

Due diligence e verifica

Le organizzazioni energetiche dovrebbero condurre processi di due diligence e di verifica approfonditi quando collaborano con fornitori, appaltatori o fornitori di servizi terzi. Ciò include la valutazione delle loro pratiche di sicurezza informatica, delle loro politiche e del loro rispetto degli standard etici al fine di mitigare i potenziali rischi.

Obblighi contrattuali

È necessario stabilire obblighi contrattuali chiari e accordi sul livello di servizio con le terze parti, delineando le loro responsabilità in materia di mantenimento della riservatezza, integrità e disponibilità dei sistemi e dei dati. Tali contratti dovrebbero includere anche disposizioni relative alla condotta etica e alla segnalazione di incidenti.

Monitoraggio continuo

Le organizzazioni dovrebbero monitorare e controllare costantemente le attività, l'accesso e la conformità di terzi agli standard di sicurezza ed etici stabiliti. Ciò contribuisce a garantire che i potenziali rischi vengano identificati e mitigati in modo tempestivo.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Riferimenti

1. IEEE. (2016). Codice etico IEEE. https://www.ieee.org/about/corporate/governance/p7-8.html
2. Codice etico e di condotta professionale ACM (2018). Association for Computing Machinery. https://www.acm.org/code-of-ethics
3. Barquin, R. C. (7 maggio 1992). Alla ricerca dei "Dieci Comandamenti'dell'etica informatica. Computer Ethics Institute. https://en.wikipedia.org/wiki/Ten_Commandments_of_Computer_Ethics
4. I Dieci Comandamenti dell'Etica Informatica, creati nel 1992 dal Computer Ethics Institute, offrono una serie di principi fondamentali per un uso etico del computer (Barquin, 1992).
5. Agenzia dell'Unione europea per la sicurezza informatica. (2022). ECSF, Quadro europeo delle competenze in materia di sicurezza informatica. Ufficio delle pubblicazioni. https://doi.org/10.2824/859537
6. R. Schoon e S. Kleinaltepohl, Cybersecurity nel settore elettrico: gestione delle infrastrutture critiche (SpringerLink, 2018).
7. J. R. Vacca, Industrial Cybersecurity for Engineers (Elsevier, 2015).
8. ECSO, "Energy Networks and Smart Grids", Cyber Security for the Energy Sector, WG3 Sectoral Demand, novembre 2018 URL: https://ecs-org.eu/ecso-uploads/2022/10/5fdb2673903c6.pdf
9. ENISA, "Panorama delle minacce alle reti intelligenti e guida alle buone pratiche", dicembre 2013 URL: https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
10. Altri riferimenti elencati in ciascun argomento del modulo CSP

Trasparenza: Fonti

1. Contenuto del video teaser: Il contenuto di questo video teaser si basa sui risultati del Work Package 3 del progetto CyberSecPro, con preziosi contributi dei partner CyberSecPro.
2. Competenza linguistica: il deliverable D3.1 è stato sottoposto a una rigorosa revisione linguistica. Ciò ha comportato l'utilizzo dell'intelligenza artificiale di Grammarly e la meticolosa revisione da parte di madrelingua inglesi.
3. Contenuti multimediali: tutte le immagini, i video e gli audio utilizzati sono stati ricavati da Pictory, Getty Images e altri database multimediali open stock.
4. Collaborazione con i partner: Ringraziamo i nostri partner CyberSecPro per il loro contributo, comprese le foto dei formatori presenti nel programma.
5. Materiali didattici: i materiali didattici per questo modulo CyberSecPro sono stati forniti da un formatore accreditato e il merito va riconosciuto agli autori.
6. Crediti creativi: video teaser creato utilizzando queste risorse dal professionista europeo della sicurezza informatica Paresh Rathod.
7. I materiali della formazione sono stati creati utilizzando letteratura accademica e di ricerca e Open Education Material (OEM), con il dovuto riconoscimento agli autori.
8. Alcuni dei materiali utilizzati includevano strumenti basati sull'intelligenza artificiale, tra cui simulatori vocali (con i dovuti crediti agli autori), per offrire ai partecipanti la migliore esperienza di apprendimento possibile.

CSP001_C_E-TOPIC-1:
Paresh Rathod, Laurea USA, Finlandia

Connettiti con CyberSecPro: Come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Si prega di inviare tutte le domande ai formatori (e/o):
paresh.rathod@laurea.fi