La sicurezza informatica per i sistemi di distribuzione elettrica abilitati all'IoT

di Adam Gauci

Riepilogo

Internet of Things sta aiutando le organizzazioni a migliorare la produttività e la redditività liberando la potenza dei dati dai limiti dei loro sistemi di distribuzione elettrica. I dispositivi IoT e le applicazioni innovative migliorano l'efficienza energetica, la sicurezza elettrica, l'affidabilità, i processi e apparecchiature e la disponibilità di alimentazione. Con l'aumento della connettività e della convergenza IT/OT, tuttavia, aumenta il rischio della sicurezza informatica. Lo standard IEC 62443 offre un sistema coerente e semplificato per definire il livello di gestione della sicurezza informatica necessario a garantire una solida infrastruttura di distribuzione elettrica.

Introduzione

Recentemente, la società globale di ricerca e consulenza Gartner Inc ha stimato 14,2 miliardi di oggetti IoT (Internet of Things).[1] connessi in tutto il mondo, con 25 miliardi previsti entro il 2025.[2]

L'IoT è oggi diventata una necessità per mantenere un vantaggio competitivo, con una stima che il 94% delle aziende registra un ritorno dell'investimento nell'IoT.[3]

Oltre che nell'automazione degli edifici e nei processi, l'IoT è entrata anche nelle infrastrutture elettriche degli edifici. Contatori, sensori e interruttori automatici intelligenti e altri tipi di dispositivi di protezione e controllo continuano a crescere in termini di intelligenza e connettività. E i dati che forniscono sono elaborati da applicazioni analitiche sempre più potenti.

Figura 1

Internet of Things continua a collegare più dispositivi, sistemi, processi ed edifici, aumentando il rischio di attacchi informatici.

Sia che si acceda al cloud oppure che si rimanga onsite nell'edge della distribuzione dell'energia, i team di facility management e finanziari utilizzano le applicazioni abilitate dall'IoT per acquisire dati dai loro sistemi di distribuzione elettrica, ottenere informazioni complete sulle prestazioni operative e sulla sicurezza e affidabilità dell'alimentazione energetica.

Ciò contribuisce a migliorare la sicurezza, la produttività e la redditività attraverso:

- **Maggiore sicurezza**: il 22% degli incendi è di origine elettrica.[4] I sensori IoT wireless consentono il monitoraggio continuo del calore su busbar e altri punti di collegamento, con software di controllo a livello periferico che consentono il rilevamento tempestivo e il preallarme in condizioni che potrebbero causare incendi. Tali sistemi, inoltre, evitano sia i costi di installazione di interruttori con sensori IR che delle scansioni IR manuali e periodiche.
- **Miglioramento delle prestazioni energetiche e di alimentazione:** La possibilità di condurre estese acquisizioni di dati con le funzionalità analitiche implementate nei dispositivi, nei desktop e nel cloud, permette ai team di facility management e ai fornitori di servizi di scoprire le inefficienze energetiche per abbattere la spesa energetica, fornendo al tempo stesso avvisi tempestivi sulle anomalie di alimentazione che possono mettere a rischio le apparecchiature e la continuità di funzionamento. In caso di blackout, l'accesso immediato ai dati acquisiti puo' aiutare i team operativi e di manutenzione a identificare l'origine del guasto e ripristinare l'alimentazione in modo rapido e sicuro.

[1] "Gartner says by 2020, more than half … Internet of Things", Gartner, 2016

[2] "Gartner Identifies Top 10 Strategic IoT Technologies and Trends", Gartner, 2018

[3] "Next big things in IoT predictions for 2020", IT Pro, 2018

[4] "Fire in the Workplace", Electrical Contractor

Casi di studio

Nelle settimane successive a un rovinoso attacco con ransomware all'inizio del 2019, il produttore norvegese di alluminio Norsk Hydro stimava che le loro perdite ammontavano a 40 milioni di dollari, per la maggior parte in mancati ricavi. L'azienda maggiormente colpita era ancora operativa solo al 70-80%, mentre l'altra era pressoché a un punto morto.

Nel 2017, il produttore alimentare Mondelez e la società norvegese di spedizioni marittime Maersk hanno subito danni rispettivamente per 100 milioni e 300 milioni di dollari a causa di attacchi con ransomware.

ZD Net

- **Miglioramento del rendimento degli asset** : una rete di dispositivi IoT consente di ottenere visibilità in tempo reale sullo stato delle risorse critiche come interruttori automatici, gruppi elettrogeni e trasformatori. In tal modo, è possibile passare dalle strategie di manutenzione reattiva a quelle di manutenzione predittiva. Le app ospitate su cloud forniscono funzioni di analisi avanzate e abilitano servizi professionali che aiutano i team di facility management a identificare i rischi, prolungare la durata delle apparecchiature e risparmiare denaro.
- **Mantenimento della conformità e raggiungimento della sostenibilità** : la tecnologia IoT rende più conveniente misurare, analizzare e segnalare le prestazioni energetiche. Ciò semplifica la conformità alle normative sulle emissioni, aiutando i team di struttura a raggiungere prestazioni energetiche superiori grazie a best practice come gli standard ISO 50001.
  I sistemi digitali sono sempre più consigliati o richiesti negli standard di progettazione elettrica come IEC 60364-8-1[5] e contribuiscono ad acquisire credito rispetto ai sistemi di classificazione degli edifici ecologici, come LEED, BREEAM e Green Mark.[6]

A fronte di un chiaro vantaggio nell'aumento di conoscenza prestazionale nelle apparecchiature di distribuzione dell'energia elettrica, le tecnologie operative (OT) che ne consentono l'implementazione, stanno diventando sempre più esposte al rischio di attacchi informatici. Analogamente ai sistemi IT, le organizzazioni devono urgentemente investire nell'implementazione delle best practice di sicurezza informatica per i sistemi elettrici intelligenti e connessi.

Sviluppare una strategia completa di gestione della sicurezza informatica per l'infrastruttura elettrica di una struttura potrebbe sembrare un compito difficile. Per fortuna lo standard IEC 62443 può fungere da quadro di riferimento per la sicurezza informatica OT, contribuendo a semplificare la definizione dei requisiti.
Questo white paper offre una breve presentazione dei driver per la sicurezza informatica dei sistemi elettrici e alle istruzioni offerte dallo standard IEC 62443.

Conseguenze di un attacco informatico al sistema elettrico

Un attacco informatico su qualunque sistema IT o OT può essere devastante per un'azienda. Il rischio di un attacco ai server e ai database aziendali è la perdita di proprietà intellettuali, di dati dei clienti e di conseguenza anche della fiducia degli stessi clienti. Un attacco ai sistemi operativi può causare lunghi e costosi tempi di inattività (si veda la barra laterale), oltre che rappresentare un grave rischio per la sicurezza.

In particolare, per gli impianti elettrici un attacco informatico può avere importanti conseguenze:

"il 67% degli intervistati afferma che negli ultimi 12 mesi le loro aziende hanno subito almeno una compromissione della sicurezza con conseguente perdita di informazioni confidenziali o interruzione delle operazioni".

Ponemon Institute / Unisys

- Se l'attacco comporta una violazione dei dati, il malintenzionato può ottenere l'accesso a profili di carico e potrebbe ottenere dei dati che potrebbero essere considerati dati competitivi (p.e. utilizzo del server)
- Se l'attacco provoca un malfunzionamento delle apparecchiature, può rappresentare un rischio per la sicurezza dei dipendenti o della popolazione. Ad esempio, in un impianto petrolchimico l'interruzione dei processi può causare pericolose esplosioni.
- L'interruzione di corrente causata da un attacco informatico può provocare perdite molto ingenti, come e' successo in un attacco a una fonderia ove a causa di un attacco cyber si è indurito del metallo liquefatto. Un guasto ai sistemi di alimentazione di riserva causata dall'interruzione di energia elettrica in un ospedale può mettere a rischio la vita delle persone come recentemente accaduto.

[5] "IEC 60364-8-1:2019 Low-voltage electrical installations ... Energy efficiency", IEC

[6] "Green Building Standards and Certification Systems", WBDG

La Tabella 1 elenca alcuni costi tipici causati dall'interruzione delle attività per vari tipi di settori.

Tabella 1

Costi di inattività tipici per i principali settori

**Fonte: Copper Development Association, Allianz Global Corporate & Specialty, testimonianza di un cliente di Schneider Electric*

Settore	Costo per interruzione dell'attività*
Semiconduttori	3.800.000 € per evento
Intermediazione finanziaria	6.000.000 € all'ora
Data Center	750.000 € per evento
Telecomunicazioni	30.000 € al minuto
Acciaierie	350.000 € per evento
Industria del vetro	250.000 € per evento
Strutture ospedaliere (200 stanze)	1.000.000 € per evento di 8 ore
Piattaforme off-shore G&P	30.000.000 € al giorno

La superficie di attacco sta aumentando

A causa degli andamenti di crescita dell'IoT e della convergenza IT/OT, la superficie di attacco delle reti aumenta e, di conseguenza, anche la loro vulnerabilità agli attacchi informatici.
Come segnalato dall'organizzazione di ricerca e formazione nella sicurezza SANS Institute, "I sistemi a cui i dispositivi IIoT [IoT industriale] si collegano raddoppiano approssimativamente a ogni periodo compreso tra tre e sette anni, comportando una maggiore complessità di rete a mano a mano che aumenta la connessione di IT e OT, [creando] rischi unici associati alla rapida crescita del volume di endpoint in espansione, alla connettività più ampia e da ultimo a maggiori livelli di accessibilità remota."[7]

Il rischio principale derivato dalla convergenza IT e OT è che una sola violazione in una rete può comportare la violazione di un'altra rete connessa. Vi sono stati molti esempi di attacchi cibernetici causati da vulnerabilità impreviste, che si sono poi propagate.

Casi di studio

Nel 2017 Verizon ha segnalato il rapporto di un'università senza riportarne il nome, i cui studenti lamentavano l'esistenza di "una connettività di rete lenta o inaccessibile". Il team per la sicurezza informatica ha scoperto che gli hacker utilizzavano una rete botnet IoT per manomettere i distributori automatici e altri 5.000 dispositivi IoT. "Anche se questi sistemi IoT erano teoricamente isolati dal resto della rete, era chiaro che erano tutti configurati per utilizzare server DNS in una subnet diversa."[8]

L'attacco informatico del 2013 al distributore internazionale Target ha causato la compromissione di 40 milioni di account di carte di credito e debito, con un costo stimato per la società pari a 290 milioni di dollari.
La violazione è avvenuta attraverso il sistema HVAC - con le credenziali sottratte a un appaltatore - consentendo agli hacker di accedere e installare malware nei sistemi dei punti di vendita Target.[9]

"Ogni nuova connessione espande la superficie di attacco alla soluzione IIoT e agli altri sistemi con cui interagisce".

SANS Institute

[7] "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns", SANS Institute

[8] "Data Breach Digest", Verizon, 2017

[9] "How Hackers Exploit Cybersecurity Vulnerabilities", FacilitiesNet

Da questi esempi non è difficile immaginare che un attacco informatico che costituisce un rischio per i dati su una rete IT possa causare, a sua volta, un attacco a una rete collegata di un impianto elettrico, tale da mettere a rischio la disponibilità di energia elettrica o viceversa.

La consapevolezza di queste minacce ha reso gli incidenti informatici la principale causa di interruzione più temuta dalle aziende.[10] È chiaro che ogni azienda deve rendere la sicurezza informatica una priorità assoluta attraverso la prevenzione: è ciò comprende la messa in sicurezza di tutti i sistemi IT e OT, inclusa l'infrastruttura elettrica intelligente e connessa.

Riconciliare le priorità IT e OT

Quando si parla di sicurezza informatica, le priorità dei team IT e OT spesso si sovrappongono ma non si allineano perfettamente. Un sondaggio IIoT, ad esempio, ha dimostrato che "il team IT è più interessato alla protezione dei dati, alle difese contro perdite finanziarie e alla conformità alle normative del settore, mentre il team OT si concentra sui miglioramenti in termini di affidabilità, disponibilità, efficienza e produzione, sicurezza all'interno dell'organizzazione e protezione delle apparecchiature e dei sistemi".[11]

Con il crescente numero di dispositivi connessi all'IoT e alla convergenza dei sistemi IT e OT, è necessario che i team IT e OT collaborino nella gestione della sicurezza informatica per garantire la protezione di tutte le superfici di attacco e che entrambi i team siano in grado di fornire una risposta rapida e coordinata a eventuali vulnerabilità o attacchi alla sicurezza informatica.

Tuttavia, lavorare insieme può essere una sfida per entrambe le parti, a causa delle differenti responsabilità e competenze. Dal momento che i reparti IT dispongono di esperti in materia di sicurezza informatica, è possibile che venga chiesto di condurre iniziative di sicurezza informatica per i sistemi OT. Tuttavia, il team IT generalmente non ha esperienza in sistemi OT come la distribuzione dell'energia elettrica. Se applicati all'OT, molte politiche e processi IT possono causare interruzioni nel sistema OT. Analogamente, i team operativi con competenza in materia di distribuzione dell'energia elettrica hanno spesso scarsa o nessuna competenza nella sicurezza informatica. Succede anche che introdurre sicurezza significa portare effetti negativi sull'loro efficienza dei sistemi.

[10] "Allianz Risk Barometer – Top Business Risks for 2019", Allianz

[11] "The 2018 SANS Industrial IoT Security Survey: Shaping IIoT Security Concerns", SANS Institute

Lo standard IEC 62443 può fornire ai team IT e OT un punto di riferimento comune. Lo standard aiuta un team OT a specificare il livello di sicurezza necessario per i sistemi OT (inclusa la distribuzione elettrica), mentre il team IT utilizza lo standard per comprendere le esigenze di sicurezza dei sistemi OT. La norma funge da punto di accordo condiviso: un "ponte" per la cooperazione tra i due team.

Valutazione dei rischi

Sviluppata congiuntamente dai comitati della International Standards Association (ISA) e della Commissione Elettrotecnica Internazionale (IEC), l'IEC 62443 è una serie di standard concepiti per “progettare robustezza e resilienza della sicurezza informatica nei sistemi di controllo dell'automazione industriale (IACS) ... nel più vasto senso possibile, che includono tutti i tipi di impianti, strutture e sistemi ... hardware e software come DCS, PLC, SCADA, sistemi elettronici di rilevamento e monitoraggio e di diagnostica di rete.”[12]

Figura 2

Lo standard di sicurezza informatica IEC 62443 si applica a tutti i tipi di sistemi OT, incluse le reti di distribuzione elettrica.

La norma IEC 62443 è stata approvata da molti paesi ed è stata adottata da molte aziende, tra cui Schneider Electric.

Lo standard aiuta nella valutazione dei rischi e nella “individuazione e applicazione di contromisure di sicurezza per ridurre tali rischi a livelli tollerabili”, analizza tutti gli scenari di incidente pertinenti e assegna i livelli di rischio in base a:

- **minacce** alle quali può essere esposto il sistema
- **probabilità** di tali minacce si possano trasformare in incidenti
- **vulnerabilità** intrinseche nel sistema
- **risorse** interessate, ad esempio, sviluppare un inventario di tutte le risorse che necessitano di protezione, incluse quelle fisiche (p.e. sistemi di monitoraggio e controllo, componenti di rete, tutto ciò che implica la gestione dei processi e dell'azienda), logiche (ad es. proprietà intellettuale, pratiche proprietarie, ecc.) e umane (ad es. un allarme erroneo nell’impianto che provoca l'arresto del personale, qualunque tipo di attacco che può provocare lesioni personali)
- **conseguenze** degli asset e dei processi aziendali compromessi

Dopo l'analisi dei rischi avviene la determinazione del *livello di tolleranza dei rischi*. A seconda del rischio che corre una determinata organizzazione, il team di gestione deve "definire con chiarezza e comprendere l'esposizione o la tolleranza dei rischi, in modo da poter analizzare meglio il suo livello di risposta ai rischi residui identificati".

[12] "i 62443 serie di standard - Industrial Automation and Control Systems Security", ISA

Sette pilastri della sicurezza informatica

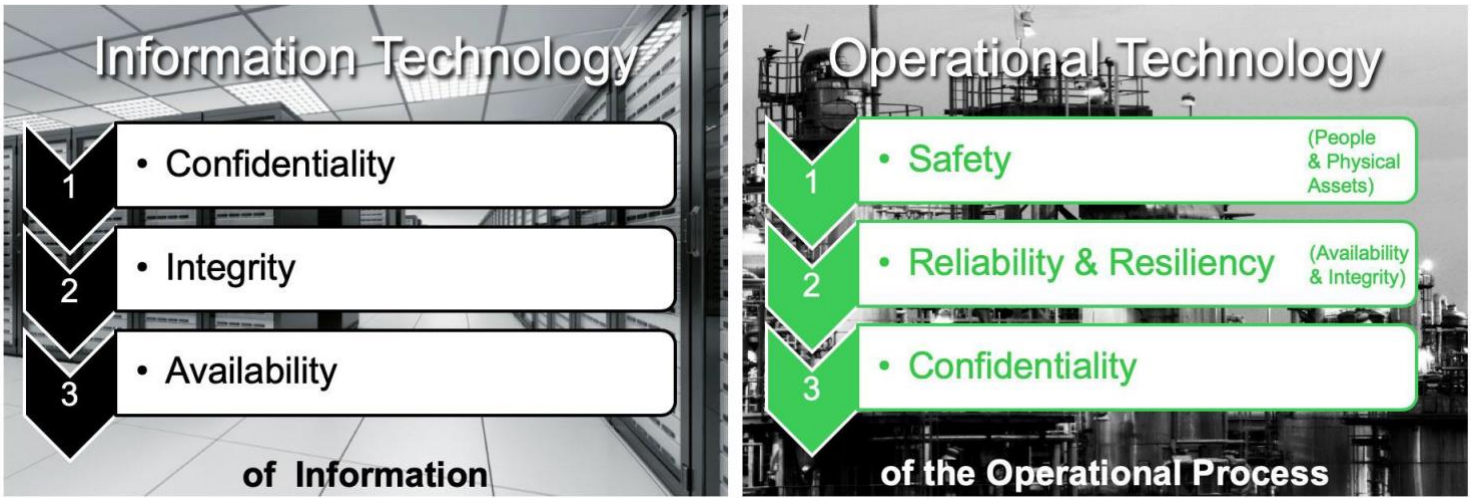
Le priorità dei gruppi IT generalmente sono incentrate sulla sicurezza del sistema attraverso: riservatezza, integrità e disponibilità. I gruppi OT sono concentrati principalmente sulla continuità operativa, attraverso: sicurezza, affidabilità e riservatezza. Lo standard IEC 62443 aiuta a proteggere i sistemi IoT ed OT con sette *requisiti fondamentali*:

1. **Controllo accessi:** Proteggere il componente verificando l'identità dell'utente che richiede l'accesso, prima di attivare la comunicazione con tale componente.
2. **Controllo utilizzi:** Protezione contro azioni non autorizzate sui componenti, verificando che i privilegi necessari siano stati concessi prima di consentire all'utente di eseguire le azioni.
3. **Integrità dei dati:** garantire che i componenti funzionino come previsto durante gli stati operativi e non operativi, quali la produzione e lo stoccaggio dell'energia o uno shutdown per manutenzione.
4. **Riservatezza dei dati:** Protezione delle informazioni riservate o sensibili generate da componenti, a riposo o in transito.
5. **Limitazione del flusso di dati:** Verificare la connessione del dispositivo a una rete segmentata in cui sono definite strategie di scollegamento, gateway unidirezionali, firewall e zone demilitarizzate per evitare inutili flussi di dati. La segmentazione della rete è una strategia in grado di arrestare un attacco informatico nel passaggio da un sistema connesso all'altro (p.e. dalla rete elettrica alla rete aziendale).
6. **Risposta tempestiva all'evento:** Risposta alle violazioni della sicurezza mediante segnalazione all'autorità competente, segnalazione dei requisiti di prova della violazione e adozione di misure correttive tempestive in caso di incidenti riscontrati in situazioni critiche per la mission aziendale o per la sicurezza.
7. **Disponibilità delle risorse:** Garantire la disponibilità dell'applicazione o del dispositivo contro il degrado dei servizi.

Ai requisiti sovrapposti tra sicurezza IT e OT (evidenziati in verde nell'elenco precedente), i team OT assegnano un diverso ordine di priorità. Nel caso degli impianti di distribuzione elettrica, la massima priorità sarà quella di garantire la sicurezza e la disponibilità dell'alimentazione (v. Figura 3).

Figura 3

Differenza nelle priorità di sicurezza tra team IT e OT



Determinazione dei livelli di sicurezza appropriati

Per ognuno di questi sette requisiti, l'organizzazione deve definire il livello di sicurezza richiesto. (v. Figura 4).

I livelli di sicurezza definiscono le funzioni di sicurezza informatica integrate a livello dei dispositivi e in tutto il sistema OT (p.e. distribuzione elettrica). L'incremento della robustezza dei dispositivi e del sistema li rende più resistenti alle minacce cibernetiche.

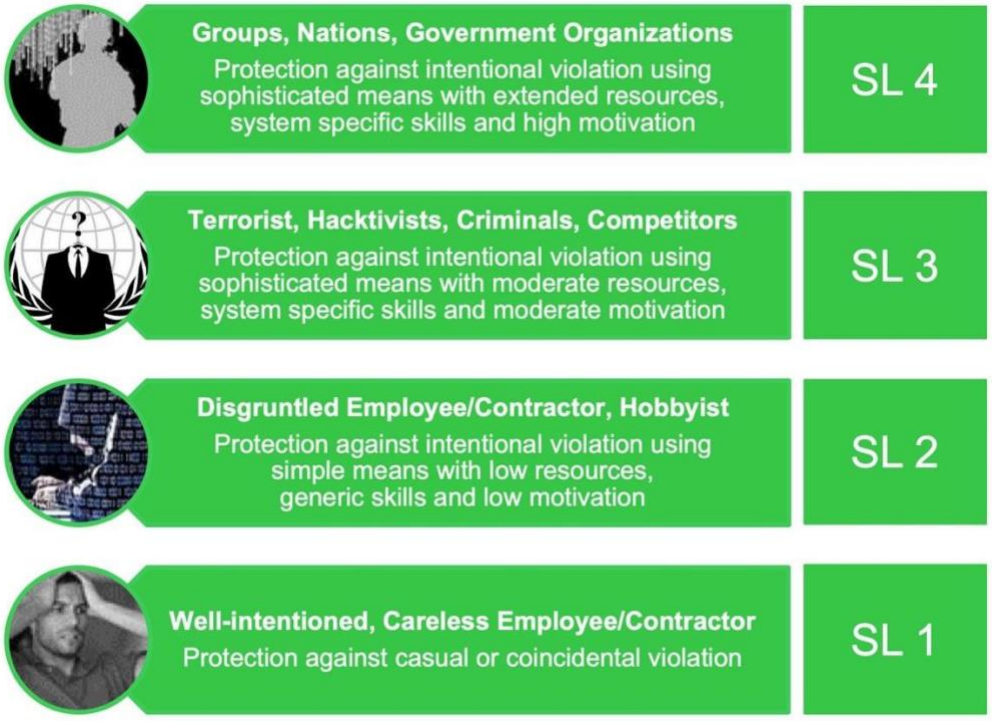


Figura 4

I quattro livelli di sicurezza informatica definiti dalla norma IEC 62443.

Per ogni livello di sicurezza, le specifiche IEC 62443 definiscono un ampio elenco di requisiti necessari per ottenere la conformità a dispositivi e sistemi finali. Ad esempio, secondo i criteri IEC 62443-3-3 per i sistemi, il livello SL1 include 37 requisiti individuali, mentre SL2 include tutti i requisiti di SL1 più 23 requisiti aggiuntivi.
Generalmente, un singolo livello di sicurezza (p.e. SL1 o SL2) verrà applicato costantemente a tutti e sette i requisiti fondamentali. L'organizzazione dell'utente finale deve scegliere il livello di sicurezza del proprio sistema in base alla tolleranza ai rischi che l'organizzazione accetta.

Caso studio

Nel 2015, una società ucraina di distribuzione elettrica a livello regionale ha subito un attacco informatico che ha consentito a un'azienda straniera di controllare da remoto il sistema di gestione della distribuzione SCADA di tre diverse società energetiche. L'attacco ha causato la disconnessione per tre ore di sette sottostazioni principali - e di altre parti della rete di distribuzione - costringendo gli operatori a passare alla modalità manuale.
In totale, ciò ha causato interruzioni dell'alimentazione che hanno interessato circa 225.000 utenti.[13] L'analisi dell'attacco ha rivelato che gli aggressori avevano avuto accesso al sistema molti mesi prima. Disporre di un adeguato livello di misure di sicurezza informatica avrebbe potuto segnalare agli operatori questa intrusione, permettendo loro di evitare l'incidente.

[13] "Analysis of the Cyber Attack on the Ukrainian Power Grid", SANS ICS / E-ISAC, 2016

Passaggi successivi

Secondo la norma IEC 62443, i progettisti di sistemi, gli amministratori e i proprietari di strutture devono seguire una serie di importanti passaggi per assicurare che i sistemi di distribuzione elettrica siano i più sicuri possibile.

1. **Consulenza**: Trovare uno specialista di distribuzione dell'energia elettrica con una profonda conoscenza dei requisiti di sicurezza informatica che assista nella valutazione dei rischi e nella definizione dei livelli di sicurezza richiesti, conformemente allo standard 62443.
2. **Fornitore di soluzioni**: Scegliere un fornitore di tecnologie per sistemi elettrici che ha adottato lo standard IEC 62443 e ha creato un processo di sviluppo sicuro per:
    - Garantire procedure progettuali resilienti
    - Fornire una risposta strutturata al cliente in caso di vulnerabilità rilevate
    - Eseguire test completi e convalidare la sicurezza di tutti i componenti e sistemi
    - Dimostrare la certificazione della sicurezza informatica di terze parti
    - Fornire soluzioni personalizzate e flessibili in linea con i requisiti dell’azienda
3. **Fornitori di servizi**: Scegliere i partner con le capacità richieste:
    - Integratore di sistemi con profonda competenza IT e OT, in particolare per la sicurezza informatica nel contesto dei sistemi operativi critici
    - Servizi di sicurezza informatica che possono fornire una risposta rapida per aiutare i clienti a valutare un attacco informatico e porvi rimedio

Conclusioni

Con il crescente utilizzo dei dispositivi IoT e della connettività in tutti i sistemi di distribuzione elettrica, così come con la tendenza alla convergenza dei sistemi IT e OT, è fondamentale che i progettisti degli impianti elettrici e gli utenti finali comprendano la necessità della sicurezza informatica. Ciò comprende la valutazione appropriata delle potenziali minacce e vulnerabilità, nonché la definizione di adeguati livelli di sicurezza a partire dal dispositivo fino al sistema.

Lo standard IEC 62443 semplifica questo processo definendo un percorso chiaro con sette requisiti fondamentali e quattro livelli di sicurezza standardizzati per le reti OT.

Direttive di legge, progettisti elettrici, fornitori di soluzioni e fornitori di servizi stanno adottando lo standard per definire i requisiti minimi, aiutare i loro clienti a progettare e supportare infrastrutture elettriche in grado di raggiungere i livelli richiesti di sicurezza informatica.

Informazioni sull'autore

Adam Gauci
è nato a Toronto, Ontario, Canada e ha conseguito un Bachelor of Science in ingegneria informatica presso la Queen's University di Kingston, Ontario. La sua precedente esperienza di lavoro comprende il ruolo di Protection and Control Engineer presso Hydro One Networks e di Field Application Engineer presso Cooper Power Systems. Attualmente lavora con Schneider Electric in qualità di Cybersecurity Marketing Leader per EcoStruxure Power, con sede a Montpellier, in Francia. Mr. Gauci è un ingegnere professionista iscritto all'albo della provincia di Ontario.

Risorse

- IEC TS 62443-1-1:2009 - Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models (with links to all other associated IEC 62443 standards)
- white paper "Cybersecurity. Power industry locks down", Schneider Electric
- White paper "Practical Overview of Implementing IEC 62443 Security Levels in Industrial Control Applications", Schneider Electric
- White paper "Cybersecurity at Schneider Electric: Addressing IT/OT convergence in a versatile Cyber ecosystem"
- white paper "Securing Power Monitoring and Control Systems", Schneider Electric
- Blog post "Seven Pillars of Cyber Defense", Schneider Electric
- Power Cybersecurity Solutions, Schneider Electric

L’organizzazione commerciale Schneider Electric

Aree	Sedi	Uffici
Nord Ovest - Piemonte (escluse Novara e Verbania) - Valle d’Aosta - Liguria (esclusa La Spezia) - Sardegna	Via Orbetello, 140 10148 TORINO Tel. 0112281211 - Fax 0112281311	Centro Val Lerone Via Val Lerone, 21/68 16011 ARENZANO (GE) Tel. 0109135469 - Fax 0109113288
Lombardia Ovest - Milano, Varese, Como - Lecco, Sondrio, Novara - Verbania, Pavia, Lodi	Via Stephenson, 73 20157 MILANO Tel. 0299260111 - Fax 0299260325	
Lombardia Est - Bergamo, Brescia, Mantova - Cremona, Piacenza	Via Circonvallazione Est, 1 24040 STEZZANO (BG) Tel. 0354152494 - Fax 0354152932	
Nord Est - Veneto - Friuli Venezia Giulia - Trentino Alto Adige	Centro Direzionale Padova 1 Via Savelli, 120 35100 PADOVA Tel. 0498062811 - Fax 0498062850	
Emilia Romagna - Marche (esclusa Piacenza)	Via del Lavoro, 47 40033 CASALECCHIO DI RENO (BO) Tel. 051708111 - Fax 051708222	Via Gagarin, 208 61100 PESARO Tel. 0721425411 - Fax 0721425425
Toscana - Umbria (inclusa La Spezia)	Via Pratese, 167 50145 FIRENZE Tel. 0553026711 - Fax 0553026725	Via delle Industrie, 29 06083 BASTIA UMBRA (PG) Tel. 0758002105 - Fax 0758001603
Centro - Lazio - Abruzzo - Molise - Basilicata (solo Matera) - Puglia	Via Vincenzo Lamaro, 13 00173 ROMA Tel. 0672652711 - Fax 0672652777	S.P. 231 Km 1+890 70026 MODUGNO (BA) Tel. 0805360411 - Fax 0805360425
Sud - Calabria - Campania - Sicilia - Basilicata (solo Potenza)	SP Circumvallazione Esterna di Napoli 80020 CASAVATORE (NA) Tel. 0817360611 - 0817360601 - Fax 0817360625	Via Trinacria, 7 95030 TREMESTIERI ETNEO (CT) Tel. 0954037911 - Fax 0954037925

Schneider Electric S.p.A.
Sede Legale e Direzione Centrale
Via Circonvallazione Est, 1
24040 STEZZANO (BG)
www.se.com/it

Life Is On | Schneider Electric

Home Page Supporto Clienti

Centro Supporto Cliente
Tel. 011 4073333

Centro Formazione Tecnica
email: it-formazione-tecnica@se.com