CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Sicurezza delle infrastrutture critiche per il settore marittimo

Corso

CSP008_C_M

PRESENTAZIONE DI: BRUNO BENDER

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

Rischi delle infrastrutture critiche marittime

o1. Identificare i rischi per la sicurezza informatica delle infrastrutture critiche marittime

o2. Corso annuale nell'ambito dei workshop marittimi – in presenza – Tolone)

o3. Infrastrutture critiche, OES, soggetti interessati del settore marittimo

o4. Specificità nazionali - direttiva NIS

o5. Importanza dei dati (EUCI, sensibili, ecc.)

o6. Valutazione e mitigazione dei rischi (ad es. crittografia)

o7. C2B Consulting

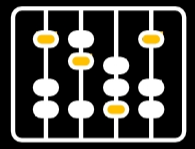
115 rue du maréchal Foch –F83.200 LE REVEST – Francia

Obiettivi: questo modulo, progettato per gli stakeholder del settore marittimo, mira a identificare i rischi per le infrastrutture critiche al fine di migliorarne la resilienza.

CHI

Infrastrutture critiche marittime e OES identificate nella direttiva NIS.

COSA



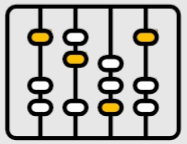
Fondamenti della sicurezza informatica Gestione dei rischi nel settore marittimo

PERCHÉ

Fornire ai partecipanti le conoscenze e le competenze necessarie per gestire i rischi di sicurezza informatica

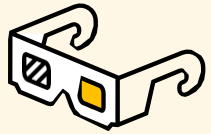
Logistica della formazione CSP: CSP003_ RISCHI DELLE INFRASTRUTTURE CRITICHE MARITTIME

QUANDO



Calendario: Autunno 2024 – Autunno 2025

DOVE

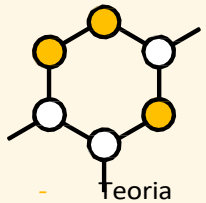


SEDE

Tolone (Francia)

NMIOTC (Grecia)

COME



- Teoria
- Formazione pratica

CHI

Profilo dei partecipanti alla formazione

- Manager e dirigenti
- Professionisti nel mondo del lavoro
- PMI e dipendenti del settore pubblico
- ~~Professionisti e appassionati di sicurezza informatica~~
- ~~Sviluppatori CIS marittimi~~

CHI

Profilo del formatore

- Bruno BENDER
- C2B CONSULTING
- Ex ufficiale della Marina Militare / Specialista CIS
- Responsabile della sicurezza informatica
  - NATO
  - A livello nazionale
  - UE
- Dal 2017 Esperto di sicurezza informatica e fondatore di C2B
- PMI specializzata in sicurezza marittima / sicurezza informatica per supporto
  - Infrastrutture critiche
  - Operatori di servizi essenziali
  - Compagnie marittime e porti
  - Amministrazioni pubbliche che operano in mare

COSA

Argomenti di formazione

- Qual è la definizione di infrastruttura critica
- Comunità di utenti
- Architetture tecniche / INFRASTRUTTURE
  - Amministrazioni
  - Descrizione tecnica
- Rischi
- Progettazione dell'architettura di sicurezza
- Implementazione della sicurezza
- Misure di mitigazione

PER

Risultati di apprendimento

- Dimostrare una condotta etica e professionale in tutti gli aspetti della gestione delle informazioni e della sicurezza informatica.
- Comprendere e articolare i concetti chiave e principi di sicurezza informatica e delle informazioni.
- Comprendere il panorama in continua evoluzione delle minacce informatiche e la vasta gamma di attacchi informatici.
- Identifica le minacce, le vulnerabilità e i rischi per la sicurezza informatica di un'organizzazione.
- Riconoscere il ruolo del fattore umano nelle violazioni della sicurezza informatica e nelle strategie di mitigazione dei rischi.
- Capacità di aiutare e selezionare controlli di sicurezza appropriati per proteggersi dalle minacce e dai rischi identificati alla sicurezza informatica.

Argomento 1:
Rischi di sicurezza informatica nel settore marittimo

Tratteremo le seguenti competenze

- Introduzione alla sicurezza delle informazioni: questa sezione introdurrà il concetto di sicurezza delle informazioni e la sua importanza per le organizzazioni. Discuterà inoltre i diversi tipi di risorse informative che devono essere protette, nonché le diverse minacce e vulnerabilità che queste risorse devono affrontare.
- Introduzione alla sicurezza informatica: questa sezione si concentrerà sulle minacce e vulnerabilità specifiche che esistono nel settore informatico. Verranno inoltre discussi i diversi tipi di attacchi informatici che possono essere sferrati, nonché i diversi modi per mitigarli.
- La triade CIA: questa sezione tratterà i tre pilastri della sicurezza delle informazioni: riservatezza, integrità e disponibilità. Spiegherà il significato di ciascun pilastro e perché è importante.
- Altri modelli di sicurezza: questa sezione tratterà altri modelli di sicurezza che possono essere utilizzati per proteggere le risorse informative. Questi modelli includono il NIST Cybersecurity Framework, lo standard ISO/IEC 27001 e il framework COBIT.

Argomento 2:

Minacce e vulnerabilità

Tratteremo le seguenti competenze

- 1. AIS: Che cos'è un'infrastruttura critica - Uso legale e specificità
- 2. Descrizione di un framework CI che include hardware, software e reti.
- 3. Modalità di minaccia alle infrastrutture critiche
- Attaccanti
- Misure di mitigazione
- 4. Piani e azioni di resilienza
- Altro

Argomento 3:
Casi d'uso

Tratteremo le seguenti competenze

- 1. Piani nazionali
- 2. Misure di mitigazione locali
- 3. Istruzione/Formazione
- 4. Indagini e lezioni apprese dal passato
- 5. Minacce e rischi
- 5. Misure di mitigazione
  - - Tecniche
  - - Organizzative
  - - Assicurative

CyberSecPro

EDUCATION AND TRAINING

CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

Next level cybersecurity education and training

Funded by the European Union

Sicurezza delle infrastrutture critiche per il settore marittimo

Corso

CSP0008_C_M

PRESENTAZIONE DI: BRUNO BENDER

Sicurezza delle infrastrutture critiche per il settore marittimo

Argomento 1 – Dati generali

- Quadro marittimo/cibernetico
- Cybersecurity e tecnologia

Sicurezza informatica: non solo tecnologia

Servizi

Servizi di protezione

EU CERT-M

Tecnico

Monitoraggio end-to-end
Manutenzione adattiva

Organizzativa

Cyber sicurezza marittima Governance

Semantica

Valutazione e gestione dei rischi, segnalazione degli incidenti, condivisione delle analisi

ETSI GS ISI 00X: "Indicatori di sicurezza delle informazioni (ISI)..."

Legale

Dati commerciali sensibili, dati personali, posizioni,

e marittima Rischio di sicurezza informatica

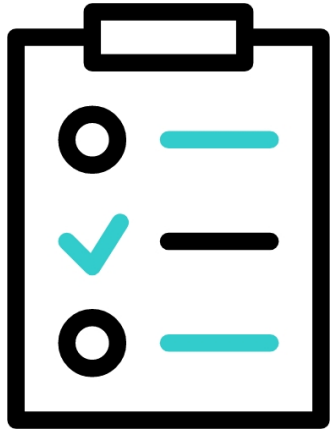
Obiettivo

Il corso C2B_CSP008 mira a descrivere i rischi per la sicurezza informatica nell'ambiente marittimo e a identificarne le specificità.

Particolare attenzione è dedicata agli standard e alle specificità dell'AIS, nonché alla normativa internazionale. Vengono descritte in dettaglio le vulnerabilità comuni dei sistemi e delle applicazioni AIS/GNSS.

Metodi Esempi di e di hacking e spoofing di questi sistemi sono dimostrati durante il corso.

Vengono presentati l'analisi dei rischi, i piani di sicurezza, le politiche e i processi, il quadro normativo e gli standard di sicurezza, le misure di continuità e di ripristino.



marittima Cybersecurity Rischio

Minaccia alla sicurezza informatica nel settore marittimo

- Panorama mondiale
- Attacchi / Incidenti
- Evoluzioni

Rischio nel settore marittimo / Mitigazioni Quali sistemi

Cybersecurity della Guardia Costiera dell'UE

Risultati - Il proseguimento degli sforzi attuali

Basarsi sull'iniziativa dei seminari ECGFF sulla "Prevenzione degli attacchi informatici nel settore marittimo" avviata dalla presidenza tedesca e attuare un "Gruppo di lavoro sulla sicurezza informatica della Guardia costiera dell'UE".

È necessario sviluppare ulteriormente un approccio comune alla sicurezza informatica per la comunità della guardia costiera. A tal fine, occorre approfondire la comprensione giuridica, organizzativa e tecnica, migliorando la cooperazione intersettoriale e transfrontaliera ed elaborando linee guida e migliori pratiche di gestione.

Animazione della comunità della guardia costiera per la sicurezza informatica e attuazione di una piattaforma di condivisione delle informazioni dedicata alla sicurezza informatica e ospitata dall'EMSA.

Convalida consensuale dei termini di riferimento del "Gruppo di lavoro sulla sicurezza informatica della Guardia costiera dell'UE"

rivolta alla Commissione europea (DG MARE).

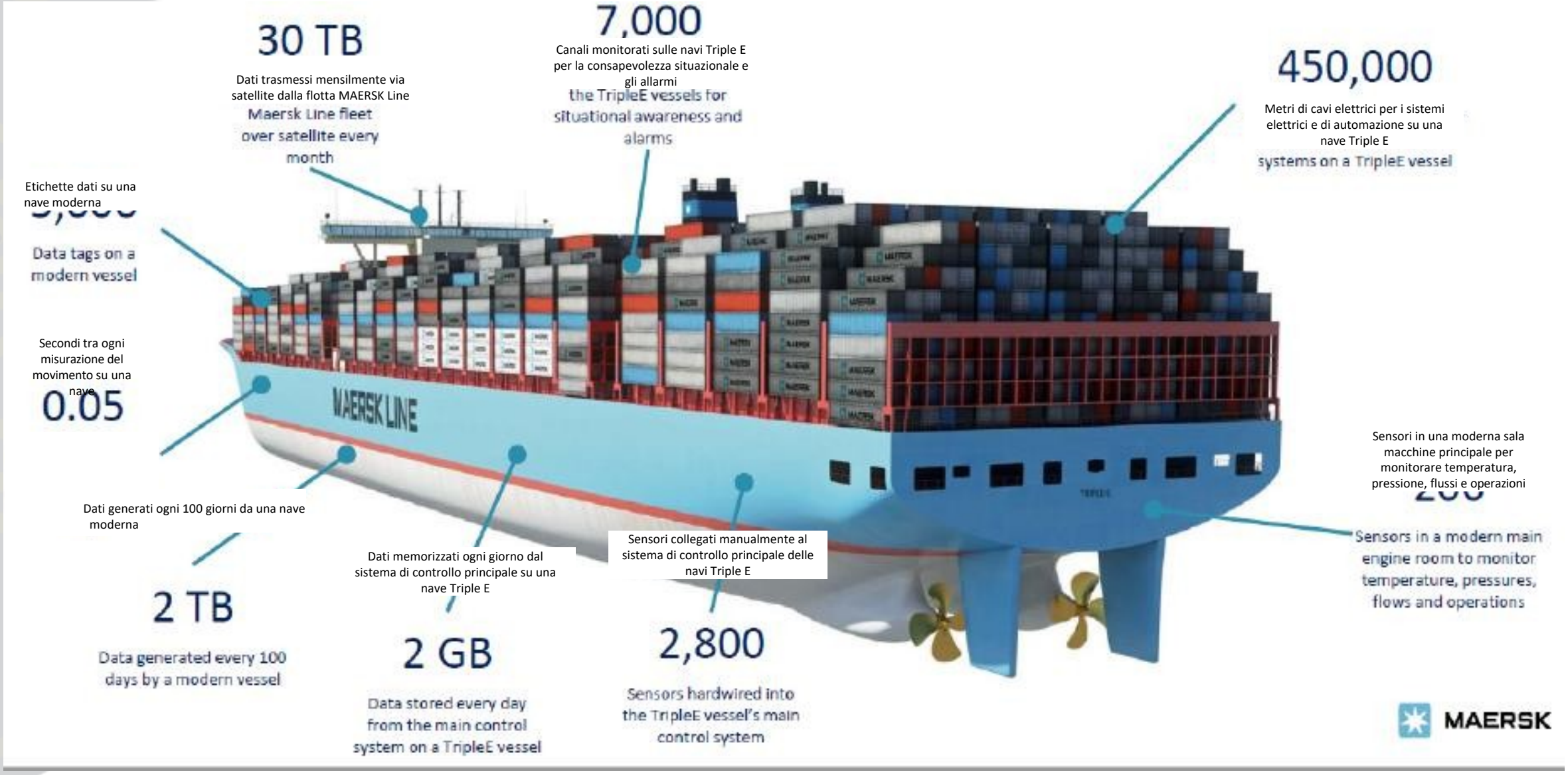
Sostegno a ulteriori miglioramenti dei processi di condivisione delle informazioni per uno scambio tempestivo di informazioni su attacchi informatici e incidenti che colpiscono la comunità marittima.

Proseguimento durante la presidenza croata dell'ECGFF (2019-2020).

Cybersecurity marittima

- **Minaccia alla sicurezza informatica nel settore marittimo**
- Dati marittimi
- Panorama mondiale
- Attacchi / Incidenti
- Rischi

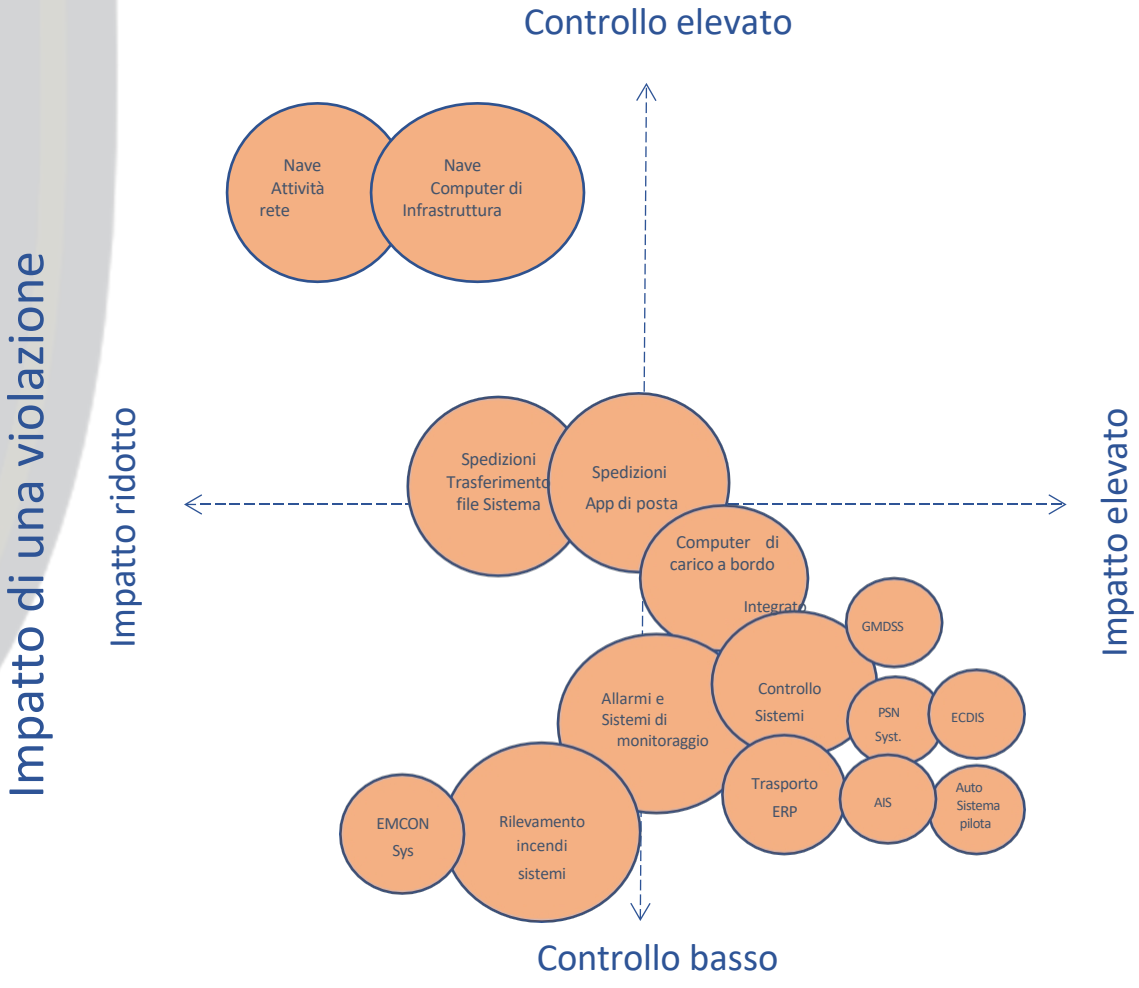
Il rischio dei dati nel settore marittimo

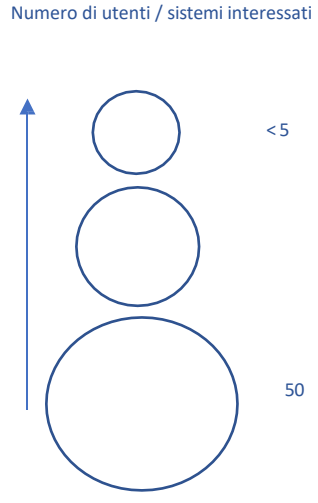


Infrastrutture critiche - Autorità marittime

Controllo della sicurezza / Impatto degli incidenti

Controllo della sicurezza da parte dell'armatore





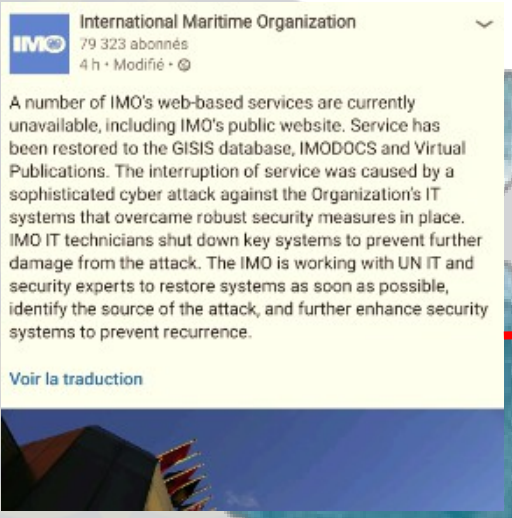
Sicurezza delle infrastrutture critiche per il settore marittimo

Argomento 2 – Minacce e vulnerabilità

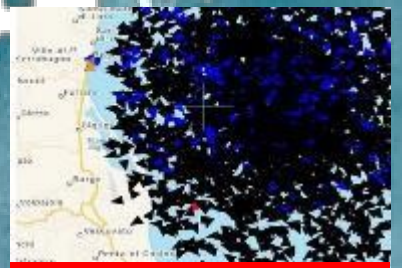
- Cartografia dei sistemi marittimi
- Minacce – A livello mondiale
- Eventi osservati Incidenti

Minacce – Attacchi gravi 2020-2023

In tutto il mondo



Marzo 2020 - Svizzera (MSC)



Dicembre 2019 – Elba (Spoofing AIS)

Aprile 2020 – Ormuz Bandar Abbas

Settembre 2020 – Int (CMA-CGM)

Maggio 2020 – California (Spoofing AIS

Settembre 2020 – Int (GEFCO)

Marzo 2020 – Marsiglia / FOS – Attacco regionale

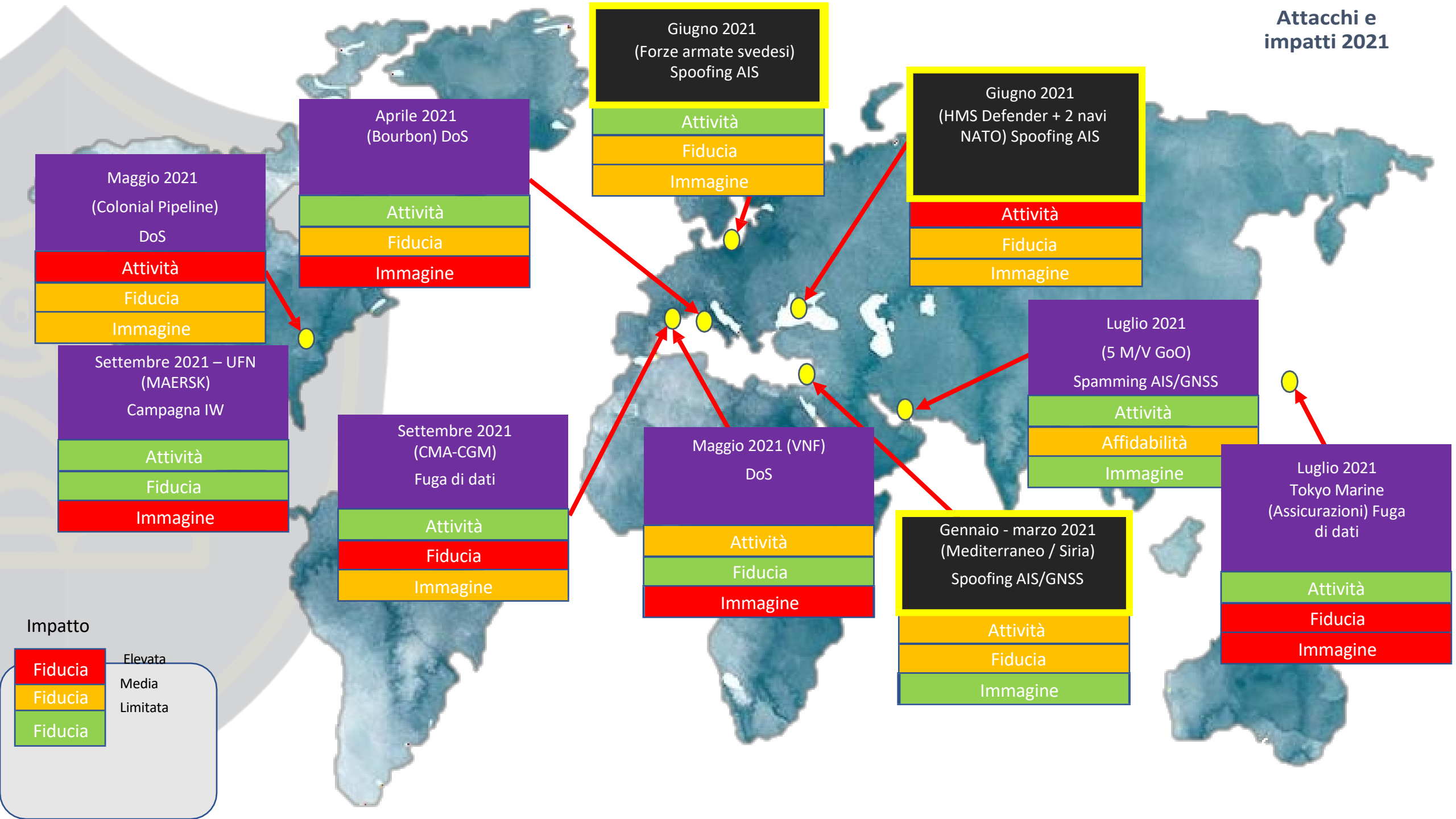
2020 – Mediterranée (interferenza GPS)

Gennaio 2020 – Cina (Spoofing AIS)

Attacchi/incidenti (2020 – 22)

Entità	Data	Impatto	Analisi
Porto di Bandar Abbas	2020	Impossibilità di realizzare terminali di carico e scarico	Attacco preventivo deliberato **contro una porta "non critica" da parte di un Paese**, con conseguente risposta immediata
MSC	2020	Servizi inutilizzabili (>12 ore) Pagina web e interfaccia cliente inaccessibili per diversi giorni in alcune aree	**I servizi ospitati localmente** hanno consentito all'operatore di continuare a operare in alcune regioni
MED EUROPE TERMINAL	2020	Servizi Internet bloccati che hanno avuto ripercussioni sul portale web e sulla messaggistica.	L'operatore marittimo è stato **vittima collaterale** di un attacco alla regione meridionale durante il contenimento del
GNSS/AIS	2018 - 2020	Saturazione dei ricevitori AIS (osservata nel Mediterraneo nel 2019, in Cina e negli Stati Uniti nel 2020) Interferenze GPS permanenti nel Mediterraneo orientale, in Cina e nel Mar Nero	L'interferenza o lo spoofing (saturazione) dei sistemi GNSS/AIS rappresenta un **pericolo** reale **per la navigazione**. Gli attacchi ai sistemi GNSS/AIS, osservabili nelle loro forme più crude, possono alla fine **distorcere tutti i dati marittimi**.
CARNIVAL	2020	Perdita dei dati dei clienti e dei dipendenti. Perdita di attività sulla crociera (prenotazioni)	Classico attacco ransomware che ha crittografato parte dei sistemi e dei dati CIS e bloccato l'attività per diverse ore.
CMA / CGM	20	Dati e servizi inaccessibili a causa di Tiocryptolocker. Perdita di clienti.	L'attacco è stato risolto in più di 2 settimane da specialisti **che non avevano familiarità con il CIS dell'azienda**. La comunicazione deve concentrarsi sulle priorità degli operatori.
BENETEAU	2021	Attacco ai sistemi e perdita di dati	BENETEAU è stata attaccata una prima volta nel 2018 e ha perso dati (elenchi di clienti) una seconda volta in meno di 3 anni
BOURBON	2021	Attacco al sistema operativo principale	Problemi nella gestione dei turni dell'equipaggio, delle attività quotidiane e dei rapporti relativi alle navi
GAZOCEAN	2021	Presidente Rip-Off	Perdita finanziaria
VNF	2021	Attacco al sistema informativo principale	Sistema di gestione bloccato per diversi giorni
Porto di Abidjan	2021	Ransomware MATRIX	Impatto limitato sul traffico marittimo segnalato dopo una reazione coordinata
DNV-GL		Spionaggio per conto dello Stato - Furto di dati Immagine della società spogliata	Le società di classe sono spesso esposte a questo tipo di rischio a causa delle informazioni a cui hanno accesso

Attacchi e impatti 2021



Attacco CMA / CGM 2020

Édition du jeudi 31 octobre 2024
Feuilleter l'édition

LA LETTRE

La Matinale | Se connecter | S'abonner

Menu | À la Une | Action publique | Entreprises | Médias | Paris-Bruxelles | Enquêtes | Entourages | Mouvements | Feuilletons

L'enquête sur la cyberattaque de CMA CGM avance à grands pas

Si la plupart des enquêtes sur les rançongiciels échouent à identifier les hackers, les cybergendarmes ont arrêté en Ukraine des suspects dans l'attaque qui a ciblé le transporteur maritime CMA CGM en 2020. L'enquête en cours confirme les premières pistes sur le gang Ragnar Locker. [...]

Publié le 07/12/2021 à 6h30 • Lecture 2 minutes

Créez une veille sur les mots-clés cités dans cet article

Agence Nationale de la Securite des Systemes d'Information

CMA CGM

L'indagine sull'attacco informatico alla CMA CGM sta procedendo rapidamente Mentre la maggior parte delle indagini sui ransomware non riesce a identificare gli hacker, la polizia informatica ha arrestato in Ucraina i sospetti responsabili dell'attacco che ha colpito la compagnia di navigazione CMA CGM nel 2020. L'indagine in corso conferma le prime piste sulla banda Ragnar Locker. [...]

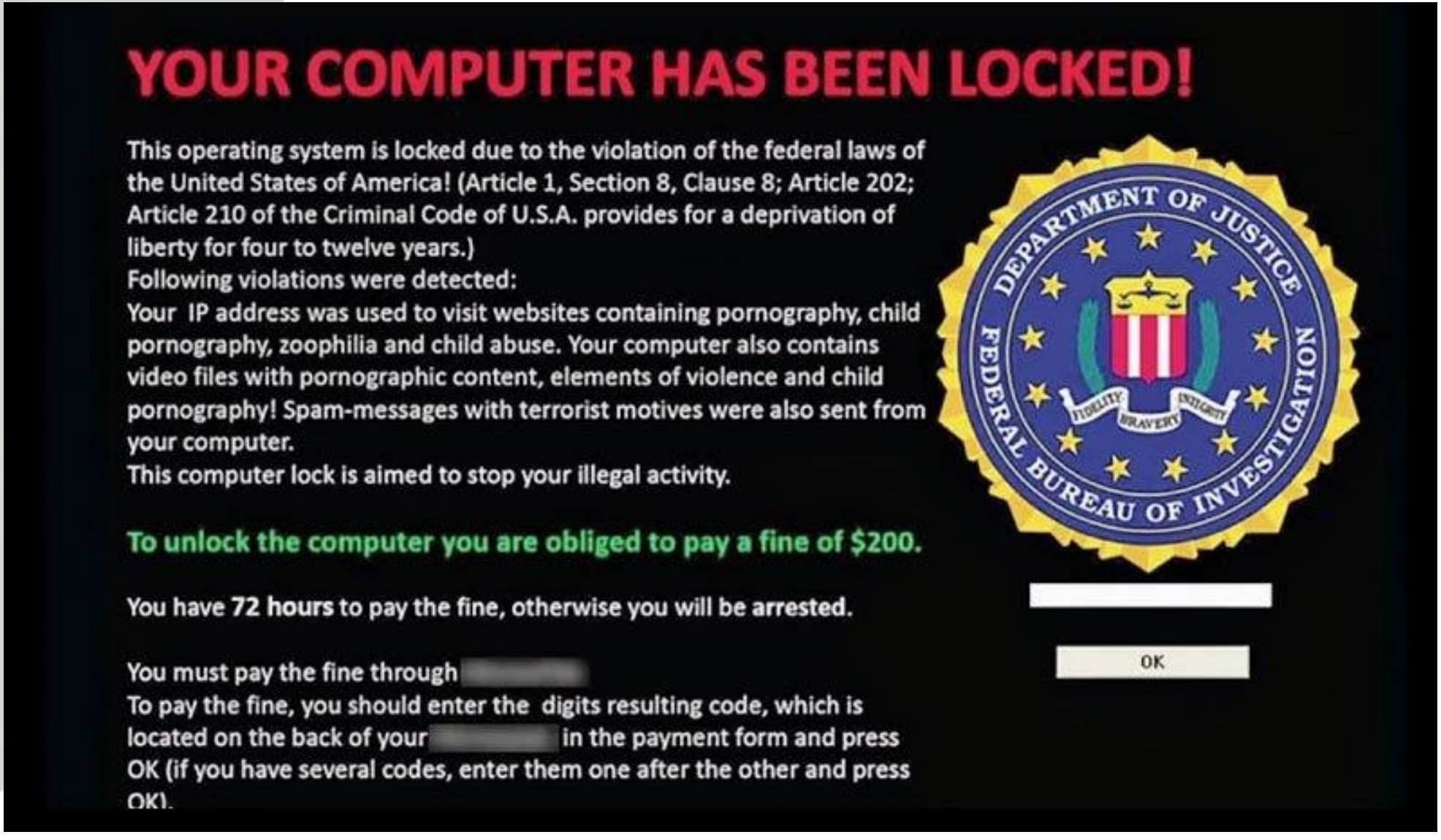
Caso d'uso - ransomware

- **Che cos'è un "ransomware"**
  - Malware che minaccia di causare danni se non viene pagato un riscatto

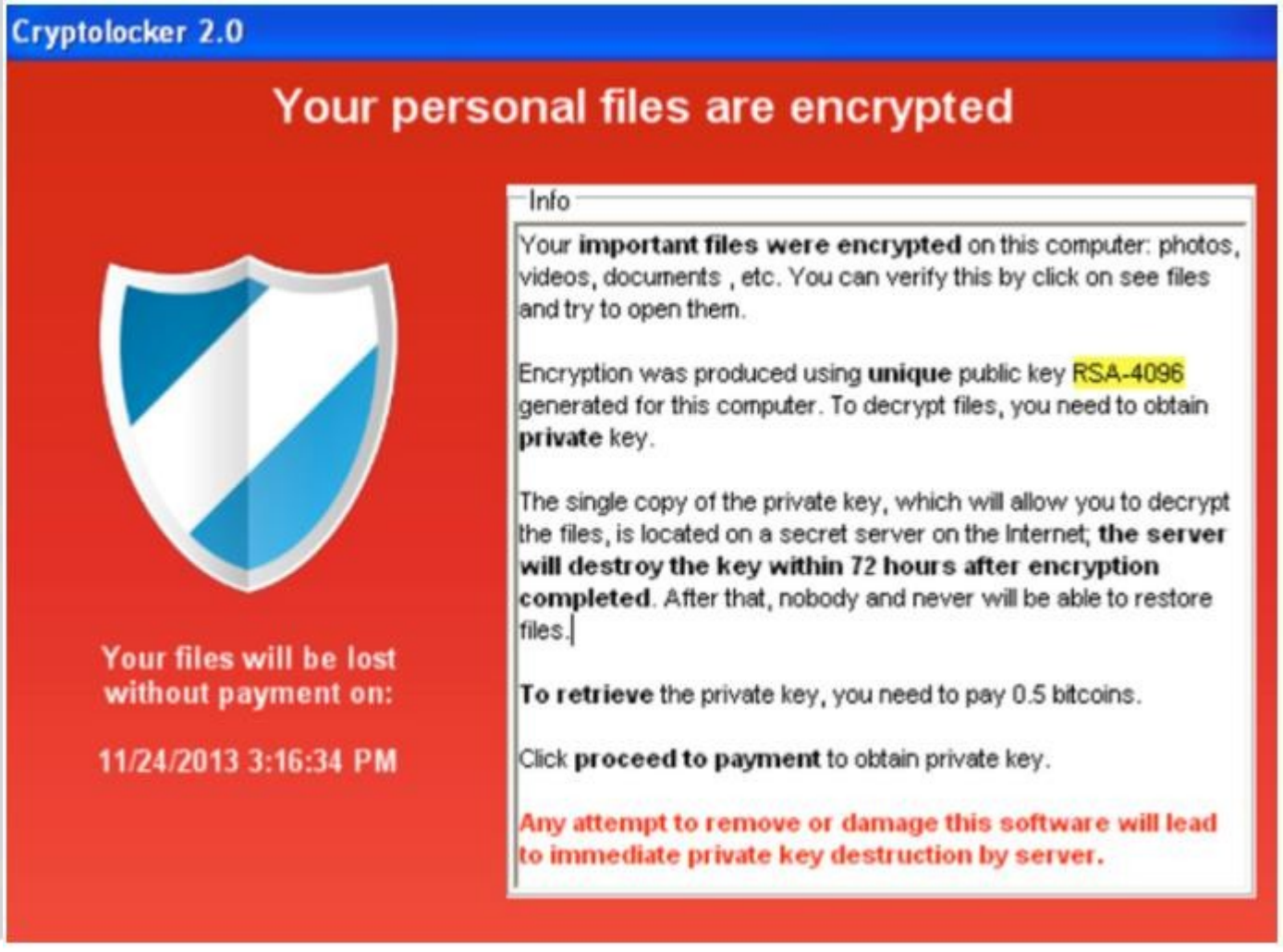
- **Tipi**
  - *Blocco dello schermo*
  - *Crittografia dei file*
  - *DDOS*
  - *Combinati*

Fonte: Trend Micro

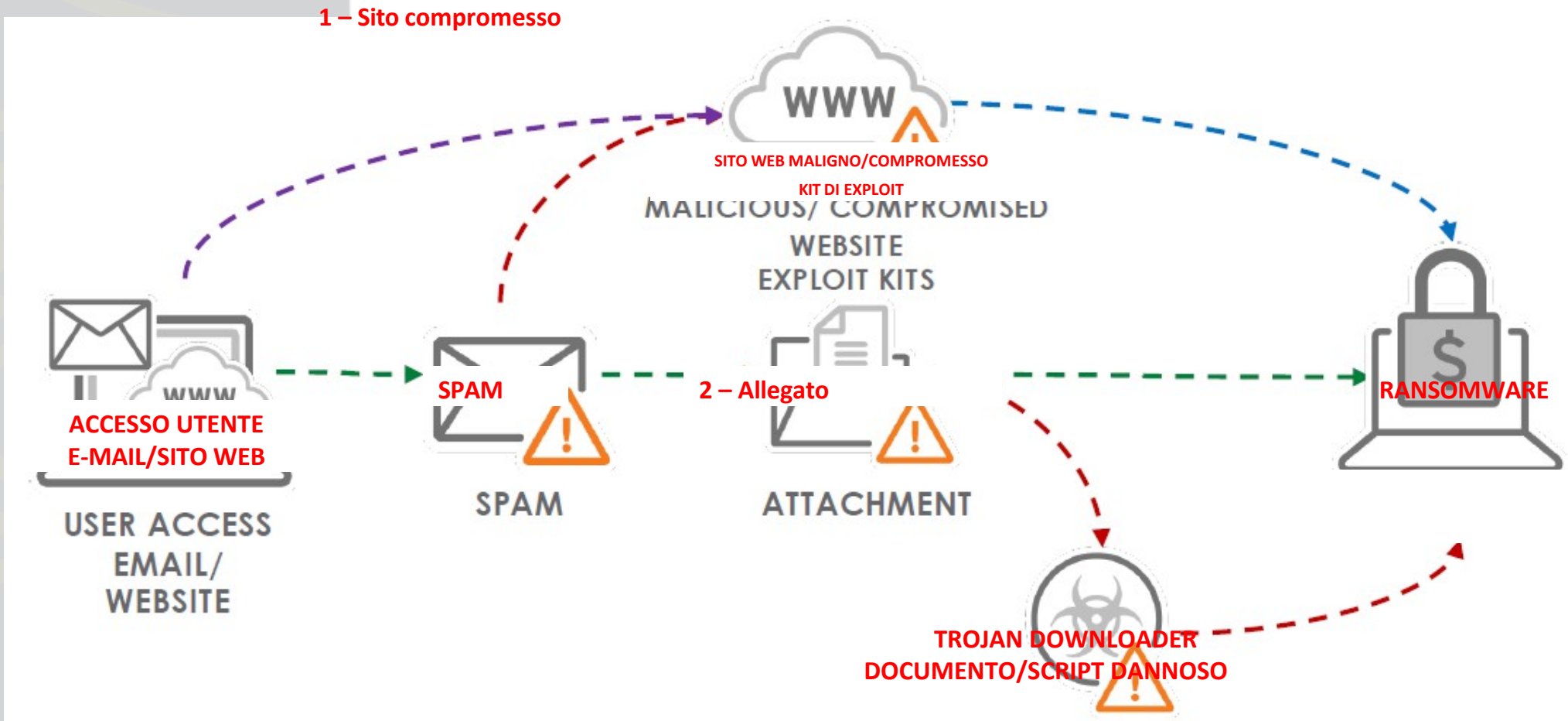
INTRODUZIONE – Blocco schermo



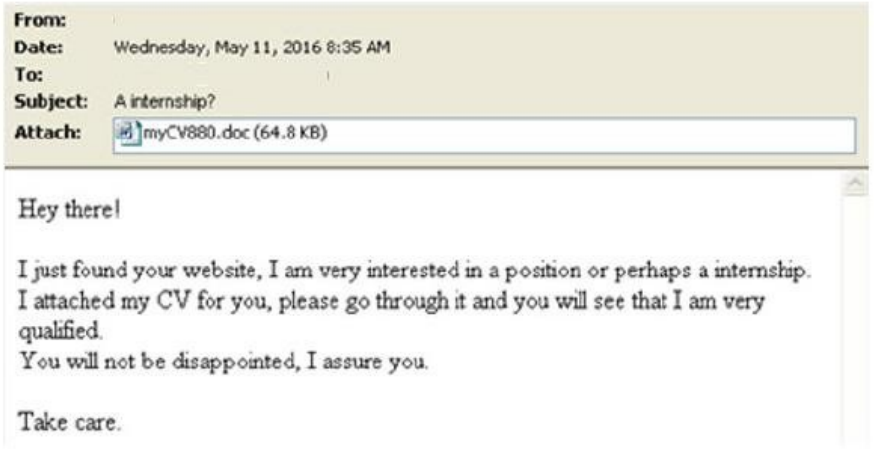
INTRO – Crittografo di file



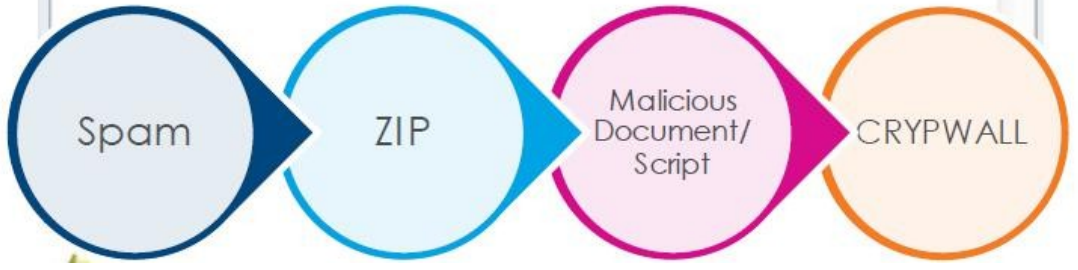
VETTORE DI ARRIVO "COMUNE"



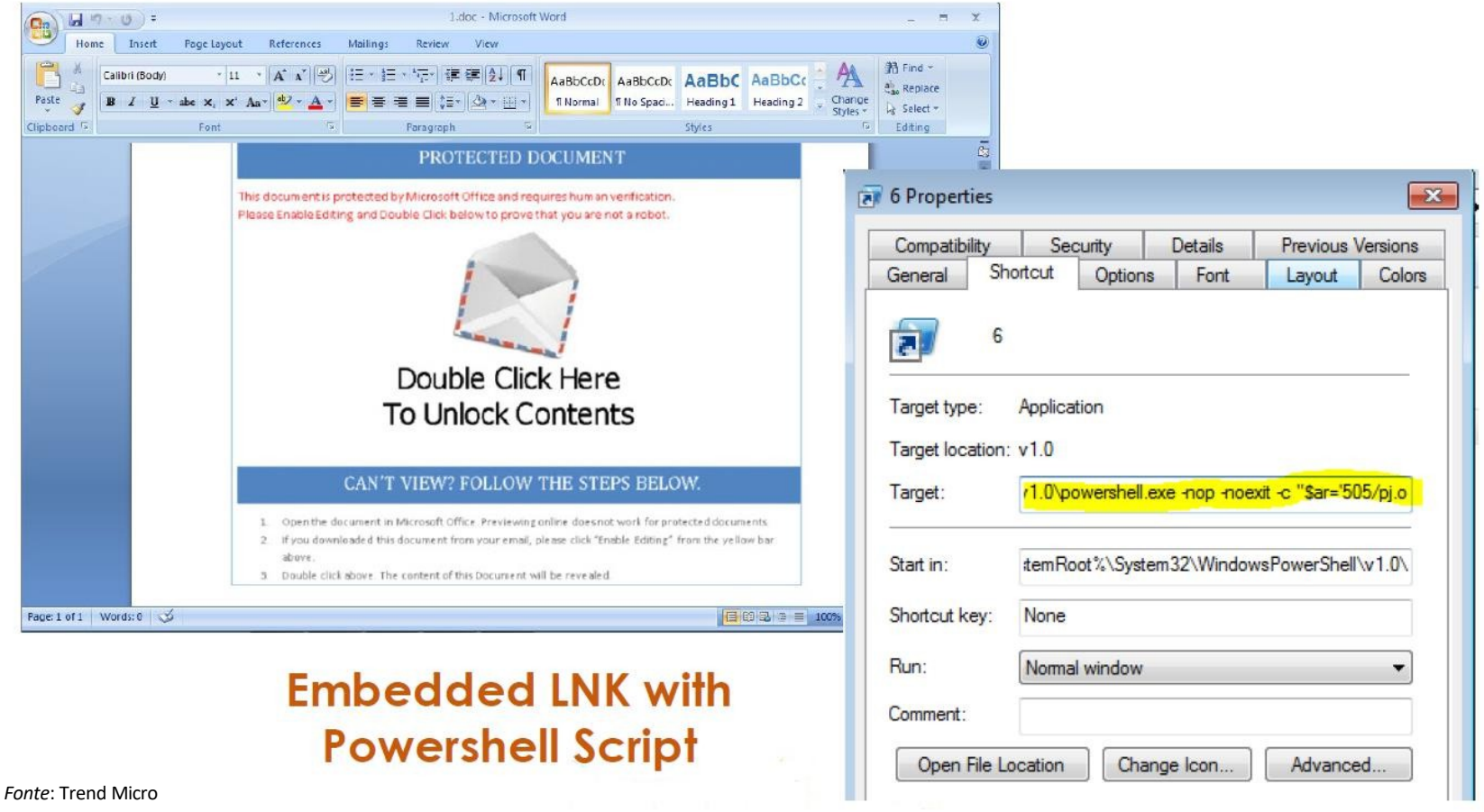
VETTORE DI ARRIVO "COMUNE"



Fonte: Trend Micro



VETTORE DI ARRIVO "COMUNE"



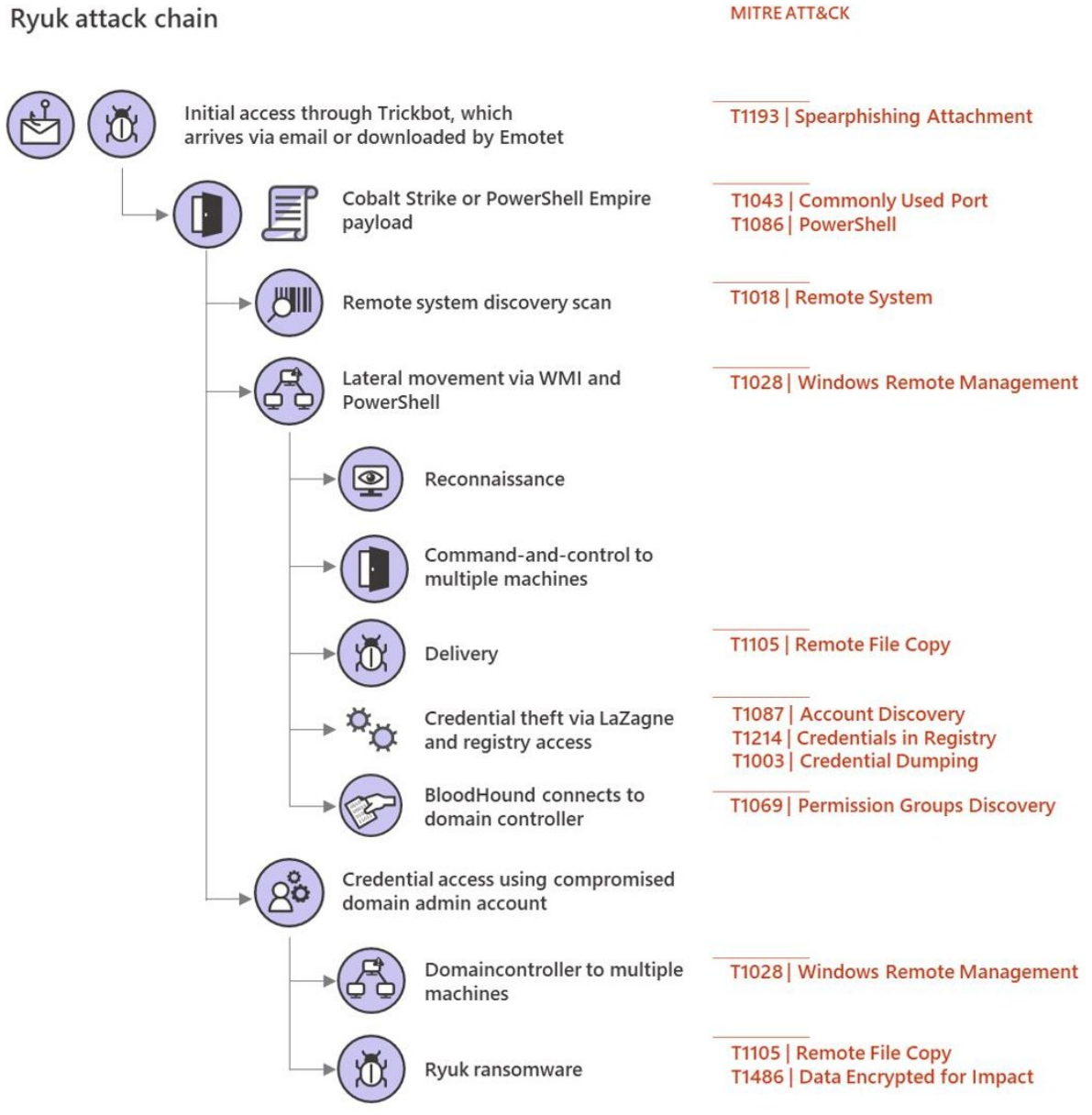
Fonte: Trend Micro

INTRODUZIONE – STORIA

- 1989 – "PC CYBORG"
  - PC bloccato per "licenza scaduta"
  - distribuito alla conferenza dell'OMS sull'AIDS (floppy disk)
  - crittografia dei file su disco
- 2005-2006 – prima ondata di ransomware "moderno" (in Russia)
- 2011 – Ransomware SMS (comporre un numero SMS a tariffa maggiorata)
- 2012 – Ransomware "Screen Locker" falso basato sulla polizia
- 2013 – Cryptolocker (crittografia avanzata, utilizzo di TOR)
- 2014 – "Frenesia" dei file cryptor: CryptoWall, CTB-Locker, Locky, TeslaCrypt …
- 2017 – WannaCry (con funzionalità "worm")
- 2018 – NotPetya (cancellatore)
  - ha colpito la compagnia marittima danese "Maersk" (10 giorni di fermo!)
- 2019 – Maze (doppia estorsione)
- 2021 – Tripla estorsione (con l'aggiunta della minaccia DDOS)

NUOVE TENDENZE

- **Ransomware gestito da esseri umani**
  - vettori di infezione personalizzati (ricognizione)
  - Individuazione di obiettivi (di alto valore)
  - Elevazione dei privilegi – Movimento laterale
  - TTP simile ad APT



TENDENZE "COMUNI" DELL'

- **Broker di accesso iniziale (IAB)**
  - Trovare un modo per ottenere un punto d'appoggio nelle reti di organizzazioni "casuali"
  - Vendere l'accesso alla rete (di solito tramite dark web, 500-10.000$)
- **RaaS** – Ransomware As a Service
  - È possibile introdurre malware
  - È possibile acquistare una piattaforma per l'utilizzo remoto del malware
    - Configurazione: riscatto, nota di pagamento, vittime...
  - la piattaforma potrebbe già fornire l'accesso alle vittime
    - ad es. Emotet (downloader generico)

Argomento 2 - Minacce

Settore marittimo

- Fonti identificate
- Casi d'uso

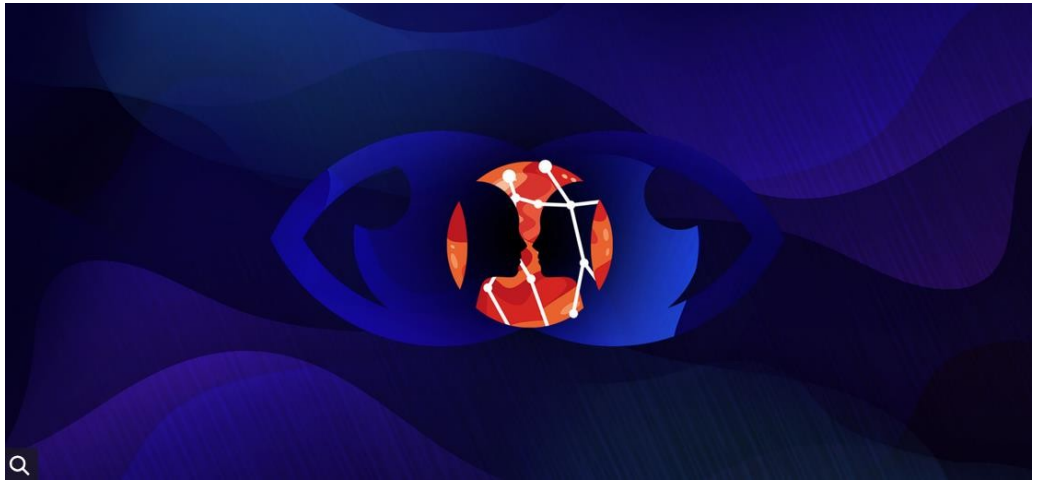
PORTI E OPERATORI MARITTIMI

Fonti di intelligence (aziende)

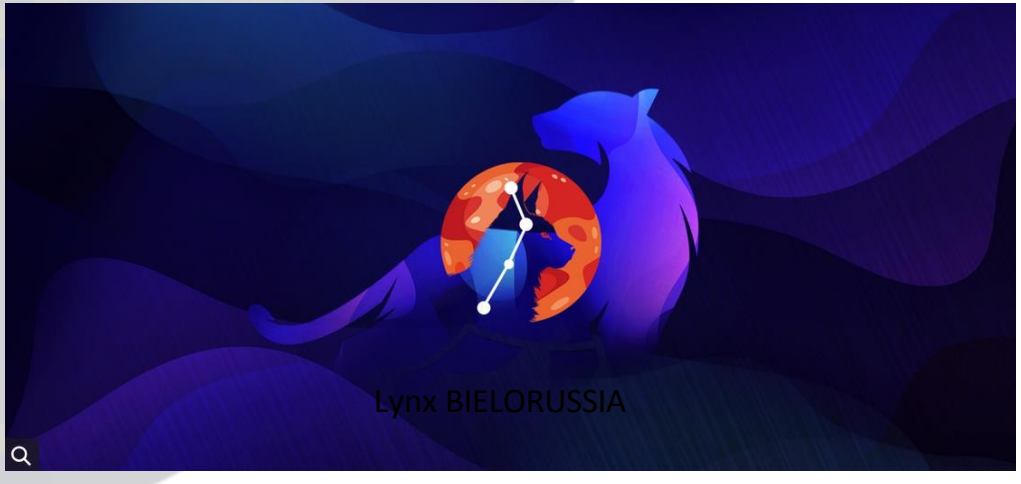
Gruppi di attori minacciosi monitorati da Palo Alto Networks Unit 42

Piattaforma RaaS: https://unit42.paloaltonetworks.com/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

Draco PAKISTAN



Gemini INDIA



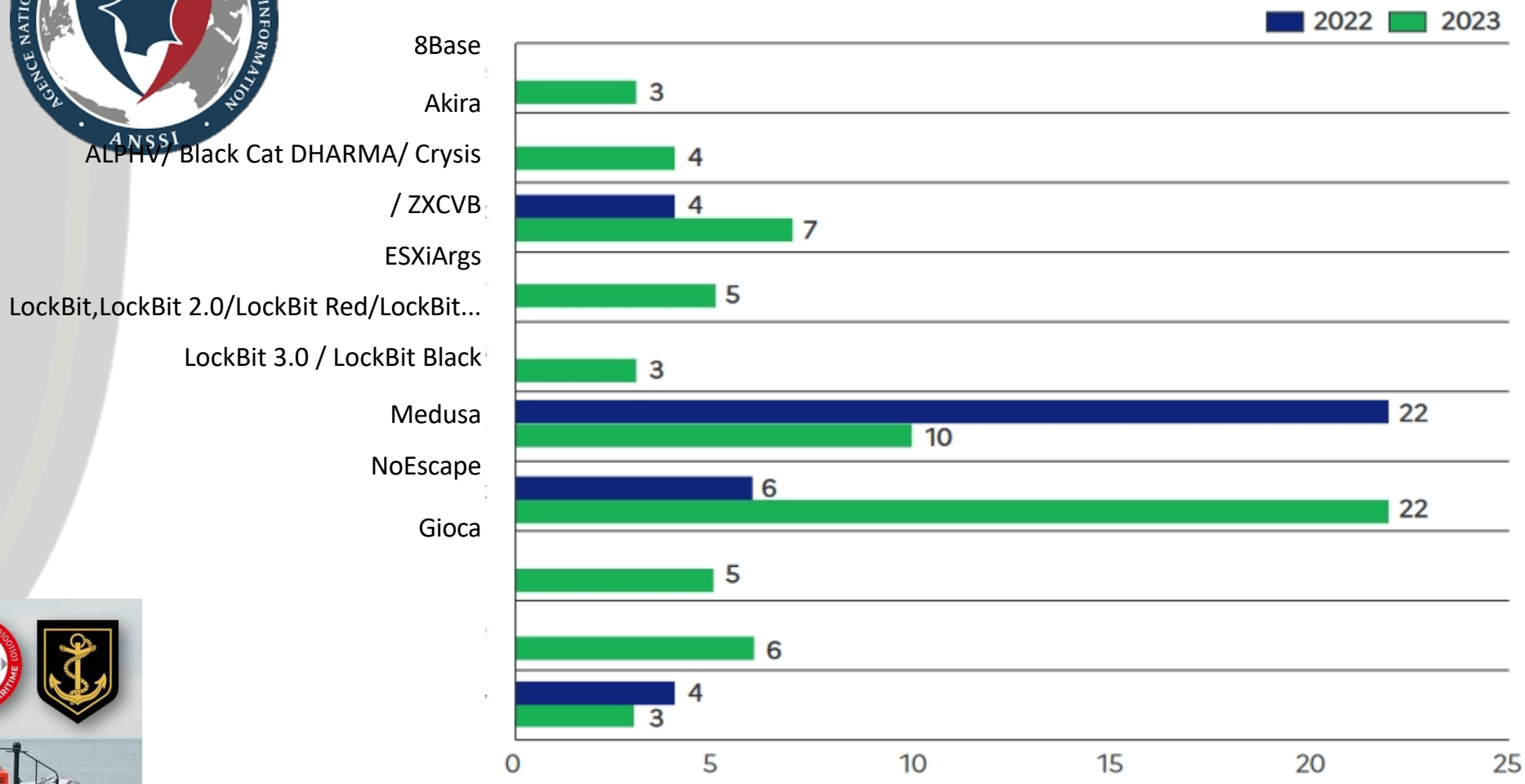
Lynx BIELORUSSIA

Problema: sede legale degli attori malintenzionati

RaaS: RANSOM As a Service

Fonti di intelligence (agenzie nazionali)

Confronto tra i principali ceppi di ransomware utilizzati negli incidenti segnalati all'ANSSI nel 2022 e nel 2023



RANSOMWARE nel settore marittimo

- **Tendenze**
  - crescente digitalizzazione
  - Passaggio naturale dalle operazioni condotte localmente a quelle remote
  - Impulso remoto dovuto al COVID-19
- **Attacchi ransomware: aspetti peculiari?**
  - stessi aggressori, stesse TTP
  - obiettivo interessante: supporta il 90% del commercio mondiale!
    - potenziale obiettivo bellico
  - ecosistemi IT complessi e integrati (anche con tecnologia operativa - OT)
    - Rischi aumentati nella catena di approvvigionamento: il "punto di ingresso" potrebbe essere un'azienda partner!
    - molti vettori di attacco disponibili per gli aggressori
  - La spedizione è un punto chiave nella catena logistica di approvvigionamento
    - possono essere utilizzati come tappa intermedia verso altri obiettivi (attacco alla catena di approvvigionamento)

RANSOMWARE nel settore marittimo

Ransomware attack on US maritime facility confirmed

Story By: Rob O'Dwyer | January 8, 2020 | Blockchain and Cyber Security

The US Coast Guard (USCG) has issued a marine safety bulletin confirming a recent ransomware attack at a Maritime Transportation Security Act (MTSA) regulated facility, which locked users out of access to critical files and saw the infection move beyond the local facility and into wider corporate networks.

Ransomware Attack on Swire Pacific Offshore Breaches Personnel Data

Swire Pacific Offshore notified authorites of a cyber attack on its systems (Swire file photo)

PUBLISHED NOV 26, 2021 12:05 PM BY **THE MARITIME EXECUTIVE**

Image: Dimitry Anikin

With today's news that French shipping giant CMA CGM has been hit by a ransomware attack, this now means that all of the four biggest maritime shipping companies in the world have been hit by cyber-attacks in the past four years, since 2017.

Previous incidents included:

1. APM-Maersk - taken down for weeks by the NotPetya ransomware/wiper in 2017.
2. Mediterranean Shipping Company - hit in April 2020 by an unnamed malware strain that brought down its data center for days.
3. COSCO - brought down for weeks by ransomware in July 2018.

Soluzioni

- **Implementa semplicemente le migliori pratiche di sicurezza IT**
- **Principali argomenti di mitigazione**
  - **autenticazione forte** (in particolare per portali Internet e VPN)
    - o **approccio zero-trust**, in un approccio senza perimetro
  - **principio del privilegio minimo** (in particolare con i privilegi utente)
  - **separazione di sistema/rete (fisica/logica)**
  - Procedure **di continuità operativa**
    - **backup** (caldo e freddo)
  - **Valutazione** continua **delle vulnerabilità** e **applicazione delle patch**
  - Monitoraggio **del centro operativo di sicurezza**
  - **Rafforzamento (**protocolli di rete, firewall host, configurazione software, sicurezza del sistema operativo, ecc.)

Caso d'uso – AIS / GNSS

Principale preoccupazione per le agenzie marittime – Spoofing AIS / GNSS / Jamming

Le posizioni AIS di due navi della NATO sono state spoofate vicino alla base navale russa nel Mar Nero.

EUROPEAN COAST GUARD FUNCTIONS FORUM

June 2021 – ECGFF cybersecurity working group Note on cybersecurity incident

N° 1/2021

UNCLASS – For Official Use Only

The AIS positions of two NATO ships were spoofed near the Russian naval base in the Black Sea.

The analysis of the present note shows an example of spoofed AIS information that could represent a threat on activities conducted by vessels conducting maritime operations. It confirms the leaks of AIS used by vessels operated by public administration an raises the need to develop our work initiated within this group.

Tracking data from two NATO warships were falsified off the coast of a Russian-controlled naval base in the Black Sea while the ships were at harbour visit 180 miles away.

The British Royal Navy's HMS Defender, a Daring Type-45-class destroyer, and the Royal Netherlands Navy's HNLMS Evertsen, a De Zeven Provincien-class frigate, at Odessa, Ukraine, on 18 June. The group was marked by Russian warships during their transit through the Black Sea, as evidenced by U.S. Navy photos dated June 17.

According to the AIS, the ships left Odessa just before midnight on 18 June. Analysis of the data shows that they would have sailed directly to Sevastopol, approaching within 2Nq of the port that houses the Russian Black Sea fleet.

The two warships, however, did never leave Odessa. The webcam streams (see USNI slide) show that they have not left Odessa, however. The webcams are streamed live on YouTube by Odessa Online. Screenshots archived by third-party weather sites like Windy.com show the two warships present in Odessa during the night.

The positioning of two NATO warships at the entrance to a major Russian naval base is widely perceived as provocative action.

Although the reasons for spoofing are not clear, this decision raises questions about the effectiveness of open source intelligence data, such as AIS, which is becoming increasingly common in the defense and by journalists.

There is irrefutable evidence that the AIS tracks were spoofed by a third party.

NATO officials did not immediately respond to requests for comment and the traks identified on AIS providers (MarineTraffic.com in the present case) were confirmed as false by the Dutch news site Marineschepen.nl.

AIS positions were probably sent to MarineTraffic.com via the Chornomorsk ground station near Odessa operated under Russian control. Other AIS operators have also reported the false

Fonti:

- EU CERT & M-CERT
- Stati membri
- Aziende private

Minacce alle infrastrutture critiche

Malware:
Malware la cui diffusione è incontrollabile

Script kiddy (adolescente ozioso o, più in generale, attaccante solitario e opportunista):

- Mezzi molto modesti (meno di 100 €)
- Motivazione: gioco d'azzardo (e possibilmente profitto)

Attacco opportunistico Dipendente malintenzionato (rancore/avidità):

- Mezzi modesti (< 1.000 €)
- Motivazione principale: danneggiare il proprio datore di lavoro, evitando vittime
- Discrezione quando possibile
- Facile accesso a tutti gli elementi della nave

Gruppo terroristico:

- Mezzi moderati (da 10.000 € a 50.000 €)
- Ricerca di vittime umane, danni materiali, elevata visibilità mediatica

Attività criminale:

- Risorse elevate (circa un milione di euro)
- Obiettivo di redditività
- Bassi vincoli morali
- Ricerca della discrezione

Stato:

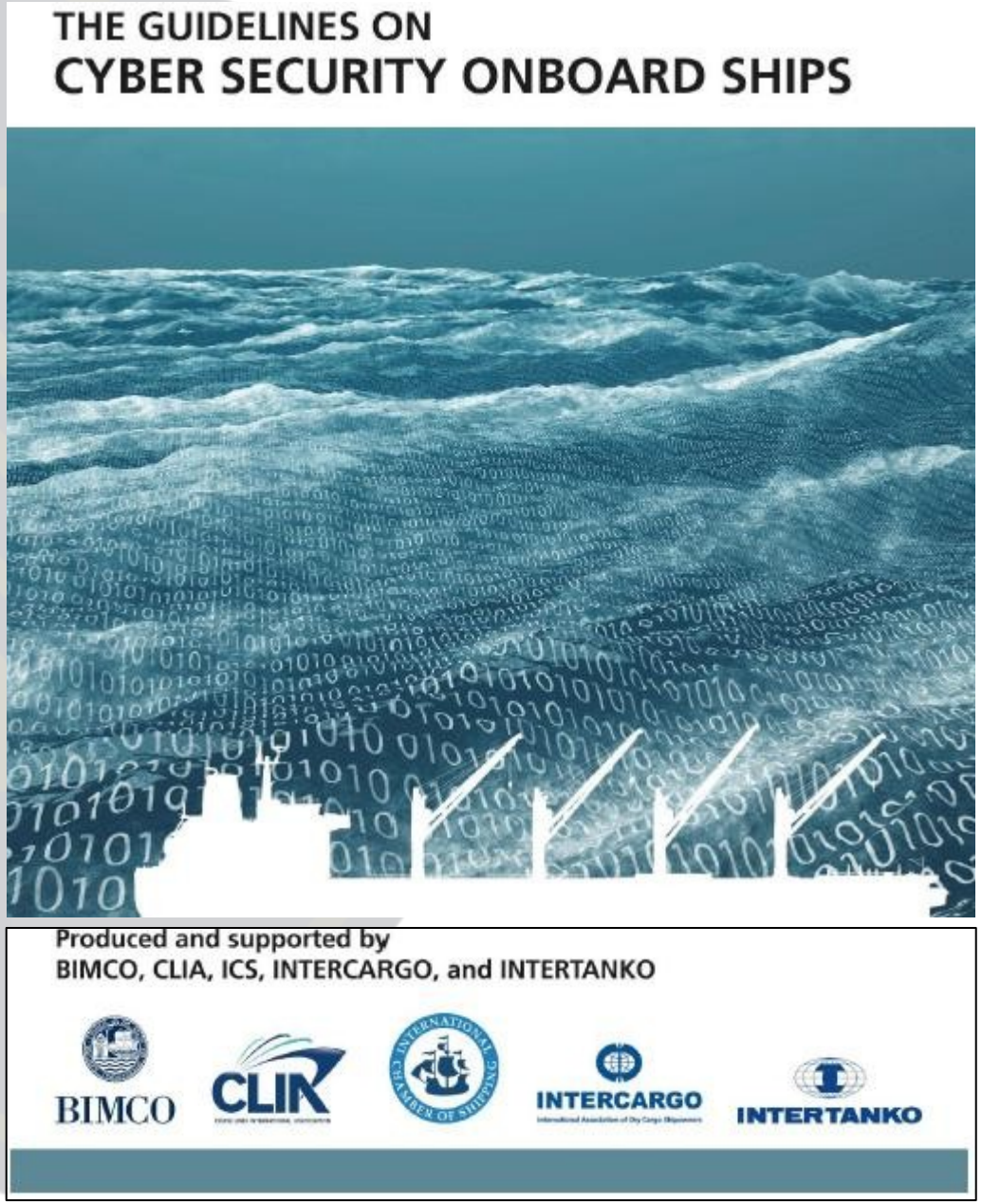
- Mezzi quasi illimitati
- Obiettivi di ogni tipo –
- Assenza di vincoli morali
- Discrezione necessaria

Minacce ai sistemi

Spoofing delle navi – Viene trasmesso un messaggio AIS che fornisce dettagli su una nave inesistente. Tra gli scenari in cui ciò potrebbe essere utilizzato vi è lo spoofing di una nave di una nazione nelle acque territoriali di una nazione ostile, inducendo quest'ultima ad adottare contromisure. In alternativa, è possibile trasmettere più versioni dei dettagli di una nave reale, collocandola in molte posizioni diverse contemporaneamente per nasconderne la vera posizione (ad esempio, pesca illegale).
Spoofing degli aiuti alla navigazione – Vengono trasmessi falsi aiuti alla navigazione, come boe che segnalano banchi di sabbia nascosti, al fine di costringere una nave a cambiare rotta. Ciò potrebbe essere fatto per costringere una nave a entrare in una regione dove può essere dirottata.
Spoofing delle collisioni – La prevenzione delle collisioni è uno degli usi principali dell'AIS. Fornendo dettagli falsificati su una nave in rotta di collisione, un aggressore può costringere una nave a cambiare rotta per evitare la collisione prevista. Ciò potrebbe, ad esempio, essere utilizzato per guidare la nave verso una collisione reale

Spoofing AIS-SART – La ricerca e il soccorso sono un altro degli usi principali dell'AIS. Questo attacco genera un segnale transponder SAR-T falsificato, che fornisce dettagli su una situazione di emergenza. Poiché le navi sono legalmente obbligate a prestare soccorso, lo spoofing SART può essere utilizzato come esca per attirare le navi in un luogo dove possono essere attaccate.
Spoofing delle previsioni meteorologiche – L'AIS può essere utilizzato per trasmettere informazioni sulle condizioni meteorologiche prevalenti tra le imbarcazioni. Una previsione falsa, in particolare una che prevede condizioni favorevoli quando è in arrivo una tempesta, potrebbe essere utilizzata per mettere in difficoltà le imbarcazioni.
Dirottamento AIS – È anche possibile sovrascrivere i segnali inviati dalle imbarcazioni, trasmettendo un segnale di potenza superiore alla stessa ora e frequenza. L'aggressore può quindi modificare alcuni dettagli del messaggio originale, ad esempio per suggerire che l'imbarcazione trasporta un carico nucleare in una zona in cui tali carichi sono illegali.

Responsabilità condivise – Grande comunità – Iniziative limitate



- Paesi di bandiera
- Armatori
- Società di gestione navale
- Porti
- Collegamenti con l'economia (regionale, trasporti)
- Agenti marittimi
- Compagnie assicurative
- Agenzie di certificazione
- Costruttori navali
- Operatori COMMS
- Fornitori di sistemi
- Fornitori di servizi di sicurezza

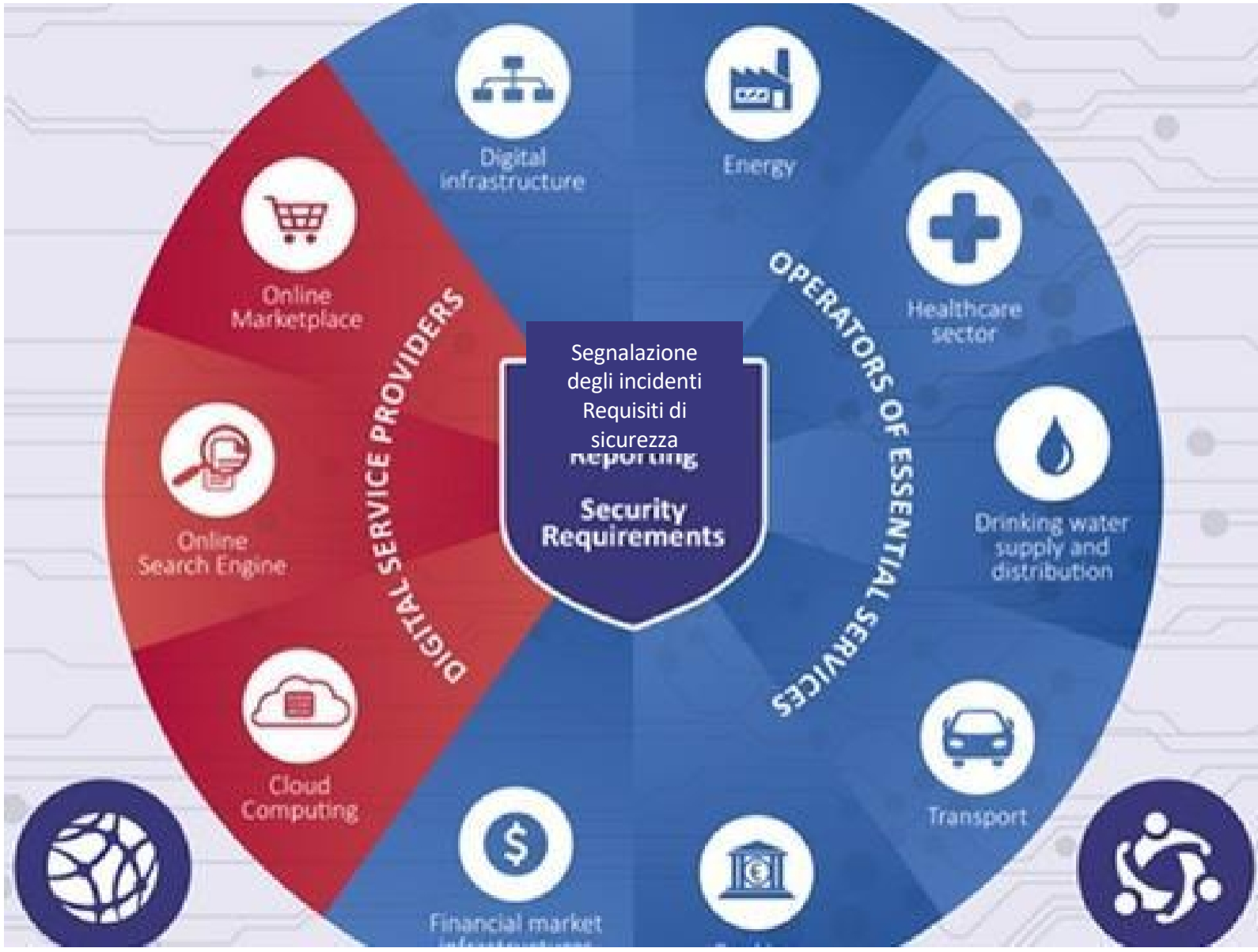
Condizioni d'uso

I consigli e le informazioni forniti nelle Linee guida sulla sicurezza informatica a bordo delle navi sono da intendersi esclusivamente come indicazioni **da utilizzare a proprio rischio**. *Gli autori, i loro membri o dipendenti di qualsiasi persona, azienda, società o organizzazione non forniscono alcuna garanzia o dichiarazione, né accettano alcun obbligo di diligenza o responsabilità per l'accuratezza delle informazioni o dei consigli forniti nelle Linee guida o per eventuali omissioni dalle Linee guida o per qualsiasi conseguenza derivante direttamente o indirettamente dal rispetto, dall'adozione o dall'affidamento alle indicazioni contenute nelle Linee guida, anche se causata da una mancata diligenza da parte di una delle parti sopra menzionate.*

Minacce / Impatti

Specificità marittime

- Comunità
- Somiglianza Marittimo / Digitale
- Dipendenza dal GNSS
- Ambiente di condivisione delle informazioni



Rischi delle infrastrutture critiche marittime

Argomento 3 – L'importanza dei dati

- Regolamento UE
- Dati classificati / Dati sensibili
- Trattamento dei dati

Analogie tra settore marittimo e digitale

	Marittimo	Digitale
Dimensione	80% della terra	Illimitata
Legale	Regolamentazione internazionale debole UNCLOS	Regolamentazione internazionale limitata GDPR
Economico	90 % del commercio internazionale Stabile	50% delle transazioni internazionali Crescita permanente
Ambiente	Imprevedibile: condizioni del mare, vento, salsedine, pericoli fisici	Imprevedibile: virtualità,
Minaccia	Attività e operazioni illegali, Pirateria, terrorismo	Portata globale delle minacce informatiche Attività illegali incentrate sui beni
Focus	Condivisione delle informazioni (IFC) Capacità di azione = Stati	Prevenire e condividere informazioni Coordinare l'azione

Marittimo e digitale: somiglianze

Mondi simili (stesse valutazioni – stesse conseguenze ???)

800 - 1260 T di rifiuti

In 10 secondi...

225.000 GB di dati

- 500.000 post su Facebook,
- 57.000 tweet,
- 46.000 ricerche su Google
- 2 milioni di messaggi su WhatsApp

Piano di comunicazione

Adattato agli operatori

Infrastrutture critiche

Direttiva ECI 2008

Rischio globale (sicurezza, spionaggio, dati, attività)

Un attacco potrebbe mettere in pericolo la sicurezza di un paese

Monitoraggio settoriale

- Analisi dei rischi
- Vulnerabilità
- Direttive

Coordinamento intersettoriale

Operatore di servizi essenziali

Direttiva NIS 2015

Rischio di spionaggio, dati, attività

Un attacco potrebbe mettere in pericolo l'attività economica

Valutazione del rischio settoriale

Avvertenze

Informazioni intersettoriali

Utente comune del dominio Maritim

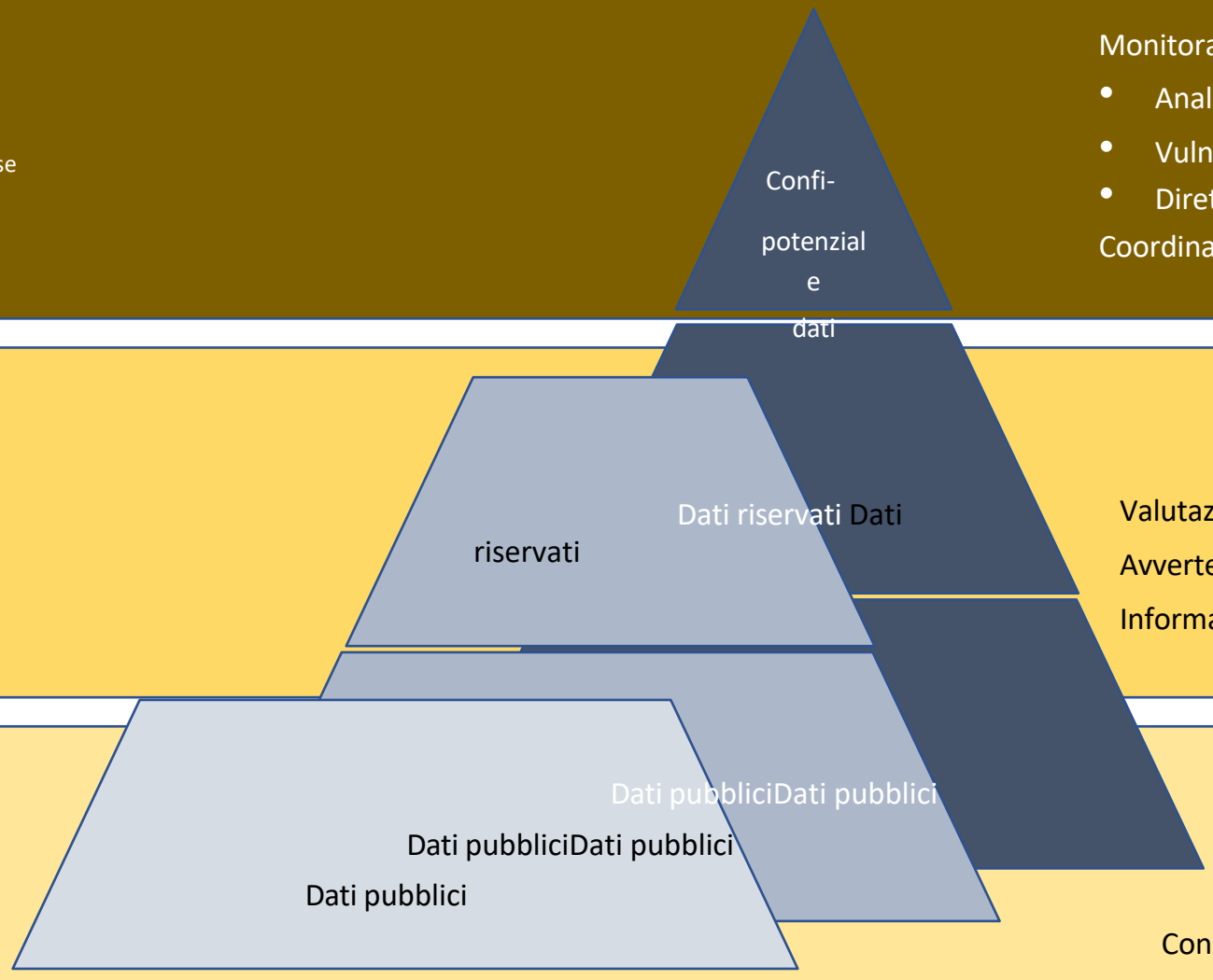
GDPR 2018

Rischio per i dati

Un attacco potrebbe rappresentare una minaccia

Consapevolezza settoriale

- Raccomandazioni
- Prevenzione



QUADRO EUROPEO DELLE COMPETENZE IN MATERIA DI SICUREZZA INFORMATICA: PROFILI PROFESSIONALI

Responsabile della sicurezza informatica CISO
Chief Information Security Officer (CISO)

Responsabile della gestione degli incidenti informatici
Responder

Responsabile legale, politico e della conformità informatica
Cyber Legal, Policy and Compliance Officer

Specialista in intelligence sulle minacce informatiche
Intelligence Specialist

Architetto della sicurezza informatica
Cybersecurity Architect

Revisore della sicurezza informatica
Cybersecurity Auditor

Formatore in sicurezza informatica
Cybersecurity Educator

Implementatore di sicurezza informatica
Cybersecurity Implementer

Ricercatore in sicurezza informatica
Cybersecurity Researcher

Responsabile della gestione dei rischi di sicurezza informatica
Cybersecurity Risk Manager

Investigatore forense digitale
Digital Forensics Investigator

Penetration tester
Penetration Tester

European Cybersecurity Skills Framework (ECSF)

https://digital-skills-jobs.europa.eu/en/cyber-skills-academy-knowledge-and-training

https://cybersecpro-project.eu/

Caso d'uso

Infrastrutture critiche

Porti marittimi

PORTI E OPERATORI MARITTIMI

Qual è l'obiettivo degli aggressori?

Garanzia delle informazioni

Riservatezza	Le informazioni non vengono divulgate alle entità del sistema (utenti, processi, dispositivi) a meno che non siano state autorizzate ad accedere alle informazioni	CRYPTO
Integrità	La proprietà per cui un'entità non è stata modificata in modo non autorizzato.	DIRITTO DI CONTROLLO DELL'ACCESSO
Disponibilità	Essere accessibile e utilizzabile su richiesta da parte di un ente autorizzato.	BCP/BRP
Non ripudiabilità	informazioni.	D.SIGN
Autenticazione		PASSWORD

Aree funzionali

(Tassonomia CYBERSECPRO)

Privacy e protezione dei dati

Gestione dei rischi di sicurezza informatica

Gestione delle minacce alla sicurezza informatica gestione

Incidenti informatici Risposta

Aspetto umano della sicurezza informatica

Test di penetrazione

Sicurezza delle reti e delle comunicazioni

Strumenti e tecnologia

Gestione della sicurezza informatica

Politica, processo e conformità in materia di sicurezza informatica

Quadro marittimo – Legale (Internazionale) RISOLUZIONI IMO

MSC.428(98) (16 giugno 2017) GESTIONE DEI RISCHI INFORMATICI MARITTIMI NEI SISTEMI DI GESTIONE DELLA SICUREZZA:
un sistema di gestione della sicurezza approvato dovrebbe tenere conto della gestione dei rischi informatici

Amministrazioni dovrebbero garantire che i rischi informatici siano siano adeguatamente affrontati in sistemi di gestione della sicurezza
sistemi di gestione della sicurezza 1° gennaio 2021 (Sondaggio ?)

Sistemi particolari da prendere in considerazione:

- Sistemi di ponte
- Sistemi di movimentazione e gestione del carico
- Sistemi di gestione della propulsione e dei macchinari e di controllo della potenza
- Sistemi di controllo degli accessi
- Sistemi di assistenza e gestione dei passeggeri
- Reti pubbliche rivolte ai passeggeri
- Sistemi amministrativi e di assistenza all'equipaggio
- Sistemi di comunicazione

Incident notification requirements
- Specific criteria/thresholds for incident notification

Quadro marittimo – Normativo (UE) - Promemoria

	Riferimento	Utente	Rete	SI	Chi è interessato	Misure preventive	Capacità di difesa	Riconquista (giudiziaria)
C I (Nazioni: dopo il 2013) 	Direttiva 2005/65/CE Normativa nazionale	+++	++	++ +	Porti Cavi Petrolio e gas HAZMAT e i loro sistemi critici	L'UE ha identificato i porti come infrastrutture critiche Porto = area specifica di terra e acqua, con confini definiti dagli Stati membri, contenente opere e attrezzature progettate per facilitare le operazioni di trasporto	Registrazione degli eventi e capacità di analizzare i registri Sonde per i sistemi (Stato o fornitore di servizi qualificato. ANSSI permalink Gestione delle crisi	Conservazione dei registri tecnici per 6 mesi
OES (NIS – 2018 - 22) 	Dir (UE) 2016/1148 del Parlamento europeo e del Consiglio (6/07/16 - misure volte a garantire un livello di sicurezza delle sistemi e reti	0	+++	++	Elenco **OES** fornito dalle Nazioni (porti, compagnie marittime)	Elenco dei servizi essenziali Governance politica e tecnica. Protezione della rete e dei sistemi informativi. Controlli delle decisioni del PM, standard Regole dei fornitori di servizi cloud	Difesa delle reti e dei sistemi informativi; Utilizzo di dispositivi hardware/software o servizi IT certificati per la sicurezza. Segnalazione degli incidenti all'Agenzia per la sicurezza nazionale.	Resilienza aziendale.
Dati (GDPR-2018) 	Regolamento UE 2016/679 - 27/04/16 dati - protezione delle persone fisiche Regolamento	+++	0	++	Soggetto responsabile del trattamento dei dati personali (Agente di trasporto traghetti)	Protezione delle libertà fondamentali nel mondo digitale (cancellazione e portabilità dei dati).	Sistemi e reti protetti a livello tale da impedire la perdita di controllo delle informazioni personali	Possibile ricorso ai CERT in caso di perdita/fuga di dati.

Sistemi di controllo portuale (PCS)

Operazioni portuali

Quali sistemi?

Navigazione e sicurezza

(Collision Avoidance)

Strumenti specifici (merci e passeggeri)

Optimum route planning

Monitoraggio della flotta

Fleet Management

Propulsione ed energia

Produzione

Propulsion/Electric System Monitoring

Operativa

Manutenzione

Preventive Maintenance, Part Replacement Guide

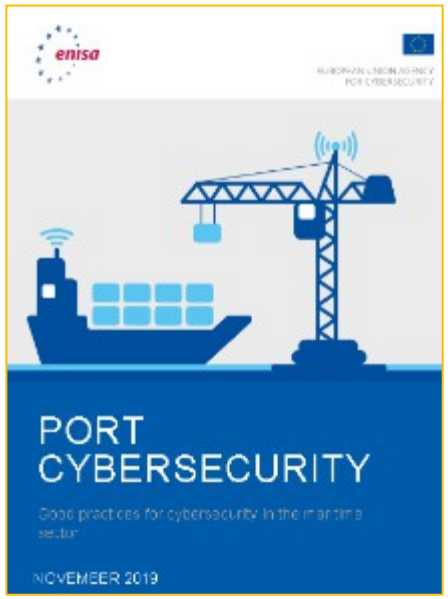
Manutenzione di sicurezza

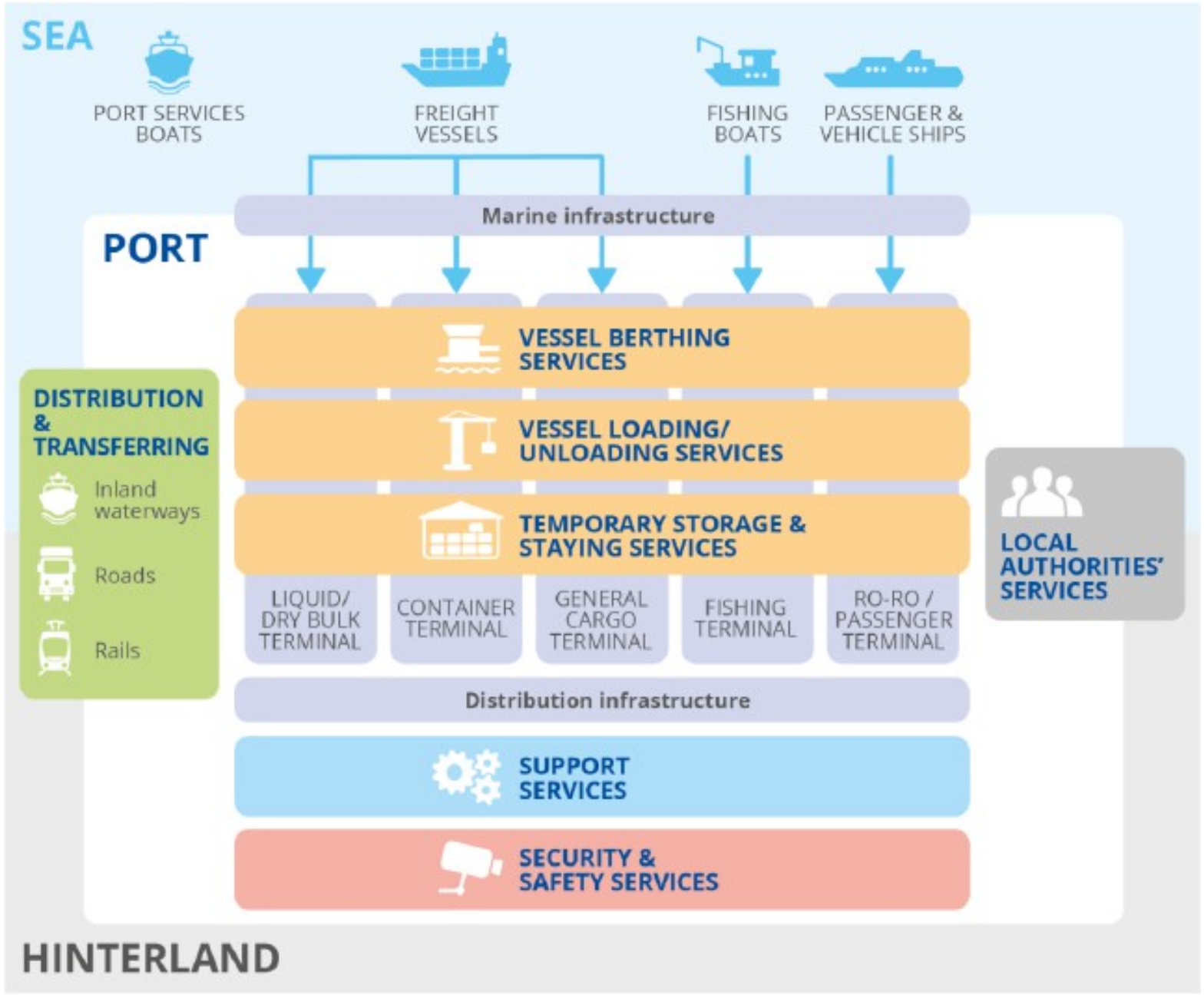
Remote Maintenance, Performance Analysis

Quadro marittimo – Tecnico

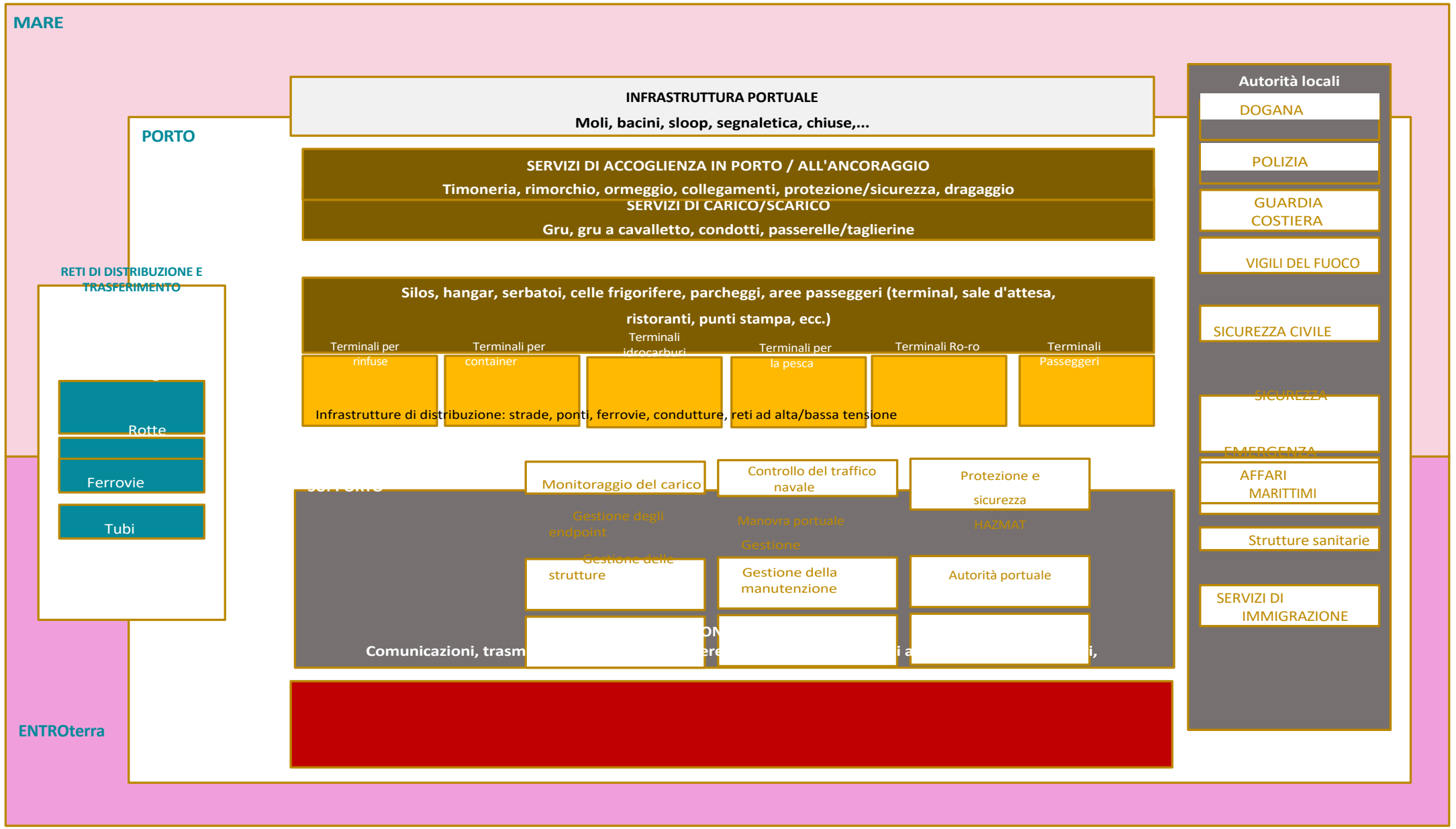
Porto digitalizzato

Cartografia

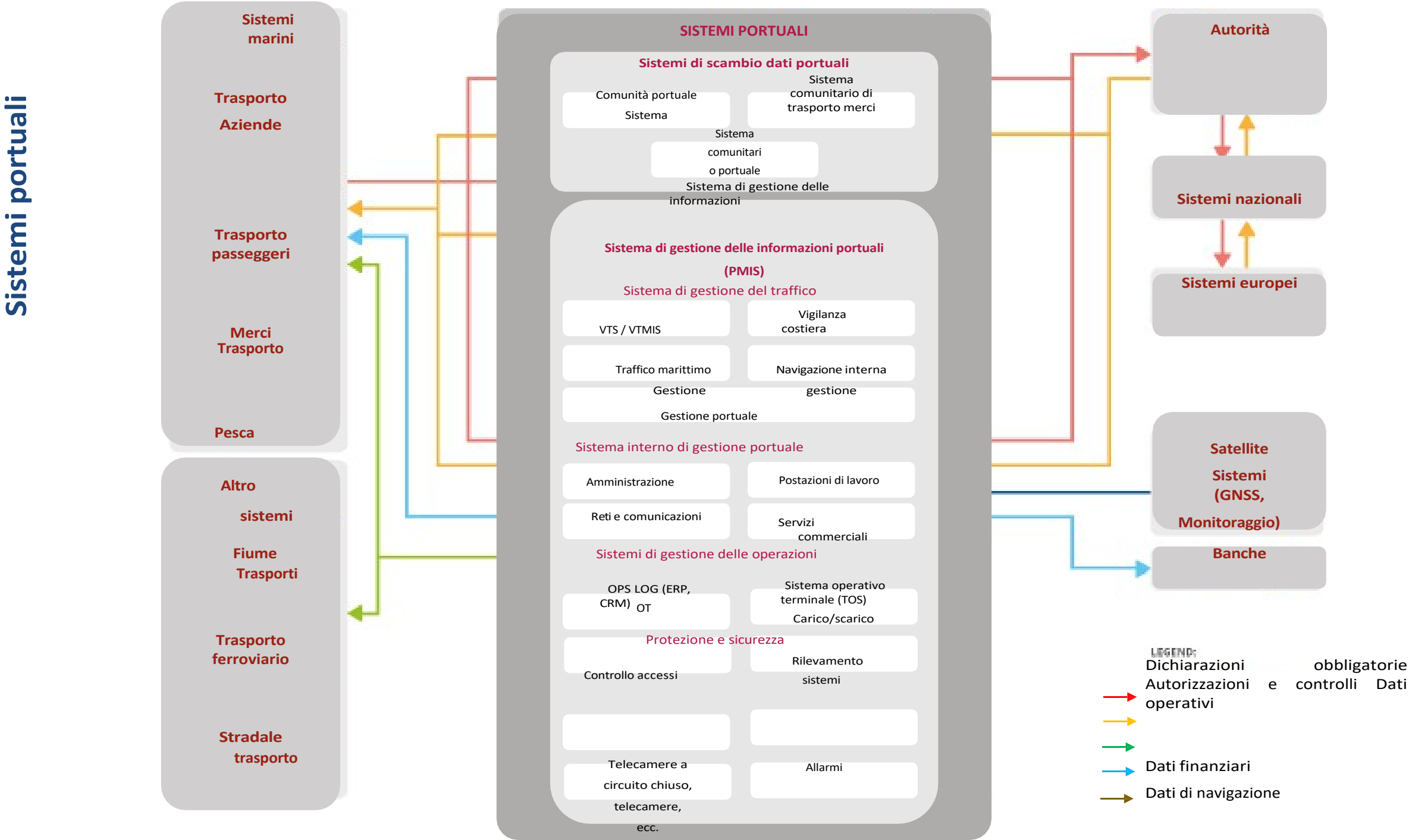




Quadro marittimo – Infrastrutture portuali



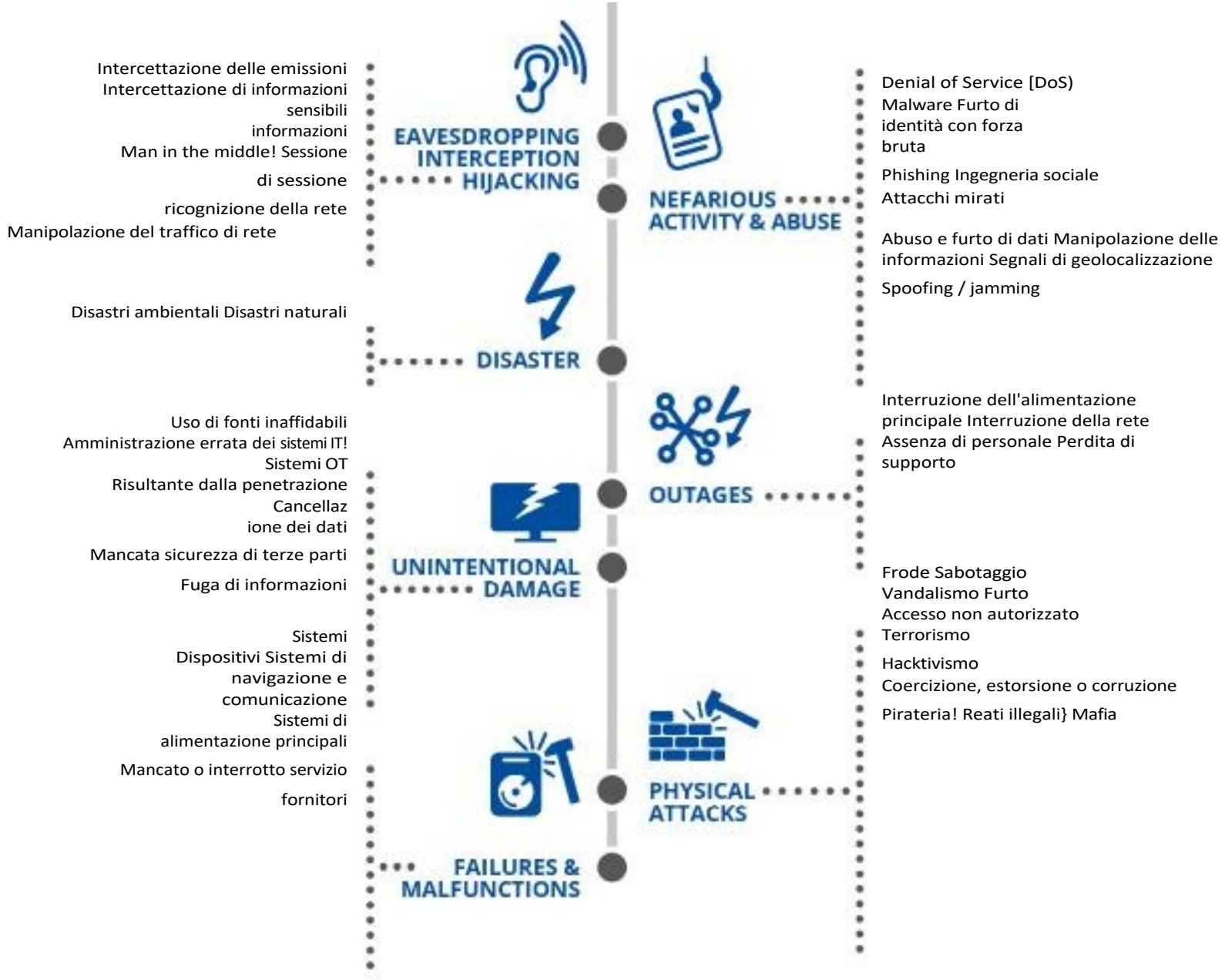
Sistemi portuali



Minacce

Minacce nel settore marittimo

Tassonomia delle minacce

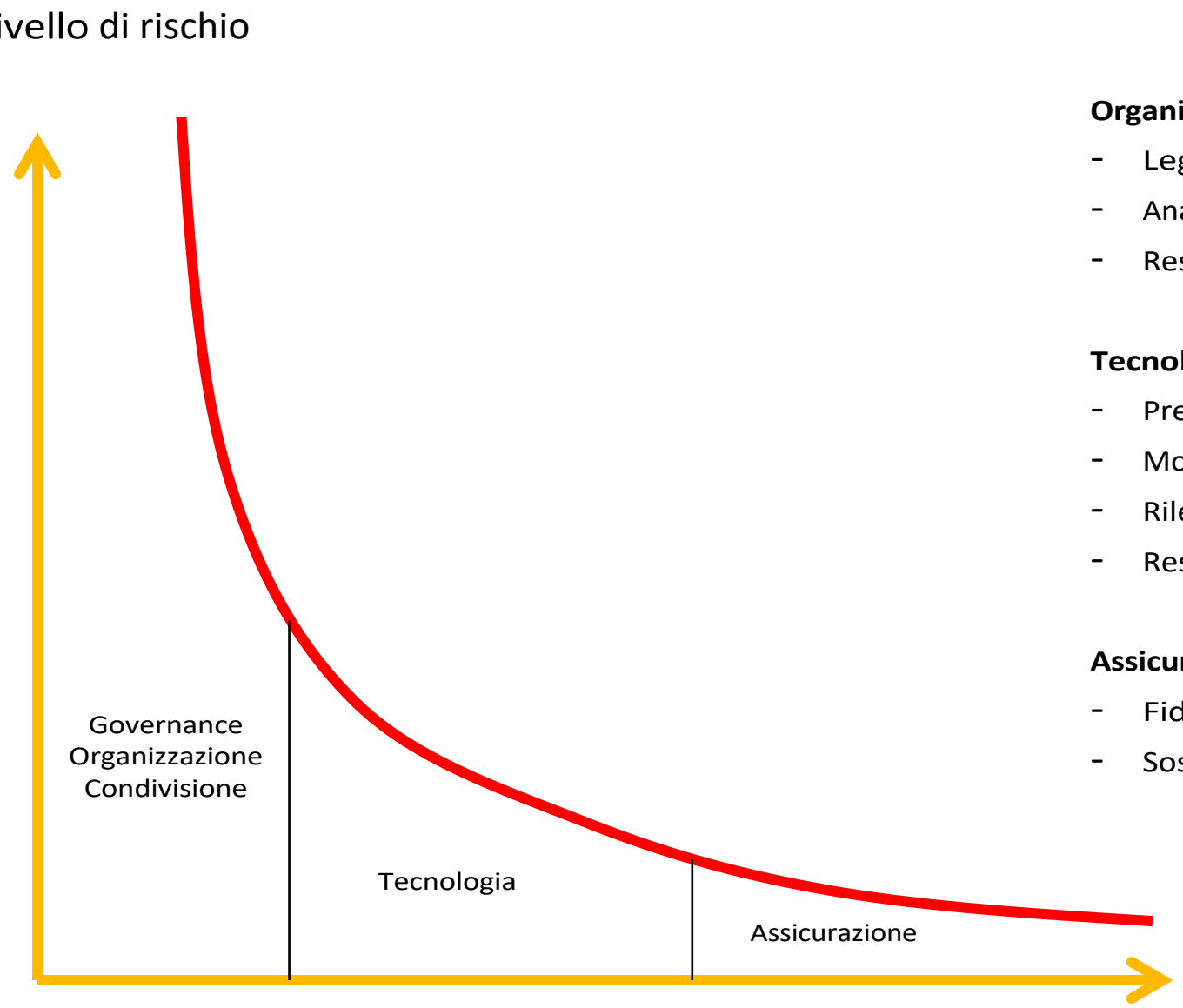


Mitigazione dei rischi per le infrastrutture critiche

Marittimo

PORTI E OPERATORI MARITTIMI

Strategie di riduzione dei rischi per la sicurezza informatica ed effetti



Organizzazione

- Legge / Governance
- Analisi dei rischi
- Resilienza funzionale / settoriale

Tecnologica

- Prevenzione
- Monitoraggio / sorveglianza
- Rilevamento Condivisione di informazioni e incidenti
- Resilienza

Assicurazione

- Fiducia
- Sostegno finanziario / ricostruzione

DOMANDE?

- PAUSA