Domenico Dominoni (*)

Proteggere i sistemi cyber-fisici: una priorità

Dal 2022 a oggi il mondo è profondamente cambiato. Le ripercussioni della guerra in Ucraina hanno, infatti, dato il via a una crisi a livello umanitario con implicazioni di portata internazionale. Tali ripercussioni hanno causato anche l'impennata dei prezzi e le interruzioni della catena di approvvigionamento in tutti i settori, dall'agricoltura, ai beni di consumo, al petrolio greggio. Il tutto è stato accompagnato da un significativo incremento degli attacchi informatici, che hanno preso di mira in particolare le infrastrutture critiche e l'Italia è tra i paesi più colpiti. Questa crescente ondata di minacce è stata possibile anche grazie al fatto che la trasformazione digitale sta accelerando. Gli asset, un tempo isolati, sono oggi sempre più connessi e le reti stanno convergendo man mano che aumenta l'adozione di sistemi cyber-fisici (CPS) sempre più diversificati.

(*) Director of Sales South Europe di Claroty **www.claroty.com**

Con circa 17 miliardi di dispositivi IoT connessi, l'adozione di nuovi paradigmi per la protezione dei sistemi cyber-fisici è una priorità

Attualmente ci sono tra i 15 e i 17 miliardi di dispositivi IoT connessi e si prevede un raddoppio nei prossimi 24 mesi. Nel corso del 2024, questo vasto numero di dispositivi genererà oltre 80 miliardi di connessioni IoT, il 70% delle quali sarà in settori di infrastrutture critiche. Gartner stima, inoltre, che entro il 2025 il 60% dei CIO delle aziende ad alta intensità di asset aumenterà i propri investimenti nell'integrazione IT/OT e che entro il 2026 oltre il 70% degli investimenti in nuovi asset industriali incorporerà funzionalità di progettazione intelligente.

XIoT ...a tre condizioni

Prevediamo che nel 2024 le reti convergenti XIoT diventeranno la norma in tutti i settori delle infrastrutture critiche. Perché una rete XIoT possa essere virtuale e convergente è necessario, però, il rispetto di tre precondizioni: 1) conoscenza approfondita dei modelli di traffico "noti come validi" per capire come le risorse dovrebbero essere rese operative in modo sicuro; 2) capacità di rilevare violazioni delle policy note e valide, in modo tale che le patch temporanee comuni possano rimanere temporanee; 3) capacità di rendere operativa la segmentazione attraverso firewall, NAC e micro-segmentazione per rafforzare i canali e garantire certezza nelle comunicazioni di rete.

Questo approccio diventerà la nuova normalità, per questo sarà fondamentale consentire alle organizzazioni di sfruttare i sistemi cyber-fisici (CPS) in modo sicuro. In tal senso la gestione tradizionale delle vulnerabilità non è più applicabile ai moderni sistemi. Il divario tra le vulnerabilità dei CPS divulgate, corrette e sfruttate, infatti, si sta allargando inesorabilmente e la rapida evoluzione e introduzione dei CPS in settori critici non fa che peggiorare la situazione.

Quasi il 70% delle vulnerabilità CPS divulgate lo scorso anno ha ricevuto un punteggio CVSS v3 di "alto" o "critico", ma da allora meno dell'8% di esse è stato sfruttato. I team di sicurezza che seguono queste raccomandazioni spesso non solo sono sopraffatti, ma potrebbero anche indirizzare erroneamente le risorse verso le vulnerabilità che hanno meno probabilità di essere sfruttate, trascurando quelle che invece ne hanno maggiore probabilità[1].

[1] In un recente sondaggio di Claroty, più del 78% dei professionisti della sicurezza, dell'IT e dell'ingegneria del settore sanitario hanno dichiarato che l'applicazione di patch alle vulnerabilità nei CPS clinici è la lacuna più significativa nelle difese informatiche. Il 63% delle vulnerabilità sfruttate note nel catalogo KEV della CISA si riscontra sulle reti sanitarie, mentre il 23% dei dispositivi medici, inclusi i dispositivi di imaging, i dispositivi IoT clinici e i dispositivi chirurgici, presenta almeno una vulnerabilità sfruttata nota. La situazione si aggrava ulteriormente negli ambienti che sfruttano CPS mission-critical con lunghi periodi di ammortamento. L'applicazione di patch è spesso vietata, soprattutto quando si tratta di dispositivi medici connessi e sistemi di controllo industriale, perché questi ambienti non sono in grado di tollerare i tempi di inattività né di assorbire il rischio potenziale che una nuova patch potrebbe introdurre nei sistemi adiacenti.

Sicurezza predittiva e zero trust

Nei prossimi anni la gestione delle vulnerabilità dovrà imprescindibilmente evolversi per sfruttare nuovi paradigmi. Questo è il motivo per cui le organizzazioni di infrastrutture critiche accelereranno l'adozione di metodologie di sicurezza predittiva e approcci Zero Trust per apportare miglioramenti nelle loro difese informatiche. Lo status quo del punteggio di vulnerabilità sarà sostituito con un modello di punteggio che prevede quali vulnerabilità gli aggressori utilizzeranno come arma. Queste informazioni consentiranno alle aziende di prendere decisioni più efficienti in termini di priorità, correzione e gestione complessiva del rischio. Anche l'accesso alla rete Zero Trust sarà fondamentale nel tentativo di proteggere le reti fino ai livelli più granulari di utenti, macchine e carichi di lavoro, ma soprattutto man mano che le fabbriche e altre applicazioni diventano più autonome, gli approcci zero-trust forniranno la copertura necessaria per garantire che i servizi non vengano interrotti o manipolati. Per avere successo nell'implementazione di questi controlli di compensazione, le organizzazioni devono avere una buona comprensione dei criteri di sicurezza "noti validi" di come i CPS dovrebbero comunicare con altre risorse nell'ambiente.

AI = arma o difesa?

Non bisogna tralasciare, inoltre, il fatto che i criminali informatici stanno trasformando l'AI in un'arma. Ne sono un esempio concreto i sofisticati strumenti utilizzati dai cyber criminali cinesi per violare il CPS in una base militare statunitense a Guam. Secondo un recente rapporto del DHS degli Stati Uniti, l'incidente di Guam è la dimostrazione della tendenza di sfruttare le tecnologie emergenti, come l'intelligenza artificiale, impiegate all'interno del CPS per sferrare attacchi informatici. La stessa Gartner stima che entro il 2025 gli attacchi che sfruttano l'intelligenza artificiale costringeranno le organizzazioni ad abbassare le soglie per il rilevamento di attività sospette, generando più falsi allarmi. Al tempo stesso, però, si prevede che entro il 2027 l'AI generativa contribuirà a una riduzione del 30% dei tassi di falsi positivi per i test di sicurezza delle applicazioni e il rilevamento delle minacce, perfezionando i risultati nell'individuazione di eventi dannosi.

Possiamo affermare, quindi, che l'AI generativa migliorerà la resilienza informatica e operativa dei sistemi cyber-fisici. Questo permetterà, inoltre, di contrastare la velocità e la sofisticazione con le quali i malintenzionati stanno armando l'AI contro i CPS. L'automazione dei principali flussi di lavoro operativi e di sicurezza, la preventiva visibilità sull'intera superficie di attacco XIoT e la possibilità di prevenire eventuali attacchi sono solo alcuni degli ambiti nei quali l'AI potrà guidare la resilienza di questi asset e dei sistemi critici verso il futuro.

Miniglossario

XIoT (Extended Internet of Things) = tutti gli asset connessi alla base dei sistemi CPS (Cyber-Physical Systems)

OT (Operational Technology) = hardware e software per monitorare e controllare processi fisici, dispositivi e infrastrutture

Sicurezza OT = misure e tecnologie per proteggere persone, risorse e informazioni; monitorare e/o controllare dispositivi fisici, processi ed eventi ed avviare cambiamenti di stato nei sistemi OT aziendali (Gartner)