Introduzione alla Gestione dei Rischi di Sicurezza Informatica nel Settore Marittimo

CSP001_S_M

PRESENTAZIONE:
PINELOPI KYRANOUDI, RICERCATRICE IN CIBERSICUREZZA, UNIVERSITÀ TECNICA DI CRETA
NINETA POLEMI, DOCENTE, UNIVERSITÀ DEL PIRAEUS

CyberSecPro

CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.

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.

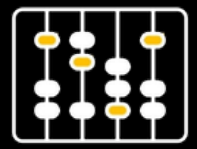
Project Agreement no. 101083594

Obiettivi: Chi, cosa e perché è necessario seguire questa formazione

CHI

Professionisti nel settore delle operazioni marittime e portuali, della sicurezza informatica e della gestione in ambito IT, OT e della catena di approvvigionamento

COSA



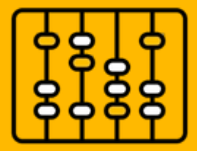
Seminario sulla gestione dei rischi di sicurezza informatica e sulla certificazione nei sistemi marittimi, che copre standard, controlli e sicurezza della catena di approvvigionamento

PERCHÉ

Consentire ai partecipanti di valutare i rischi, supportare la certificazione e garantire operazioni marittime sicure e resilienti

CSP Formazione Logistica: Quando-Dove-Come

QUANDO



Orario (da pubblicare sulla piattaforma DCM)

DOVE

Di persona, online o entrambi (da pubblicare sulla piattaforma DCM)

COME

Sessioni tenute da un istruttore

Proposte di valore

Vantaggiper i partecipanti

- Livello del modulo di formazione: Avanzato
- Formazione professionale in materia di sicurezza informatica
- Basato sul Quadro europeo delle competenze in materia di sicurezza informatica
- Approfondimenti all'avanguardia da parte di esperti del mondo industriale e accademico
- Certificato di completamento
- Aiuta lo sviluppo delle competenze e l'avanzamento di carriera

COSA

Argomentidella formazione

- Introduzione alla sicurezza informatica marittima
- Comprendere i rischi informatici nel settore marittimo
- Standard e best practice di sicurezza informatica
- Certificazione in sicurezza informatica marittima

PERCHÉ

Risultati di apprendimento

Conoscenze:

- Comprensione delle minacce alla sicurezza informatica specifiche del settore marittimo.
- Familiarità con i quadri normativi, i regolamenti e gli standard pertinenti in materia di sicurezza informatica nel settore marittimo.
- Conoscenza dei rischi informatici prevalenti nelle operazioni marittime.
- Consapevolezza dei casi di studio e degli esempi reali di incidenti di sicurezza informatica nel settore marittimo.
- Comprensione delle metodologie e degli strumenti di valutazione del rischio su misura per il settore marittimo.
- Comprensione dei concetti di sicurezza delle informazioni e del settore marittimo.
- Comprensione delle migliori pratiche per la protezione dei sistemi IT e OT marittimi.
- Conoscenza degli standard e degli schemi di certificazione in materia di sicurezza informatica specifici per il settore marittimo.
- Familiarità con i concetti fondamentali relativi alla certificazione in materia di sicurezza informatica.
- Comprensione delle migliori pratiche per ottenere e mantenere la certificazione di sicurezza informatica marittima.

CHI

Profilidei formatori

- PinelopiKyranoudiha conseguito il master in Sicurezza dei sistemi di informazione e comunicazione pressol'Universitàdell'Egeo (Dipartimento di Ingegneria dei sistemi di informazione e comunicazione). Haricoperto ilruolo di Responsabile della sicurezza delle reti e delle informazioni presso l'Agenzia dell'Unione Europea per la sicurezza informatica (ENISA), contribuendo a cinque pubblicazioni nei settori della sicurezza informatica in ambito marittimo, della sanità digitale e delle strategie nazionali di sicurezza informatica; alla creazione di strumenti web e all'organizzazione di eventi dell'UE sulla sicurezza informatica. Nel corso della sua carriera decennale ha ricoperto diversi ruoli e posizioni, quali sviluppatrice web e di applicazioni, ingegnere della sicurezza informatica, ricercatrice in sicurezza informatica e docente presso aziende e organizzazioni quali, rispettivamente, Express Publishing SA, Cosmote SA, Maggioli SpA e Aegean College, tra le altre. Attualmente sta svolgendo il dottorato di ricerca nel campo della sicurezza informatica presso l'Università del Pireo (Dipartimento di Informatica). Ricopre la carica di ricercatrice in sicurezza informatica presso l'Università Tecnica di Creta (Facoltà di Ingegneria Elettrica e Informatica), contribuendo a progetti di ricerca dell'UE. I suoi interessi di ricerca riguardano il campo della sicurezza cyber-fisica, in particolare nei settori marittimo, OT/IoT e Threat Intelligence.

- Nineta Polemi è professoressa di sicurezza informatica presso l'Università del Pireo (UNIPI) (Cyber Security Lab, Dipartimento di Informatica) e CTO/Co-fondatrice di Trustilio. Dal 2017 al 2020 ha ricoperto il ruolo di responsabile di programma e funzionaria politica presso la DG CONNECT della Commissione Europea (Unità H1 intitolata "Tecnologie e capacità di sicurezza informatica"). Ha conseguito il dottorato di ricerca in Matematica Applicata (Teoria della Codifica) presso la City University di New York (Graduate Center). Ha ricoperto incarichi di insegnamento e ricerca presso la City University di New York (Queens & Baruch Colleges), la State University of New York (Farmingdale) e l'Université Libre de Bruxelles (ULB) - Solvay Brussels School. Ha al suo attivo oltre 150 pubblicazioni nel campo della sicurezza (ad esempio, sicurezza portuale, sicurezza marittima, sicurezza della catena di approvvigionamento marittima) e ha organizzato numerosi eventi scientifici e politici internazionali sulla sicurezza informatica. Ha ricevuto numerosi finanziamenti per la ricerca (NATO, IEEE) e premi (NSA, MSI Army Research Office IEEE, CYNY, Ministero marittimo ellenico, Direzione generale della difesa nazionale ellenica) e ha partecipato come responsabile di progetto e tecnico a oltre 60 progetti internazionali, europei e nazionali di ricerca e sviluppo e commerciali nel campo della sicurezza informatica. Svolge il ruolo di esperta/revisore/consulente esterna presso ENISA, la Commissione europea (DG CNECT, DG HOME), FORTH e Focal Point.

Schema del corso

Argomento 1: Introduzione alla sicurezza informatica marittima

Panoramicadelle minacceallasicurezzainformatica nel settore marittimo Importanza della sicurezza informatica marittima

Introduzione ai quadri normativi e alle normative pertinenti in materia di sicurezza informatica (ad es. Linee guida dell'IMO sulla gestione dei rischi informatici)

Argomento 2: Comprensione dei rischi informatici nel settore marittimo

Identificazione dei rischi informatici nelle operazioni marittime
Casi di studio ed esempi reali di incidenti di sicurezza informatica nel settore marittimo

Valutazione dei rischi VS gestione dei rischi

Schema del corso

Argomento3:Standardebestpracticedisicurezza informatica

Panoramica degli standard di sicurezza informatica applicabili al settore marittimo (ad es. ISO 27001, NIST Cybersecurity Framework)

Panoramica sulla sicurezza delle informazioni e sui concetti

fondamentali del settore marittimo

Migliori pratiche per la protezione dei sistemi IT e OT marittimi (ad es.

Linee guida ENISA - Gestione dei rischi informatici per i porti, Metodologia di gestione dei rischi CYSMET)

Argomento 4: Certificazione della sicurezza informatica nel settore marittimo

Standard e schemi di certificazione della sicurezza informatica applicabili al settore marittimo (ad es. Common Criteria, EUCC)

Panoramica dei concetti fondamentali della certificazione in materia di

sicurezza informatica

Migliori pratiche per la certificazione della sicurezza informatica marittima

(ad es. Metodologia CYRENE di valutazione dei rischi e della conformità)

Conoscenze di base e prerequisiti

Conoscenze di base:

Conoscenza di base dei computer e delle reti

Familiarità con le minacce e le vulnerabilità comuni alla sicurezza su Internet

Consapevolezza della sicurezza informatica

Prerequisiti:

Nessuno

Risorse:

Materiale di riferimento

1. ISO/IEC 27001:2022, Sistemi di gestionedellasicurezzadell'informazione — Requisiti
2. ISO/IEC 27005:2018, Gestione dei rischiperlasicurezzadelleinformazioni
3. ISO/IEC 15408, Criteri comuni per lavalutazionedellasicurezza delle tecnologie dell'informazione
4. ISO/IEC 18045, Metodologia comune per la valutazione della sicurezza delle tecnologie dell'informazione
5. NIST SP 800-30 Rev. 1, Guida per la conduzione delle valutazioni dei rischi
6. NIST SP 800-37 Rev. 2, Quadro di riferimento per la gestione dei rischi per i sistemi informativi e le organizzazioni
7. NIST SP 800-82 Rev. 2, Guida alla sicurezza dei sistemi di controllo industriale (ICS)
8. NIST, Quadro di riferimento per la sicurezza informatica (CSF) 2.0
9. Serie IEC 62443, Sicurezza per i sistemi di automazione e controllo industriale
10. Organizzazione marittima internazionale (IMO), Linee guida sulla gestione dei rischi informatici nel settore marittimo
11. ENISA, Buone pratiche per la sicurezza informatica nel settore marittimo
12. ENISA, Linee guida sulla gestione dei rischi informatici per i porti
13. ENISA, Panorama delle minacce nel settore dei trasporti
14. Unione Europea, EUCC (Schema europeo di certificazione della sicurezza informatica)
15. Progetto CYRENE, Metodologia di valutazione dei rischi e della conformità per le catene di approvvigionamento marittime
16. Frontiers in Computer Science, Metodologia di gestione dei rischi di sicurezza informatica per i sistemi della catena di approvvigionamento (CYSMET), 2023

Stato di avanzamento del corso

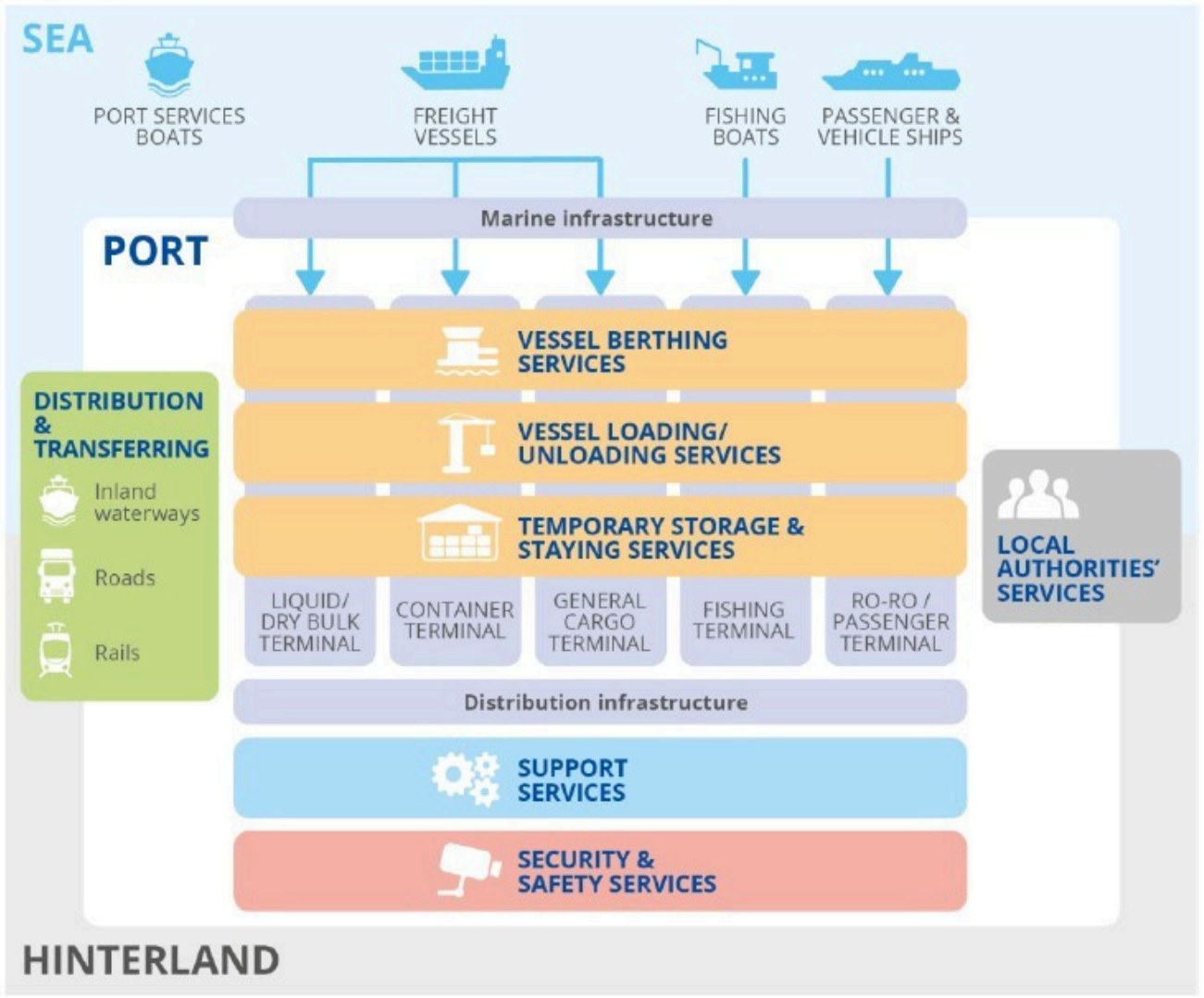
o1. Introduzione alla sicurezza informatica marittima

o2. Comprendere i rischi informatici nel settore marittimo

o3. Standard e migliori pratiche in materia di sicurezza informatica

o4. Certificazione sulla sicurezza informatica marittima

Servizi portuali e infrastrutture



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2=1

Che cos'è la sicurezza informatica marittima

Protezione dei **sistemi IT, OT e IoT marittimi interconnessi** tra porti, navi e reti logistiche

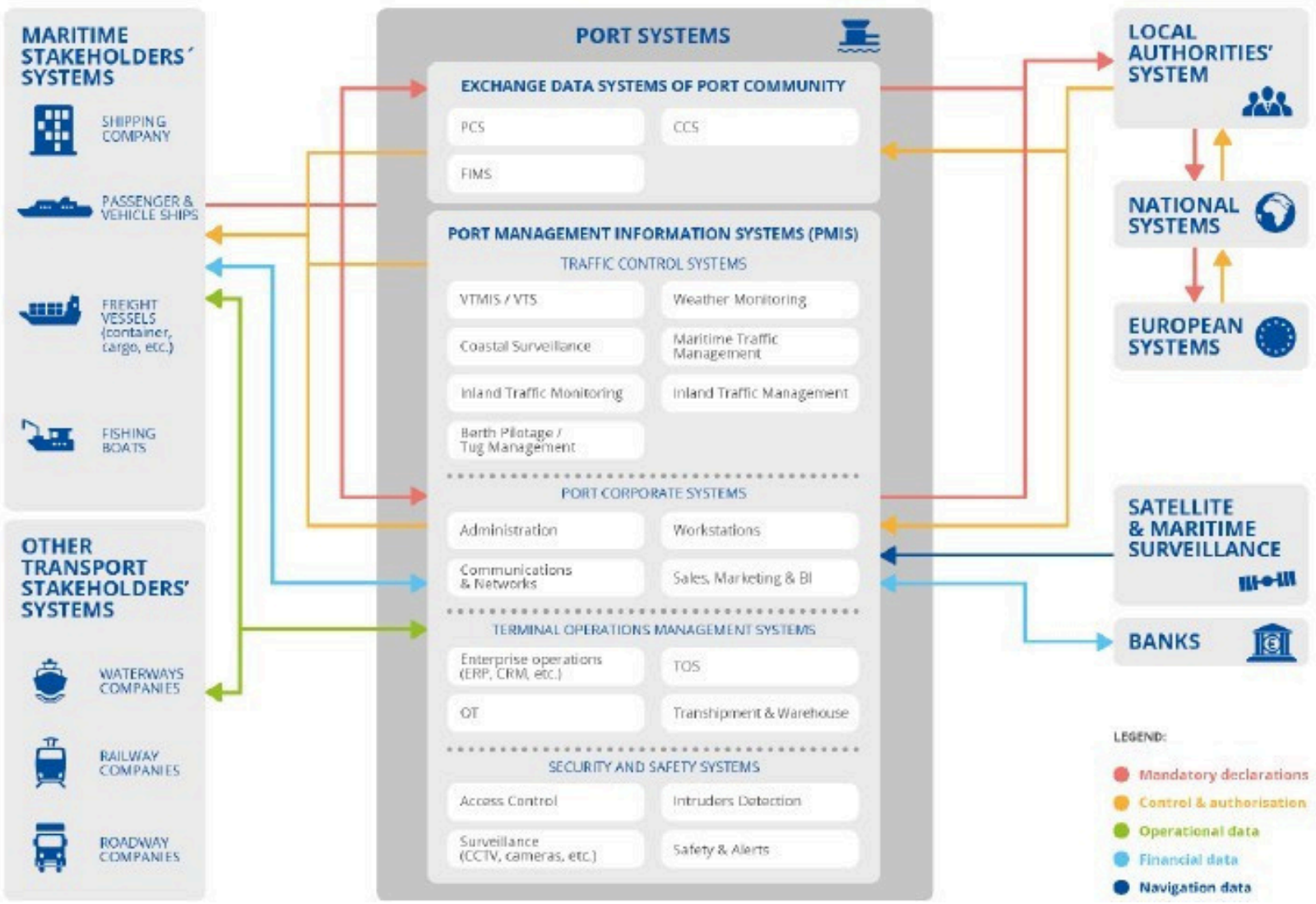
Concentrarsi sul garantire:

- **Sicurezza** delle navi, dell'equipaggio e delle operazioni
- **Integrità** dei sistemi di navigazione e dei sistemi mission-critical
- **Disponibilità e continuità** delle operazioni portuali e della catena di approvvigionamento

Affronta le sfide specifiche di:

- Ambienti altamente **interconnessi e distribuiti**
- Integrazione dei **sistemi IT, OT e IoT**
- Esposizione sia a **rischi informatici che fisici**

Modello di riferimento di alto livello dei sistemi portuali



https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector?v2= 1

Sistemi IT, OT e IoT in ambienti marittimi

Sistemi IT:

- Piattaforme di prenotazione
- Sistemi ERP
- Sistemi comunitari portuali

Sistemi OT:

- Sistemi di navigazione
- Attrezzature portuali (gru, sistemi di controllo)
- Sistemi di controllo delle navi

Sistemi IoT / IIoT:

- Sensori (carico, ambiente, attrezzature)
- Dispositivi intelligenti e sistemi di monitoraggio
- Risorse connesse tra porti e navi

Maggiore integrazione tra sistemi IT, OT e IoT

L'IoT amplia significativamente la superficie di attacco

Che cos'è una minaccia?

Minaccia: causa potenziale di un incidente indesiderato, che può comportare un danno a un sistema o a un'organizzazione.

[ISO/IEC 27000:2018]

In questo contesto, una minaccia è un fattore esterno in grado di sfruttare una vulnerabilità in un sistema.
Le minacce possono essere di origine umana (come attacchi informatici o minacce interne), ambientale (come disastri naturali) o tecnica (come malware o vulnerabilità del software).
Il panorama delle minacce nella sicurezza informatica marittima include i rischi derivanti sia da attacchi intenzionali (ad esempio, ransomware) sia da incidenti non intenzionali (ad esempio, errori umani).

https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Tipi di minacce informatiche nel settore marittimo

Minaccelegate all'IT:

- Attacchi informatici(ransomware,phishing,malware)
- Attacchi alle applicazioni web
- Compromissione delle credenziali

Minacce relative all'OT:

- Attacchi alla navigazione (ad es. spoofing GPS)
- Attacchi a ICS / sistemi di controllo
- Attacchi fisici-cibernetici

Minacce relative all'IoT / IIoT:

- Sensori e dispositivi compromessi
- Meccanismi di autenticazione deboli
- Sfruttamento di dispositivi su larga scala

Minaccelegate all'uomo:

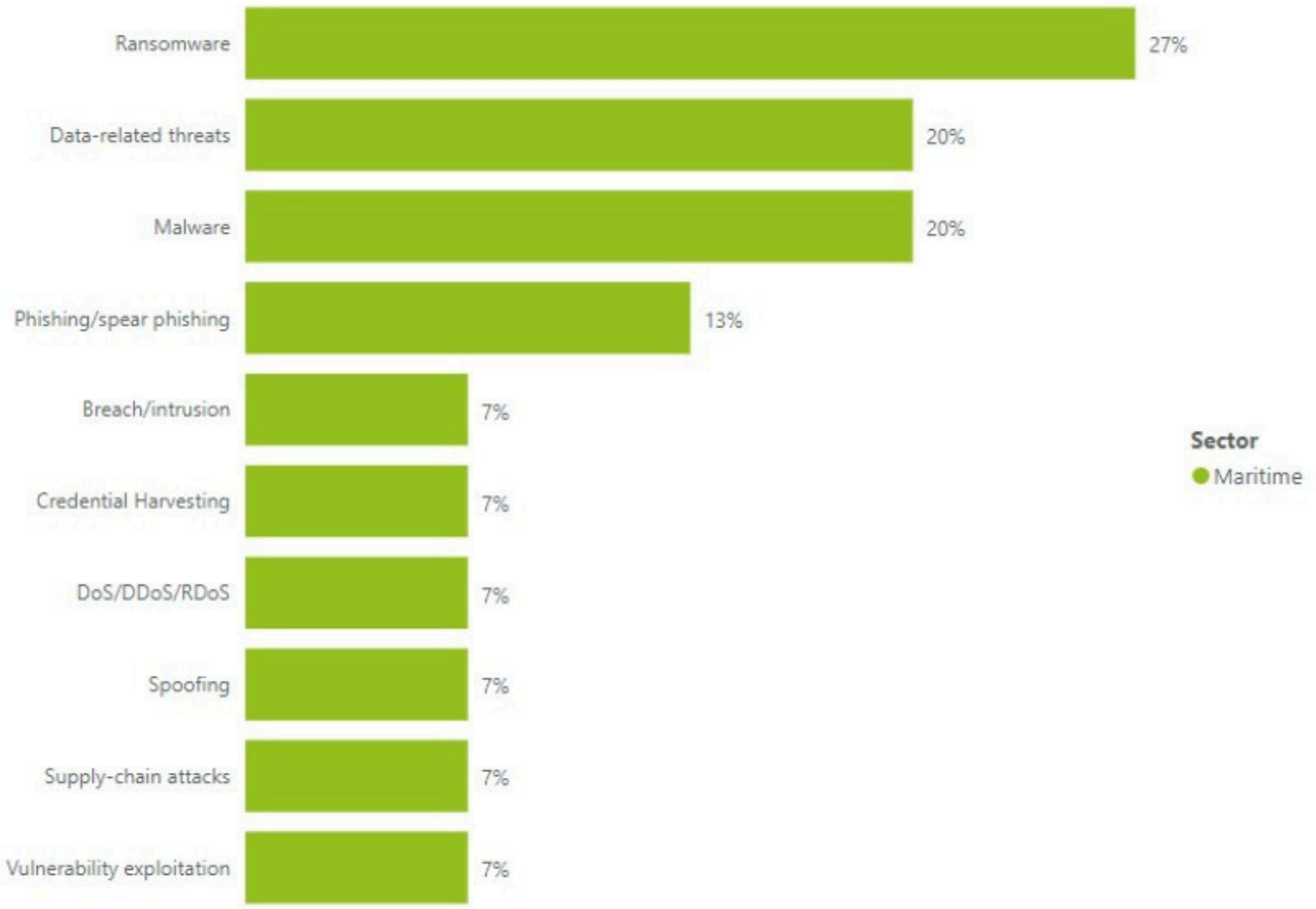
- Minacce interne
- ing sociale
- Errore umano e configurazione errata

Minacce cross-domain:

- Attacchi alla catena di approvvigionamento

Le minacce possono avere un impatto sui sistemi a bordo delle navi, nei porti e nelle infrastrutture marittime

Principali minacce marittime



https://www.enisa.europa.eu/publications/enisa-transport-threat-landscape?v2=1

Perché i sistemi marittimi sono altamente esposti alle minacce informatiche

Ecosistema complesso: porti, navi, logistica e autorità

Convergenza IT/OT: interconnessione tra sistemi operativi e aziendali

Elevata connettività: comunicazioni satellitari, accesso remoto, integrazione di terze parti

Sistemi legacy: difficili da proteggere e mantenere, spesso privi di controlli di sicurezza moderni

Ambiente critico per la sicurezza: gli incidenti informatici possono avere un impatto fisico diretto

Questi fattori aumentano significativamente la superficie di attacco e l'esposizione al rischio

Importanza della sicurezza informatica marittima

https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030

L'importanza della sicurezza informatica nel settore marittimo

- **Protezione delle infrastrutturecritiche:**leoperazionimarittimesonoparteintegrantedelcommercioglobale,poiché trasportano oltre l'80%dellemerciintuttoilmondo.Lasicurezzainformaticagarantiscelaprotezionediporti,compagniedi navigazione e reti logistichedalle minacceinformatiche.

- **Prevenzione delle interruzioni:** gli attacchi informatici possono causare gravi interruzioni nelle operazioni di spedizione e portuali. Ad esempio, incidenti come l'attacco informatico a Maersk nel 2017 hanno provocato notevoli ritardi operativi e perdite superiori a 300 milioni di dollari.

- **Tutela dell'integrità dei dati:** garantire l'integrità e la riservatezza dei dati sensibili, come i sistemi di navigazione e i manifesti di carico, è fondamentale. Le violazioni possono compromettere la sicurezza e causare perdite finanziarie.

- **Conformità normativa:** le normative sempre più severe, come le linee guida dell'Organizzazione marittima internazionale (IMO), impongono solide misure di sicurezza informatica per proteggere navi e porti; garantire la conformità può prevenire ripercussioni legali.

- **Miglioramento della sicurezza:** la sicurezza informatica protegge dalle minacce che potrebbero mettere a rischio la sicurezza dell'equipaggio e delle navi. Gli incidenti informatici possono compromettere i sistemi di navigazione, mettendo a rischio la sicurezza marittima.

- **Costruire fiducia:** una solida strategia di sicurezza informatica favorisce la fiducia tra le parti interessate, inclusi governi, clienti e partner. Questa fiducia è essenziale per il regolare funzionamento delle catene di approvvigionamento marittime.

Fattori normativi per la sicurezza informatica marittima

Normativa: requisiti legali obbligatori che le organizzazioni devono rispettare

- Requisiti dell'Organizzazione marittima internazionale (IMO)
- Regolamenti UE (ad es. GDPR, NIS2)

Standard: requisiti formalizzati per l'implementazione e la gestione della sicurezza

- ISO/IEC 27001

Framework: approcci strutturati per la gestione dei rischi di sicurezza informatica

- Quadro di riferimento per la sicurezza informatica del NIST

Linee guida: migliori pratiche raccomandate e indicazioni non vincolanti

- Linee guida ENISA
- Linee guida IMO sulla gestione dei rischi informatici

Le normative richiedono alle organizzazioni di implementare misure di sicurezza informatica

Gli standard e i quadri di riferimento vengono utilizzati per garantire la conformità e dimostrare la sicurezza

Stato di avanzamento del corso

o1. Introduzione alla sicurezza informatica marittima

o2. Comprensione dei rischi informatici marittimi

o3. Standard e migliori pratiche in materia di sicurezza informatica

o4. Certificazione sulla sicurezza informatica marittima

Che cos'è un rischio?

Rischio: l'effetto dell'incertezza sugli obiettivi (ISO 31000:2018; ISO/IEC 27000:2018). Il rischio è spesso caratterizzato dal riferimento a eventi e conseguenze potenziali o a una combinazione di questi (compresi i cambiamenti delle circostanze) e dalla relativa "probabilità" di verificarsi. [ISO/IEC 27000:2018, ISO 31000:2018]

Vulnerabilità vs Minaccia vs Rischio

Definizioni:

- **Vulnerabilità:** un punto debole che può essere sfruttato
- **Minaccia:** una potenziale causa di danno
- **Rischio:** la probabilità e l'impatto di una minaccia che sfrutta una vulnerabilità

Esempio:

- **Vulnerabilità:** accesso remoto ai sistemi portuali scarsamente protetto
- **Minaccia:** tentativo di accesso non autorizzato
- **Rischio:** Compromissione dell'account

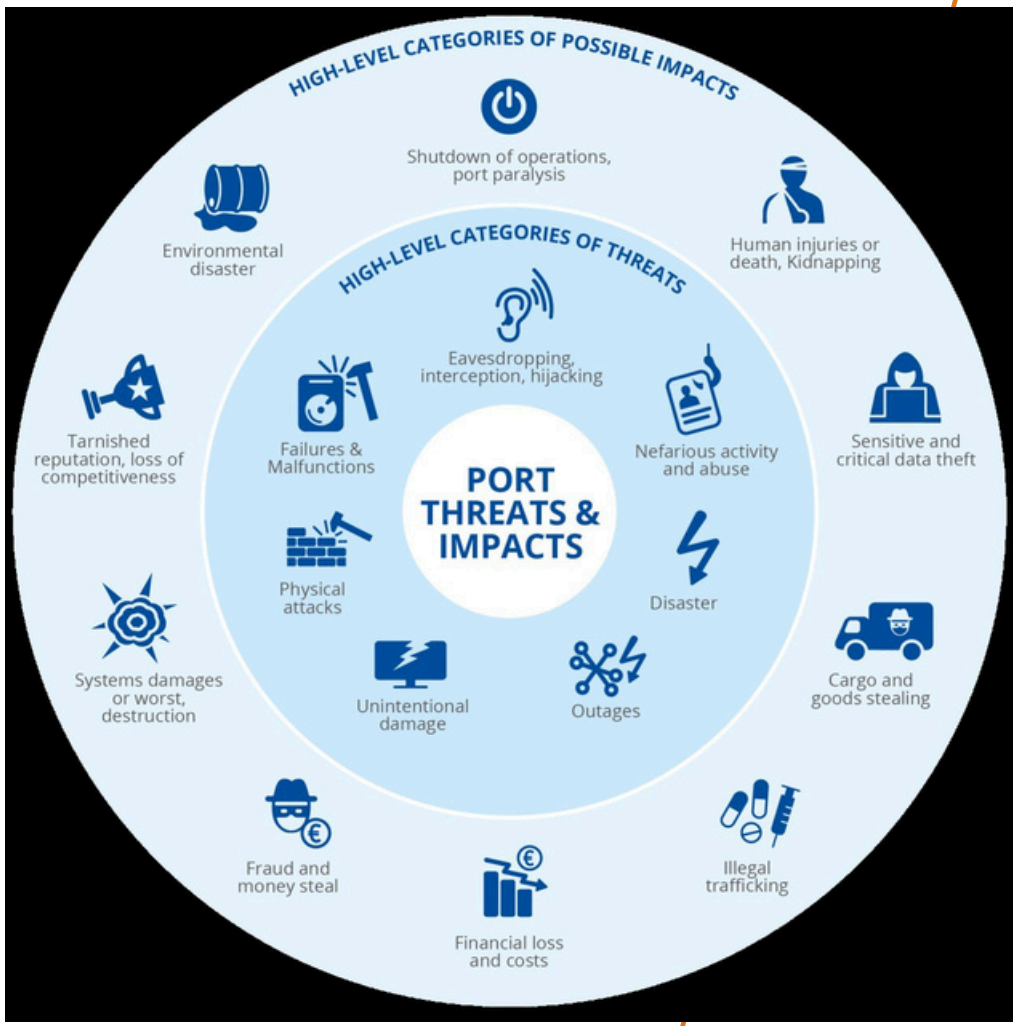
Il rischio esiste solo quando c'è una minaccia in grado di sfruttare una vulnerabilità

Scenari di rischio informatico marittimo e loro impatto

Scenario dell'evento di rischio	Impatto potenziale
Manipolazione del sistema di navigazione (ad es. spoofing GPS)	Posizionamento errato e potenziale impatto sulla sicurezza dell'imbarcazione
Violazione dei dati relativi al carico	Divulgazione di dati sensibili e ripercussioni finanziarie e reputazionali
Interruzione delle operazioni portuali	Ritardi, congestione e impatto sulla catena di approvvigionamento
Ransomware sui sistemi dei terminal	Indisponibilità dei sistemi, interruzione delle operazioni e perdite finanziarie

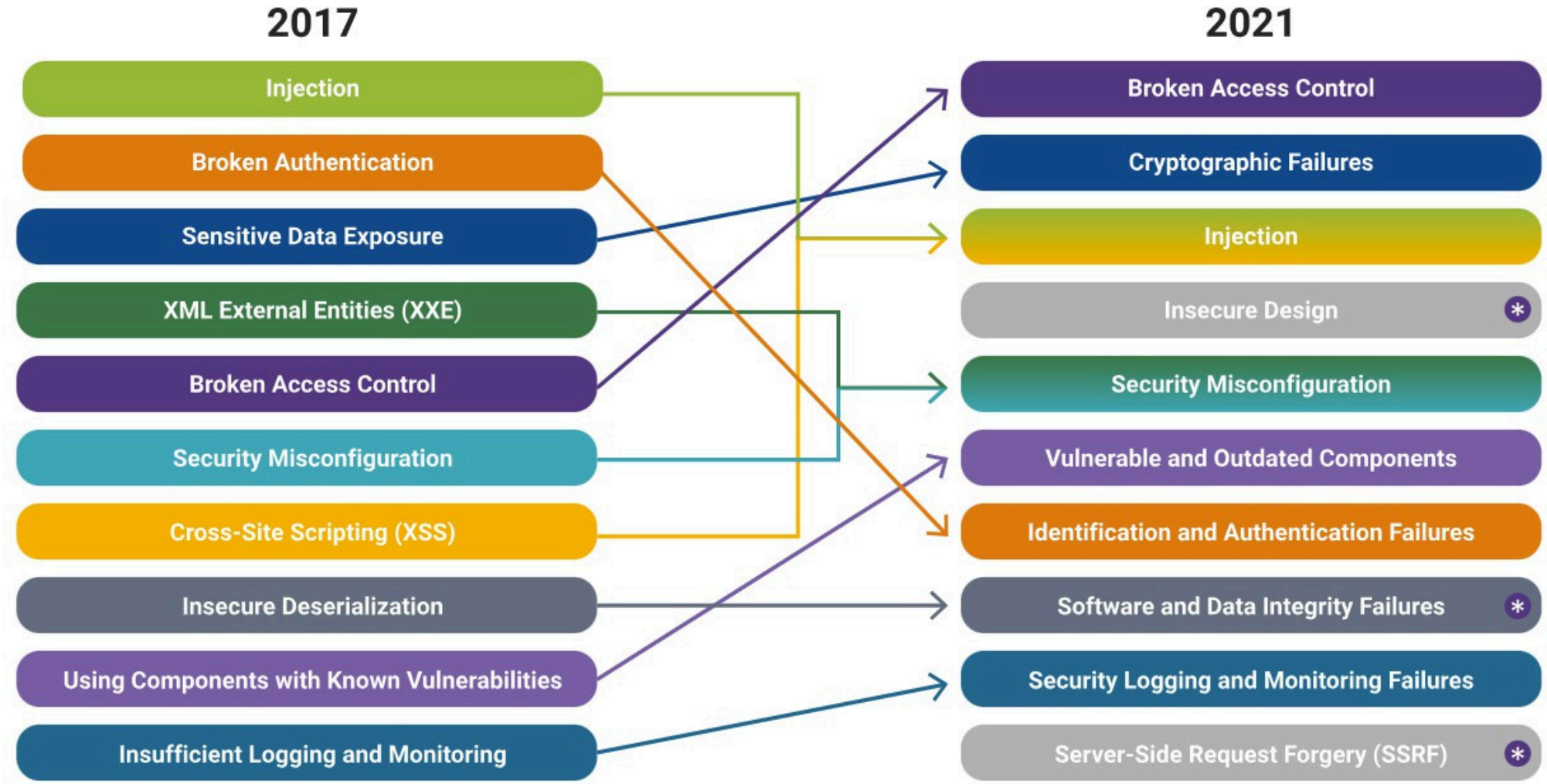
I rischi informatici in ambito marittimo possono influire sulla sicurezza, sulle operazioni e sulla continuità operativa

Identificazione dei rischi informatici nelle operazioni marittime



https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

OWASP Irischi di sicurezza più critici per le applicazioni web



OWASP Top 10:2024: https://www.owasptopten.org

Incidenti di sicurezza informatica nel settore marittimo

Police warning after drug traffickers' cyber-attack

16 October 2013

Earlier this year drug traffickers hacked into the computer controlling shipping containers at the port of Antwerp

"Inquestocasohannoassuntohacker[cheerano]di altissimo livello,personeintelligenti,chesioccupavanomolto di software", aggiunge.

Racconta che l'operazione per hackerare le società portuali si è svolta in diverse fasi, a partire dall'invio via e-mail di software dannoso al personale, che ha permesso al gruppo criminale organizzato di accedere ai dati da remoto.

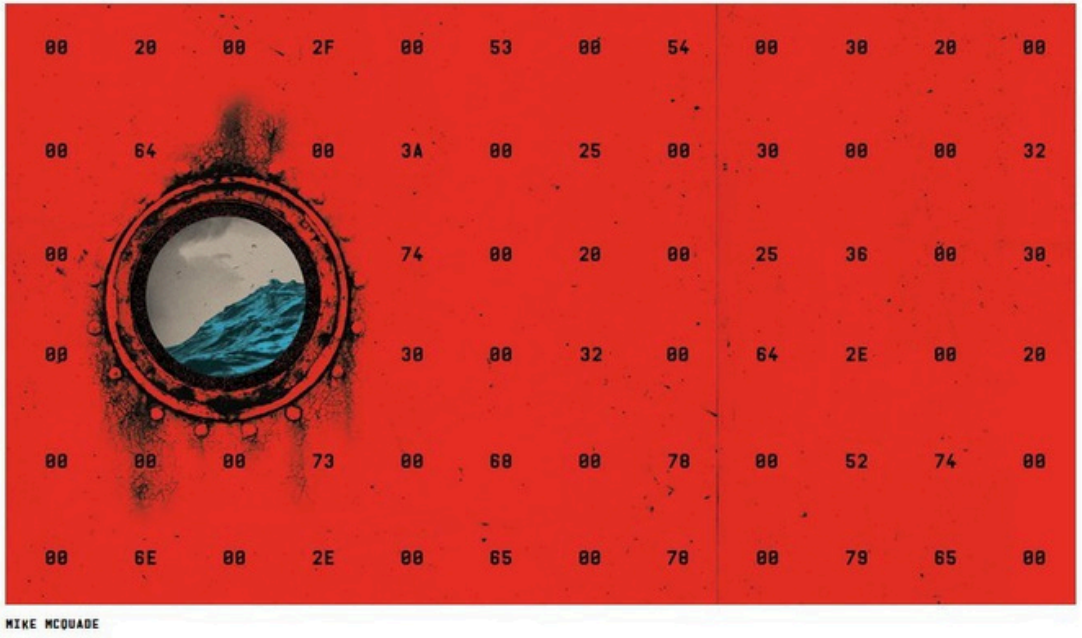
Quando è stata scoperta la violazione iniziale ed è stato installato un firewall per prevenire ulteriori attacchi, gli hacker hanno fatto irruzione nei locali e hanno installato dispositivi di registrazione della digitazione sui computer.

Ciò ha permesso loro di ottenere l'accesso wireless alle battute digitate dal personale, nonché di acquisire schermate dai loro monitor.

Incidenti di sicurezza informatica marittima

The Untold Story of NotPetya, the Most Devastating Cyberattack in History

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.



Jensen alzò lo sguardo per chiedere se qualcun altro nel suo ufficio open space, pieno di tecnici informatici, fosse stato interrotto in modo così brusco. E mentre allungava il collo, vide tutti gli altri schermi dei computer nella stanza spegnersi in rapida successione.

«Ho visto un'ondata di schermi diventare neri. Nero, nero, nero. Nero nero nero nero nero», racconta. Jensen e i suoi colleghi scoprirono rapidamente che i PC erano bloccati in modo irreversibile. Il riavvio li riportava solo allo stesso schermo nero.

[...] Gli ideatori di NotPetya hanno combinato quella "chiave universale" digitale con un'invenzione precedente nota come Mimikatz, creata come prova di fattibilità dal ricercatore francese di sicurezza Benjamin Delpy nel 2011. Delpy aveva originariamente rilasciato Mimikatz per dimostrare che Windows lasciava le password degli utenti nella memoria dei computer. Una volta che gli hacker ottenevano l'accesso iniziale a un computer, Mimikatz poteva estrarre quelle password dalla RAM e utilizzarle per hackerare altre macchine accessibili con le stesse credenziali. Su reti con computer multiutente, poteva persino consentire a un attacco automatizzato di passare da una macchina all'altra.

Incidenti di sicurezza informatica in ambito marittimo

Troubled waters: Cyber-attacks on San Diego and Barcelona's ports

03 Oct 2018

Our AI is actively defending ports across the world – such as Harwich Haven Authority and Belfast Harbour.

Last summer's wave of ransomware attacks compromised port terminals and disrupted global shipping. Since then, cyber security has quickly risen to the top of the agenda for the maritime sector. Earlier this year, another port was hit with ransomware, and then, last week, the ports of Barcelona and San Diego revealed that they had been the victims of further ransomware attacks.

La crescente convergenza tra sistemi IT e OT non accenna tuttavia a rallentare. I porti "intelligenti" iperconnessi stanno apportando efficienza e precisione, riducendo al contempo i costi. Tuttavia, l'intreccio tra fisico e digitale nei porti rimane una sfida significativa per i team di sicurezza informatica incaricati della loro difesa. Senza trarre conclusioni affrettate, non sorprende forse che il porto di Barcellona sia impegnato in un "progetto Porto Digitale", lanciato lo scorso anno per promuovere la digitalizzazione dell'ambiente portuale.

Il fattore umano nella sicurezza informatica marittima

Inmoltiincidentimarittimi,**l'uomoèil punto più debole** piuttostocheilsistema

Il phishing e l'ingegneria sociale sono punti di accesso comuni per gli attacchi informatici

Le minacce interne comprendono sia azioni dolose che errori involontari da parte di dipendenti o collaboratori

L'errore umano, come una configurazione errata o credenziali deboli, introduce vulnerabilità nei sistemi

La mancanza di consapevolezza e di formazione sulla sicurezza informatica aumenta l'esposizione agli attacchi e riduce la capacità di risposta

Le azioni umane possono avere un impatto **sui sistemi IT, OT e IoT** in tutti gli ambienti marittimi

Dall'IT all'OT: come gli attacchi si intensificano nel settore marittimo

Fase 1: Accesso iniziale (livello IT)

- E-mail di phishing
- Credenziali compromesse
- Vulnerabilità delle applicazioni web

Fase 2: Movimento laterale (rete IT)

- Accesso ai sistemi interni
- Elevazione dei privilegi
- Movimento attraverso la rete aziendale

Fase 3: Passaggio ai sistemi OT / IoT

- Connessione ai sistemi operativi
- Segmentazione debole della rete
- Credenziali o interfacce condivise

Fase 4: Impatto operativo

- Interruzione delle operazioni portuali
- Interferenza con il sistema di navigazione
- Malfunzionamento delle apparecchiature

Gli incidenti informatici spesso hanno origine nel settore IT, ma si ripercuotono sulle operazioni OT

Analisi degli incidenti utilizzando concetti di rischio

Quale risorsa è stata colpita?

Quale vulnerabilità è stata sfruttata?

Quale minaccia ha causato l'incidente?

Qual è stato l'impatto sulle operazioni, sulla sicurezza o sull'attività aziendale?

Quali controlli avrebbero potuto prevenire o mitigare l'incidente?

Valutazione del rischio vs Gestione del rischio

Ambito: la valutazionedeirischisiconcentrasull'identificazionee la valutazionedeirischi,mentre la gestione dei rischi comprende l'intero processo, inclusi la risposta e il monitoraggio.

Processo: la valutazione dei rischi è un sottoinsieme della gestione dei rischi; una gestione efficace dei rischi non può avvenire senza una valutazione approfondita dei rischi.

Obiettivi finali: L'obiettivo della valutazione dei rischi è comprendere i rischi, mentre l'obiettivo della gestione dei rischi è gestire tali rischi in modo da proteggere l'organizzazione e sostenerne gli obiettivi.

Processo di valutazione dei rischi

Fase	Fase	Azioni
Valutazione del rischio	1. Definizione dell'ambito	Definirel'ambito tra porti, naviesistemi marittimi (IT, OT, IoT)
	2. Comprensione delle risorse e dei sistemi	Identificare le risorse critiche, i ruoli e le dipendenze
	3. Identificazione dei rischi	Identificazione delle minacce, individuazione delle vulnerabilità, punti di esposizione
	4. Analisi dei rischi	Valutare la probabilità e l'impatto sulla sicurezza, sulle operazioni e sull'attività aziendale
	5. Valutazione dei rischi	Assegnare una priorità ai rischi in base a criteri definiti
Gestione dei rischi	6. Selezione dei controlli	Selezionare i controlli di sicurezza appropriati
	7. Definizione della strategia di trattamento	Definire la strategia (mitigare, accettare, trasferire, evitare)
	8. Implementazione dei controlli	Implementare i controlli negli ambienti IT, OT e IoT
Monitoraggio e revisione	9. Monitoraggio e revisione	Monitorare continuamente i rischi, valutare i controlli e apportare modifiche

Un esempio di alto livello della metodologia di gestione dei rischi informatici marittimi dell'ENISA

https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports?v2=1

Un altro esempio di metodologia di gestione dei rischi

Main axes of risk analysis	CYSMET methodology
1. Perimeter/boundaries setting	Step 0: Scope of SCS risk assessment Step 1: Analysis of SCS *1.1 Scope and objectives of SCS* *1.2 Identification of SCS-BPs* *1.3 SCS modeling*
2. Threat analysis	Step 2: SCS threat analysis *2.1 Identification of cyber and/or physical individual threats linked to an SCS asset* *2.2 SCS threat assessment*
3. Vulnerability analysis	Step 3: SCS vulnerability and impact analysis *3.1 Determination of attacker profile* *3.2 Identification of confirmed individual vulnerabilities* *3.3 Identification of confirmed/zero-day vulnerabilities* *3.4 Creation of vulnerability chains in SCS* *3.5 Identification of attack methods and graphs* *3.6 Assessment of individual vulnerability severity level*
4. Impact analysis	
5. Risk assessment	Step 4: Risk assessment *4.1 Assessment of risk level of individual assets* *4.2 Vulnerability chain risk level assessment*
6. Risk mitigation strategy	Step 5: Risk mitigation—Selection of security controls

https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2023.1156726/full

Progressi del corso

o1. Introduzioneallasicurezzainformatica marittima

o2. Comprendere i rischi informatici nel settore marittimo

o3. Standard e migliori pratiche di sicurezza informatica

o4. Certificazione in sicurezza informatica marittima dell'

Perché gli standard e i quadri di riferimento per la sicurezza informatica sono importanti

La sicurezzainformaticanonpuò basarsisumisureadhocosoluzioni isolate

Le organizzazioni necessitano di un **approccio strutturato** per gestire i rischi in modo coerente

Gli standard garantiscono **una protezione coerente nei sistemi IT, OT e IoT**, definiscono **controlli di sicurezza** chiari e misurabili e consentono **l'allineamento con i requisiti normativi e operativi**

Consentono alle organizzazioni di prendere **decisioni basate sul rischio**, dimostrare la sicurezza attraverso **gli audit** e prepararsi alla **certificazione e alla conformità**

Principali standard e quadri di riferimento per la sicurezza informatica marittima

ISO/IEC 27001:2022: standard internazionaleperl'istituzionee il mantenimentodi unsistemadigestionedella sicurezza delle informazioni (ISMS), che garantisce la riservatezza, l'integrità e la disponibilità delle informazioni attraverso un approccio sistematico.

Quadro di riferimento per la sicurezza informatica del NIST: quadro di riferimento basato sul rischio che aiuta le organizzazioni a identificare, proteggere, rilevare, rispondere e riprendersi dalle minacce alla sicurezza informatica.

GDPR (Regolamento generale sulla protezione dei dati): regolamento dell'UE che definisce i requisiti per la protezione dei dati personali, applicabile anche alle organizzazioni marittime che trattano i dati dei cittadini dell'UE.

Gestione dei rischi informatici dell'IMO: Linee guida per l'integrazione della sicurezza informatica nelle operazioni marittime e nei sistemi di gestione della sicurezza al fine di proteggere le attività di navigazione e portuali.

Linee guida ENISA (Agenzia dell'Unione Europea per la sicurezza informatica): Raccomandazioni e best practice in materia di sicurezza informatica per gli ambienti marittimi e portuali, a sostegno della protezione basata sul rischio e della resilienza delle infrastrutture critiche.

Sfide nell'applicazione degli standard di sicurezza informatica nel settore marittimo

Isistemi OTlegacysonodifficilidaaggiornareoproteggere,poichénon sonostatiprogettatitenendocontodella sicurezza informaticaespessononsonoingradodisupportare i controlli moderni

Spesso non è possibile mettere i sistemi fuori servizio, poiché è richiesto un funzionamento continuo, il che limita la possibilità di applicare patch o eseguire interventi di manutenzione

Le misure di sicurezza non devono interferire con la sicurezza e le operazioni, il che richiede un attento equilibrio tra protezione e continuità operativa

Molteplici parti interessate (porti, operatori, fornitori) condividono sistemi e responsabilità, rendendo più complessa l'implementazione coerente dei controlli

Controlli di sicurezza fondamentali nei sistemi marittimi

Ilcontrollodegliaccessielagestionedelleidentitàgarantisconochesologliutentieisistemiautorizzati possano accedere ai sistemi marittimi critici

La segmentazione della rete limita la diffusione degli attacchi tra gli ambienti aziendali e quelli operativi

Il monitoraggio e il rilevamento degli incidenti consentono l'individuazione tempestiva di attività sospette in tutti i sistemi

Il rafforzamento della sicurezza dei sistemi e la gestione delle patch riducono le vulnerabilità, tenendo conto dei vincoli operativi

Il backup e il ripristino garantiscono che i sistemi e i dati possano essere ripristinati in seguito a interruzioni o incidenti informatici

Progressi del corso

o1. Introduzioneallasicurezzainformatica marittima

o2. Comprendere i rischi informatici nel settore marittimo

o3. Standard e best practice di sicurezza informatica dell'

o4. Certificazione in materia di sicurezza informatica marittima

Che cos'è la certificazione in sicurezza informatica

Un processo formale volto a valutare e verificare la sicurezza di sistemi o prodotti

Basato su schemi di certificazione e standard di valutazione (ad es. Common Criteria, EUCC)

Eseguito da **organismi di valutazione indipendenti e accreditati**

Richiede **requisiti di sicurezza, livelli di test e di garanzia definiti**

Si traduce in un livello certificato di fiducia nella sicurezza del sistema o del prodotto

Certificazione vs Conformità

Aspetto	Conformità	Certificazione
Definizione	Rispettare i requisiti normativi o legali	Valutazione formale rispetto a criteri di sicurezza definiti
Valutazione	Autodichiarata o interna	Valutazione indipendente condotta da terzi
Ambito di applicazione	Leggi, regolamenti, politiche	Standard e schemi di certificazione (ad es. Common Criteria, EUCC)
Risultato	Dimostra la conformità	Fornisce garanzie verificate e fiducia

Perché la certificazione è importante nel settore marittimo

Aspettativenormativeediconformità: la certificazioneaiuta leorganizzazioni adallinearsi ai requisitinormativi

Requisiti aziendali e contrattuali: spesso richiesta da partner, clienti e soggetti della catena di fornitura

Riduzione del rischio nei sistemi interconnessi: offre garanzie in ecosistemi marittimi complessi

Fiducia e credibilità: crea fiducia tra porti, operatori e terze parti

Vantaggio competitivo: dimostra maturità e differenzia le organizzazioni sul mercato

Standard e schemi comuni di certificazione della sicurezza informatica

Critericomuni (ISO/IEC15408)–Certificazionediprodotti esistemi informaticibasatasulla valutazione dellasicurezza

Metodologia di valutazione comune (ISO/IEC 18045) – Definisce la metodologia per la valutazione dei prodotti secondo i Criteri comuni

EUCC (European Cybersecurity Certification Scheme) – Quadro dell'UE per la certificazione di prodotti e servizi ICT

Panoramica del processo di certificazione

Definizione dell'Oggetto di Valutazione (TOE) (sistema o prodotto nell'ambito di applicazione)

Selezionare un Profilo di Protezione (PP) applicabile o definire i requisiti per la valutazione

Definire l'obiettivo di sicurezza (ST) descrivendo in che modo il TOE soddisfa gli obiettivi di sicurezza richiesti

Eseguire una valutazione e dei test di sicurezza indipendenti basati su una metodologia di valutazione consolidata

Valutazione effettuata da laboratori di valutazione e organismi di certificazione accreditati

Certificazione rilasciata con un livello di garanzia definito che indica il grado di affidabilità della sicurezza del sistema

Mantenimento della certificazione tramite aggiornamenti, sorveglianza e rivalutazione

Sfide nella certificazione marittima

Definizionedell'ambitodicertificazionetranavieporti:isistemiabbracciano navi, infrastrutture portuali e reti logistiche, rendendo difficileisolarel'oggetto dellavalutazione

Valutazione dei sistemi in ambienti operativi: capacità limitata di eseguire test su sistemi in produzione a causa del funzionamento continuo e dei vincoli di sicurezza

Sistemi marittimi eterogenei e legacy: tecnologie diverse e apparecchiature obsolete complicano l'allineamento con i moderni requisiti di valutazione

Dipendenze della catena di approvvigionamento marittima: la certificazione deve tenere conto dei sistemi interconnessi tra operatori, porti, fornitori e operatori logistici

Valutazione dei rischi e della conformità nelle catene di approvvigionamento marittime

La certificazione si estende dai singoli sistemi **ai servizi interconnessi della catena di approvvigionamento marittima** (porti, navi, logistica, fornitori di servizi)

Lavalutazione si basasu:

- **Analisi dei rischi tra processi aziendali, risorse e partner commerciali (BP) interconnessi**, comprese le dipendenze e gli effetti a cascata
- **Implementazione di controlli** oltre i confini organizzativi e tecnici
- **Raccolta di prove** da più parti interessate (sistemi, processi, operazioni)

La metodologia CYRENE Risk & Conformity Assessment introduce un approccio orientato alla catena di fornitura marittima che supporta sia gli implementatori che i valutatori

Enfasi su entrambi:

- Sicurezza **basata sul rischio** a livello di ecosistema
- Conformità **basata su prove** e valutazione continua

Valutazione del rischio e della conformità nelle catene di approvvigionamento marittime

Rappresentazione schematica della metodologia CYRENE

Grazie

Invia le tue richieste a:
pkyranoudi@tuc.gr
dpolemi@unipi.gr