SuperYacht24

Il quotidiano online del mercato superyacht

Privacy e sicurezza nello yachting: “La confidenzialità crescente e il rischio di cyber crimini”

Nicola Capuzzo · Wednesday, August 7th, 2024

Bruno Frati è amministratore delegato di My Dpo, società con sede a Livorno con una lunga esperienza nel settore della gestione della privacy e della sicurezza a supporto di aziende e professionisti che devono confrontarsi con la complessità delle normative europee e difendersi dai cyber criminali. Con lui SUPER YACHT 24 ha voluto parlare dei gravi rischi che incombono sul comparto dello yachting.

Quella degli attacchi informatici nel mondo dello yachting è un rischio reale con risvolti potenzialmente pesantissimi eppure nell’ambiente non se ne parla: come mai?

“E’ vero, forse si glissa per scaramanzia. A monte di un attacco c’è un’attività che parte dal controllo dei dati dai social, dal recupero di questi anche da altri data base e dalla loro integrazione. Unendo tutti questi dati vengono creati profili assolutamente compiuti che vengono utilizzati per attaccare soggetti che hanno la capacità di pagare grandi riscatti, con criptovalute non rintracciabili. Lo yachting, per la sua ricchezza, è naturalmente a rischio”.

E’ un problema italiano o più generalizzato quello della ‘non consapevolezza’ del rischio nello yachting?

“Direi che questa ‘non consapevolezza’ nasce dal fatto che percentualmente gli attacchi allo yachting sono ancora pochi rispetto a quelli attuati verso altri settori; questo perché i cyber criminali non hanno ancora messo bene a fuoco e preso di mira il settore e quello della yachting industries. Ma questa situazione sta cambiando, anche per l’estrema importanza delle cifre in gioco. C’è inoltre un problema di confidenzialità crescente dell’informazione legata a questi grandi progetti navali.”

Cosa intende con la confidenzialità crescente?

“L’ampliamento del settore lo rende sempre più visibile e quindi più nel mirino del cyber criminale. Per quanto intorno a proprietari e cantieri si lavori per circondarli della massima riservatezza a tutela della loro sicurezza, se un cyber criminale riesce a tracciare un dispositivo come uno smartphone e ad associarlo ad altri dati, può rivelarne non solo i dati sensibili a fini di riscatto, ma anche dove la persona si trovi fisicamente in un dato momento mettendone a rischio la

sicurezza.

La percezione è che il sistema di delega sia aggredibile, sia nella fase di costruzione che nella fase di gestione della governance della nave, perché basato sulla sensibilità delle singole persone.

Il comandante o l'information technology officer, soprattutto nel caso di figure senior attive da 30 o 40 anni, sono persone di grandissime capacità nella navigazione che però percepiscono molto poco l'importanza di questo tema. Per quanto riguarda l'armatore, credo invece che la sua attenzione sia più concentrata su aspetti orientati alla ricerca del massimo comfort e divertimento, perché convinto che per una materia altamente tecnica come la sicurezza informatica ci sia già nel team una figura specializzata in grado di seguirla.

Come detto ritengo che sia proprio in questo sistema di delega che viene a crearsi il problema, per la mancanza di sensibilità da parte dei soggetti apicali a bordo. Fortunatamente nel caso di comandanti più giovani, di 30-35 anni, il tema è decisamente più conosciuto e considerato."

Come può proteggersi efficacemente l'armatore?

"Sotto il profilo normativo in questo ambito, un po' come in ambito internet, in Italia e in Europa, in generale, esistono norme e regolamenti sulla materia – salvo per alcuni piccoli stati – e sanzioni che nel tempo sono state anche inasprite. Purtroppo però, questo tipo di attività non ha confini e i paesi più attivi e capaci in questo tipo di crimine provengono sostanzialmente dal medio e dell'estremo Oriente, quindi da aree in cui non esistono norme per attività criminali di tipo cyber, quindi per la polizia internazionale è molto difficile risalire ai responsabili.

Tutto ciò considerato ritengo che occorra mettersi preventivamente in una situazione di sicurezza passiva perché appunto, una volta che si è sotto attacco, gestire la situazione e, ancor più, risalire ai responsabili, 'è pura accademia'.

Credo invece che il tema sia preso in considerazione dai cantieri solo come un compito sul quale dovranno cominciare ad organizzarsi per essere pronti nel medio periodo, non ritenendolo un pericolo immediato. Questo è a mio avviso un grave problema perché gli hacker sono invece già al lavoro e in grado da subito di creare danni molto seri. Inoltre in un cantiere – essendo questo un'azienda che costruisce navi che data la loro complessità costituiscono altre aziende – la problematica si genera a catena".

Quanti superyacht oggi si tutelano da questo tipo di rischi con una propria business unit specializzata oppure con l'intervento di professionisti?

"Posso dirle che il potenziale di lavoro che ci sarebbe da svolgere in questo senso è enorme se anche consideriamo l'attività di assessment e verifiche del solo 10% della flotta esistente."

Oggi quali sistemi di sicurezza dati trovate a bordo nei vostri sopralluoghi?

"Attualmente tutto quello che riguarda questi aspetti viene posposto ad altre priorità. Per far fronte alla necessità del rispetto dei tempi di consegna dello yacht se manca un componente, si cerca e si installa quello che si trova, con il risultato di trovare prodotti scadenti montati su superyacht da 40 milioni di euro, il cui livello di sicurezza è talmente basso da consentire praticamente a chiunque di accedervi e visionare le immagini a totale discapito, nel migliore dei casi, della riservatezza dell'armatore.

Mettere in secondo piano i temi legati alla sicurezza digitale è un grave errore. Oggi fortunatamente non è facile per il cyber crimine accedere al governo dell'imbarcazione e prendere il controllo del mezzo, perché ancora la maggioranza dei sistemi di governo della nave non si interfacciano con la rete internet, ma molte aziende si stanno muovendo verso la guida della nave senza una persona fisica, in modalità remota, quindi temo che fra pochi anni il rischio aumenterà nettamente."

Come si può risolvere il problema visto che lo studio di soluzioni digitali avanzate sembra andare in parallelo a quello criminale che mira a intaccare la sicurezza di queste soluzioni?

"Non dobbiamo mai dimenticare che qualsiasi progetto informatico contiene il tema della sicurezza informatica. Spesso, anche per una questione culturale, si tende a pensare che una volta fatto l'investimento si sia a posto. Invece in questo campo, estremamente complesso, è fondamentale l'aggiornamento tempestivo del sistema."

La vostra società My Dpo, che ha fra i suoi clienti alcuni dei più grandi terminal portuali italiani, come ha approcciato allo yachting?

"Lavoriamo nello yachting da circa due anni, la nostra è un'attività quasi di studio, di approfondimento quotidiano di questo settore che riteniamo di dover approcciare cercando di curare pochi progetti con la massima attenzione. Il nostro è un metodo critico per verificare la bontà, sicurezza e affidabilità e i tempi di vita dei dispositivi, delle procedure, controlli e materiali utilizzati. Veniamo contattati per questo dall'armatore, o società di charter, o da cantieri e dialoghiamo con chi svolge per queste realtà un lavoro di ingegneria, oppure se questa figura non esiste, possiamo indicare al cliente una rosa di professionisti a cui, se vuole, potrà rivolgersi".

Dove possono essere riscontrati i maggiori rischi a bordo?

"Le potenziali fragilità a bordo possono essere rilevate in molti ambiti: da un sistema di propulsione ibrida che viene controllato e gestito da tecnologia internet – e lo stesso vale per la domotica – sempre più sviluppata a bordo nave. Sempre più spesso il proprietario di superyacht chiede spazi per lavorare a bordo con i suoi dispositivi rendendo l'esposizione al rischio di violazione di dati aziendali sempre più alta. Senza considerare poi i rischi dell'intelligenza artificiale che è un ulteriore arma molto affilata per gli attacchi di tipo cyber, in grado di aprire scenari davvero impressionanti."

Quali priorità si avvertono nel campo del charter?

"Nelle fasi intermedie di cambio periodico di ospiti sul superyacht è necessaria una serie di attività di 'bonifica' digitale con cambi di password. Considerando i tempi stretti che caratterizzano queste attività a bordo dovrebbe essere presente una persona esperta che segua questo tipo di lavoro redigendo una precisa checklist e studiando un sistema di password che ogni settimana crei nuovi codici di accesso con procedure rapide e sicure. Per questioni di tempi le password del wi.fi di bordo spesso non vengono sostituite con il rischio che le persone che ne erano titolari trovandosi successivamente nelle vicinanze dello stesso yacht potrebbero continuare a vedere dai loro smartphone tutte le reti di bordo. In questo caso una persona esperta e malintenzionata saprebbe come approfittarne.

Tutto questo fa capire che lo yachting, inteso nel suo complesso, è un settore altamente sofisticato nel quale nulla può essere tralasciato e dove la sicurezza informatica è ormai, ben più di un

dettaglio”.

ISCRIVITI ALLA NEWSLETTER GRATUITA DI SUPER YACHT 24

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

This entry was posted on Wednesday, August 7th, 2024 at 5:00 pm and is filed under Services, Suppliers
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.