Come gestire il rischio in un mondo ESTESO?

Metodologia CRISP per l'analisi e la mitigazione delle minacce cyber-fisiche

Chi sono

BACKGROUND

PhD in Ingegneria dell'informazione con oltre 25 anni di esperienza nella scrittura e gestione di progetti di Ricerca, di innovazione tecnologica e trasformazione digitale.

AREAS OF EXPERTISE

Digital Trasformation, E-government, Business Process Engineering, Industry 4.0, Risk analysis, GDPR, Project Management

EXEPERIENCE

Consulente della Presidenza del Consiglio dei ministri per la transizione digitale della PA

Responsabile Tecnico GSALAb @ Unisalento

Docenza

Docente di Sistemi Informativi @ Università del Salento.

Certificatore del Credito di Imposta per le Attività di ricerca e sviluppo

Iscritto all'Albo dei certificatori del credito d'imposta per attività di ricerca e sviluppo, di innovazione tecnologica presso il MIMIT.

Manager di numerosi progetti di Ricerca e di trasferimento tecnologico in partnership con istituti di ricerca e aziende nazionali e internazionali.

Ricerca e Pubblicazioni Scientifiche

Numerose pubblicazioni scientifiche sul tema delle metodologie di progettazione di sistemi informativi collaborativi.

Innovation Manager ICT Unisalento

Coordinamento di numerosi progetti di Innovazione e Digital Trasformation dell'Università del Salento, from scratch to delivery.

Ideazione, coordinamento e stesura del Piano Strategico dei Sistemi Informatici di Unisalento.

Informatica per i Beni Culturali

Progettazione e Realizzazione di Sistemi Informativi Geografici on-line per la gestione di Scavi Archeologici e Beni culturali

Consulente

Consulenza per aziende private sul tema della Digital Trasformation e Risk Analysis nell'Industria 4.0. Consulente in ambito giudiziario.

Fellowship

@UCL (London): ICT service management.

@UTS (Sydney): Engineering service delivery design.

La trasformazione digitale: una rivoluzione dell'informazione

Internet ed il Web costituiscono un ecosistema tecnologico in grado di trasferire l'informazione senza lo spostamento di un mezzo fisico. Questa caratteristica fondamentale ha rivoluzionato il modo in cui accediamo, condividiamo e processiamo le informazioni nella società moderna.

La natura immateriale del trasferimento digitale ha eliminato molte barriere tradizionali: distanza geografica, costi di distribuzione fisica, tempi di consegna. Tuttavia, questa facilità di accesso e condivisione ha anche creato nuove sfide che non esistevano nell'era pre-digitale.

La velocità con cui le informazioni si propagano online, combinata con la capacità di raggiungere simultaneamente milioni di persone, ha amplificato sia le opportunità che i rischi associati alla comunicazione digitale. È essenziale comprendere come questa trasformazione stia influenzando non solo i singoli individui, ma l'intera struttura sociale ed economica.

Prima di esplorare i rischi specifici, è importante riconoscere che stiamo vivendo un momento di transizione storica paragonabile all'invenzione della stampa o alla rivoluzione industriale, con implicazioni che si estendono ben oltre la sfera tecnologica.

Una domanda fondamentale

Nel panorama della cybersecurity moderna, la domanda non è più **"se"** il nostro sistema sarà violato, ma **"quando"** accadrà.

Questa consapevolezza rappresenta un cambio di paradigma fondamentale nella gestione della sicurezza informatica. Mentre in passato ci si concentrava sulla prevenzione totale degli attacchi, oggi è necessario adottare un approccio che assuma la inevitabilità delle violazioni.

Accettare questa realtà non significa arrendersi, ma piuttosto:

- Progettare sistemi resilienti che possano resistere e riprendersi rapidamente da un attacco
- Implementare strategie di rilevamento precoce e risposta rapida
- Sviluppare piani di continuità operativa che minimizzino l'impatto degli incidenti
- Investire in formazione e preparazione del personale per gestire le emergenze

Questa nuova prospettiva ci porta a concentrarci sulla **gestione del rischio** piuttosto che sulla sua eliminazione completa, preparandoci per un mondo in cui la sicurezza assoluta è un'illusione.

Uno scenario plausibile...

Come mostrato nella serie TV "Zero Day" di Netflix, un attacco informatico può paralizzare infrastrutture critiche e minacciare la sicurezza nazionale, rendendo realistici scenari che fino a poco tempo fa sembravano fantascienza.

Non solo Fiction...

La storia recente ha dimostrato come le minacce cyber-fisiche possano causare danni significativi alle infrastrutture critiche. Ecco alcuni esempi emblematici:

Stuxnet - Centrale Nucleare Iraniana (2010)

Obiettivo: Impianto di arricchimento dell'uranio di Natanz

Impatto: Distruzione di circa 1.000 centrifughe attraverso l'alterazione della velocità di rotazione

Metodo: Malware sofisticato che colpiva i sistemi SCADA Siemens, rimanendo nascosto per mesi

Conseguenze: Primo esempio documentato di cyber-arma che causa danni fisici significativi

Colonial Pipeline - Stati Uniti (2021)

Obiettivo: Oleodotto che trasporta il 45% del carburante della costa orientale USA

Impatto: Interruzione completa delle operazioni per 6 giorni

Metodo: Attacco ransomware del gruppo DarkSide attraverso credenziali compromesse

Conseguenze: Carenza di carburante, aumento dei prezzi, pagamento di 4,4 milioni di dollari di riscatto

Rete Elettrica Ucraina (2015-2016)

Obiettivo: Centrali elettriche e sistemi di distribuzione

Impatto: Blackout per 230.000 utenti (2015) e interruzioni prolungate (2016)

Metodo: Combinazione di spear phishing, malware BlackEnergy e intervento manuale

Conseguenze: Primo attacco cyber a causare un blackout su larga scala

Impianto Siderurgico Tedesco (2014)

Obiettivo: Acciaieria in Germania

Impatto: Impossibilità di spegnere in sicurezza un altoforno

Metodo: Attacco spear phishing seguito da movimento laterale nei sistemi di controllo

Conseguenze: Danni fisici significativi all'impianto e perdite di produzione

Attacco ai Cercapersone - Libano (2024)

Obiettivo: Cercapersone utilizzati da membri di Hezbollah

Impatto: Esplosione simultanea di migliaia di dispositivi, causando morti e feriti

Metodo: Compromissione della supply chain con inserimento di esplosivi nei dispositivi

Conseguenze: Dimostrazione della vulnerabilità dei dispositivi di comunicazione e dell'efficacia degli attacchi alla catena di fornitura

6

Data Breach Equifax - Stati Uniti (2017)

Obiettivo: Agenzia di credito Equifax

Impatto: Compromissione dei dati personali di 147 milioni di americani

Metodo: Sfruttamento di vulnerabilità non corretta in Apache Struts

Conseguenze: Esposizione di numeri di sicurezza sociale, date di nascita, indirizzi e numeri di carta di credito - considerato uno dei peggiori data breach della storia

Infrastruttura critica

Le **infrastrutture critiche** sono sistemi e asset essenziali per il funzionamento di una società e di un'economia. La loro distruzione o interruzione avrebbe un impatto debilitante sulla sicurezza nazionale, sulla salute pubblica, sull'economia e sul benessere sociale.

Energia

Centrali elettriche, reti di distribuzione, impianti petroliferi e del gas naturale. Garantiscono l'alimentazione energetica di tutto il paese.

Acqua

Sistemi di trattamento, purificazione e distribuzione dell'acqua potabile. Fondamentali per la salute pubblica e le attività industriali.

Trasporti

Aeroporti, porti, ferrovie, strade e sistemi di controllo del traffico. Essenziali per la mobilità di persone e merci.

Comunicazioni

Reti telefoniche, internet, sistemi satellitari e infrastrutture di telecomunicazione. Permettono lo scambio di informazioni.

Sanità

Ospedali, sistemi sanitari, laboratori e infrastrutture per la produzione di farmaci. Vitali per la salute pubblica.

Servizi Finanziari

Banche, mercati finanziari, sistemi di pagamento e infrastrutture economiche. Sostengono l'economia nazionale.

La crescente **digitalizzazione** di questi sistemi ha aumentato significativamente la loro vulnerabilità agli attacchi informatici. La convergenza tra tecnologie dell'informazione (IT) e tecnologie operative (OT) ha creato nuovi vettori di attacco che possono causare danni fisici attraverso mezzi digitali.

La protezione delle infrastrutture critiche richiede un approccio multidisciplinare che combini sicurezza fisica, cybersecurity, resilienza operativa e coordinamento tra settori pubblico e privato.

Cyber Attack: Conseguenze

La compromissione di un impianto industriale/ infrastruttura critica da parte di un aggressore remoto può avere conseguenze devastanti, tra cui:

Conseguenze Operative

- Interruzione dei processi produttivi
- Malfunzionamento dei sistemi di controllo
- Perdita di controllo sugli asset critici
- Alterazione dei parametri di processo

Conseguenze sulla Sicurezza

- Disattivazione dei sistemi di sicurezza
- Incidenti con potenziali danni a persone
- Rilascio di sostanze pericolose
- Esplosioni o incendi

Conseguenze Economiche

- Perdite finanziarie dirette
- Costi di ripristino dei sistemi
- Danni reputazionali
- Sanzioni normative

Cyber Attack: Contromisure

La difesa efficace contro i cyber attacchi richiede un approccio multistrato che combini tecnologie, processi e formazione del personale. Le contromisure devono essere progettate per prevenire, rilevare e rispondere agli attacchi.

Segmentazione di Rete

- Isolamento dei sistemi OT dai sistemi IT
- Implementazione di firewall industriali
- Controllo degli accessi basato su zone
- Monitoraggio del traffico di rete

Gestione delle Identità e Accessi

- Autenticazione multi-fattore (MFA)
- Principio del privilegio minimo
- Gestione centralizzata degli accessi
- Audit regolari delle autorizzazioni

Monitoraggio e Rilevamento

- Sistemi SIEM per la correlazione degli eventi
- Monitoraggio comportamentale degli asset
- Rilevamento delle anomalie di processo
- Threat intelligence e indicatori di compromissione

Gestione delle Vulnerabilità

- Scansioni regolari delle vulnerabilità
- Gestione delle patch in ambiente OT
- Valutazione dei rischi di sicurezza
- Test di penetrazione periodici

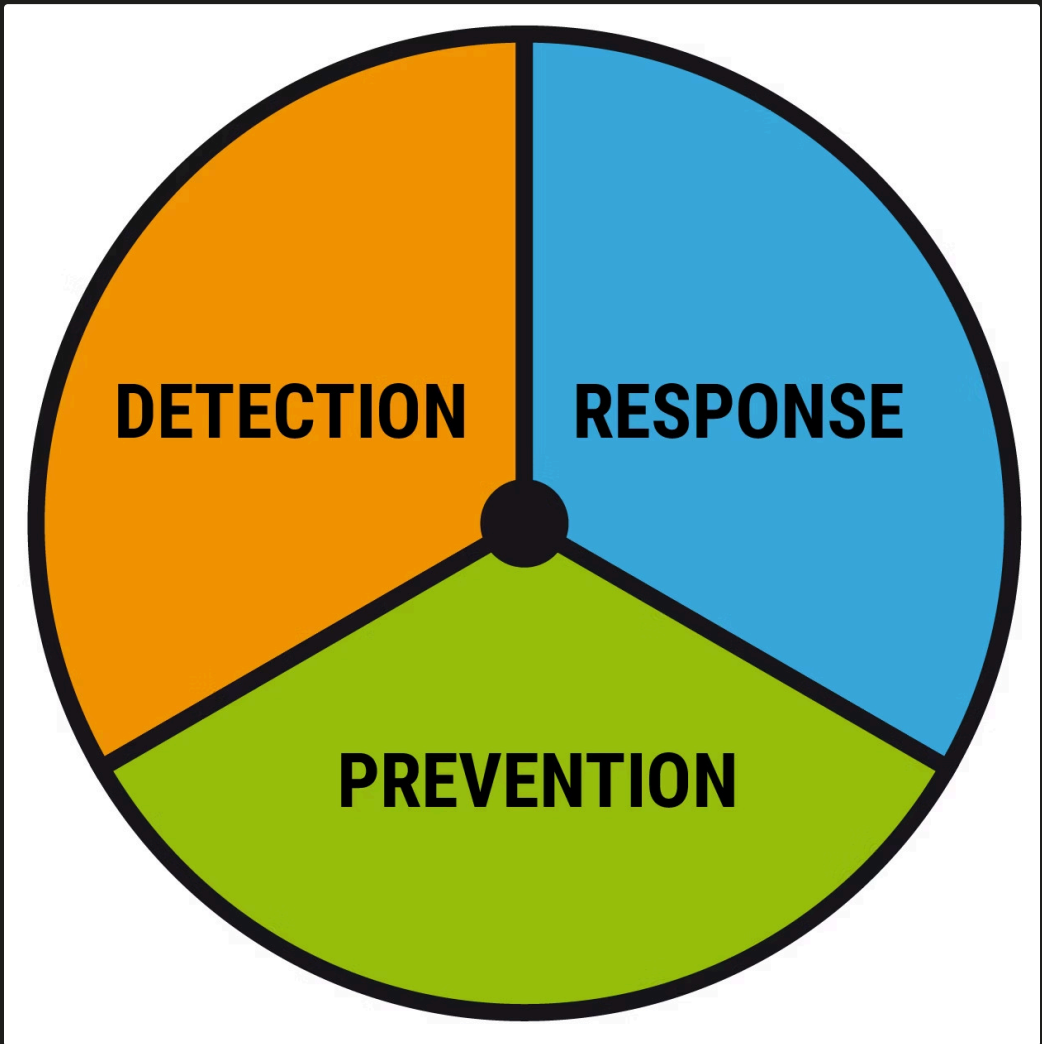
Formazione e Sensibilizzazione

- Training del personale sulla cybersecurity
- Simulazioni di attacchi phishing
- Procedure di incident response
- Cultura della sicurezza aziendale

Business Continuity e Recovery

- Backup sicuri e testati regolarmente
- Piani di continuità operativa
- Procedure di ripristino dei sistemi
- Comunicazione di crisi

Le funzioni per la gestione della Cyber Security



- **Detection**: rivisitare ed estendere ad infrastrutture ed ambienti OT le modalità di monitoraggio e protezione degli end-point utilizzate in ambito IT potendo quindi operare con dispositivi variegati come PC, Server, Router, ICS, SCADA, PLC, RTU ecc.;
- **Prevention**: ridefinire i processi di censimento degli assets e prevenzione degli incidenti alla luce dei nuovi assets critici (impianti industriali, infrastrutture IT e OT, fornitori si servizi di pubblico interesse), includendo elementi di sicurezza fisica ed organizzativa oltre che cyber e metodi estrumenti di Cyber Profilassi, sfruttando anche tecnologie cognitive e di Threat Intelligence ;
- **Response**: definire nuovi protocolli di intervento e cooperazione, da automatizzare attraverso strumenti di process automation, tra tutti i principali attori della sicurezza, ovvero, operatori cyber security, forze di difesa e pronto intervento, al fine di poter attivare e coordinare risposte physical oltre che Cyber ad incidenti informatici con impatti fisici sulle infrastrutture critiche, sulla popolazione e le istituzioni.

Cyber-Physical Response Plan

Cos'è il Cyber-Physical Response Plan

Un piano di risposta strutturato che integra la gestione degli incidenti cyber con la gestione degli impatti fisici sui sistemi industriali.

Il piano definisce procedure specifiche per rispondere a incidenti che coinvolgono sia la dimensione cyber che quella fisica degli impianti industriali.

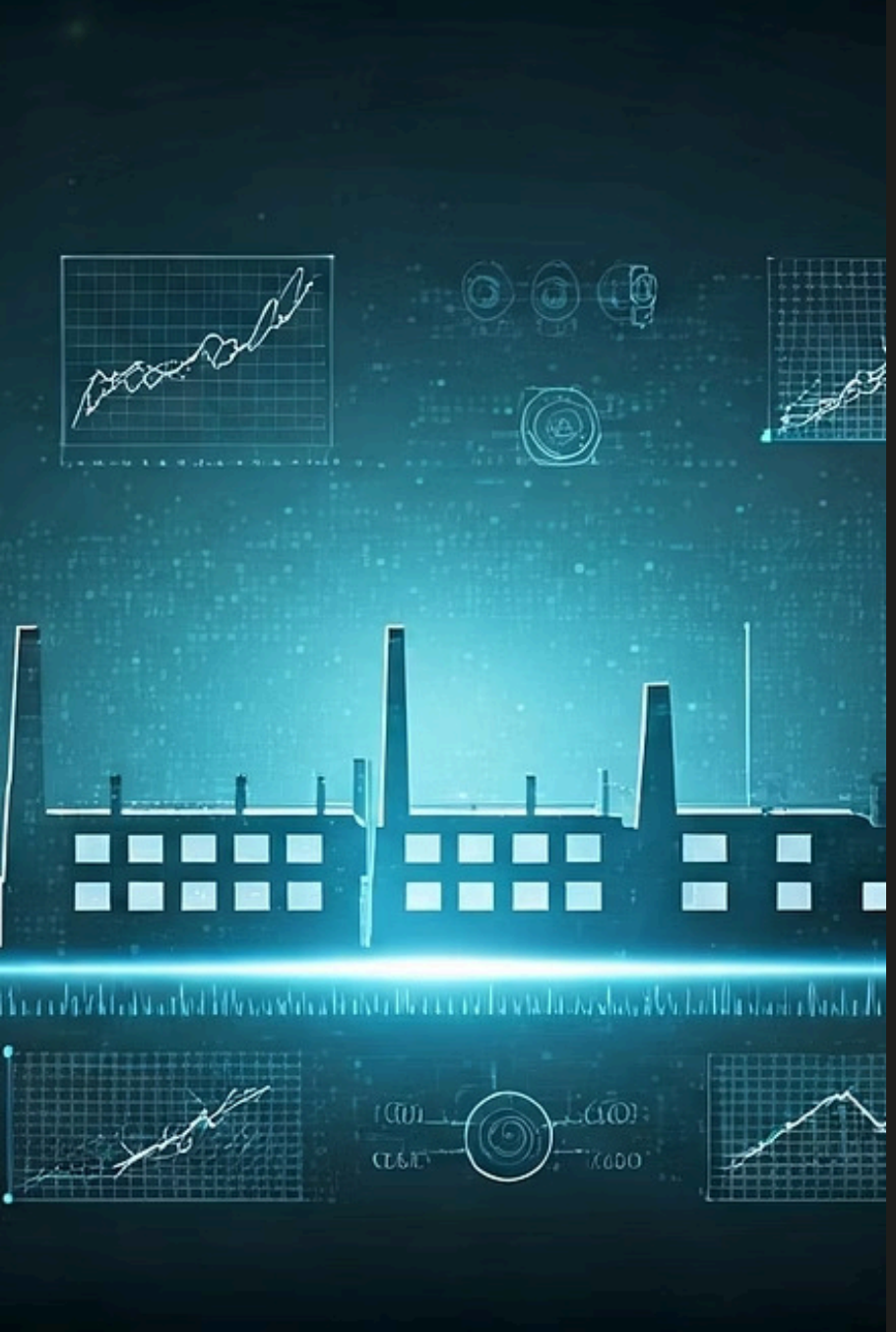
Obiettivi Principali

- Minimizzare i danni e i tempi di recupero
- Garantire la sicurezza del personale e dell'ambiente
- Mantenere la continuità operativa
- Coordinare le risposte tra team IT e OT
- Documentare gli incidenti per l'analisi post-evento

Componenti del Piano

- Procedure di escalation e notifica
- Ruoli e responsabilità del team di risposta
- Protocolli di isolamento e contenimento
- Strategie di backup e ripristino
- Comunicazione con stakeholder interni ed esterni

Il Cyber-Physical Response Plan rappresenta un elemento cruciale per la gestione integrata della sicurezza negli impianti industriali moderni, dove la distinzione tra mondo digitale e fisico diventa sempre più sfumata.



Metodologia CRISP per l'Analisi del Rischio in Ambito Cyber Fisico

La metodologia CRISP (Cyber Risk Analysis in Industrial Process System Environment Strategy), un approccio sistematico per l'identificazione e l'analisi delle conseguenze di attacchi cyber su impianti industriali.

Obiettivi della Metodologia CRISP

Analisi Sistematica

Fornire uno strumento sistematico per la "security review" degli impianti, simile alle tecniche di identificazione dei pericoli per la Safety (HazOp, FMEA).

Identificazione Conseguenze

Individuare in maniera sistematica le conseguenze di una manomissione dell'impianto in seguito ad un attacco telematico.

Analisi Globale e Locale

Analizzare sia le conseguenze globali di un attacco (CRISP in the Large) sia le conseguenze locali (CRISP in the Small).

La metodologia si basa sull'analisi dei P&ID (Process and Instrumentation Diagram) e dell'Asset Management System dell'impianto, richiedendo una conoscenza approfondita di tutti gli asset e delle loro interconnessioni.

Assunzioni di Base della Metodologia

Scenario "Worst Case"

La metodologia CRISP si basa su due assunzioni fondamentali che rappresentano uno scenario "worst case" della capacità di azione malevola:

- Il "terrorista" ha piena conoscenza dell'impianto
- Il "terrorista" è in grado di manipolare qualsiasi PCS/SIS collegato ai dispositivi attivi (di processo e di sicurezza)

La metodologia è volta a individuare i potenziali pericoli posti dagli attacchi informatici piuttosto che a stimarne un profilo di rischio e/o probabilità di successo.

La struttura della metodologia CRISP

Figura 1 CRISP - Cyber Risk Analysis in Industrial Process System Environment Strategy

Strategia della Metodologia CRISP

Analisi degli impianti P&ID

P&ID Process and Instrumentation Diagram, ovvero i diagrammi della strumentazione di processo dell'impianto che si intende analizzare.

Analisi e gestione degli Assett

Analisi e gestione di tutte le attrezzature tramite un Assett Management System, ovvero il repertorio dettagliato dei dispositivi installati nell'impianto.

CRISP in the Small

Analizza le conseguenze di deviazioni cyber su singole macchine o sistemi relativamente semplici e modulari.

CRISP in the Large

Analizza le conseguenze di attacchi cyber sull'intero sistema costituito dall'impianto di processo.

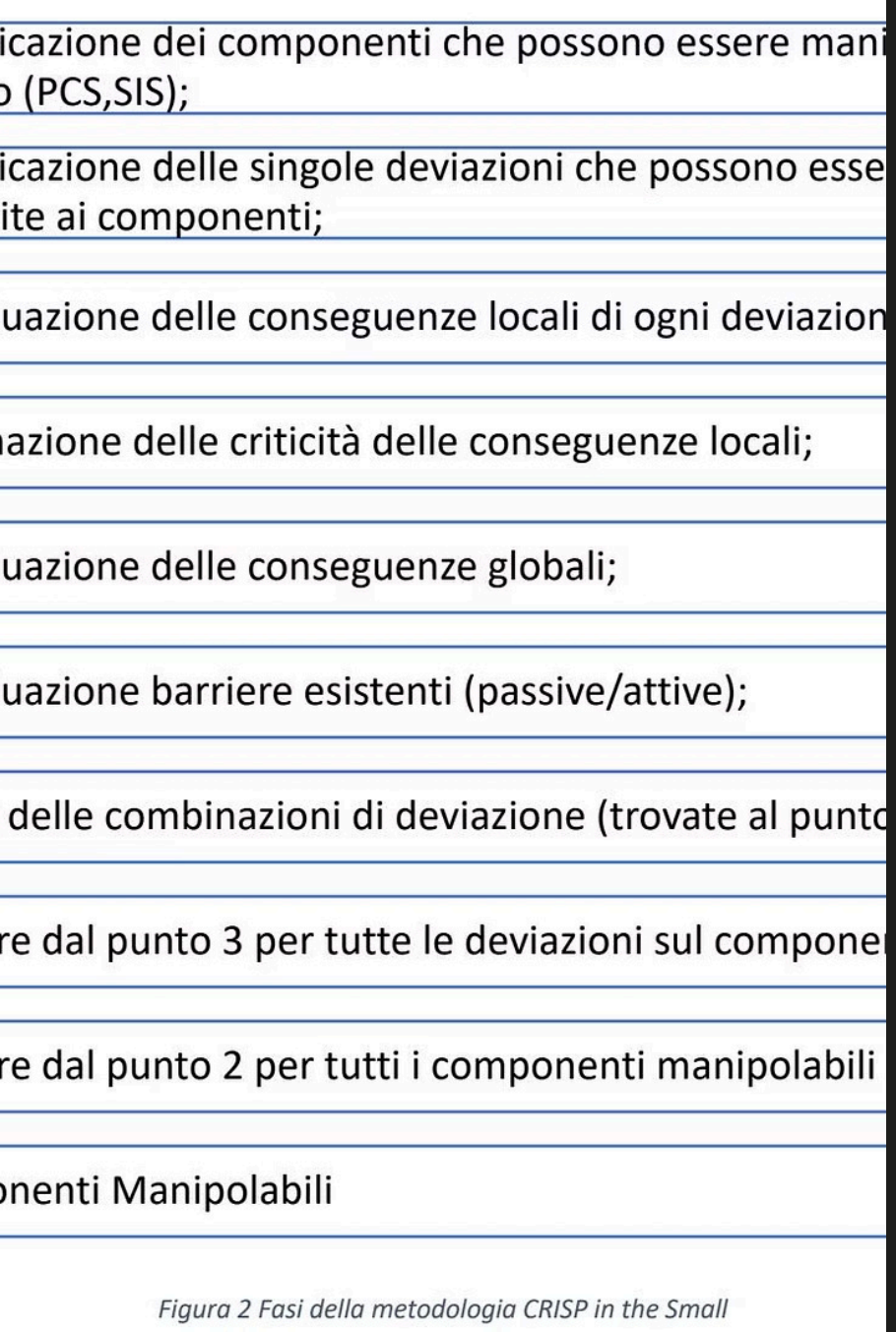


Figura 2 Fasi della metodologia CRISP in the Small

CRISP in the Small: Metodologia

La CRISP in the Small mira a identificare e analizzare le conseguenze di attacchi cyber su singole macchine o sistemi relativamente semplici e modulari.

Questa metodologia è basata su una struttura simile alla FMECA (Failure Modes, Effects and Criticality Analysis), appositamente adattata all'analisi degli attacchi per mezzo informatico.

Fasi della CRISP in the Small

1

Identificazione dei componenti manipolabili

Identificazione dei componenti che possono essere manipolati da remoto (PCS,SIS)

2

Identificazione delle deviazioni

Identificazione delle singole deviazioni che possono essere impartite ai componenti

3

Conseguenze locali

Individuazione delle conseguenze locali di ogni deviazione

4

Assegnazione criticità

Assegnazione delle criticità delle conseguenze locali

5

Conseguenze globali

Individuazione delle conseguenze globali

6

Barriere esistenti

Individuazione barriere esistenti (passive/attive)

7

Combinazioni di deviazione

Analisi delle combinazioni di deviazione (trovate al punto 2)

8

Ripetizione per deviazioni

Ripetere dal punto 3 per tutte le deviazioni sul componente

9

Ripetizione per componenti manipolabili

Ripetere dal punto 2 per tutti i componenti manipolabili

Indici di Criticità nella CRISP in the Small

Criticità I (critico)

Eventi che portano un danno irreversibile al componente analizzato, o una conseguenza locale importante.

Criticità II (poco critico)

Eventi con un danno locale reversibile, oppure facilmente risolvibile.

Criticità III (non problematico)

Eventi che portano una conseguenza locale non rilevante.

Nella CRISP in the Small, l'analisi della criticità è limitata solamente alle conseguenze locali, poiché considerare la criticità della conseguenza globale risulta poco attendibile in questa fase.

Classificazione delle Barriere

Barriere Attive/Procedurali

Tutti quegli elementi attivi di sicurezza (dispositivi controllori, interblocchi, sistemi di shutdown di emergenza) finalizzati a rilevare le variazioni di processo potenzialmente dannose e ad intraprendere le opportune azioni correttive.

Le barriere attive/procedurali potrebbero essere, almeno in linea di principio, vittime loro stesse di attacco cyber.

Barriere Passive

Sistemi hardware opportunamente inseriti in impianto che riducono o eliminano i pericoli attraverso caratteristiche di progetto, senza necessitare del funzionamento attivo di qualsivoglia dispositivo (es. PSV - valvola di sicurezza).

Il funzionamento di queste barriere non può essere alterato ad opera dell'attacco cyber.

Template CRISP in the Small

Per supportare la raccolta sistematica delle informazioni è stato definito un template sotto forma di tabella:

Ogni riga della tabella è dedicata ad un singolo componente e include: componente manipolato, variazione impartita, conseguenza locale, criticità componente, conseguenza globale, sicurezza attiva e sicurezza passiva.

SISTEMA OGGETTO D'ANALISI							
COMPONENTE MANIPOLATO	n. EVEN-TO	DEVIAZIONE IMPARTITA	CONSE-GUENZA LOCALE	CRITICITà COMPONENTE	CONSEGUENZA GLOBALE	SICUREZZA ATTIVA	SICUREZZA PASSIVA
VALVOLA SULLA MAN-DATA	1	.....	.....	I	.....	.....	.....
MOTORE POMPA	2	Arresto	Nessun Danno	III	"No portata in out"	.....	.....
VALVOLA + MOTORE	3	.....		II	.....	.....	.....

CRISP in the Large: Metodologia

Lo scopo della metodologia CRISP in the Large è individuare quali variazioni e/o deviazioni sui componenti dell'impianto, effettuate da un cyber attack, possano effettivamente causare un evento critico in un sistema complesso costituito da molteplici componenti.

La procedura può essere assimilata ad una Reverse Hazop modificata in cui, preso un nodo, si individuano solo le deviazioni che possono effettivamente produrre un top event.

Concetti Chiave nella CRISP in the Large

1

Nodo

Un sottosistema elementare dell'impianto (ad esempio unità di accumulo, impianto di pompaggio, impianto di miscelazione). Tale scomposizione viene fatta tenendo presente il livello di dettaglio dello studio che si vuole realizzare.

2

Top Event

Incidenti rilevanti che portano a perdita di contenimento di materiali pericolosi o al rilascio acuto di energia. Si prendono come riferimento i Critical Events definiti nel progetto ARAMIS.

3

Deviazioni

La procedura considera due tipi di deviazioni: le "deviazioni nel nodo" (scostamenti delle variabili di processo dalle corrette condizioni operative) e le "deviazioni impartite" (variazioni indotte ai parametri operativi dei componenti manipolabili).

1. Suddivisione dell'impianto in nodi
2. Selezione di un nodo da analizzare
3. Identificazione dei top event di interesse
4. Elenco delle possibili deviazioni nel nodo
5. Identificazione di quali delle possibili deviazioni nel nodo possono causare i top event di interesse
6. Identificazione degli elementi manipolabili nel nodo
7. Identificazione delle deviazioni impartite agli elementi manipolabili in grado di causare le deviazioni nel nodo
8. Identificazione di cause di deviazione nel nodo, provenienti da altri nodi
9. Identificazione barriere attive e passive
10. Ripetere procedura per tutti i nodi (ritorno al punto 2 e iterazione)
11. Verificare se tutte le deviazioni nel nodo provenienti da altri nodi (punto 8) sono state sviluppate come 'deviazioni nel nodo' nei rispettivi nodi
12. Integrare le deviazioni mancanti nei rispettivi nodi (ripeter punti 7 e 9 per le deviazioni nel nodo individuate al punto 11)

Figura 4 Fasi della metodologia CRISP in the Large

Step della CRISP in the Large

Deviazioni nel Nodo

Il formalismo per descrivere le 'deviazioni nel nodo' è analogo a quello utilizzato negli studi HazOp:

$$Deviazione\ nel\ nodo = Parola\ guida + Variabile\ operativa$$

Esempi di Parole guida

- NO → negazione dell'intenzione progettuale
- PIÙ → accrescimento quantitativo
- MENO → diminuzione quantitativa
- PARTE DI → diminuzione qualitativa

Esempi di Deviazioni nel nodo

- NO PORTATA (linea X) → Portata nulla nella linea X
- PIÙ LIVELLO → livello nel nodo che eccede il massimo previsto

Template CRISP in the Large

Anche per la metodologia CRISP in the Large è stato creato un template in forma tabellare per supportare la raccolta sistematica delle informazioni.

Per ogni Nodo vengono individuati i Top Event possibili. Una riga della tabella è riferita ad un singolo Top Event; ad un nodo sono riferiti un set di Top Event.

Le colonne descrivono: Conseguenza Top Event, Deviazione Impartita/Componenti Manipolabili, Deviazione da altri nodi, Sicurezza (Attiva e Passiva), Consigli Eventuali.

CRISP in the Large

N.	NODO	CONSEGUENZA	DEVIAZIONE	DEVIAZIONE IMPARTITA COMPONENTI MANIPOLABILI					DEVIAZIONI	SICUREZZA		CONSIGLI
		TOP EVENT	SUL NODO	SDV 001	SDV 002	POMPA P1	VALVOLA 002	VALVOLA 003	DA ALTRI NODI	ATTIVA E PROCEDURALE	PASSIVA	EVENTUALI
1												
2	SERBATOIO 001	CE10	PIÙ PORTATA			"no portata out"						
3												
4												

Analisi SWOT della Metodologia CRISP

Punti di Forza

- Capacità di analizzare analiticamente un intero impianto sia in termini di componenti installati sia di conseguenze di deviazioni
- Glossario e approccio simile ad altre metodologie tipo "Reverse HazOp" molto diffuse in ambito industriale

Opportunità

- Realizzazione di un'analisi completa e puntuale degli Asset installati
- Adozione di un sistema di Asset management
- Aggiornamento e revisione dei diagrammi impianti di processo

Punti Deboli

- Onerosità e complessità applicativa della metodologia a impianti di elevate dimensione
- Eccessiva onerosità nell'aggiornamento e dell'allineamento dell'analisi rispetto all'evoluzione degli impianti

Pericoli

- Un eventuale disallineamento dell'impianto rispetto all'analisi potrebbe portare a trascurare situazioni dannose
- Eccessiva "burocratizzazione" della gestione dell'impianto
- L'applicazione della sola fase CRISP in the Large potrebbe portare a sottovalutare conseguenze globali individuabili nella fase CRISP in the Small

Relazione tra la Metodologia CRISP e i controlli CIS

L'analisi dei diagrammi degli impianti e degli asset corrisponde all'applicazione dei controlli CIS 1, CIS 2 e CIS 5.

CIS 1: Inventario e controllo delle dotazioni Hardware

Gestire attivamente tutti i dispositivi hardware sulla rete in modo che i dispositivi autorizzati abbiano accesso e che vengano bloccati nell'accesso i dispositivi non autorizzati.

CIS 2: Inventario e Controllo delle Risorse Software

Gestire attivamente tutto il software sulla rete in modo che solo il software autorizzato sia installato e possa essere eseguito.

CIS 5: Configurazione Sicura di Hardware e Software

Stabilire, implementare e gestire attivamente la configurazione di sicurezza dei dispositivi utilizzando una gestione rigorosa della configurazione.

Ulteriori Controlli CIS Correlati

CIS 3: Gestione Continua delle Vulnerabilità

Acquisire, valutare e agire continuamente in base alle nuove informazioni al fine di identificare le vulnerabilità e ridurre al minimo la finestra di opportunità per gli aggressori.

CIS 4: Utilizzo Controllato dei Privilegi Amministrativi

Processi e strumenti utilizzati per tracciare/controllare/prevenire/correggere l'uso, l'assegnazione e la configurazione dei privilegi amministrativi.

CIS 8: Difesa dal Malware

Controllo dell'installazione, diffusione ed esecuzione di codice dannoso in più punti dell'azienda.

CIS 9: Limitazione e Controllo delle Porte di Rete, dei Protocolli e dei Servizi

Gestire l'uso di porte, protocolli e servizi sui dispositivi di rete al fine di ridurre al minimo le finestre di vulnerabilità disponibili per gli aggressori.

CRISP Tool: Obiettivi

Il CRISP Tool è uno strumento software prototipale che supporta l'applicazione della metodologia CRISP. I suoi obiettivi principali sono:

Supporto Metodologico

Supportare l'applicazione della metodologia CRISP in un impianto di processo, sia nella struttura CRISP in the Small sia nella struttura CRISP in the Large.

Gestione Multi-Impianto

Gestire più applicazioni della metodologia in diversi impianti e/o porzioni di essi, consentendo di salvare uno stato parziale dell'analisi e passare ad un'altra fase o un altro nodo.

Produzione Documentale

Supportare la produzione della documentazione e i report conseguenti all'analisi, in un formato che sia poi editabile offline dagli operatori.

Gestione Vocabolari

Gestire i "vocabolari" e le "ontologie" dei singoli elementi oggetto dell'analisi, come componenti degli impianti, barriere di protezione ed eventi critici top.

Architettura del CRISP Tool

Architettura Logica

Il core dell'applicazione è rappresentato dai moduli per l'applicazione delle metodologie CRISP. Il core viene alimentato, da un punto di vista informativo, dagli altri moduli che si occupano della gestione delle singole componenti dell'impianto.

Architettura Funzionale

L'architettura funzionale comprende quattro aree principali:

- Gestione Impianti (Asset e Nodi)
- Gestione Vocabolari e Ontologie generali
- Gestione Metodologie CRISP
- Strumenti di Reporting

Moduli Funzionali del CRISP Tool

Gestione Impianti

Consente la gestione di più impianti e diverse analisi sullo stesso impianto. Include funzionalità per creare, cancellare e modificare istanze di impianto, nodi e analisi.

Gestione Asset

Permette di gestire tutti i componenti manipolabili da remoto che sono oggetto della Metodologia CRISP, con funzionalità per inserire, cancellare e modificare elementi.

Gestione Vocabolari e Ontologie

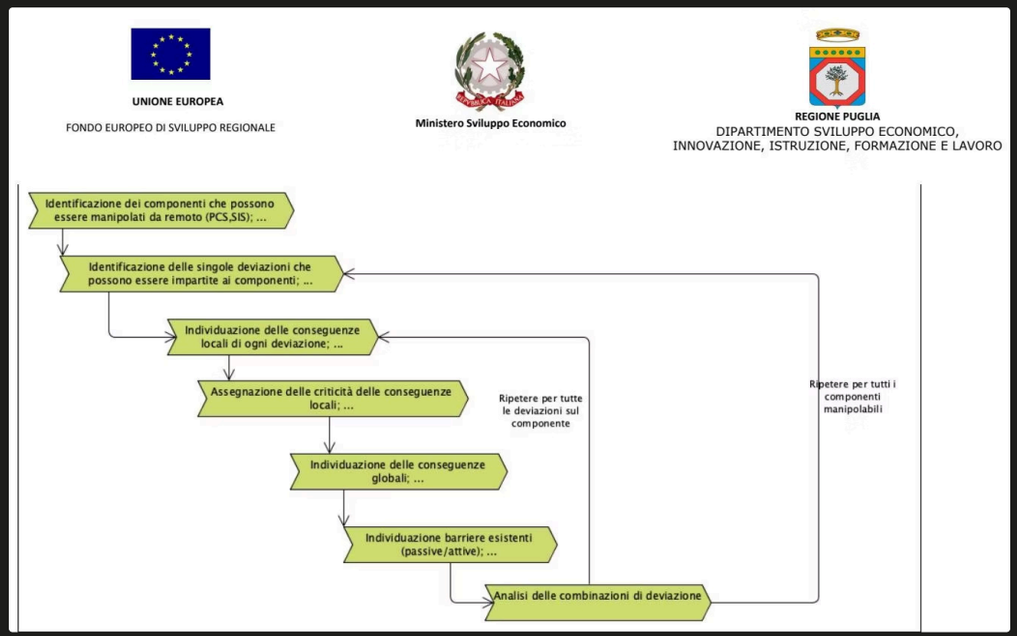
Dedicata alla gestione degli elementi di base del sistema, come barriere di sicurezza, deviazioni e critical events, standardizzando l'applicazione della metodologia.

Gestione Metodologie CRISP

Il "core" del prototipo, comprende i moduli per la gestione dei progetti di analisi CRISP in the Small e CRISP in the Large.

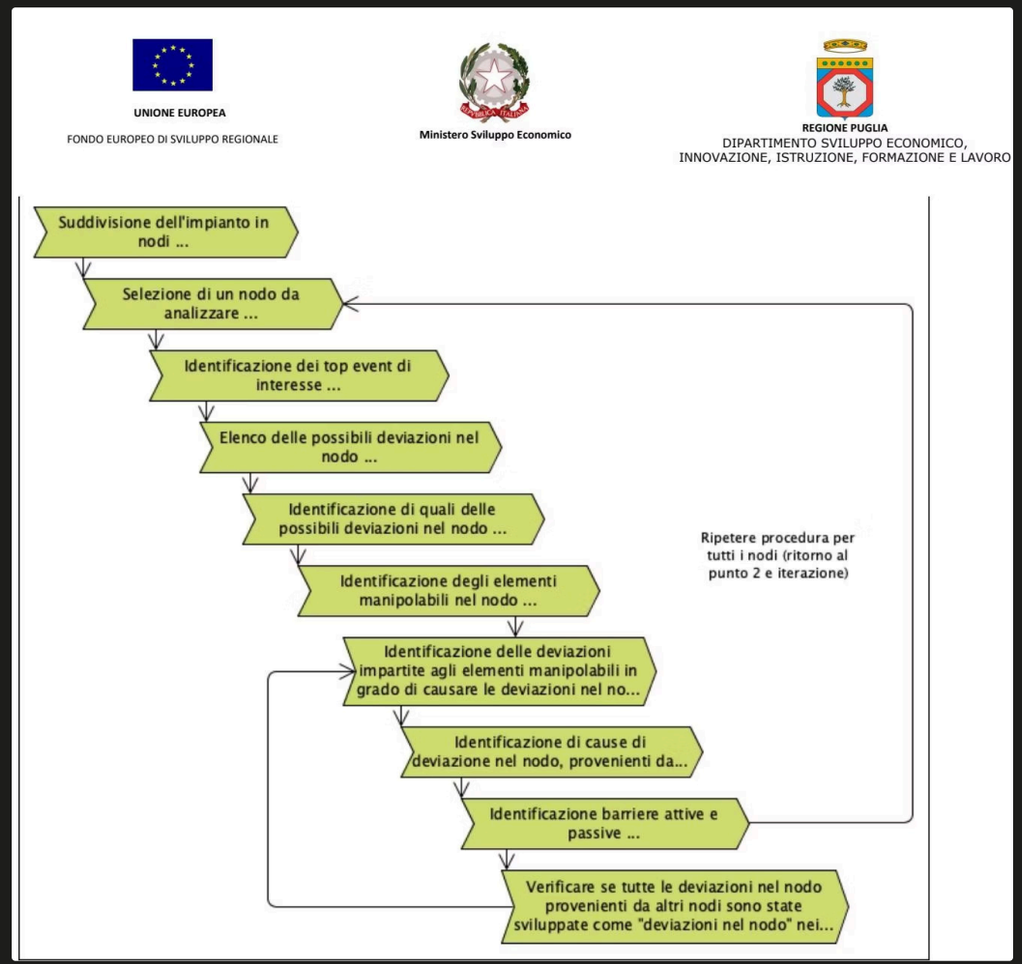
Workflow Applicativo delle Metodologie

CRISP in the Small Workflow



Il workflow della CRISP in the Small segue le fasi di identificazione dei componenti, analisi delle deviazioni, valutazione delle conseguenze e individuazione delle barriere.

CRISP in the Large Workflow



Il workflow della CRISP in the Large parte dall'identificazione dei nodi e dei top event, per poi analizzare le deviazioni che possono causarli e le relative barriere di protezione.

Strumenti di Reporting

Il modulo di gestione dei Report consente la generazione di un report per ogni istanza della metodologia.

Report CRISP in the Small

Il template del report include informazioni su:

- Componente manipolato
- Deviazione impartita
- Conseguenza locale
- Criticità componente
- Conseguenza globale
- Sicurezza attiva e passiva

Report CRISP in the Large

Il template del report include informazioni su:

- Conseguenza Top Event
- Deviazione Impartita/Componenti Manipolabili
- Deviazione da altri nodi
- Sicurezza (Attiva e Passiva)
- Consigli Eventuali

I report sono esportabili in un formato editabile offline dall'utente finale, per consentire una personalizzazione degli aspetti e dei dettagli.

Conclusioni sulla Metodologia CRISP

La metodologia CRISP, nelle sue due strutture CRISP in the Small e CRISP in the Large, offre un approccio completo e sistematico per l'analisi del rischio cyber in ambito industriale.

Le due strutture si intersecano e si completano a vicenda:

- CRISP in the Small rileva gli eventi dannosi su ogni singolo componente
- CRISP in the Large individua i Top Event critici per ogni Nodo

I punti di forza e le opportunità offerti dall'adozione della CRISP sono importanti e certamente superiori ai punti di debolezza, che si riassumono in una certa onerosità nella fase di primo impianto dell'analisi e di aggiornamento degli asset installati.

Questi aspetti possono essere uno stimolo ad un miglioramento della gestione degli impianti anche relativamente agli aspetti manutentivi.

Vantaggi dell'Applicazione della Metodologia CRISP

100%

Analisi Sistematica

Copertura completa di tutti i componenti manipolabili dell'impianto

360°

Visione Globale

Analisi sia delle conseguenze locali che di quelle globali

2X

Doppia Prospettiva

Approccio bottom-up (CRISP in the Small) e top-down (CRISP in the Large)

L'applicazione della metodologia CRISP consente di identificare in modo sistematico le vulnerabilità degli impianti industriali agli attacchi cyber, permettendo di implementare adeguate misure di protezione e mitigazione.

Applicazioni Pratiche della Metodologia

Settori di Applicazione

- Impianti Oil & Gas
- Impianti petrolchimici
- Impianti di generazione elettrica
- Impianti di trattamento acque
- Impianti manifatturieri
- Infrastrutture critiche

Benefici per le Organizzazioni

- Miglioramento della sicurezza cyber degli impianti
- Riduzione del rischio di incidenti
- Ottimizzazione degli investimenti in sicurezza
- Conformità con standard e normative
- Miglioramento della gestione degli asset

Integrazione con Altre Metodologie

HazOp (Hazard and Operability Study)

La CRISP può essere integrata con l'analisi HazOp tradizionale, estendendo l'analisi dei rischi operativi ai rischi cyber.

FMECA (Failure Mode, Effects, and Criticality Analysis)

La CRISP in the Small si basa su una struttura simile alla FMECA, facilitando l'integrazione delle due metodologie.

ARAMIS (Accidental Risk Assessment Methodology for Industries)

La CRISP utilizza i Critical Events definiti nel progetto ARAMIS, permettendo una facile integrazione con questa metodologia.

L'integrazione della CRISP con altre metodologie di analisi del rischio consente di ottenere una visione più completa e integrata dei rischi associati agli impianti industriali.

Importanza della Formazione

Competenze Necessarie

L'applicazione efficace della metodologia CRISP richiede competenze sia nel campo della sicurezza informatica che in quello dell'ingegneria di processo.

È fondamentale che il personale coinvolto nell'analisi abbia una conoscenza approfondita:

- Dei sistemi di controllo industriale
- Dei processi produttivi specifici
- Delle tecniche di analisi del rischio
- Delle minacce cyber e delle relative contromisure

Programmi di Formazione

Per garantire un'applicazione corretta ed efficace della metodologia, è opportuno sviluppare programmi di formazione specifici che includano:

- Formazione teorica sulla metodologia
- Esercitazioni pratiche su casi di studio
- Affiancamento da parte di esperti nelle prime applicazioni
- Aggiornamenti periodici sulle nuove minacce e tecniche di attacco

Sfide nell'Implementazione

Complessità degli Impianti

Gli impianti industriali moderni sono sistemi complessi con numerosi componenti interconnessi, rendendo l'analisi completa particolarmente onerosa.

Evoluzione Tecnologica

La rapida evoluzione delle tecnologie di automazione e controllo richiede un costante aggiornamento della metodologia e delle competenze.

Integrazione IT/OT

La crescente integrazione tra sistemi IT e OT (Operational Technology) aumenta la superficie di attacco e richiede un approccio olistico alla sicurezza.

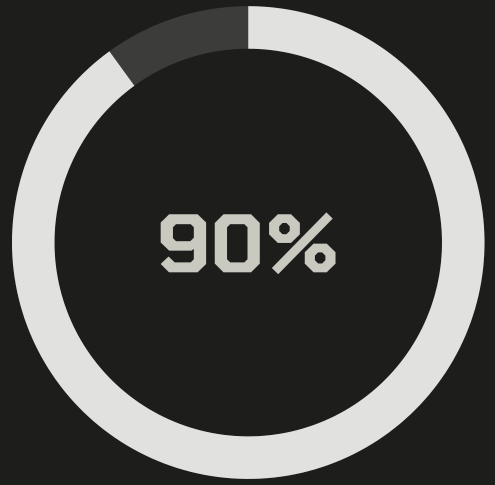
Resistenza al Cambiamento

L'introduzione di nuove metodologie può incontrare resistenze organizzative, specialmente in settori tradizionali come quello industriale.

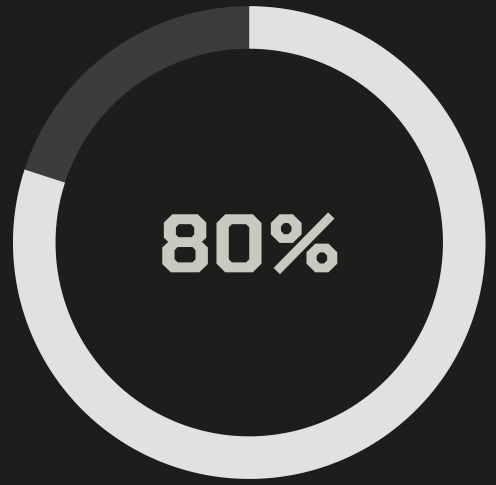
Affrontare queste sfide richiede un approccio strutturato e un forte commitment da parte del management.

Impatto della Metodologia CRISP sulla Sicurezza degli Impianti

Copertura completa dei componenti manipolabili dell'impianto



Riduzione delle vulnerabilità attraverso l'identificazione sistematica



Miglioramento della consapevolezza dei rischi cyber

L'applicazione della metodologia CRISP contribuisce significativamente al miglioramento della sicurezza cyber degli impianti industriali, permettendo di identificare e mitigare le vulnerabilità prima che possano essere sfruttate da potenziali attaccanti.

La combinazione delle due strutture, CRISP in the Small e CRISP in the Large, consente una visione completa e integrata dei rischi, facilitando l'implementazione di misure di protezione efficaci.

Benefici per la Gestione degli Asset

Inventario Completo

Creazione e mantenimento di un inventario completo e aggiornato di tutti gli asset dell'impianto.

Manutenzione Migliorata

Identificazione dei componenti critici che richiedono particolare attenzione in termini di manutenzione.

Predictive Maintenance

Base di conoscenza utile per l'implementazione di strategie di manutenzione predittiva.

L'applicazione della metodologia CRISP, oltre a migliorare la sicurezza cyber, offre importanti benefici per la gestione complessiva degli asset dell'impianto, contribuendo all'ottimizzazione dei processi di manutenzione e alla riduzione dei costi operativi.

Evoluzione del Panorama delle Minacce

Tendenze Attuali

Il panorama delle minacce cyber agli impianti industriali è in continua evoluzione, con attacchi sempre più sofisticati e mirati.

Alcune tendenze rilevanti includono:

- Aumento degli attacchi ransomware specifici per sistemi industriali
- Crescente interesse degli attori statali verso le infrastrutture critiche
- Sfruttamento delle vulnerabilità nella supply chain
- Attacchi che combinano vettori IT e OT

Implicazioni per la Metodologia

L'evoluzione delle minacce richiede un continuo aggiornamento della metodologia CRISP per mantenerla efficace nel tempo.

Aspetti da considerare:

- Inclusione di nuovi vettori di attacco nell'analisi
- Aggiornamento dei modelli di minaccia
- Considerazione delle vulnerabilità emergenti
- Adattamento alle nuove tecnologie di automazione e controllo

Integrazione con il Cyber-Physical Response Plan

La metodologia CRISP nasce in un contesto prettamente industriale e viene evoluta come uno degli input del Cyber-Physical Response Plan.

Identificazione delle Vulnerabilità

La CRISP identifica le vulnerabilità degli impianti agli attacchi cyber, fornendo input essenziali per il piano di risposta.

Valutazione degli Impatti

L'analisi delle conseguenze locali e globali permette di valutare gli impatti potenziali degli attacchi, facilitando la prioritizzazione delle risposte.

Definizione delle Contromisure

L'identificazione delle barriere di sicurezza contribuisce alla definizione delle contromisure da implementare nel piano di risposta.

Pianificazione della Risposta

La comprensione delle modalità di attacco e delle loro conseguenze permette di sviluppare procedure di risposta efficaci.

Aspetti Normativi e di Compliance

Framework di Riferimento

L'applicazione della metodologia CRISP contribuisce alla conformità con diversi standard e normative in materia di sicurezza cyber per i sistemi industriali:

- IEC 62443: Sicurezza per i sistemi di automazione e controllo industriale
- NIST Cybersecurity Framework
- Direttiva NIS (Network and Information Security)
- ISO 27001 e ISO 27019 (specifico per il settore energetico)

Requisiti Specifici

La metodologia CRISP supporta in particolare i seguenti requisiti normativi:

- Identificazione e gestione dei rischi
- Protezione dei sistemi e delle reti
- Rilevamento di eventi di sicurezza
- Pianificazione della risposta agli incidenti
- Ripristino delle normali operazioni

Direttiva NIS2

La nuova Direttiva NIS2, entrata in vigore nel 2023, amplia significativamente il campo di applicazione della precedente normativa, includendo nuovi settori e rafforzando i requisiti di sicurezza. La metodologia CRISP si allinea perfettamente con i nuovi obblighi previsti dalla NIS2, in particolare per quanto riguarda:

- La gestione del rischio cyber con approccio olistico
- La valutazione delle catene di approvvigionamento (supply chain)
- La reportistica degli incidenti alle autorità competenti
- Le misure di sicurezza per i sistemi OT (Operational Technology)
- La governance e la supervisione da parte del management

Collaborazione tra Team IT e OT

L'applicazione efficace della metodologia CRISP richiede una stretta collaborazione tra i team IT (Information Technology) e OT (Operational Technology).

Competenze IT

Conoscenza delle reti, dei sistemi informatici, delle minacce cyber e delle tecniche di protezione.

Competenze OT

Conoscenza dei processi industriali, dei sistemi di controllo, delle dinamiche operative e dei requisiti di sicurezza funzionale.

Approccio Integrato

Combinazione delle competenze IT e OT per una comprensione completa delle vulnerabilità e delle loro potenziali conseguenze.

Governance Condivisa

Definizione di ruoli e responsabilità chiari per la gestione della sicurezza cyber degli impianti industriali.

Formazione e Sensibilizzazione

Programmi di Formazione

Per garantire un'applicazione efficace della metodologia CRISP, è fondamentale sviluppare programmi di formazione specifici per:

- Analisti di sicurezza
- Ingegneri di processo
- Operatori di impianto
- Management

La formazione dovrebbe coprire sia gli aspetti metodologici che quelli tecnici, con un focus particolare sull'integrazione tra sicurezza cyber e sicurezza funzionale.

Sensibilizzazione

Oltre alla formazione tecnica, è importante promuovere una cultura della sicurezza cyber attraverso:

- Sessioni di sensibilizzazione per tutto il personale
- Comunicazioni regolari sulle minacce emergenti
- Esercitazioni pratiche e simulazioni di attacco
- Condivisione di best practice e lezioni apprese

La sensibilizzazione dovrebbe coinvolgere tutti i livelli dell'organizzazione, dal management operativo fino ai vertici aziendali.

Prospettive Future

Intelligenza Artificiale

Integrazione di tecniche di AI per automatizzare parti dell'analisi e migliorare l'identificazione delle vulnerabilità.

Digital Twin

Utilizzo di gemelli digitali per simulare gli attacchi e valutarne le conseguenze in un ambiente virtuale.

Cloud Integration

Evoluzione del CRISP Tool verso soluzioni cloud-based per facilitare la collaborazione e l'accesso alle informazioni.

Security by Design

Integrazione della metodologia CRISP nei processi di progettazione degli impianti per garantire la sicurezza cyber fin dalle prime fasi.

Standardizzazione

Evoluzione della metodologia verso uno standard internazionale per l'analisi del rischio cyber in ambito industriale.

Conclusioni

La metodologia CRISP rappresenta un approccio sistematico e completo per l'analisi del rischio cyber in ambito industriale, combinando due strutture complementari:

- CRISP in the Small: analisi delle conseguenze di deviazioni cyber su singole macchine o sistemi relativamente semplici
- CRISP in the Large: analisi delle conseguenze di attacchi cyber sull'intero sistema costituito dall'impianto di processo

L'applicazione della metodologia consente di identificare le vulnerabilità degli impianti agli attacchi cyber e di implementare adeguate misure di protezione.

I punti di forza della metodologia includono:

- Approccio sistematico e strutturato
- Integrazione con metodologie consolidate di analisi del rischio
- Considerazione sia delle conseguenze locali che globali
- Supporto alla gestione degli asset

Il CRISP Tool fornisce un supporto informatico all'applicazione della metodologia, facilitando la raccolta e l'analisi delle informazioni e la produzione di report.