IL PICCOLO
Dir. Resp.: Omar Monestier
www.datastampa.it Tiratura: 19759 - Diffusione: 19307 - Lettori: 117000: da enti certificatori o autocertificati
11-FEB-2021
da pag. 21
foglio 1 / 2
Superficie: 63 %

## Il team Fincantieri che protegge le navi dai pirati del web

GARAU / A PAG. 21

IL CENTRO DI ECCELLENZA IN MARINERIA A TRIESTE

# Team Fincantieri contro i pirati del web: «Sempre più attacchi ai dati e ai sistemi»

Daniele Alì, capo dell'Information security e ad di E-phors: «Preveniamo i sabotaggi e insegniamo agli altri come farlo»

**Incursioni pericolose su apparati gps con il rischio di errori sulla rotta o i fondali**

Giulio Garau / TRIESTE

«Il momento più delicato è quello delle fasi iniziali delle commesse e delle trattative prima dell'ordine. C'è lo scambio delle informazioni più confidenziali, la proposta commerciale con l'invio dei disegni del prototipo della nave, ed è molto importante che ci sia la massima segretezza anche per tutelare il lavoro dei designer. Un attacco cyber per un sabotaggio o ancor peggio rubare i segreti industriali sarebbe gravissimo. Impensabile poi con le navi militari».

**CYBER ATTACCHI**

Quarantatre anni, romano ma da anni trapiantato a Trieste, un passato nelle Poste Italiane a capo della It Security, ora chief information security officer alla Fincantieri e amministratore delegato di E-phors (azienda specializzata nella fornitura si servizi e prodotti di cybersecurity anche per clienti extra-Fincantieri) Daniele Francesco Alì è alla guida di una task force di 45 persone, 10 di queste costituiscono il nucleo leader a Trieste, nel palazzo della Marineria.

**GRUPPO DI GIOVANI**

«Siamo un gruppo molto giovane – prosegue Alì – io sono di Roma ma ci sono anche alcuni triestini come il capo del Centro operativo di sicurezza o quello della conformità. Tutto è nato 8 anni fa quando in azienda è sorta la necessità di proteggere i dati aziendali. Stava crescendo il pericolo dell'attacco cyber, nessuno aveva previsto che sarebbe stato un rischio così grave per i dati e l'know how di un'azienda come Fincantieri che opera sia nel civile che nel militare. Ci sono informazioni di valenza nazionale, un patrimonio che abbiamo l'obbligo di protegge».

Fincantieri ha deciso di fondare a Trieste un centro di eccellenza con lo scopo di proteggere dati e tecnologie. «Una realtà che non ha a che fare con il mondo della produzione navale – continua il chief officer – ma abbiamo capito che era necessario impegnarsi ad alto livello preparando contromosse verso avversari che attraverso web e reti possono rivelarsi pericolosi. Si tratta di gente estremamente preparata con conoscenze di alto livello. Il nostro compito era ostacolare gli attacchi».

**DATI DA PROTEGGERE**

Sotto attacco non solo le procedure della costruzione delle navi. Ma anche le le trattative con i clienti, i disegni dei prototipi e le idee sulle tecnologie da applicare alle nuove navi da crociera o militari con apparecchiature top secret.

«Queste sono le fasi più delicate che devono rimanere segrete dal punto di vista tecnologico e commerciale – aggiunge l'ad– e il nostro compito è quello di individuare gli attacchi che lasciano sempre traccia. E di tentativi ce ne sono stati, abbiamo stoppato diversi attacchi. Tentativi di incursione da parte di gruppi cyber che utilizzano spesso robot che in maniera automatica cercano di penetrare i sistemi. Noi li intercettiamo e li blocchiamo. La rilevazione è importantissima, perché l'incursore è sempre silenzioso».

Informazioni che poi vengono condivise con il nucleo informatico della Polizia postale con la quale la task force di Fincantieri ha un rapporto privilegiato.

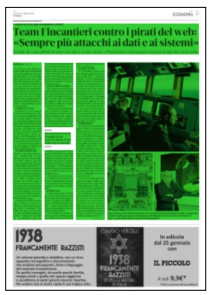
**LE MINACCE**

«In questi anni però ci siamo accorti che che la minaccia era trasversale e il rischio degli attacchi – spiega il capo della task force informatica di Fincantieri – poteva riguardare anche le navi passeggeri che ospitano sei mila persone».

Uno scenario da incubo visto che sono tutti collegati alla rete della nave e non c'è solo il rischio di rubare i dati o clonare le carte di credito.

**IL SABOTAGGIO**

«Ci potrebbero essere minacce di sabotaggio di tutti i sistemi della nave – conferma Daniele – la rete informatica, quella dei Gps con attacchi al sistema di navigazione che ti potrebbe far credere di essere su un'altra rotta o di trovarti a navigare in acque più profonde di quelle in cui sei. Incursioni pericolosissime. Sabotaggi che potrebbero far scattare o non scattare allarmi di rotta

IL PICCOLO

Dir. Resp.: Omar Monestier

11-FEB-2021
da pag. 21
foglio 2 / 2

www.datastampa.it

Tiratura: 19759 - Diffusione: 19307 - Lettori: 117000: da enti certificatori o autocertificati

Superficie: 63 %

fondamentali. E i cyber pirati sono diventati sempre più bravi». Le navi per ora non hanno ancora subito attacchi, ma ce ne sono stati altri, alle centrali di arricchimento di uranio iraniane, ai porti di San Diego e Barcellona nel 2018.

**CYBER PIRATI**

«Un anno fa è stato deciso di aprire E-Phors specializzata nella fornitura si servizi e prodotti di cyber-security per formare anche all'esterno il personale di navigazione – conclude Alì – ma anche far fronte alla possibile domanda esterna di realtà come porti o altre aziende simili alla nostra. A dicembre per la prima volta abbiamo fatto un corso con l'Accademia italiana della Marina mercantile. È stato molto bello, siamo riusciti a mettere sullo stesso tavolo sia coloro che devono difendersi dagli attacchi che quelli che conoscono l'operatività navale che se subiscono il sabotaggio sanno come intervenire».

Una nuova realtà della Fincantieri promossa dallo stesso ad Giuseppe Bono nell'ambito dell'ampliamento delle competenze. E che in una realtà anche come quella di Trieste ricca di competenze scientifiche di alto livello ha terreno fertile per crescere. Con Fincantieri che, dopo aver avuto un riconoscimento anche sul fronte della sicurezza dei dati pure dalla Marina militare Usa (con commesse miliardarie), è sempre più competitiva sul mercato delle tecnologie navali. —



Sopra, in alto una foto della plancia di una nave con tutti i sistemi tecnologici di controllo e navigazione, qui sopra a sinistra una foto aerea del palazzo della Marineria a Trieste dove ha sede il centro di cyber-security di Fincantieri e a destra l'ad Giuseppe Bono