Shipping: alzata l'attenzione contro gli attacchi cyber

Volta (UniGe) "Porto interconnesso, rischio effetto domino"

15 febbraio

Shipping: alzata l'attenzione contro gli attacchi cyber

"L'organizzazione di un porto è molto articolata e ricca di interazioni fra le società e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi.
Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare le minacce digitali serve dunque una buona strategia di security governance". E' l'avvertimento lanciato da Alessandro Volta, dell'Università di Genova, nel corso del webinar di stamattina organizzato da Assarmatori in collaborazione con Fise Uniport su "Cyber security nell'ambito marittimo portuale". Tutti i partecipanti concordano sulla necessità di alzare il livello di attenzione e le competenze per contrastare i rischi degli attacchi cyber. Le tecnologie informatiche di gestione di dati e informazioni e l'automazione sempre più avanzata dei sistemi di bordo delle navi e delle operazioni a terra offrono grandi opportunità di sviluppo al settore, ma lo espongono di più alle minacce digitali. "La cybersecurity è sempre più un aspetto critico, essenziale per preservare continuità, sicurezza operativa, della nave, degli asset e delle persone" ha spiegato Orietta Campironi, chief Information officer di Ignazio Messina & C . E proprio guardando ai nuovi scenari operativi, anche accelerati dal periodo di emergenza pandemica "la strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto" ha aggiunto. Per Giacomo Speretta di Leonardo: "Il supporto da parte di aziende specializzate in sicurezza globale in questo contesto diventa imprescindibile per tutelarsi".

(ANSA)

Informatica, nei porti e sulle navi sta creando un mare di opportunità ma anche di pericoli

martedì, 15 febbraio 2022

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo sia delle operazioni di terra, rappresentano una medaglia a due facce: la prima, bella, è quella che mostra un vero e proprio mare di opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa; la seconda, decisamente più brutta, è quella che evidenzia invece la crescente esposizione agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Attacchi che non risparmiano nessuno e che vedono proprio il trasporto marittimo esposto talvolta più degli altri a queste minacce. E' partendo da questa premessa che i responsabili di Assarmatori (associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) hanno deciso di varare, in collaborazione con Fise Uniport (associazione delle imprese portuali) un webinar dal titolo "Cybersecurity nell'ambito marittimo-portuale". Un appuntamento in rete che ha evidenziato innanzitutto la necessità, ribadita anche dall'International maritime organization, di "creare un ecosistema cyber resiliente", come ha esordito Giacomo Speretta , vicepresidente senior e responsabile dell'area marketing, sviluppo aziendale e strategia di vendita di Leonardo Spa , azienda che opera nei settori della difesa, dell'aerospazio e della sicurezza e di cui il maggiore azionista è il ministero dell'Economia, confermando che "la tutela dal rischio cibernetico è diventata cruciale anche per il settore marittimo" e che "in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici". In altre parole, ha sintetizzato Giacomo Speretta con un felice gioco di parole, "non si può più navigare a vista". Una necessità di far salpare al più presto sistemi di "cyberdifesa" ribadita anche da Giorgio Volta, in rappresentanza del dipartimento di Ingegneria navale, elettrica, elettronica e delle telecomunicazioni, Diten, dell'Università degli Studi di Genova. Che ha spiegato come "l'organizzazione di un porto sia è molto articolata e ricca di interazioni fra le società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi" e come "se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Minacce da combattere con una buona strategia di Security Governance". "Urge un innalzamento del livello di competenza, attenzione e consapevolezza", ha aggiunto il suo collega, Rodolfo Zunino, "in questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche

organizzative, di governance e comportamentali". Una mission che appare imprescindibile anche vista dal "ponte di comando" di una storica compagnia di navigazione come Ignazio Messina & C. SpA, che nel 2022 celebra il suo primo secolo di vita, come ha confermato Orietta Campironi, responsabile dell'ufficio stampa: "La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati anche dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".

MAREONLINE.it

TRASPORTO MARITTIMO SEMPRE PIÙ SOTTO ATTACCO INFORMATICO, SERVONO SISTEMI DI CYBERDIFESA

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo sia delle operazioni di terra, rappresentano una medaglia a due facce: la prima, bella, è quella che mostra un vero e proprio mare di opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa; la seconda, decisamente più brutta, è quella che evidenzia invece la crescente esposizione agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Attacchi che non risparmiano nessuno e che vedono proprio il trasporto marittimo esposto talvolta più degli altri a queste minacce. E' partendo da questa premessa che i responsabili di Assarmatori (associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) hanno deciso di varare, in collaborazione con Fise Uniport (associazione delle imprese portuali) un webinar dal titolo "Cybersecurity nell'ambito marittimo-portuale". Un appuntamento in rete che ha evidenziato innanzitutto la necessità, ribadita anche dall'International maritime organization, di "creare un ecosistema cyber resiliente", come ha esordito Giacomo Speretta , vicepresidente senior e responsabile dell'area marketing, sviluppo aziendale e strategia di vendita di Leonardo Spa , azienda che opera nei settori della difesa, dell'aerospazio e della sicurezza e di cui il maggiore azionista è il ministero dell'Economia, confermando che "la tutela dal rischio cibernetico è diventata cruciale anche per il settore marittimo" e che "in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici". In altre parole, ha sintetizzato Giacomo Speretta con un felice gioco di parole, "non si può più navigare a vista." Una necessità di far salpare al più presto sistemi di "cyberdifesa" ribadita anche da Giorgio Volta, in rappresentanza del dipartimento di Ingegneria navale, elettrica, elettronica e delle telecomunicazioni, Diten, dell'Università degli Studi di Genova. Che ha spiegato come "l'organizzazione di

un porto sia è molto articolata e ricca di interazioni fra le società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi" e come ".se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Minacce da combattere con una buona strategia di Security Governance". "Urge un innalzamento del livello di competenza, attenzione e consapevolezza", ha aggiunto il suo collega, Rodolfo Zunino, "in questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali". Una mission che appare imprescindibile anche vista dal "ponte di comando" di una storica compagnia di navigazione come Ignazio Messina &C. SpA, che nel 2022 celebra il suo primo secolo di vita, come ha confermato Orietta Campironi, responsabile dell'ufficio stampa: "La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati anche dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".

ShipMag.

Cyber security e shipping, i rischi spiegati dagli esperti: “Serve maggiore competenza”

15 FEBBRAIO 2022 - Redazione

Nel webinar di Assarmatori e Uniport fari puntati su un argomento sempre più centrale per il comparto

Milano – Gli **attacchi informatici** sono sempre più frequenti, sofisticati e non risparmiano nessuno. Tanto più il trasporto marittimo e i porti, potenziali vittime alla luce della diffusione di tecnologie informatiche di gestione e di comunicazione di dati e informazioni, automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra. Rischi che la pandemia da Covid-19 ha alzato in modo esponenziale come dimostrano i recenti attacchi cyber a importanti compagnie di navigazione e di logistica.

Questi temi sono stati al centro del webinar dal titolo “**Cybersecurity nell’ambito marittimo-portuale**”, organizzato da **Assarmatori** (associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con **Fise Uniport** (associazione delle imprese portuali), entrambe aderenti a **Conftrasporto-Confcommercio.**

“La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone”, osserva **Orietta Campironi**, Chief Information Officer del gruppo Ignazio Messina&C.

“I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l’utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l’approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l’intento di eludere le difese e muoversi senza ostacoli. La strategia e l’approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto”, sottolinea **Campironi.**

“L’International Maritime Organization ci invita a creare un ecosistema cyber resiliente – ricorda **Giacomo Speretta**, senior vice president – marketing, business development & sales strategy di Leonardo SpA – la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.”.

Dal lato porti, intervengono **Giorgio Volta e Rodolfo Zunino,** professori del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni dell’Università degli Studi di Genova.

“L’organizzazione di un porto è molto articolata e ricca di interazioni fra le società presenti nell’ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi – spiega **Volta** -. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance”.

Zunino rilancia: “Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l’intervento del prof. Zunino – In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali”.

L'Argomento

INNOVAZIONE

PORTI E CYBERSECURITY, TUTTE LE OPPORTUNITA' SECONDO ASSARMATORI E UNIPORT

Cresce la consapevolezza che la tutela dal rischio cibernetico diventa cruciale anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale è imprescindibile

GIOIA TAURO PORTO GRANDI INFRASTRUTTURE HUB CONTAINER GRU

Tempo di lettura stimato 3 minuti

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del **trasporto marittimo** difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da **COVID-19** ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli **attacchi informatici** che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.

È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "Cybersecurity nell'ambito marittimo-portuale", organizzato da **Assarmatori** (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con Fise Uniport (Associazione delle imprese portuali), entrambe aderenti a Confitrasporto-Confcommercio.

Dopo i saluti introduttivi dell'ing. Enrico **Allieri** (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul

versante nave e terminalistico, curate rispettivamente dall'ing. Stefano **Beduschi** (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e dal Com.te Dott. Vito Leo Totorizzo (**ISTO SPAMAT SRL**, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.
"L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente – le parole dell'Ing. Giacomo **Speretta** (Senior Vice President – Marketing, Business Development & Sales Strategy di **Leonardo SpA**) – la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.".
Non è mancata una illustre rappresentanza accademica con il dott. Giorgio **Volta** ed il prof. ing. Rodolfo **Zunino** del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN dell'Università degli Studi di Genova. "L'organizzazione di un porto – ha spiegato il dott. Volta – è molto articolata e ricca di interazioni fra le Società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance".
"Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l'intervento del prof. Zunino – In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali".

A completare il giro di interventi, l'ing. Orietta **Campironi** (Chief Information Officer di **Ignazio Messina &C. SpA**): "La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il **cyber-crime** rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".

Assarmatori e Uniport puntano il faro sulla cyber security marittimo portuale

(FERPRESS) – Roma, 15 FEB – Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da COVID-19 ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.
È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "Cybersecurity nell'ambito marittimo-portuale", organizzato da Assarmatori (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con Fise Uniport (Associazione delle imprese portuali), entrambe aderenti a Conftrasporto-Confcommercio.

Dopo i saluti introduttivi dell'ing. Enrico Allieri (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul versante nave e terminalistico, curate rispettivamente dall'ing. Stefano Beduschi (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e dal Com.te Dott. Vito Leo Totorizzo (ISTO SPAMAT SRL, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.

"L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente – le parole dell'Ing. Giacomo Speretta (Senior Vice President – Marketing, Business Development & Sales Strategy di Leonardo SpA) – la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.".

Non è mancata una illustre rappresentanza accademica con il dott. Giorgio Volta ed il prof. ing. Rodolfo Zunino del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN dell'Università degli Studi di Genova. "L'organizzazione di un porto – ha spiegato il dott. Volta – è molto articolata e ricca di interazioni fra le Società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance".

"Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l'intervento del prof. Zunino – In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali".

A completare il giro di interventi, l'ing. Orietta Campironi (Chief Information Officer di Ignazio Messina &C. SpA): "La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".

SHIPPING ITALY.IT

Il quotidiano online del trasporto marittimo

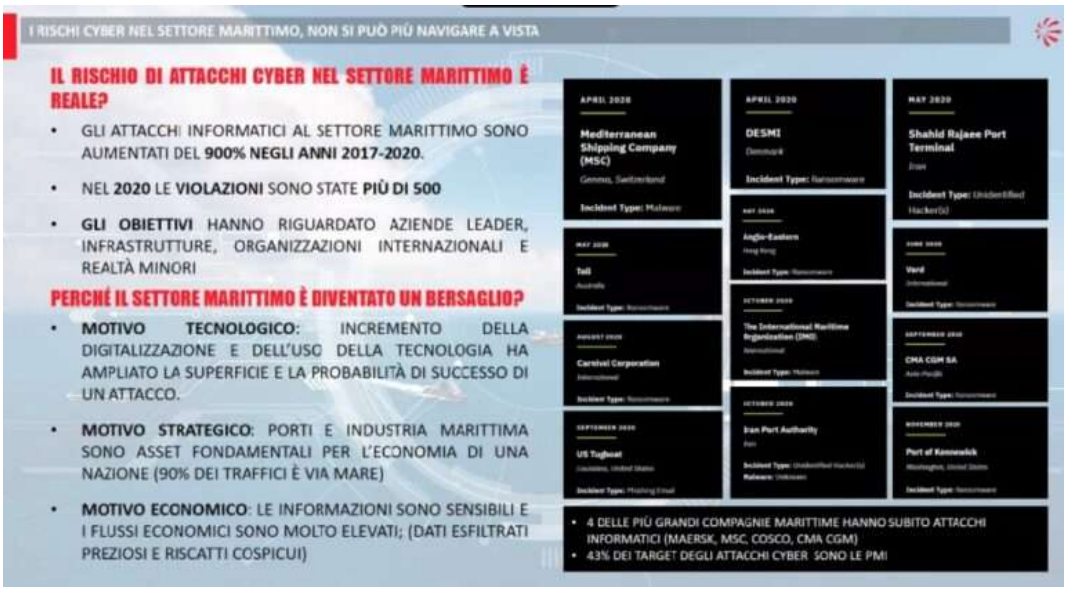
POLITICA&ASSOCIAZIONI

Cyber security in ambito marittimo-portuale: “In Italia servono maggiori investimenti”

Da Beduschi (Italia Marittima), Speretta (Leonardo) e Campironi (Messina) un monito a porre grande attenzione al rischio di attacchi come quello che a Maersk è costato oltre 250 milioni di dollari

DI **NICOLA CAPUZZO**

15 FEBBRAIO 2022



La cyber security in ambito marittimo-portuale è stato il tema al centro del webinar organizzato da Assarmatori e Fise Uniport durante il quale **Stefano Beduschi (Italia Marittima)** ha sottolineato la necessità di uno sforzo maggiore a livello di operational technology. “Serve uno sforzo anche da parte dell’amministrazione” ha detto, specificando di fare riferimento “ad esempio al Gps che è uno dei potenziali rischi dell’It dove poco possono fare gli armatori ma che bisognerebbe strutturare in maniera diversa da parte delle amministrazioni”.

Secondo il dirigente della compagnia di navigazione triestina “mentre il bordo, le navi, hanno dovuto fare questo sforzo, non tutti i settori interessati allo shipping sono stati obbligati a occuparsi del rischio cyber. Non è stato fatto altrettanto per tutti gli uffici e le attività che si interfacciano con le navi e possono portare pericoli legali alla cybersecurity”. Va ricordato infatti che dal 1° gennaio 2021 è obbligatorio per le navi avere una certificazione che comprovi la valutazione dei rischi cyber nell’ambito del proprio sistema Sms (Safety Management System).

Particolarmente d’impatto è stato l’intervnto di **Giacomo Speretta (Leonardo)** che ha spiegato come “gli attacchi informatici sono finalizzati a riscatti economici; è un mercato purtroppo. Non

sono “diretti solo ai grandi gruppi” e le navi in particolare “sono viste come dei grandi data center. Gps e sistemi di controllo della navigazione sono oggetto di vulnerabilità”.

Speretta ha sottolineato che “spesso dietro al buon successo di un attacco cyber c’è un errore umano, scarsa formazione o disattenzione. Un’azione che espone l’azienda al rischio”. Per comprendere meglio le dimensioni del fenomeno aiuta l’esempio portato a proposito dell’attacco a Maersk “avvenuto a causa dell’obsolescenza dei sistemi informativi” e che “ha generato un danno per l’azienda da 250-300 milioni di dollari”. In quel caso tutto ha avuto inizio con l’apertura di un file malevolo da parte di un dipendente”. Ex post il gruppo danese ha avviato un accurato percorso di formazione e awareness all’interno della propria forza lavoro.

Uno degli altri case study portati da Leonardo ha mostrato come un flusso di attacco cyber a un’azienda può avvenire anche attraverso una macchietta del caffè collegata a una rete aziendale informatica aperta.

“Nel settore dei trasporti non c’è sicuramente un’attenzione adeguata ai rischi informatici, servono investimenti e lavorare su una cultura cyber, implementare architetture per proteggere il sistema informatico e formare il personale (anche nel rapporto con l’indotto)” ha concluso Speretta annunciando che Leonardo inaugurerà a breve una sua Cyber Security Academy.

Giorgio Volta (Università degli studi di Genova), trattando il tema della security governance del sistema portuale, ha posto l’accenti sulle scalate ostili crescenti dal 2012 in poi nei confronti di aziende strategiche con conseguente attenzione crescente al Golden Power anche da parte dell’Italia non solo. “L’organizzazione di un porto – ha spiegato Volta – è molto articolata e ricca di interazioni fra le società presenti nell’ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance”.

Orietta Campironi ha infine portato l’esperienza della compagnia di navigazione **Ignazio Messina & C.**, di cui è Chief Information Officer, individuando tre fattori fondamentali nella propria roadmap in matera di cyber security. Un primo fattore tecnico, “volto al consolidamento del sistema tecnico di sicurezza aziendale; un secondo normativo, riguardante “la regolamentazione sui rischi informatici che guida la risk analysis e le norme che sono d’auto per stabilire le misure da attuare”. A questo proposito Campironi ha sottolineato che “talvolta le misure sono complesse e difficilmente adattabili all’eterogeneità di alcuni casi concreti”.

Il terzo è il fattore umano che “spesso è sfruttato dagli attori malevoli. Se su questo fronte non si fanno azioni mirate gli strumenti tecnologici sono inutili” ha affermato. “Occorre dedicare molto tempo e dare molta importanza al processo di formazione e di apprendimento continuo”.

N.C.

SHIPPING ITALY.IT
Il quotidiano online del trasporto marittimo

Cyber security nei terminal portuali: “Lo Stato deve contribuire”

Sia Luigi Merlo (Federlogistica) che Vito Totorizzo (Fise Uniport) richiamano un’intervento pubblico per sostenere gli investimenti necessari a prevenire i rischi di attacchi in banchina

DI **REDAZIONE SHIPPING ITALY**

15 FEBBRAIO 2022

“Il vero e unico faro per programmare e gestire i processi di innovazione tecnologica nei porti

sono le Autorità di Sistema Portual. È venuto il momento di affrontare, con serietà e concretezza e quindi nella gestione delle risorse del Pnrr, le tematiche relative all’innovazione tecnologica e alla digitalizzazione, dalle quali dipende la sicurezza così come l’efficienza e la competitività dei porti, ma anche dell’intera catena logistica”. Lo ha detto Luigi Merlo, presidente di Federlogistica-Conftrasporto, anticipando i temi in discussione nel corso del webinar organizzato da Assarmatori e Fise Uniport dal titolo ‘Cybersecurity nell’ambito marittimo – portuale’.

Secondo Merlo i tempi sono stretti: “Il 2022 sarà l’anno chiave con l’entrata in vigore della Direttiva Europea Nis 2 sulla sicurezza delle reti e dei sistemi informativi. Una direttiva che estenderà il raggio di azione in molti settori delicati tra i quali i trasporti e i porti, amplierà gli obblighi non solo alle grandi imprese ma anche a quelle medie e prevederà sanzioni elevate per chi non si adegua”. Per il vertice di Federlogistica “le risorse del Pnrr per la digitalizzazione devono quindi essere impiegate per aiutare le imprese ma anche le Autorità di Sistema Portuale a strutturarsi. È il caso di ricordare che le stesse AdSP si trovano a far fronte a carichi di lavoro rilevanti per la progettazione e l’implementazione delle opere da realizzare; e proprio in questo scenario devono poter contare su sistemi inviolabili, introducendo da subito la figura del cyber manager”.

Per il Presidente di Federlogistica-Conftrasporto il rischio di attacchi hacker non è un’ipotesi aleatoria, è invece “terribilmente concreto”. Solo un percorso di digitalizzazione che sfoci rapidamente in Cyber Security Assessment e quindi nell’impiego dei relativi piani di gestione del rischio cyber “può consentire un salto di qualità non più rinviabile”.

Dello stesso avviso è parso Vito Totorizzo, vicepresidente di Fise Uniport, che intervenendo al webinar ha detto: “C’è sempre una falla dove i pericoli e le minacce informatiche possono insinuarsi. I costi e i danni potenziali sono elevatissimi, soprattutto per i grandi terminal perché anche solo con una piccola o involontaria falla ci si espone a rischi di attacchi rilevanti. Anche semplicemente aprendo un file che non si riteneva preoccupante”.

Totorizzo ha evidenziato la vulnerabilità del fattore umano come fattore di rischio numero uno: “Anche il più modesto dei lavoratori potrebbe essere la chiave per far accedere gli hacker ai sistemi informatici”.

A proposito della questione dei costi il terminalista barese la pensa come Merlo: “Siccome la battaglia è di interesse pubblico bisognerebbe trovare il modo di coinvolgere lo Stato ai fini di contribuire a migliorare i sistemi (che sono onerosissimi per i piccoli terminal, un po’ meno per i grandi). È essenziale che il pubblico faccia la sua parte. Ogni azienda, in funzione delle proprie capacità economiche, deve organizzarsi. I grandi terminal non possono limitare solo a pochi addetti l’accesso al sistema informatico aziendale. Mi auguro che l’importanza della materia richiami lo Stato a trovare misure adeguate”.

Cybersecurity nell'ambito marittimo-portuale. Assarmatori e Uniport puntano il faro su un argomento sempre più centrale per il comparto

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da COVID-19 ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.

È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "Cybersecurity nell'ambito marittimo-portuale", organizzato da Assarmatori (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con Fise Uniport (Associazione delle imprese portuali), entrambe aderenti a Conftrasporto-Confcommercio.

Dopo i saluti introduttivi dell'ing. Enrico Allieri (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul versante nave e terminalistico, curate rispettivamente dall'ing. Stefano Beduschi (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e dal Com.te Dott. Vito Leo Totorizzo (ISTO SPAMAT SRL, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.

"L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente – le parole dell'Ing. Giacomo Speretta (Senior Vice President – Marketing, Business Development & Sales Strategy di Leonardo SpA) – la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in

sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.”.

Non è mancata una illustre rappresentanza accademica con il dott. Giorgio Volta ed il prof. ing. Rodolfo Zunino del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN dell’Università degli Studi di Genova. “L’organizzazione di un porto – ha spiegato il dott. Volta – è molto articolata e ricca di interazioni fra le Società presenti nell’ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance”.

“Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l’intervento del prof. Zunino – In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali”.

A completare il giro di interventi, l’ing. Orietta Campironi (Chief Information Officer di Ignazio Messina &C. SpA): “La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l’utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l’approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l’intento di eludere le difese e muoversi senza ostacoli. La strategia e l’approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto”.

Cyber security sempre più al centro delle attività portuali

Se ne è parlato nel webinar organizzato da Assarmatori e Fise Uniport

Pubblicato 24 minuti fa il giorno 15 Febbraio 2022
Da **Redazione**

ROMA - È ormai un tema centrale quello della **cyber security** in ambito marittimo-portuale. Ne hanno parlato oggi diversi relatori nel webinar organizzato da **Assarmatori e Fise Uniport.** Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la

Trasporti-Italia.com

La sfida della Cybersecurity in ambito marittimo-portuale: un webinar Assarmatori e Uniport

martedì 15 febbraio 2022

Il ricorso sempre più massiccio a tecnologie informatiche per la gestione e lo scambio di dati e informazioni, la disponibilità di **sistemi sempre più avanzati** per la navigazione e per la gestione delle operazioni di terra rappresentano un'opportunità di crescita e di sviluppo per il comparto del **trasporto marittimo** difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da Covid-19 ha contribuito in questo senso, portando alla luce il valore del lavoro a distanza come opportunità per questo settore, che certamente acquisterà un crescente peso anche a emergenza finita.

Il rovescio della medaglia di questi che sono fattori incontrovertibilmente positivi è costituito dalla crescente esposizione di operatori e istituzioni ad **attacchi informatici**, ormai sempre più frequenti e sempre più sofisticati. Attacchi che non risparmiano neanche il trasporto marittimo, esposto quanto e talvolta più di altri comparti a queste minacce.

Queste le premesse da cui è partito il webinar **"Cybersecurity nell'ambito marittimo-portuale"**, organizzato da **Assarmatori** (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con **Fise Uniport** (Associazione delle imprese portuali), entrambe aderenti a Conftrasporto-Confcommercio.

La discussione è stata aperta dai saluti di **Enrico Allieri**, responsabile dell'area Ship Technology, Maritime Safety & Environment di Assarmatori, e da due interventi introduttivi sul versante nave e terminalistico, curati rispettivamente da **Stefano Beduschi**, deputy senior vice president Italia Marittima Spa e presidente della Commissione Tecnica Ship Technology, Maritime Safety &

Environment di Assarmatori, e dal com.te **Vito Leo Totorizzo**, ISTO SPAMAT Srl, vicepresidente di Uniport con delega all'Information & Communication Technology.

Creare un ecosistema cyber resiliente

Nel suo intervento **Giacomo Speretta**, senior vice president Marketing, Business Development & Sales Strategy di Leonardo Spa, ha sottolineato come dall'**International Maritime Organization** arrivi l'indicazione a creare un ecosistema cyber resiliente: la tutela dal rischio cibernetico diventa, dunque, cruciale anche per il settore marittimo, e in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. "Non si può più navigare a vista".

Gli aspetti strettamente tecnici e organizzativi del problema sono stati affrontati da **Giorgio Volta** e **Rodolfo Zunino** del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN dell'Università degli Studi di Genova.

I docenti hanno spiegato nei loro interventi quanto l'organizzazione di un porto sia articolata e ricca di interazioni fra le società presenti e molte infrastrutture critiche che erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un "effetto domino" non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque, ha sottolineato Volta "una buona strategia di **Security Governance**".

Alla luce di questa complessità e articolazione di soggetti e professionalità, il prof. Zunino ha sottolineato la necessità di un innalzamento del livello di competenza, attenzione e consapevolezza. In questo senso si delinea come imprescindibile una mission di **formazione strutturata e multidisciplinare**, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali.

In conclusione l'intervento di **Orietta Campironi**, chief Information Officer di Ignazio Messina &C. Spa, che ha ribadito come la cybersecurity costituisca sempre più un aspetto critico, essenziale per **preservare la continuità e la sicurezza operativa**, la sicurezza della nave, degli asset e delle persone, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. Di conseguenza: "La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".

Cybersecurity nell'ambito marittimo-portuale. Assarmatori e Uniport puntano il faro su un argomento sempre più centrale per il comparto

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da COVID-19 ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.

È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "***Cybersecurity nell'ambito marittimo-portuale***", organizzato da **Assarmatori** (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con **Fise Uniport** (Associazione delle imprese portuali), entrambe aderenti a **Confrasporto-Confcommercio.**

Dopo i saluti introduttivi dell'**ing. Enrico Allieri** (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul versante nave e terminalistico, curate rispettivamente dall'**ing. Stefano Beduschi** (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e **dal Com.te Dott. Vito Leo Totorizzo** (ISTO SPAMAT SRL, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.

"*L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente* - le parole dell'Ing. **Giacomo Speretta** (Senior Vice President - Marketing, Business Development & Sales Strategy di Leonardo SpA) – *la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.".*

Non è mancata una illustre rappresentanza accademica con il **dott. Giorgio Volta** ed il **prof. ing. Rodolfo Zunino** del Dipartimento di ingegneria navale,

elettrica, elettronica e delle telecomunicazioni – DITEN dell'Università degli Studi di Genova. "*L'organizzazione di un porto* – ha spiegato il dott. Volta – *è molto articolata e ricca di interazioni fra le Società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance".*

"Urge un innalzamento del livello di competenza, attenzione e consapevolezza - l'intervento del prof. Zunino - *In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali".*

A completare il giro di interventi, l'**ing. Orietta Campironi** (Chief Information Officer di Ignazio Messina &C. SpA): *"La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".*

Assarmatori e Uniport puntano il faro sulla cybersecurity nell'ambito marittimo-portuale

di Redazione

Un argomento sempre più centrale, anche a fronte della crescente esposizione delle organizzazioni agli attacchi informatici sempre più sofisticati

Martedì 15 Febbraio 2022

"L'organizzazione di un porto è molto articolata e ricca di interazioni fra le società e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare le minacce digitali serve dunque una buona strategia di security governance". **E' l'avvertimento lanciato da Alessandro Volta, dell'Università di Genova, nel corso del webinar di stamattina organizzato da Assarmatori in collaborazione con Fise Uniport su "Cyber security nell'ambito marittimo portuale".**

Tutti i partecipanti concordano sulla necessità di alzare il livello di attenzione e le competenze per contrastare i rischi degli attacchi cyber. Le tecnologie informatiche di gestione di dati e informazioni e l'automazione sempre più avanzata dei sistemi di bordo delle navi e delle operazioni a terra offrono grandi opportunità di sviluppo al settore, ma lo espongono di più alle minacce digitali.

"La cybersecurity è sempre più un aspetto critico, essenziale per preservare continuità, sicurezza operativa, della nave, degli asset e delle persone" ha spiegato Orietta Campironi, chief Information officer di Ignazio Messina & C . E proprio guardando ai nuovi scenari operativi, anche accelerati dal periodo di emergenza pandemica "la strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto" ha aggiunto.

Per Giacomo Speretta di Leonardo: "Il supporto da parte di aziende specializzate in sicurezza globale in questo contesto diventa imprescindibile per tutelarsi"

PERIODICO MARITTIMO INDIPENDENTE A DIFFUSIONE INTERNAZIONALE A BILINGUAL SHIPPING NEWSPAPER
L'INFORMATORE NAVALE
FONDATO NEL 1964 di NAPOLI

Cybersecurity nell'ambito marittimo-portuale. Assarmatori e Uniport puntano il faro su un argomento sempre più centrale per il comparto

È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "***Cybersecurity nell'ambito marittimo-portuale***", organizzato da **Assarmatori** (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con **Fise Uniport** (Associazione delle imprese portuali), entrambe aderenti a **Conftrasporto-Confcommercio.**
Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da COVID-19 ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.

Dopo i saluti introduttivi dell'**ing. Enrico Allieri** (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul versante nave e terminalistico, curate rispettivamente dall'**ing. Stefano Beduschi** (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e **dal Com.te Dott. Vito Leo Totorizzo** (ISTO SPAMAT SRL, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.

"*L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente* - le parole dell'Ing. **Giacomo Speretta** (Senior Vice President – Marketing, Business Development & Sales Strategy di Leonardo SpA) – *la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.".*
Non è mancata una illustre rappresentanza accademica con il **dott. Giorgio Volta** ed il **prof. ing. Rodolfo Zunino** del Dipartimento di ingegneria navale, elettrica, elettronica e delle

telecomunicazioni – DITEN dell'Università degli Studi di Genova. "*L'organizzazione di un porto* – ha spiegato il dott. Volta – *è molto articolata e ricca di interazioni fra le Società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance".*

"Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l'intervento del prof. Zunino – *In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali".*

A completare il giro di interventi, l'**ing. Orietta Campironi** (Chief Information Officer di Ignazio Messina &C. SpA): *"La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto".*

Cybersecurity nell'ambito marittimo-portuale: Assarmatori e Uniport puntano il faro su un argomento sempre più centrale per il comparto

15 Febbraio 2022

Le tecnologie informatiche di gestione e di comunicazione di dati e informazioni, l'automazione sempre più avanzata sia dei sistemi di bordo che delle operazioni di terra, stanno fornendo opportunità di crescita e di sviluppo al comparto del trasporto marittimo difficilmente immaginabili fino a qualche anno fa. Anche la pandemia da COVID-19 ha messo ugualmente in evidenza nel settore le opportunità offerte dal lavoro a distanza che acquisterà un crescente peso anche ad emergenza finita.

Il "contro canto" di questo indiscusso progresso è rappresentato dalla crescente esposizione delle organizzazioni agli attacchi informatici che sono ormai all'ordine del giorno e sempre più sofisticati. Questi attacchi non risparmiano nessuno ed anche il trasporto marittimo è esposto quanto e talvolta più degli altri a queste minacce.

È la premessa che ha accompagnato lo svolgersi del webinar dal titolo "***Cybersecurity nell'ambito marittimo-portuale***", organizzato da **Assarmatori** (Associazione che riunisce numerose compagnie italiane di navigazione e alcune tra le principali compagnie estere attive in ogni settore del trasporto marittimo) in collaborazione con **Fise Uniport** (Associazione delle imprese portuali), entrambe aderenti a **Conftrasporto-Confcommercio.**

Dopo i saluti introduttivi dell'**ing. Enrico Allieri** (Responsabile dell'area "Ship Technology, Maritime Safety & Environment di Assarmatori) ed una anteprima contenutistica sul versante nave e terminalistico, curate rispettivamente dall'**ing. Stefano Beduschi** (Deputy Senior Vice President Italia Marittima S.p.A. e Presidente della Commissione Tecnica "Ship Technology, Maritime Safety & Environment" di Assarmatori) e **dal Com.te Dott. Vito Leo Totorizzo** (ISTO SPAMAT SRL, Vice Presidente di Uniport con delega all' "Information & Communication Technology"), si è dato inizio ai lavori lasciando ampio spazio ai relatori chiamati al tavolo della discussione.

"*L'International Maritime Organization ci invita a creare un ecosistema cyber resiliente* – le parole dell'Ing. **Giacomo Speretta** (Senior Vice President – Marketing, Business Development & Sales

Strategy di Leonardo SpA) – *la tutela dal rischio cibernetico diventa cruciale, dunque, anche per il settore marittimo, ed in questo contesto il supporto da parte di aziende specializzate in sicurezza globale diventa imprescindibile per le società del settore che vogliono tutelarsi dai rischi cibernetici. Non si può più navigare a vista.”*.

Non è mancata una illustre rappresentanza accademica con il **dott. Giorgio Volta** ed il **prof. ing. Rodolfo Zunino** del Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni – DITEN dell'Università degli Studi di Genova. "*L'organizzazione di un porto* – ha spiegato il dott. Volta – *è molto articolata e ricca di interazioni fra le Società presenti nell'ambito portuale e molte infrastrutture critiche che nello stesso ambito portuale erogano i loro servizi. Se uno degli attori fosse vittima di un attacco informatico potrebbe causare un effetto domino non voluto, mettendo in crisi diverse strutture. Per contrastare tali minacce digitali serve dunque una buona strategia di Security Governance”.*

“Urge un innalzamento del livello di competenza, attenzione e consapevolezza – l'intervento del prof. Zunino – *In questo senso appare imprescindibile una mission di formazione strutturata e multidisciplinare, capace di offrire un quadro organico di competenze non solo tecniche ma anche organizzative, di governance e comportamentali”.*

A completare il giro di interventi, l'**ing. Orietta Campironi** (Chief Information Officer di Ignazio Messina &C. SpA): *“La cybersecurity è sempre più un aspetto critico, essenziale per preservare la continuità e la sicurezza operativa, la sicurezza della nave, degli asset e delle persone. I nuovi scenari operativi, dettati dal periodo di emergenza pandemica, con l'utilizzo crescente del lavoro da remoto e di nuove modalità di collaborazione, richiedono di rimodellare l'approccio di difesa di postazioni di lavoro sempre più virtuali, nella consapevolezza che il cyber-crime rinnova continuamente tattiche, tecniche e procedure con l'intento di eludere le difese e muoversi senza ostacoli. La strategia e l'approccio alla sicurezza richiedono un livello di consapevolezza e di attenzione ancor più alto”.*