Quanto rischia una nave per un attacco informatico?

Dic 13, 2018 Marco Schiaffino News, RSS, Scenario 0

I sistemi iper-tecnologici di navigazione e gestione dei natanti sono esposti come qualsiasi PC. Il rischio è che un incidente porti a veri e propri disastri.

La tecnologia rende tutto più facile, anche quando ci si trova a traversare il globo per mare. Il rovescio della medaglia di strumenti di navigazione automatici e sistemi di comunicazione satellitari è però la loro vulnerabilità agli attacchi informatici.

Per farsi un'idea dei rischi che corrono le navi moderne quando "incocciano" in un malware, basta leggersi l'interessantissimo paper dal titolo "The Guidelines on cyber Security Onboard Ships", che può essere scaricato da questa pagina Web.

Il documento, oltre a fissare le policy a cui gli operatori si dovrebbero attenere, elenca **una serie di incidenti di sicurezza** avvenuti nel recente passato che possono dare l'idea di quanto la cyber-security sia diventata importante anche in questo settore.

I dispositivi più vulnerabili agli attacchi, e più "critici" dal punto di vista di chi deve garantire la sicurezza, sono naturalmente quelli relativi alla navigazione. Come abbiamo già visto in un precedente articolo, infatti, si tratta di sistemi delicati il cui malfunzionamento può provocare davvero grossi guai.

Uno dei casi citati nel paper riguarda una nave che è rimasta

bloccata per giorni prima di poter prendere il mare a causa di un malware che aveva messo K.O. il sistema **ECSID (Electronic Chart Display and Information System)** per la navigazione.

Nel caso specifico, infatti, si trattava di una imbarcazione "paperless", cioè per la quale **non era nemmeno prevista la presenza a bordo di cartine tradizionali**. Se l'incidente si fosse verificato nel corso della navigazione, sarebbero stati guai grossi.

Ma quali sono i vettori di infezione più comuni che portano a incidenti di sicurezza in questo settore? A guardare la casistica riportata nel documento, le email sono in ogni caso uno degli anelli deboli, ma un particolare rilievo viene posto sulle **chiavi di memoria USB**.

In due casi citati, infatti, la minaccia proveniva esattamente dall'uso di unità esterne collegate ai sistemi IT delle imbarcazioni. Il primo riguarda una nave che ha subito un'infezione a causa diun malware "importato" da **un ispettore**

portuale che ha utilizzato un computer per stampare dei documenti.

Nel secondo caso, l'infezione tramite USB aveva come origine una procedura di installazione di un software. In quel caso il malware, un trojan residente in memoria programmato per agire non appena fosse riuscito a contattare il **server Command and Control**, era finito su un sistema che per motivi di sicurezza non era mai stato collegato a Internet.

In seguito al suo rilevamento, i ricercatori hanno stabilito che **il malware era rimasto "dormiente" nel sistema per la bellezza di 875 giorni**.

Se in quel periodo di tempo fosse stata attivata la connessione a Internet del dispositivo (si trattava di un sistema di gestione dell'energia elettrica che prevedeva la possibilità di **ricevere aggiornamenti via Internet**) le cose sarebbero potute andare molto diversamente.

Please follow and like us:

Truffa da 1 milione di dollari a Save the Children
L'operazione Sharpshooter prende di mira bersagli di alto livello

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2018/12/13/quanto-rischia-una-nave-per-un-attacco-informatico/