TEAM82 DI CLAROTY IN UNA NUOVA RICERCA RIVELA I RISCHI LEGATI AGLI ACCESSI DA REMOTO PER GLI ASSET OT MISSION-CRITICAL.

Claroty potenzia la propria soluzione di accesso remoto per garantire la protezione delle operazioni sui sistemi cyber-fisici.

Milano, 21 maggio 2024 – Claroty, azienda specializzata nella protezione di sistemi cyber-fisici (CPS), attraverso il Team82, il proprio pluripremiato gruppo di ricercatori, ha condotto un nuovo studio che rivela che il 13% degli asset di tecnologia operativa (OT) mission-critical dispone di una connessione Internet poco sicura. Inoltre, i dati di Claroty evidenziano che il 36% di queste risorse presenta almeno una vulnerabilità sfruttata nota (KEV), rendendole accessibili da remoto e facilmente sfruttabili da parte di malintenzionati con il fine di interrompere le operazioni. Per far fronte a questi rischi, alimentati dall'adozione crescente di tecnologie di accesso remoto negli ambienti CPS, Claroty ha lanciato il nuovo xDome Secure Access (prima conosciuto come Secure Remote Access). Questa soluzione è in grado di bilanciare un accesso agevole con un controllo sicuro sulle interazioni con i CPS, migliorando così la produttività, riducendo le complessità e i rischi e garantendo la conformità sia per gli utenti proprietari che di terze parti.

Secondo Gartner, "le tecnologie CPS (spesso identificate, in modo intercambiabile, come OT/IoT/IIoT/ICS/IACS/SCADA, ecc.), che supportano i processi produttivi o mission-critical, sono state inizialmente pensate per rimanere isolate, con il tempo, però, sono diventate sempre più connesse tra loro e con i sistemi aziendali. Inoltre, le organizzazioni oggi hanno bisogno di OEM, appaltatori e dipendenti per operare, mantenere e aggiornare tali dispositivi da remoto".[1]

Per chiarire quali sono le implicazioni di sicurezza legate a questa maggiore connettività, Team82, il pluripremiato gruppo di ricercatori Claroty, ha analizzato un campione di oltre 125.000 asset OT, la loro connessione a Internet e la loro sfruttabilità. Ecco alcuni dei principali risultati emersi:

- **Il 3,7% di tutte le risorse OT esaminate ha una connessione Internet non sicura**, ovvero comunica genericamente con Internet, escluse le comunicazioni di sicurezza unidirezionali, del produttore e degli endpoint. Questo consente agli aggressori di scansionare facilmente lo spazio degli indirizzi IP per trovare e tentare di accedere alle risorse da remoto.

[1] Gartner, Innovation Insight: CPS Secure Remote Access Solutions, Katell Thielemann, Abhyuday Data, Wam Voster, 18 April 2024. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

- **Il 13% delle engineering Workstation (EWS) e delle interfacce uomo-macchina (HMI) ha una connessione Internet poco sicura.** Queste risorse fondamentali sono utilizzate per monitorare, controllare e aggiornare i sistemi di produzione. Poiché possono connettersi sia a monte che a valle dell'architettura Purdue Model per ICS, e in alcuni casi alla rete IT, gli aggressori possono utilizzarle come punto di appoggio iniziale per muoversi all'interno dei sistemi aziendali.

- **Il 36% degli EWS e degli HMI con una connessione internet poco sicura presenta almeno una KEV.** La combinazione di alta criticità, alta esposizione e alta sfruttabilità rende questi asset obiettivi primari per i malintenzionati che cercano di massimizzare le interruzioni operative.

"La nostra ricerca avvalora l'idea che l'aumento degli accessi da remoto si traduce inevitabilmente in un'estensione della superficie di attacco e in un maggiore rischio di interruzione per le infrastrutture critiche, con un conseguente impatto sulla sicurezza pubblica e sulla disponibilità di servizi vitali", ha dichiarato **Amir Preminger, Vice President of Research del Team82 di Claroty**. "*Poiché l'accesso remoto agli asset OT mission-critical, come EWS e HMI, è ora diventato uno standard, le aziende devono assicurarsi di essere attrezzate per concedere l'accesso a specifici asset in modo intenzionale e su base privilegiata*".

Tutti i dati rilevati dal Team82 sono contenuti nel report: "An Open Door."

Bilanciare un accesso senza restrizioni e un controllo sicuro

Secondo Gartner, "Sebbene [la gestione, la manutenzione e l'aggiornamento dei CPS da remoto] siano state storicamente effettuate con approcci basati su VPN e jump-server, questi si sono rivelati sempre più insicuri e complessi da gestire. Le vulnerabilità delle VPN si sono moltiplicate negli ultimi anni, portando a direttive di sfruttamento e di emergenza come la ED-24-01 della CISA.1. Inoltre, la maggior parte delle VPN fornisce ampio accesso alla rete e gli sforzi per limitare tale accesso a un livello più granulare portano a una supervisione costosa e complessa".[2]

Per affrontare le sfide di sicurezza uniche e complesse imposte dall'aumento degli accessi remoti ai CPS, Claroty ha appositamente progettato la soluzione xDome Secure Access, che soddisfa le specifiche esigenze del dominio OT. xDome Secure Access garantisce il giusto equilibrio tra accesso senza restrizioni e controllo sicuro delle interazioni di terze parti con i CPS, migliorando così la produttività, riducendo le complessità e i rischi e garantendo la conformità sia per gli utenti proprietari che di terze parti. Integrando principi di sicurezza fondamentali, come Identity Governance and Administration (IGA), Privileged Access Management (PAM) e Zero Trust Network Access (ZTNA), xDome Secure Access stabilisce nuovi standard di resilienza ed eccellenza operativa nel panorama CPS.

[2] Gartner, Innovation Insight: CPS Secure Remote Access Solutions, Katell Thielemann, Abhyuday Data, Wam Voster, 18 April 2024.

I principali vantaggi di questa soluzione includono:

- **Aumento della produttività:** l'accesso senza soluzione di continuità per gli utenti, sia di primo che di terzo livello, riduce efficacemente il tempo medio di riparazione (MTTR), facilitando una più rapida risoluzione dei problemi, operando in condizioni di bassa larghezza di banda, assicurando un'elevata disponibilità del sistema e sostenendo la sopravvivenza dei siti critici.

- **Riduzione del rischio**: la soluzione incorpora un framework Zero Trust su misura, funzionalità PAM e IGA per migliorare la gestione degli incidenti, i controlli degli accessi e il monitoraggio del sistema, riducendo al minimo i rischi e salvaguardando le risorse critiche. In questo modo le aziende possono gestire e governare l'intero ciclo di vita dell'identità, dall'avvio al ritiro, con la massima precisione e sicurezza.

- **Riduzione della complessità**: una riduzione significativa della complessità amministrativa, grazie a un'architettura scalabile e gestita dal cloud, offre la flessibilità necessaria per operare senza problemi sia on-premises che nel cloud. La soluzione semplifica, inoltre, le attività amministrative che richiedono un controllo operativo costante, integrandosi perfettamente con gli strumenti di Identity and Access Management (IAM), migliorando la gestione delle identità e consentendo il coordinamento centralizzato dei plant e la creazione di policy.

- **Mantenere la conformità**: La soluzione aderisce ai principali standard di conformità e fornisce i controlli necessari per la registrazione e la verifica in tempo reale delle identità degli utenti, fondamentale per mantenere audit trail completi e soddisfare i requisiti normativi, proteggendo l'azienda da potenziali sanzioni legali e finanziarie.

"*Un facile accesso ai CPS industriali è essenziale per massimizzare i risultati aziendali, ma molte risorse OT sono state storicamente progettate senza pensare alla sicurezza. Un accesso sicuro e protetto ai CPS richiede funzionalità precise di gestione degli accessi, gestione delle identità, accesso privilegiato e governance delle identità, il tutto realizzato per rispettare i rigorosi requisiti operativi, i vincoli ambientali e la tolleranza al rischio tipici degli ambienti OT. Ogni accesso a una risorsa OT è privilegiato per definizione, poiché può potenzialmente avere un impatto sulla sicurezza e sulla disponibilità*", ha affermato **Grant Geyer, Chief Product Officer di Claroty**. "*xDome Secure Access non solo permette un facile accesso per massimizzare la produttività, ma lo fa garantendo una sicurezza integrata, invisibile all'operatore, fondamentale per la salvaguardia delle infrastrutture critiche*".

Maggiori informazioni su Claroty xDome Secure Access sono disponibili:

- Consultando il documento Claroty xDome Secure Access solution overview o il seguente blog
- Registrandosi al webinar, "Zero Trust Meets Privileged Access for Enhanced Operational Resilience," del 13 giugno 2024 alle 11:00 a.m. EDT

Claroty

Claroty è specializzata in soluzioni di sicurezza volte a proteggere i sistemi cyber-fisici in ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT): il cosiddetto Extended Internet of Things (XIoT). La piattaforma unificata dell'azienda si integra con l'infrastruttura esistente dei clienti per fornire una gamma completa di controlli per la visibilità, la gestione dei rischi e delle vulnerabilità, il rilevamento delle minacce e un accesso sicuro da remoto. Supportate dalle più grandi società di investimento e provider di automazione industriale del mondo, le soluzioni Claroty vengono distribuite da centinaia di organizzazioni in migliaia di siti in tutto il mondo. La società ha sede a New York e filiali in Europa, Asia-Pacifico e America Latina. Per maggiori informazioni: www.claroty.com

Ufficio Stampa

Meridian Communications Srl

Via Cuneo, 3 – 20149 Milano Tel. +39 02 48519553

Silvia Ceriotti	335 7799816	silvia.ceriotti@meridiancommunications.it
Viviana Bandieramonte	329 4776937	viviana.bandieramonte@meridiancommunications.it
Ilaria Malgrati	339 2143042	ilaria.malgrati@meridiancommunications.it