Cyber

Mosaic warfare. Così l'Iot trasforma il campo di battaglia

In un mondo sempre più interconnesso, procede la crescita dei sistemi di Internet of things (Iot) a livello globale. Questi sono presenti anche nel mondo militare, con l'acronimo Iobt, una rete di dispositivi che permette di aumentare la consapevolezza situazionale degli operatori impegnati sul campo e che trova applicazione nel C5isr e nel multidominio

MARCO BRACCIOLI
co-direttore Cybersec initiatives Fondazione Icsa e vice presidente Defense & cybersecurity DigitalPlatforms spa

La crescita dei sistemi di Internet of things connessi in rete continua inarrestabile. Nel 2020 sono stati censiti circa cinquanta miliardi di *device* Iot a livello globale progettati per essere connessi a una rete informatica (tra cui, ma non solo, Internet). Questi strumenti devono essere identificabili, manutenuti e monitorati dalle unità di sicurezza nelle grandi aziende e nelle grandi organizzazioni. Alcuni (pochi) di questi prodotti Iot comunicano una misurazione di informazioni di base al produttore del *device* stesso, o ricevono degli aggiornamenti sul *software*. Nella gran parte dei casi ciò è impossibile e il cliente finale IT non sa nemmeno che essi esistono sulla sua rete.
Il rovescio della medaglia è però un'espansione della superficie di attacco da parte di attori malevoli che intendono aggredire le infrastrutture critiche.
Tali attori possono utilizzare i *device* come porte di ingresso e, una volta all'interno della rete, possono muoversi alla ricerca di *account* e dati di valore.
Dopo essere entrati su ogni strumento Iot della rete possono, attraverso un Tcpdump, un comune strumento per il *debug* delle reti, intercettare tutto il traffico della rete e delle sottoreti locali, una pratica detta "sniffing". I *device* Iot hanno molte applicazioni: dai sistemi di gestione urbani alla sanità, dalle industrie ai servizi di pubblica utilità come gas, acqua, elettricità e trasporto. In una parola, sulle infrastrutture critiche. Questi *device embedded* non possono essere protetti con la tecnologia basata sugli *agent*: molto spesso non sono aggiornati o configurati correttamente e i responsabili della sicurezza delle reti necessitano di nuove strategie per mitigare. Una scelta per le installazioni di Iot di nuova generazione può essere la "Custom Iot", dotata di un *software* originale a bordo prodotto esclusivamente per un determinato gestore di un'infrastruttura critica.
Quale approccio, dunque, si può utilizzare per affrontare questi rischi? Innanzitutto bisogna proteggere i processi strategici. Non si può difendere tutto, ma si può irrobustire la tutela dei processi più importanti. Poi serve mappare il terreno digitale, dalla rete interna alle terze parti e i manutentori con accesso remoto. Poi è necessario analizzare il rischio, valutando vulnerabilità attraverso modelli di *threat intelligence* o *red-team* che cercano altri vettori di attacco. Infine, mitigare e proteggere, riducendo il numero degli *entry point*, usando *policy* di accesso *zero trust* e segregando i *device* Iot dalle altre reti.
Da ultimo, serve deviare tutti gli *alert* verso il Centro per la sicurezza delle operazioni (Soc) e poi verso i sistemi Security information and event management (Siem) e l Security orchestration, automation and

Come difendersi?

I *device embedded* non possono essere protetti con la tecnologia basata sugli *agent*: molto spesso non sono aggiornati o configurati correttamente e i responsabili della sicurezza delle reti necessitano di nuove strategie per mitigare. Una scelta per le nuove installazioni di Iot di nuova generazione può essere la "Custom Iot", ovvero una Iot con un *software* originale a bordo prodotto esclusivamente per un gestore di infrastruttura critica.

Quali sono le applicazioni militari?

L'implementazione della capacità C5ISR e l'implementazione di sistemi logistici per l'impiego di sensori montati su aerei, Uav, satelliti e navi. L'Internet of battlefield things sarà utile anche per monitorare le condizioni fisiche dei soldati con sensori incorporati nei corpetti antiproiettile, negli elmetti e nei tessuti speciali delle uniformi. Servirà inoltre a svolgere attività di manutenzione predittiva dei vari dispositivi attraverso l'analisi dei *big data* con l'aiuto di applicazioni IA.

response (Soar) per rispondere rapidamente agli incidenti. Gli Iot, del resto, sono presenti anche nel mondo militare, con l'acronimo Iobt (Internet of the batterfield things), una rete di dispositivi che permette di aumentare la consapevolezza situazionale degli operatori impegnati sul campo. Attraverso un sistema di sensori interconnessi in grado di restituire dati e informazioni utili, questi dispositivi garantiscono una percezione dell'ambiente circostante aumentando così le capacità di Intelligence, sorveglianza e ricognizione e implementando contestualmente i sistemi di identificazione amico/nemico (Iff).
Tra le principali applicazioni militari fondamentali c'è la capacità di Comando, controllo, computer, comunicazioni, *cyber*, Intelligence, sorveglianza e ricognizione (C5isr) e l'implementazione di sistemi logistici per l'impiego di sensori montati su aerei, droni, satelliti e navi. L'Iobt sarà utile anche per monitorare le condizioni fisiche dei soldati con sensori incorporati nei corpetti antiproiettile, negli elmetti e nei tessuti speciali delle uniformi. Servirà inoltre a svolgere attività di manutenzione predittiva dei vari dispositivi attraverso l'analisi dei *big data* con l'aiuto di applicazioni IA. Non meno interessante è il tema dell'Ocean of things (Oot), un programma della Darpa americana che mira a consentire una consapevolezza della situazione marittima persistente su vaste aree oceaniche. Questo programma agisce dispiegando migliaia di piccoli galleggianti a basso costo che potrebbero formare una rete di sensori distribuita e orientata allo studio delle scie di navi militari. Nel mondo militare le Iot devono lavorare, inoltre, nel multidominio: terra, mare, aria, spazio e *cyber*. La chiave per la supremazia militare del futuro consisterà nell'abilità di poter rendere scalabile un ecosistema connesso per supportare non solo le operazioni di una singola Forza armata, ma anche quelle interforze e con le coalizioni alleate. Da queste considerazioni si afferma sempre più come modello quello del "Mosaic warfare": un'espressione, questa, utilizzata per spiegare un approccio di "sistema di sistemi", promosso come tecnica per confondere e sopraffare le forze avversarie schierando strumenti tecnologici adattabili, a basso costo, che svolgeranno più ruoli e coordineranno le azioni tra di loro, complicando così il processo decisionale per il nemico. Si sta, dunque, prefigurando uno scenario di campo di battaglia a maglia, con milioni di nodi che informano i decisori di strategie e tattiche, che si uniranno alle nuove tecnologie *disruptive* quali IA e *quantum computing*.