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

NAVAL DOME CONCLUDE IL PROGETTO DI CYBER SECURITY A BORDO DI IMPIANTI DI PERFORAZIONE OFFSHORE

La **Naval Dome** esperta di difesa informatica ha completato un progetto per identificare e mitigare i rischi informatici comuni alle piattaforme di trivellazione offshore.

I risultati del progetto biennale, culminato nell'installazione e nei test pilota del sistema di difesa informatica Endpoint di Naval Dome a bordo degli impianti di perforazione nel Golfo del Messico, indicano che i regolamenti e le tecniche di sicurezza non sono al passo con l'attuale tecnologia della piattaforma, requisiti di connettività e metodologia di attacco informatico.

In un documento di ricerca congiunto presentato a una conferenza sulla tecnologia offshore a Houston la scorsa settimana, gli autori affermano: *"Le attività in due anni hanno dimostrato carenze e sfide reali che devono essere affrontate se vogliamo creare un ambiente di perforazione in acque profonde più sicuro dal punto di vista informatico. ."*

Nel presentare il documento *Cyberdefence of Offshore Deepwater Drilling Rigs* ai delegati della conferenza, Adam Rizika, Head of Strategy, Naval Dome, ha dichiarato: *"Laddove i sistemi installati su piattaforme offshore erano stati tradizionalmente isolati e non collegati, limitando il successo dell'hacking informatico, l'aumento del monitoraggio remoto e il controllo autonomo, l'IOT e la digitalizzazione hanno reso le piattaforme molto più suscettibili agli attacchi".*

Passando a rivelare come le reti OT (tecnologia operativa) dei banchi di prova sono state penetrate utilizzando un file di installazione del software per il posizionamento dinamico (DP) e i grafici delle workstation, Rizika, ha spiegato che Naval Dome ha simulato un tecnico dell'assistenza OEM utilizzando inconsapevolmente una chiavetta USB con software contenente tre exploit zero-day.

"Il file modificato è stato confezionato in un modo che sembrava e si comportava come quello originale e ha superato la scansione antivirus senza essere identificato come un attacco informatico o rilevato dal sistema di monitoraggio del traffico della rete informatica installato", ha affermato.

Sebbene l'attacco sia stato effettuato internamente, Rizika ha notato che l'esecuzione remota era fattibile utilizzando le connessioni di rete rivolte verso l'esterno del rig.

"I test di penetrazione hanno confermato come un attacco informatico mirato a un impianto di perforazione in acque profonde potrebbe provocare un grave incidente di sicurezza del processo, con un impatto finanziario e reputazionale associato", ha affermato.

Nel documento, gli autori affermano che i test pilota confermano che le tradizionali soluzioni di sicurezza informatica OT "tipo perimetro" trapiantate dall'IT, come antivirus, monitoraggio della rete e firewall, non sono sufficienti per proteggere la sicurezza critica e le apparecchiature di elaborazione dagli attacchi, lasciando le piattaforme vulnerabile.

"È evidente che sono necessarie soluzioni mirate più avanzate per proteggere meglio una piattaforma offshore dall'esposizione ad attacchi informatici esterni e interni, mirati o meno", ha riferito Rizika.

Il documento prosegue evidenziando una carenza di personale specializzato nel dominio informatico OT, regolamenti e controlli che sono lenti ad evolversi e ad essere implementati, un approccio incentrato sull'IT applicato a un ambiente OT e una discrepanza tra i sistemi e le attrezzature delle piattaforme di perforazione e i loro software di supporto.

Rizika ha dichiarato: *"Sebbene le linee guida e le normative del settore offrano requisiti standard minimi, abbiamo riscontrato che il progresso nella tecnologia degli impianti di perforazione, nella connettività e nella metodologia di attacco informatico ha superato le normative, determinando la necessità di un approccio più completo".*

Commentando i risultati del progetto, l'amministratore delegato di Naval Dome Itai Sela, ha dichiarato: "Il progetto e i test pilota di successo di una soluzione di difesa informatica multistrato a bordo di queste piattaforme hanno dimostrato che sia i sistemi OEM nuovi che quelli legacy possono essere protetti meglio da interni e vettori di attacchi informatici esterni, senza la necessità di costosi aggiornamenti delle apparecchiature o costi generali più elevati che comportano un aumento del costo totale di proprietà.

"I risultati fino ad oggi dimostrano che il sistema endpoint è robusto e può funzionare senza interferire con le operazioni di rig in corso. Il costo dell'aggiornamento dei sistemi obsoleti è elevato e, anche se vengono effettuati aggiornamenti, le vulnerabilità possono comunque rimanere".