SuperYacht24

Il quotidiano online del mercato superyacht

Massimo Centofanti (aizoOn) lancia l’allarme sul rischio cyber per gli yacht

Nicola Capuzzo · Tuesday, April 22nd, 2025

Massimo Centofanti è Ciso – consulente cyber security It/Ot, Dpo della pubblica amministrazione e del settore privato, ma soprattutto ethical hacker. Lavora come direttore della Divisione Cyber Security in aizoOn. Precedentemente direttore nei Security Operation Centers di varie infrastrutture critiche nel settore Oil & Gas e in altri settori industriali è membro permanente del tavolo dedicato alla cyber security presso la Camera di Commercio Americana e partecipa attivamente al gruppo di lavoro sulla cyber security di Anfia-Associazione Nazionale Filiera Industria Automobilistica. SUPER YACHT 24 lo incontra per parlare di quanto il settore nautico sia consapevole dei rischi derivanti dai cyber attack.

Direttore Centofanti, può darci una panoramica della divisione Cyber Security di aizoOn e di come si approccia al settore dei superyacht?

“Cyber aizoOn ha 18 anni di esperienza nella cybersecurity a livello globale. Nel momento in cui abbiamo fondato le sedi in Italia, il primo passo è stato coprire in Australia, poi negli Stati Uniti, e poi in Europa. Abbiamo voluto un taglio internazionale per poter garantire ai nostri più grandi clienti l’assistenza in qualsiasi parte del mondo operassero; questo ci permette inoltre di imparare, crescere e confrontarci con culture e realtà diverse. Esportare il nostro know-how ed acquisire quello di altri paesi, ci ha fatto conseguire competenze dominanti. La nostra è una multinazionale “scalabile” formata da 750 persone. La nautica, e in generale il settore marittimo, ci ha interessato fin dall’inizio: quella navale rappresenta infatti una delle nostre tre divisioni, insieme a quella aerospaziale (tra loro i punti in contatto sono molti), e della difesa; questo perché è un settore nel quale abbiamo riscontrato immaturità sotto il profilo della cybersecurity.”

Qual è lo stato dell’arte della cybersecurity nel settore marittimo?

“Oggi la nautica moderna è sempre più dipendente da tecnologie avanzate, come i sistemi di navigazione, comunicazione e automazione. Questa interconnessione aumenta la superficie di attacco cyber. C’è un problema di fondo: manca la cultura della sicurezza. Spesso, chi costruisce navi e sistemi di navigazione non è sufficientemente attento alla cybersecurity. Cito l’esempio del ragazzino di 15 anni che a gennaio scorso ha deviato navi nel Mediterraneo, sfruttando la vulnerabilità nei sistemi di navigazione. Questo dimostra che c’è un problema a monte: non stiamo proteggendo adeguatamente i sistemi.”

Perché c’è questa mancanza di attenzione alla cyber security nel settore marittimo?

“Mancano cultura e percezione del rischio. Molti produttori non hanno ancora sviluppato la capacità di creare oggetti cyber-sicuri. A differenza del settore automobilistico, che grazie a una norma europea emanata dall’UNESE impone alle case automobilistiche di mettere in sicurezza un veicolo e subordina la sua omologazione a test rigorosi di cybersecurity, nel settore marittimo questa imposizione non esiste. Esistono solo linee guida, come quelle dell’Imo, che vengono spesso disattese.”

Perché vengono disattese?

“Le linee guida Imo, ma anche gli standard Iacs E26 ed E27, non avendo un “controllo a valle” consentono ai manufatti prodotti di andare sul mercato senza essere effettivamente verificati sotto questo profilo. Adeguare gli yacht e le navi a queste linee e a questi standard permetterebbe un livello di resilienza molto più ampio, quantomeno sufficiente. Non adeguato, perché i sistemi di sicurezza non sono mai adeguati, poiché l’attaccante è sempre un passo avanti.”

Ci sono stati casi concreti di attacchi cyber nel settore della nautica da diporto?

“Sì, ci sono incidenti quotidianamente in tutto il mondo, anche in Italia. Molti non vengono riconosciuti come attacchi cyber, ma attribuiti a malfunzionamenti dei sistemi. Abbiamo anche lavorato a perizie forensi che hanno dimostrato come alcuni incidenti fossero stati causati da violazioni dei sistemi.”

Quali sono le motivazioni degli attacchi cyber nel settore nautico?

“Tipicamente, la motivazione è economica. Gli attaccanti bloccano i sistemi e chiedono un riscatto. Ci sono stati casi in cui i sistemi di navigazione degli yacht sono stati bloccati e i proprietari hanno pagato il riscatto.”

È possibile che i soccorsi esterni, come la guardia costiera, non siano sufficienti in caso di attacco cyber di questo tipo?

“Anche se si chiamano i soccorsi, lo yacht rimane bloccato. Il ripristino dei sistemi è un’operazione complessa e costosa, che richiede l’intervento di tecnici specializzati e può comportare costi di decine di migliaia di euro. Spesso, in queste situazioni, pagare un riscatto di 5.000-10.000 euro sembra quindi la soluzione più economica, ma questo non fa altro che alimentare il problema.”

Cyber aizoOn è coinvolta in iniziative per promuovere la consapevolezza e l’adozione di misure di cyber security nel settore?

“Sì, siamo attivi a livello istituzionale. In Europa, siamo in Exo, che è la associazione europea della cybersecurity che poi fa capo all’ Enisa e collabora con i governi per promuovere normative in questa direzione. Il problema è che spesso non veniamo ascoltati: i legislatori sono riluttanti a imporre obblighi onerosi alle aziende. Avere invece un sistema sicuro, e magari certificato, visto che oggi molti sistemi di questo tipo possono esserlo, è un valore aggiunto che dà anche un vantaggio commerciale all’azienda.”

Esistono normative specifiche in altri paesi?

“Sì, in Giappone, ad esempio, c’è una normativa stringente che impone alle aziende che producono dispositivi informatici per le navi di rispettare rigorosi standard di cybersecurity. Negli Stati Uniti, c’è un embrione di normativa in questa direzione. In Europa e nella maggior parte dei paesi del mondo questi apparati sarebbero già in parte normati dagli standard, ma il problema è che disattendiamo questi standard, che non rappresentano un obbligo, ma una facoltà.”

L’intelligenza artificiale influenza il panorama della cybersecurity nel settore nautico?

“Sì, complica le cose: gli attaccanti utilizzano l’AI per generare attacchi più sofisticati, difficili da identificare. La parte di applicazione dell’AI alla difesa attualmente non è matura quanto la parte di intelligenza artificiale applicata alla parte di attacco. Come aizoOn stiamo lavorando con l’intelligenza artificiale per produrre strumenti di monitoraggio e di protezione evolutivi. È un percorso irto di ostacoli, perché ancora molte tecnologie dell’AI non sono mature. Stiamo comunque sviluppando 6 tecnologie basate su Spac neural networks, quindi su intelligenza artificiale basata su quello che è la simulazione del cervello umano: una tecnologia estremamente promettente nell’ambito cyber security, anche se non ancora matura.

La mancanza di dati di addestramento sufficienti e la necessità di hardware specializzato e costoso rendono difficile implementare sistemi di sicurezza avanzati. Questa difficoltà si scontra con la diversa realtà degli attaccanti informatici, spesso legati a organizzazioni criminali o terroristiche, che dispongono di risorse nettamente superiori rispetto a chi si difende individualmente.”

Gli attacchi cyber nel settore nautico prendono di mira anche la sicurezza delle persone?

“Sì, e normalmente in questi casi, l’obiettivo non è bloccare il mezzo, ma usarlo come strumento per accedere alle informazioni private del proprietario. In altri casi, gli attacchi possono compromettere i sistemi di navigazione, creando situazioni pericolose per la sicurezza delle persone a bordo. Ad esempio, uno yacht potrebbe essere reso invisibile ai radar marittimi in zone di traffico intenso, ma anche potrebbe veder alterati i parametri del motore e portare a un incendio a bordo, oppure allo scoppio degli stessi motori: gli incidenti possibili sono davvero molti.

L’implementazione di sistemi di monitoraggio efficaci è essenziale per rilevare e rispondere tempestivamente a eventuali anomalie. La cyber security non è comunque una soluzione statica, ma un processo dinamico e continuo, che richiede una base solida di formazione e consapevolezza per l’equipaggio e il personale di bordo, oltre a un impegno costante nell’aggiornamento dei sistemi e delle procedure di sicurezza.

Investire nella formazione specializzata, implementare tecnologie di sicurezza all’avanguardia e aderire a standard internazionali riconosciuti rappresenta l’unica via percorribile per garantire la resilienza e la sicurezza operativa degli yacht nel lungo termine.”

Qual è il suo messaggio per il settore della nautica da diporto?

“Dobbiamo superare il problema di ordine culturale. Una spinta normativa aiuterebbe questo percorso di maturazione nel comprendere quanto sia importante la parte cyber. Se fossi il responsabile di un cantiere navale, sentendo che un quindicenne con le giuste competenze può dirottare una nave, credo che qualche seria riflessione sulla sicurezza dei miei prodotti la farei immediatamente”.

SUPER YACHT 24 È ANCHE SU WHATSAPP: BASTA CLICCARE QUI PER ISCRIVERSI AL CANALE ED ESSERE SEMPRE AGGIORNATI