Cybersecurity nella distribuzione di energia nella bassa tensione

Dal campo al cloud
www.siemens.it/sentron-digital

La digitalizzazione ha molti vantaggi, ma aumenta anche il rischio di perdite economiche a causa dell'incremento dei cyberattacchi da parte di professionisti. Nel caso di infrastrutture come le reti elettriche, esiste anche l'eventualità di colli di bottiglia nell'approvvigionamento. Poiché questa eventualità è particolarmente elevata nell'ambito della bassa tensione, Siemens ha sviluppato un approccio globale alla cybersecurity, per garantire la protezione e il funzionamento sicuro dei componenti e degli impianti.

La protezione globale alla cybersecurity viene garantita dal concetto di defense-in-depth, che Siemens stessa propone. È un concetto di cybersecurity di livello superiore e onnicomprensivo, che garantisce la sicurezza dell'impianto e della rete, nonché l'integrità del sistema.

Un elemento importante di questo concetto è il collegamento diretto con il campo. Per i componenti con capacità IoT, la connettività a Internet significa dover soddisfare gli stessi standard elevati di cybersecurity degli altri sistemi connessi. Solo così possono garantire l'affidabilità operativa, a lungo termine, di un'azienda o di un edificio. Le caratteristiche di sicurezza integrate direttamente nei dispositivi devono essere parte di ogni concetto globale di cybersecurity. Punti di partenza specifici sono la gestione sistematica delle vulnerabilità durante l'intero ciclo di vita di un componente, la gestione degli account, le restrizioni all'accesso in scrittura e il firmware autenticato.

La Cybersecurity è la base per operazioni sicure

Di norma Siemens utilizza solo firmware autenticati nei propri prodotti con capacità di comunicazione. Questo significa che solo il software prodotto da Siemens può essere installato e utilizzato su un dato dispositivo IoT, il che impedisce a terzi di modificarne il firmware.
L'installazione degli aggiornamenti è una procedura critica perché terze parti possono teoricamente caricare codici malware con aggiornamenti contraffatti. Il firmware autenticato Siemens impedisce che tutto questo avvenga. Un tentativo di manomissione del codice causa automaticamente la modifica della firma. Il dispositivo riconosce quindi che l'aggiornamento non è affidabile e ne impedisce l'installazione.
In molti dispositivi la protezione tramite password può anche essere utilizzata per impedire una modifica non autorizzata della configurazione. Inoltre, la configurazione di un filtro per gli indirizzi IP assicura che solo specifici indirizzi riconosciuti dall'utente saranno autorizzati a comunicare con i dispositivi.

SIEMENS

Sicurezza a tutti i livelli

Un esempio di come una cybersecurity sistematica ed end-to-end può essere implementata dal campo al cloud è l'interruttore aperto 3WA. Le caratteristiche di sicurezza integrate nel dispositivo stesso proteggono da tentativi di manomissione. Per esempio, il modulo PROFINET IO/Modbus TCP COM190 ha una protezione di scrittura dei parametri e di comando a distanza integrata direttamente nell'hardware. Ciò significa che quando la protezione da scrittura hardware è attivata, nessun parametro può essere modificato, mentre quando la protezione da comando a distanza è attivata, i dispositivi non possono essere accesi o spenti attraverso un processo di comunicazione. Entrambe le funzioni sono sempre attivate di default e devono essere disattivate manualmente - cioè deliberatamente - sul modulo di comunicazione stesso. Se l'interruttore 3WA è installato in un locale di servizio ad accesso limitato, la protezione di scrittura dei parametri e di comando a distanza diventa un ostacolo insormontabile per le persone non autorizzate.
A seconda delle applicazioni in cui viene utilizzato l'interruttore 3WA, può essere utile attivarle o disattivarle a distanza tramite l'interfaccia di comunicazione. Il modulo di comunicazione COM190 con protezione di comando a distanza assicura che la manovra a distanza sia possibile solo se l'operatore lo consente. La disattivazione della protezione di comando a distanza comporta il collegamento di due morsetti.
Come la protezione di scrittura dei parametri, la protezione di comando a distanza è attivata di default e deve essere disattivata intenzionalmente, quando necessario.
Il comando da remoto viene attivato tramite un canale separato - per esempio un PLC – se necessario e viene poi bloccato.
Il comando da remoto stesso viene eseguito da un'altra applicazione, come un sistema di gestione dell'energia.
Come risultato, il comando da remoto può avvenire solo attraverso due percorsi indipendenti, il che rende molto più difficile la connessione non autorizzata da parte di hacker o malware.

L'accesso al Bluetooth è ben protetto

La funzionalità Bluetooth del 3WA permette di accedervi tramite l'applicazione mobile SENTRON powerconfig.
Vengono adottate tutte le precauzioni di sicurezza come la crittografia. Anche l'interfaccia Bluetooth viene disattivata di default e deve essere attivata tramite il display dell'unità elettronica ETU600. Dopo l'utilizzo, l'interfaccia Bluetooth deve essere disattivata per evitare un accesso non autorizzato.
Per l'accoppiamento con l'interruttore aperto 3WA viene utilizzato un PIN monouso, assegnato da Siemens
Questo viene generato ex novo per ogni interruttore 3WA e caricato sulle unità in fase di produzione.
Dopo l'accoppiamento iniziale, l'operatore deve cambiare questo PIN.
La piattaforma dati IoT 7KN Powercenter 3000 può essere implementata come gateway per il cloud. Essa raccoglie informazioni sui valori energetici dai dispositivi di livello inferiore con capacità di comunicazione. Questi dati vengono poi visualizzati e valutati tramite applicazioni basate su cloud (per esempio MindSphere). La comunicazione attraverso un unico gateway protetto da funzioni di sicurezza garantisce la protezione dei dati. L'utilizzo delle caratteristiche di sicurezza del 7KN Powercenter 3000 è reso possibile, per esempio, utilizzando la whitelist Modbus TCP del 3WA e inserendo il 7KN Powercenter 3000 nell'elenco degli indirizzi IP approvati.
Il software SENTRON powerconfig mette in funzione e parametrizza gli interruttori aperti 3WA.
L'accesso può essere limitato utilizzando la whitelist Modbus TCP e la protezione della scrittura dei parametri sul modulo di comunicazione COM190.

Una Cybersecurity sempre al passo con i tempi

Adottando queste misure, Siemens ha gettato le basi per la sicurezza informatica dei prodotti. Poiché le minacce cambiano ed evolvono in modo continuo, Siemens è costantemente impegnata nello sviluppo di nuove tecnologie di sicurezza per ridurre i rischi. I dispositivi con capacità di comunicazione contribuiscono a rendere più efficiente il funzionamento di Industry 4.0 e a risparmiare risorse.
Il numero di applicazioni basate sulla comunicazione è in costante aumento. Un efficiente concetto di cybersecurity, supportato da funzioni di sicurezza installate sui dispositivi, assicura che gli operatori possano utilizzare in sicurezza queste applicazioni e goderne tutti i benefici.

Pubblicato da
Siemens S.p.A.
Smart Infrastructure
Electrical Products
Via Vipiteno 4,
20128 Milano
Italia

SIEMENS