INTERVENTI DI RISANAMENTO A SEGUITO DELLA VICENDA DEI SENSORI CHIYU UTILIZZATI DA SOLAR-OT

Implementazione dell'ultima versione del firmware e potenziamento della piattaforma di monitoraggio SOLAR-OT

Autore	Convalidato da
Deirdre STARSKY, Responsabile tecnico di progetto	Elena PIZARI, Direttore generale industria

OBIETTIVO

Il presente documento indica i 2 interventi di risanamento eseguiti a seguito del problema con i sistemi di controllo accessi utilizzati da SOLAR-OT:

1. Dispiegamento d'emergenza dell'aggiornamento del firmware su tutti i sistemi
2. Potenziamento della configurazione della piattaforma di supervisione

1. DISPIEGAMENTO D'EMERGENZA DELL'AGGIORNAMENTO DEL FIRMWARE

Il produttore, CHIYU, ha sviluppato per i sistemi di controllo accessi 'SEMAC'un aggiornamento del firmware che ne corregge la vulnerabilità => questo dovrà essere implementato con urgenza su tutti i siti SOLAR-OT

Questo il numero di versione del firmware da implementare sui SEMAC S2 (67% del parco): 670VYJLN
Questo il numero di versione del firmware da implementare sui SEMAC S3V3 (33% del parco): 628AUYSD

2. POTENZIAMENTO DELLA CONFIGURAZIONE DELLA PIATTAFORMA DI SUPERVISIONE

CONFIGURAZIONE

L'obiettivo è limitare gli elementi tecnici che potrebbero essere utilizzati per sferrare un attacco, installando solo servizi e attrezzature essenziali.

Il livello di sicurezza è stato potenziato attraverso un rafforzamento delle misure di sicurezza, tra cui:

- La limitazione delle funzioni della piattaforma
- Il controllo delle parti fisiche della piattaforma

A. Modifica della configurazione predefinita

Ogni componente è configurato secondo gli standard, inclusi:

- Account tecnici ed elementi di autenticazione associati
- Porte di rete utilizzate
- Directory d'installazione e di lavoro
- Diritti di accesso a directory e file
- L'account utilizzato per eseguire un servizio o un processo, e i diritti associati a tale account
- I file di configurazione degli elementi di sicurezza, in particolare la tracciabilità.

B. Limitazione della funzionalità accessibili

Vengono mantenuti solo i moduli essenziali al funzionamento e alla sicurezza della piattaforma, sottoposti a un'adeguata configurazione, manutenzione regolare e supervisione.
A tal proposito, l'operatore analizza il funzionamento tecnico della piattaforma per escludere servizi o funzionalità installate ma non utilizzate.
Ogni configurazione hardware o software è inventariata come configurazione di riferimento.

C. Inventario degli elementi collegati

L'operatore esegue un inventario tecnico completo delle parti che costituiscono la piattaforma e le mappe. L'inventario comprende attrezzature capaci di connettersi alla piattaforma in modo permanente o temporaneo, fisicamente o a distanza (workstation, server, periferiche, ecc.).

Nel caso in cui terzi si connettano alla piattaforma, l'operatore annoterà il fatto nella propria mappatura e lo terrà in considerazione durante l'analisi dei rischi.

D. Impiego di elementi controllati

L'operatore gestisce gli elementi direttamente, inclusi:

- Implementazione degli aggiornamenti
- Amministrazione degli elementi
- Configurazione remota

PARTIZIONAMENTO

La piattaforma segue una logica di segmentazione che limita ciascun sottosistema alle proprie funzioni, al fine di:

- Ridurre la superficie d'attacco
- Contenere eventuali attacchi
- Limitare l'impatto di una compromissione
- Permettere un livello di sicurezza adeguato ad ogni sottosistema

Il partizionamento si applica sia ai mezzi fisici che a quelli logici.

A. Segmentazione in sottosistemi

La segmentazione in sottosistemi si effettua secondo i seguenti criteri:

- Funzionalità
- Livello di protezione dei dati
- Livello di esposizione
- Livello di sicurezza

Ogni collegamento tra sottosistemi deve essere funzionamente necessario..

B. Partizionamento fisico

Un server è dedicato alle applicazioni più critiche

C. Partizionamento logico

Tutti i dati memorizzati sul server sono crittografati in via preliminare. Ogni sottosistema dispone di un proprio meccanismo di crittografia.

Tutte le comunicazioni tra sottosistemi avvengono attraverso una rete privata virtuale, crittografata e autenticata.

ACCESSO REMOTO

A. Accesso pubblico

L'accesso pubblico segue il protocollo HTTPS e la piattaforma si autentica presentando un certificato server.

Per gli utenti della piattaforma è implementata l'autenticazione a due fattori.

B. Accesso mobile

Le postazioni mobili sono configurate per stabilire verso la piattaforma un tunnel autenticato e crittografato. Il tunnel non è disattivabile ed è impossibile accedere a Internet o a una rete locale.

La partizione di sistema e la partizione dati sono interamente crittografate Sulla workstation è attiva l'autenticazione a due fattori.

FILTRAGGIO DELLA RETE

In aggiunta al partizionamento, vengono implementati dei meccanismi di filtraggio.

A. Punti di filtraggio

Le interconnessioni tra sottosistemi sono i principali punti di filtraggio a cui si applicano il filtraggio perimetrale e quello locale.

B. Regole di filtraggio

La matrice di flusso globale comprende le regole di filtraggio attualmente in vigore. Viene aggiornata su base annuale

C. Implementazione

Il filtraggio è fornito da appositi firewall, fondati sul principio degli elenchi di permessi.