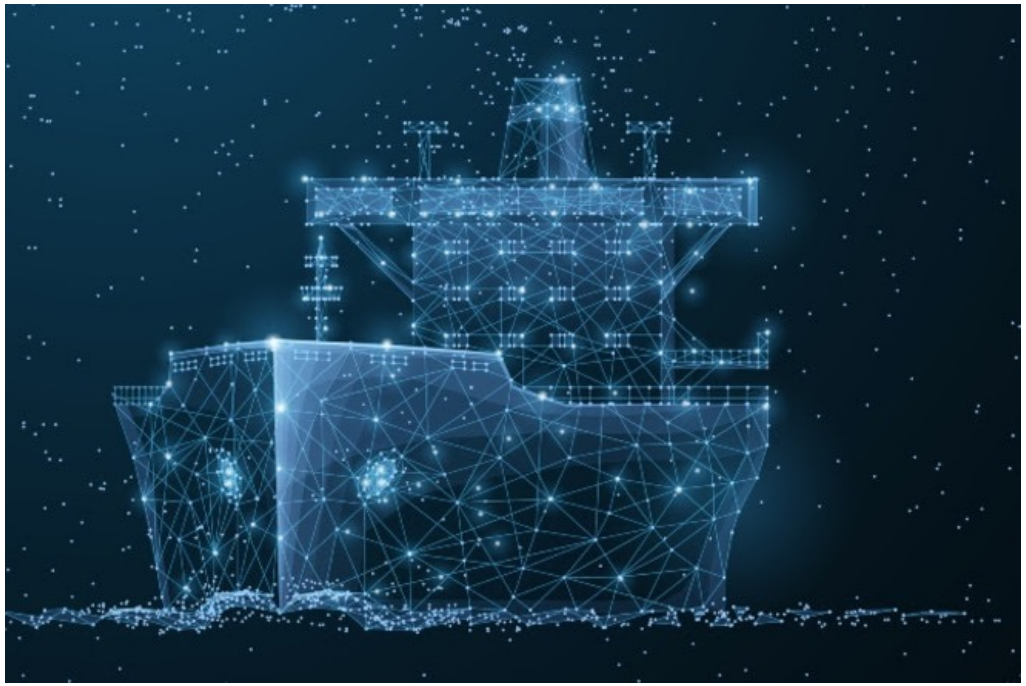
CYBER SECURITY EXPO

La sicurezza informatica non solo quale arma strategica difensiva ma anche come fattore competitivo per aziende ed enti del cluster marittimo-portuale-logistico



La cybersecutity in ambito marittimo

Piacenza, 29/05/2023

Capitano di fregata (CP)
Dany Massimo MUGNAINI

AGENDA

- Premessa
- Il panorama delle minacce
- La normativa di settore e non solo
- Cosa è stato fatto
- Cosa ancora da fare

Per il settore marittimo, la sicurezza informatica non può più essere considerata una preoccupazione emergente poiché gli avvenimenti degli ultimi anni (in particolare dal 2020) hanno dimostrato come essa si sia ormai saldamente affermata come fattore determinante.

Questo perché la digitalizzazione si è fatta profondamente strada in ogni settore, specialmente all'interno delle infrastrutture critiche.

È opportuno tenere sempre ben presente che le minacce informatiche non hanno confini delimitati come avviene per invece per quelle fisiche e ciò le pone in grado di colpire ovunque ogni tipologia di bersaglio, utilizzando tuttavia tecnologia a costi relativamente bassi.

In ambito internazionale, questa consapevolezza sta fortunatamente emergendo.

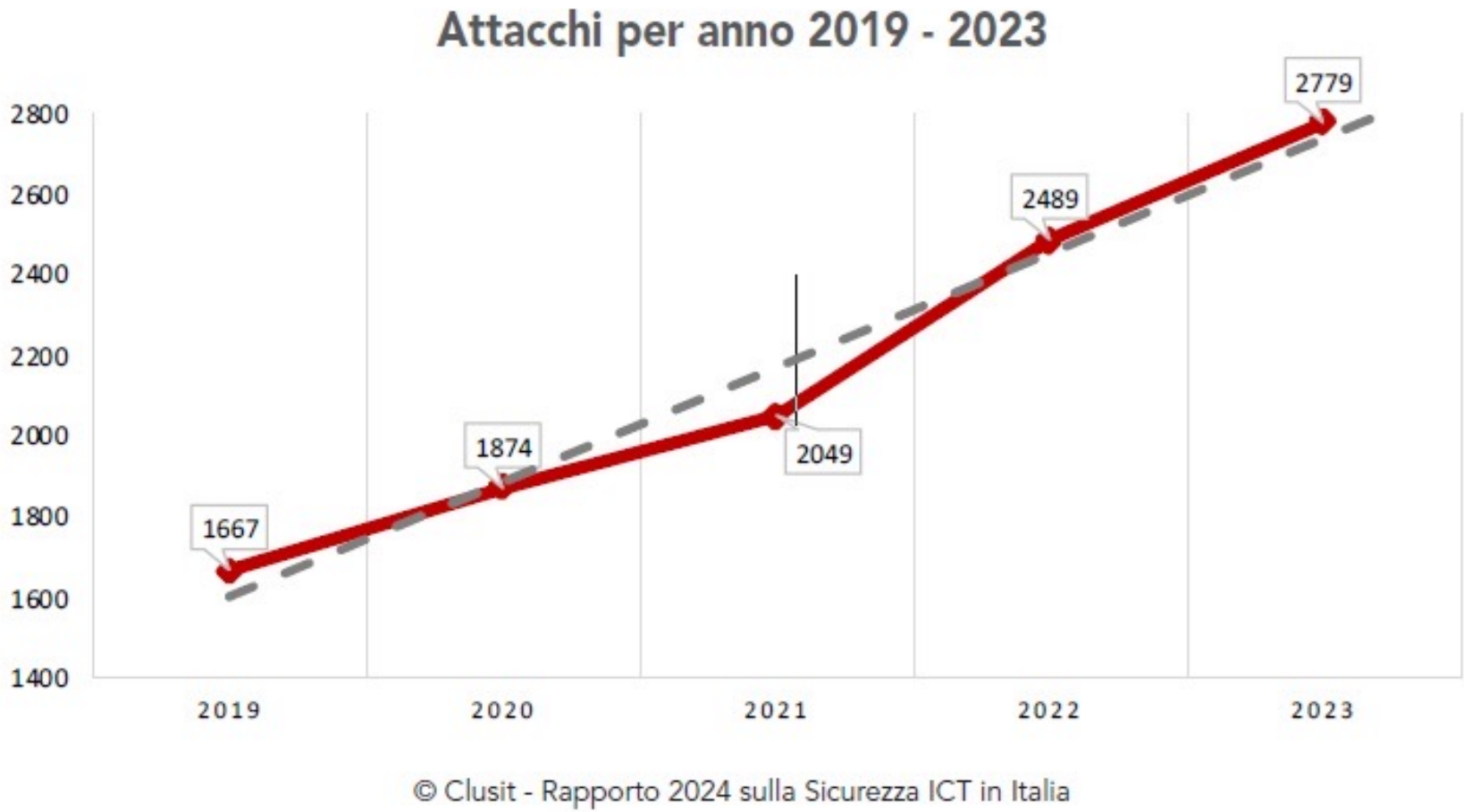
Dal lato delle istituzioni, è un'esigenza che si è sentita da diversi anni e che ha visto l'interessamento della Stessa UE (NIS - NIS2), delle sue agenzie (EMSA, ENISA, DGMOVE, DGMARE, ecc.) ed anche di altri organismi trasversali che nel tempo hanno prodotto linee guida, direttive e normativa, cercando parallelamente di sensibilizzare l'utenza e le parti interessate.

Nel settore privato il processo è stato avviato più lentamente.

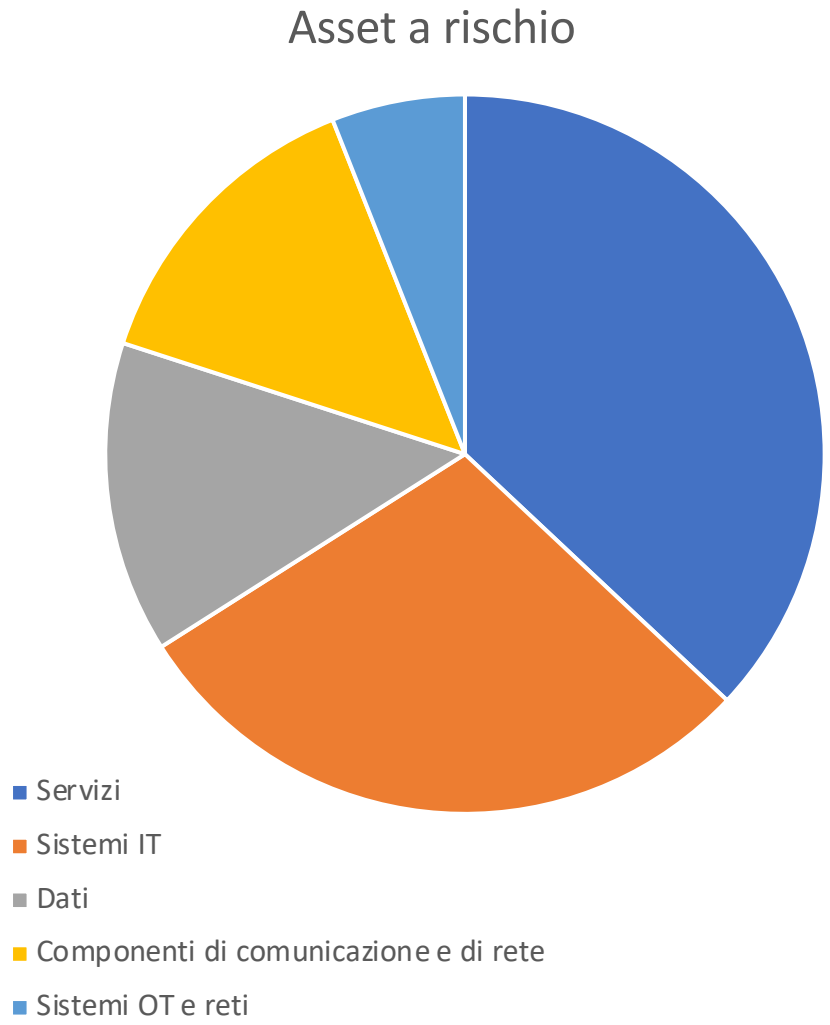
Sono serviti casi eclatanti come quello che ha coinvolto la Soc. MAERSK e perdite di milioni di dollari per far si che la questione assumesse le caratteristiche per essere attenzionata a livello globale.

Per questi motivi sono diventate ormai numerose le conferenze, i *workshop* e le tavole rotonde incentrate sull'argomento della *cybersecurity* in ambito marittimo.

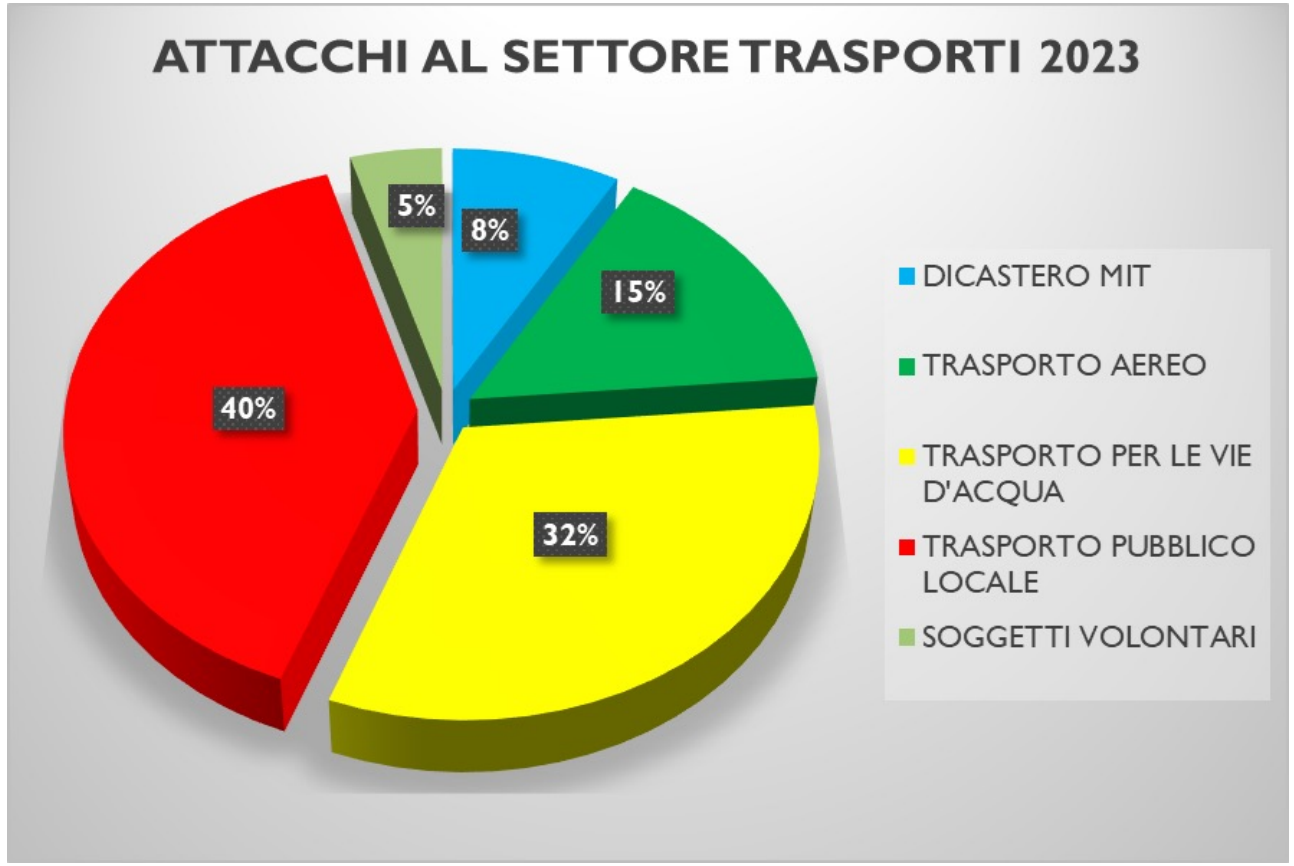
Al momento, le maggiori compagnie, gli istituti di classifica e numerosi altri soggetti che rappresentano anche le infrastrutture critiche del settore si stanno muovendo con decisione, seppur in maniera non sempre uniforme.


Attacchi per anno 2019 - 2023
2800
2600
2400
2200
2000
1800
1600
1400
1667
1874
2049
2489
2779
2019
2020
2021
2022
2023
© Clusit - Rapporto 2024 sulla Sicurezza ICT in Italia

Il panorama delle minacce

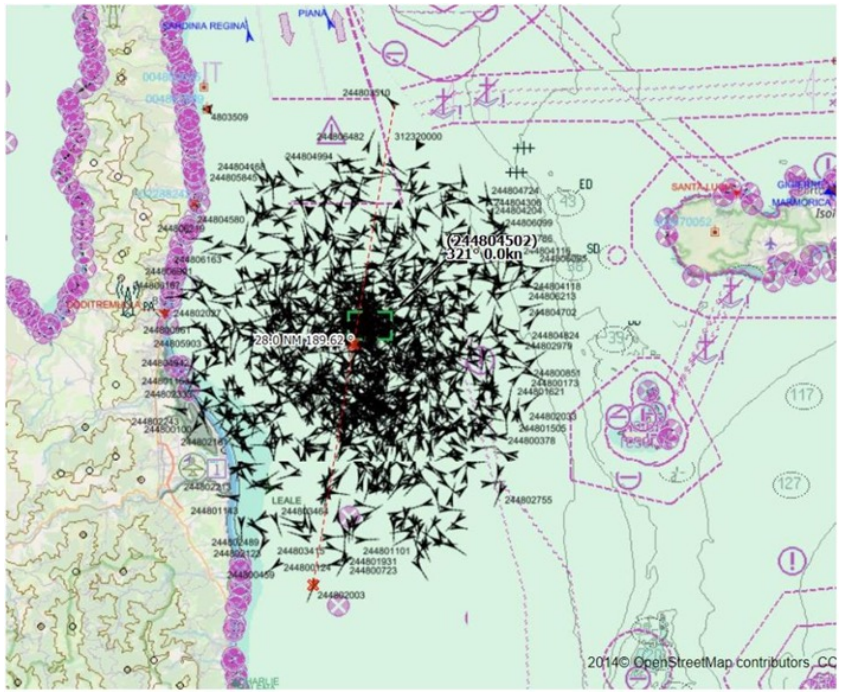


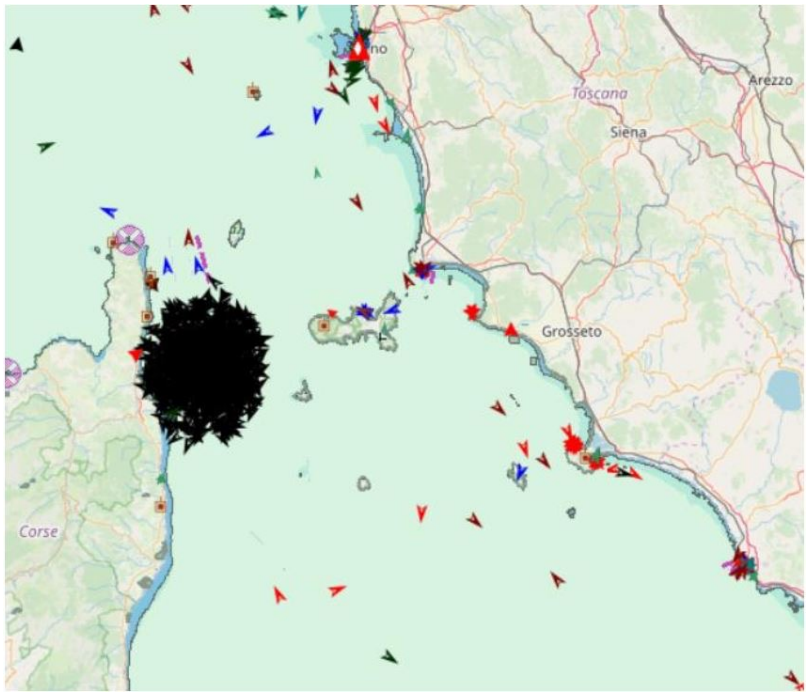
Fonti ENISA



- Nel corso del 2023 sono stati registrati n. 133 attacchi di rilievo nei trasporti.
- Secondo la classificazione degli OSE (settore trasporti e relativi sottosettori - ai sensi della c.d. Dir. NIS), quello maggiormente colpito è stato il «Trasporto pubblico locale» con il 40%, seguito dal «trasporto per le vie d'acqua» (compagnie di navigazione e ADSP) con il 32%, dal «Trasporto aereo» (vettori aerei e gestori aeroportuali) con il 15%, nonché figura lo stesso MIT con l'8% ed infine altri soggetti volontari con il 5%.

Il 3 dicembre 2019, a partire dalle ore 13:13 UTC, nell'area marittima compresa tra l'Isola d'Elba e la Corsica, sono state ricevute centinaia di informazioni AIS da unità navali battenti bandiera olandese, create artificialmente, aventi codici identificativi, posizioni, rotte e velocità diverse.





Normativa principale

- Decreto legislativo 18 maggio 2018, n. 65 “Attuazione della direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione” c.d. **Dir. NIS**

- Decreto-legge 21 settembre 2019, n. 105 - “Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica”

- Decreto del Presidente del Consiglio dei ministri 30 luglio 2020, n. 131 “Regolamento in materia di perimetro di sicurezza nazionale cibernetica, ai sensi dell'articolo 1, comma 2, del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133”

- Decreto del Presidente del Consiglio dei ministri 14 aprile 2021, n. 81 “Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza”

- Decreto-legge 14 giugno 2021, n. 82 – “Disposizioni urgenti in materia di cybersicurezza, definizione dell'architettura nazionale di cybersicurezza e istituzione dell'Agenzia per la cybersicurezza nazionale”

- Strategia nazionale di cybersicurezza 2022-2026 e Piano di implementazione (ACN - Agenzia per la cybersicurezza nazionale).

DIRETTIVA NIS 2

Estensione ambito di applicazione

- Nuovi settori: 9 settori altamente critici (originariamente 8), 7 settori critici (originariamente 0) + soggetti identificati come critici dalla Direttiva
- Intera infrastruttura ICT

Processo di identificazione

- Soggetti distinti tra entità essenziali (ex OSE) e importanti
- Automaticamente identificati sulla base di criteri oggettivi (dalle medie imprese in su, salvo eccezioni)
- Il Governo ha la facoltà di identificare ulteriori soggetti

Rafforzamento degli obblighi

- Misure di sicurezza più dettagliate (ma proporzionali)
- Approccio multi-rischio (coordinamento con Direttiva CER - **Direttiva (UE) 2022/2557** sulla resilienza dei soggetti critici)
- Processo di notifica più comprensivo
- Poteri ispettivi e sanzionatori rafforzati (allineamento alle sanzioni GDPR)

Paris MoU instruction PSCC 55/2022/09: fornisce una linea guida per gli ispettori PSC in merito al Codice ISM. “L’audit dell’ISM è responsabilità dello Stato di bandiera e della compagnia e non rientra nell’ambito del controllo dello Stato di approdo”.

Paris MoU instruction PSCC 54/2021/02: fornisce una linea guida per l’ispettore PSC sugli aspetti di sicurezza, descrivendo il processo di ispezione per quanto riguarda i requisiti ISPS.

Resolution MSC.428(98) (2021) concernente il *maritime cyber risk management* in ambito SMS (*Safety Management System*).

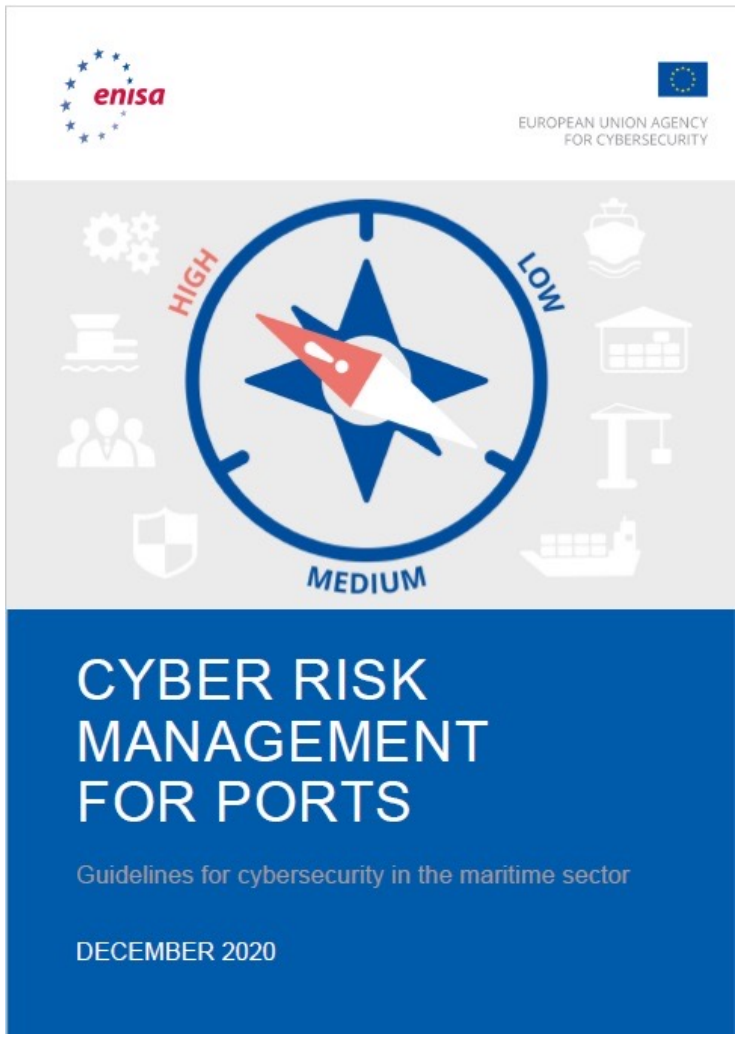
Guidance MSC-FAL.1/Circ.3 (2021) concernente i ruoli delle Compagnie, le attività e le misure da adottare e contenente, tra l'altro, riferimenti alle linee guida prodotte da IACS (UR E26 – UR E27), BIMCO come *best practices* per l'implementazione della gestione del rischio informatico.

- **IACS UR E27 -** *Cyber resilience of on-board systems and equipment*.
- **IACS UR E26 -** *Cyber resilience of ships*.

NUOVE LINEE GUIDA IMO

- Sono in corso di elaborazione nuove linee guida sulla gestione del rischio informatico marittimo;
- Revisioneranno quelle già emanate nel 2017;
- Dovranno integrarsi ed armonizzarsi con le Dir. NIS/NIS2 e CRA (*Cyber Resilience Act*);
- Dovranno tener conto della *supply chain*;
- Pongono una particolare attenzione sul tema del *CYBER RISK MANAGEMENT*, includendo processi, procedure, formazione, definizione di ruoli e responsabilità, gestione degli incidenti al fine di garantire dei livelli minimi di sicurezza comuni.

Cosa è stato fatto



Cosa è stato fatto

EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR MOBILITY AND TRANSPORT
Directorate A - Policy coordination
A.5 - Security

MARSEC Doc. 9209

Guidance on how to address cybersecurity onboard ships during audits, controls, verifications and inspections

Guida su articoli specifici del Reg. 725/2004

- La sicurezza informatica nella valutazione della sicurezza della nave (*assessment*)
- La cybersecurity nel piano di sicurezza della nave
- Ispezioni PSC e *cybersecurity*
  - Misure minime raccomandate per l'igiene informatica di base a bordo:
    - Inventario dei beni
    - Gestione degli aggiornamenti
    - Protezione e *backup* dei dati
    - Gestione e protezione dei dispositivi rimovibili USB
    - Gestione *account* e controllo accessi
    - Gestione della rete
    - Protezione delle connessioni remote
    - Sensibilizzazione e formazione sulla sicurezza informatica
    - Rilevamento degli incidenti, attività di risposta e di ripristino

Su richiesta diretta da parte dell'Unione Europea, EMSA si è assunta l'incarico di progettare e sviluppare un corso di formazione in materia di *cybersecurity* in ambito marittimo, prevedendo un apprendimento misto con elementi pratici e teorici in modalità sincrona e asincrona, ossia una parte da seguire *on-line* ed una parte in presenza presso la sede di Lisbona.

Esso è destinato prioritariamente alla formazione di ispettori abilitati degli Stati membri, inclusi anche i soggetti responsabili di assicurare la conformità con gli standard EU ed internazionali in materia di *safety* e *security* marittima.

EMSA ha da tempo reso anche disponibile sul proprio sito un corso *online* denominato «Awareness in Maritime Cybersecurity».

Atre iniziative, come quelle portate avanti dal *Cybersecurity Working Group dell'European Coast Guard Function Forum*, mirano a fornire competenze e consulenza alle autorità degli Stati membri dell'UE che svolgono funzioni di guardia costiera nel settore marittimo, a condividere l'analisi dei rischi e le migliori pratiche per la sicurezza informatica, a contribuire ad una più efficiente consapevolezza della *cybersecurity* e condivisione delle informazioni, in conformità alle leggi e ai regolamenti europei e nazionali.

Il gruppo di lavoro ha inoltre come obiettivo a lungo termine la capacità di integrare una comunità più ampia e di contribuire alla stesura di un concetto comune di sicurezza informatica della Guardia costiera europea.

Una delle attività più importanti è la condivisione di informazioni relative ad esperienze acquisite o concernenti azioni già avviate nel settore che possano rappresentare un aiuto o un esempio per la comunità e che possano raffigurare uno spunto per intraprendere ulteriori iniziative a livello comune.

Tutti gli utenti dei sistemi presenti sia a bordo delle navi che presso le infrastrutture a terra dovrebbero essere consapevoli dei potenziali rischi per la sicurezza informatica ed essere formati per identificare e mitigare tali rischi.

Le iniziative per aumentare i livelli di sicurezza informatica, sia di tipo tecnico che procedurale, dovrebbero pertanto essere coordinate con campagne di formazione e sensibilizzazione su misura dell'equipaggio e dei dipendenti in generale.

Pur essendo quello della sicurezza fisica un argomento ormai ben radicato nella cultura di molti, la sicurezza informatica pare essere un concetto tuttora forse troppo acerbo.

Servono formazione e sensibilizzazione a tutti i livelli, anche all'interno delle varie organizzazioni in cui i sistemi IT e OT sono spesso gestiti da soggetti diversi che non hanno nessuna visione generale della sicurezza.

Per ridurre la vulnerabilità sia agli incidenti informatici che agli attacchi informatici e garantire operazioni sicure ed efficienti delle navi e delle infrastrutture portuali, DG MOVE, EMSA, ENISA ed anche altri soggetti come IACS consigliano agli Stati membri ed alle compagnie di rivedere e affrontare la sicurezza informatica mediante la formazione del personale e l'adeguamento delle proprie *policy* in materia, in modo da avere requisiti procedurali, interpretazioni unificate, raccomandazioni e regole strutturali comuni.

Il processo deve avviarsi a partire dal livello dirigenziale e non essere delegato unicamente al responsabile della sicurezza della compagnia, dell'agenzia o della nave.

Grazie per l'attenzione

C.F. (CP) Dany Massimo MUGNAINI

Ufficiale del Corpo delle Capitanerie di porto – Guardia costiera

Membro dell'European Coast Guard Functions Forum (ECGFF) – CYBERSECURITY WORKING GROUP

dany.mugnaini@mit.gov.it