Fonte: foto Shutterstock

I Cybersecurity Performance Goal pubblicati da Cisa stabiliscono delle priorità in ambito di sicurezza informatica IT e OT e forniscono una pratica 'lista di controllo'

LA SICUREZZA IN 5 PUNTI

I 5 ASPETTI PIÙ RILEVANTI DEI CPG (CYBERSECURITY PERFORMANCE GOAL) PUBBLICATI DA CISA: UNA GUIDA PER AIUTARE LE AZIENDE DI PICCOLE DIMENSIONI E CON POCHE RISORSE A STABILIRE LE PRIORITÀ IN AMBITO DI SICUREZZA INFORMATICA E RIDURRE I RISCHI

A cura di Grant Geyer

Sono stati recentemente pubblicati da Cisa (Cybersecurity Infrastructure & Security Agency) i 'Cybersecurity Performance Goal', ossia un insieme di pratiche e linee guida IT e OT trasversali, per aiutare le aziende di piccole dimensioni, e con meno risorse, a stabilire le priorità in ambito di sicurezza informatica e ridurre i rischi. I CPG potrebbero diventare una guida preziosa per la sicurezza informatica e una lista di controllo per chi gestisce delle infrastrutture critiche, molte delle quali, appartenenti al settore privato, sono di piccole o medie dimensioni. Alcune di queste realtà, infatti, servono comunità relativamente ristrette, fornendo acqua o elettricità, mentre altre più grandi si occupano della gestione delle condutture vere e proprie.

Sebbene la protezione delle infrastrutture critiche sia un argomento molto complesso, sia dal punto di vista politico, sia da quello della sicurezza informatica, Cisa e altre istituzioni del settore hanno evidenziato una forte carenza di risorse, che contribuisce a ostacolare gli sforzi messi in campo da queste aziende. I CPG da soli non possono risolvere questa problematica,

ma sicuramente le pratiche economicamente vantaggiose, orientate ai risultati e facilmente attuabili in essi contenute, rappresentano un valido contributo per le aziende. Nello specifico, Claroty si è concentrata su 5 aspetti molto importanti legati ai nuovi CPG. Vediamoli.

1. Un aiuto per l'implementazione del Nist Cybersecurity Framework (CSF)

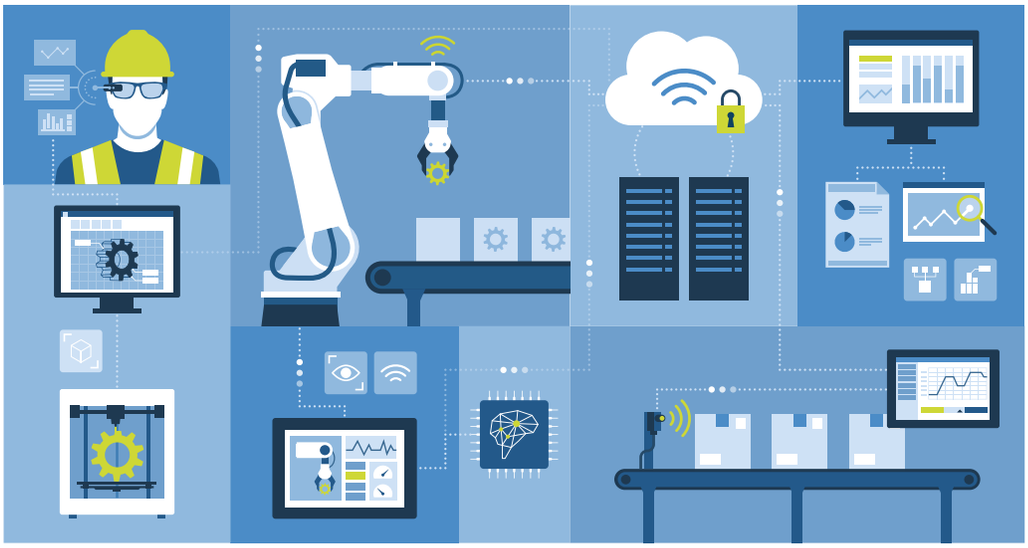
Il Nist CSF è un insieme di linee guida destinate a tutte le organizzazioni che desiderano implementare e seguire standard e best practice comuni per gestire al meglio il rischio.

Negli ultimi 2 anni è diventato chiaro che le piccole aziende che gestiscono le infrastrutture critiche hanno meno risorse a disposizione e maggiore difficoltà nel capire come muoversi quando si tratta di attacchi informatici. Infatti, per chi non si occupa nello specifico di cybersecurity, riuscire ad attuare qualcosa di concreto, dopo aver letto una guida tecnica di 400 pagine, è molto complicato. In questo contesto, la pubblicazione dei nuovi CPG rappresenta un primo e importante passo per semplificare l'implementazione del Nist. Secondo Cisa, infatti, i CPG possono essere visti come una 'guida rapida' per identificare e implementare le pratiche di sicurezza informatica di base. Ciascuno dei 7 CPG include un modello visivo che descrive il risultato desiderato, i rischi affrontati, le mitigazioni e le azioni consigliate. Ogni CPG è mappato alle sottocategorie corrispondenti all'interno del framework Nist, ma a un livello molto più 'semplice' rispetto all'intero set di controlli descritto nel CSF.

Inoltre, le imprese possono utilizzare le linee guida contenute all'interno dei CPG non solo per dare priorità ai controlli che desiderano implementare, ma anche per comunicare ai dirigenti aziendali e ai tecnici il costo e l'impatto di tali controlli.

2. Potenziare le aziende ricche di obiettivi, ma povere di cybersecurity

Gran parte delle infrastrutture critiche, negli Stati Uniti ma non solo, sono private e nella maggior parte dei casi si tratta di piccole utility, che ignorano quali siano le vere implicazioni che un'infrastruttura IT e OT sempre più connessa porta con sé. Anche se queste organizzazioni comprendono i rischi che devono affrontare, la mancanza di finanziamenti e un focus incentrato principalmente sui servizi critici forniti impediscono alla sicurezza informatica di avere la priorità su altri aspetti.



Fonte: foto Shutterstock

Alcuni punti contenuti nei CPG particolarmente importanti per l'ambito OT - Operation Technology

Queste aziende sono gli obiettivi ideali per i cyber criminali ed esemplificano perfettamente il binomio di 'impresa ricca di obiettivi, ma povera di cyber sicurezza'.

I risultati dell'indagine *'2021 Water Sector Coordinating Council cybersecurity state of the industry'* (*www.waterisac.org/2021survey*) hanno dipinto un quadro cupo della situazione, in particolare per quanto riguarda l'identificazione delle risorse IT e OT in rete, la scarsa frequenza delle valutazioni del rischio e la mancanza di formazione sulla sicurezza informatica e di finanziamenti a livello di settore.

L'attacco subito nel febbraio 2021 a un impianto di trattamento delle acque a Oldsmar, in Florida, ha messo in luce i problemi sistemici che minano le infrastrutture critiche negli Stati Uniti, tra cui le vulnerabilità legate ai software legacy e agli accessi da remoto non sicuri. I CPG di Cisa definiscono chiaramente i risultati e le vittorie che i responsabili aziendali e tecnologici possono ottenere. Ancora più importante, gli obiettivi e le relative liste di controllo possono aiutare a mitigare il rischio di attacchi, che possono violare le credenziali predefinite per ottenere l'accesso ai sistemi critici.

3. Cambiamento di mentalità sulla sicurezza informatica OT

Le infrastrutture critiche sono ormai nel mirino di criminali informatici o di hacker al servizio dei governi. Entrambe queste categorie hanno dimostrato la volontà di spingersi sempre più in là, utilizzando gli attacchi informatici per provocare danni nel mondo fisico, al fine di raggiungere obiettivi finanziari o geopolitici. Nel corso del 2022, per esempio, il governo russo aveva in programma di utilizzare il toolkit Incontroller per causare interruzioni alle infrastrutture critiche ucraine.

Nonostante l'elevato rischio rappresentato dagli attacchi ai sistemi cyber-fisici, che possono avere un impatto sul mondo fisico e sulla sicurezza pubblica, le risorse OT (Operation Technology) obsolete rimangono spesso esposte ai rischi e, quindi, sono vulnerabili. Cisa ha riconosciuto questa lacuna e ha creato obiettivi e azioni specifiche per l'OT all'interno dei CPG. Senza questa opportuna specifica, infatti, molto spesso si è ancora convinti che le risorse OT non siano a rischio, o che le pratiche elencate nei CPG non vadano applicate all'OT. Nello specifico, alcuni punti contenuti nei CPG che sono particolarmente importanti per l'Operation Technology:

- **Leadership sulla sicurezza informatica OT:** Cisa raccomanda alle organizzazioni di istituire un unico leader responsabile della sicurezza informatica delle risorse OT. Questo permette alle aziende di designare la figura di riferimento, per esempio un Ciso, che gestisca la sicurezza IT e OT, oppure di stabilire responsabili separati. All'interno della gerarchia organizzativa è fondamentale assegnare un ruolo e un titolo che definisca in maniera chiara le responsabilità legate alla sicurezza informatica OT.
- **Formazione sulla sicurezza informatica OT:** Cisa riconosce anche il ruolo unico che

Fonte: foto Shutterstock

Ogni CPG è mappato alle sottocategorie corrispondenti all'interno del framework Nist, ma a un livello molto più 'semplice' rispetto all'intero set di controlli descritto nel CSF

possono rivestire gli ingegneri nella difesa delle reti e dei dispositivi OT dalle minacce, e raccomanda una formazione annuale specializzata sulla sicurezza informatica incentrata sull'OT. Sebbene le aziende possano disporre di un team per le operazioni di sicurezza, abilitare e potenziare gli ingegneri OT come prima linea di difesa per individuare e mitigare il rischio informatico è di fondamentale importanza. Stabilire un obiettivo di formazione per la sicurezza informatica OT può servire a individuare e mitigare i rischi prima che si realizzino: è come addestrare gli utenti IT a non fare click su collegamenti sospetti o aprire allegati.

- **Mitigazione della vulnerabilità:** la gestione della vulnerabilità è un'altra area all'interno dei CPG per la quale Cisa ha formulato raccomandazioni specifiche nel campo dell'Operation Technology. Non sempre, infatti, le reti OT possono essere patchate in modo tempestivo, e le imprese hanno manifestato sempre più spesso la loro avversione proprio verso tempi di inattività, o il fatto che alcuni dispositivi sul campo e sistemi di controllo non possano essere patchati. In questi casi, al fine di mitigare i rischi, Cisa consiglia di utilizzare la segmentazione della rete e i controlli di accesso, fino a quando non possano essere applicate patch software, o non si effettuano gli aggiornamenti del firmware.
- **Accesso e autenticazione:** diversi obiettivi dei CPG indicano la necessità di rimuovere le password predefinite, stabilire l'autenticazione a più fattori e implementare credenziali univoche per le risorse. Sebbene alcune risorse OT possano avere password condivise e credenziali hardcoded, sono disponibili controlli per mitigare molti di questi rischi intrinseci delle risorse OT, fornendo un livello di astrazione che consente l'accesso granulare basato sui ruoli, oltre che sui rischi intrinseci legati all'identità delle risorse OT. Una tecnologia che consente l'accesso remoto sicuro può consentire ai team di sicurezza informatica di raggiungere diversi obiettivi contemporaneamente.

È doveroso, inoltre, sottolineare il fatto che, oltre a mappare gli obiettivi del Nist CSF, i CPG sono anche strettamente allineati con IEC62443, un insieme di standard, specifiche tecniche e rapporti seguiti dagli operatori del settore, al fine di garantire l'automazione industriale e i sistemi di controllo. Le raccomandazioni OT all'interno dei CPG sono strettamente allineate a questa serie di standard e dimostrano una piena consapevolezza delle differenze che intercorrono tra sicurezza IT e OT; contribuiscono così a creare una maggiore comprensione di tali concetti anche tra gli addetti all'industria.

4. Impatto futuro sulla normativa e sull'assicurazione informatica

Sebbene i CPG non siano obbligatori, vi sono prove e convinzioni crescenti che le forze del libero mercato da sole non cambieranno approccio per proteggere al meglio le infrastrutture critiche dalle minacce informatiche. I CPG di Cisa non sono solo una guida rapida per le piccole aziende, ma possono anche essere un punto di partenza per i prossimi Regolamenti provenienti, per esempio, dalla Casa Bianca e dal Congresso. Le autorità di regolamentazione dispongono ora di un elenco di controllo predefinito approvato da Cisa e di aree critiche su cui concentrarsi per affrontare temi chiave, come la sicurezza degli account, l'integrità dei dati e dei dispositivi, la catena di fornitura e il rischio di terze parti, la risposta e il ripristino.

Lo stesso vale per i provider di assicurazioni in campo informatico. Prevediamo, infatti, che anche questi attori possano utilizzare i CPG come base minima di best practice e standard che gli utenti devono mettere in atto, prima che le polizze vengano emesse e le richieste pagate.

5. Cisa si impegna a fornire informazioni e a soddisfare le specifiche esigenze dei diversi settori

La recente pubblicazione dei CPG va riconosciuta come una prima 'prova'. Molto probabilmente seguiranno CPG specifici, che sposeranno le particolari esigenze di ciascun settore, a partire dalle 16 tipologie di infrastrutture critiche identificate dal governo federale USA. I CPG contenuti in questa prima versione (V1) sono trasversali a tutti i settori e possono aiutare a guidare la strategia e le decisioni di investimento, ma è importante continuare a soddisfare le esigenze specifiche rilevanti per ciascun ambito.

Oggi, le imprese ricche di target, ma povere di cybersecurity, nei settori critici, hanno un mezzo con cui i responsabili tecnici (e non) possono iniziare ad affrontare i crescenti rischi informatici legati alla propria attività.

Claroty - www.claroty.com