La Cyber Security nei sistemi elettrici

Giorgio Picciau, Riccardo Dellora, Cristina Zardetto, Fabio Veronese *Enel Global Infrastructure & Networks*

L'importanza della sicurezza nei sistemi di controllo industriali

Introduzione

Parlando di Cyber Security e di reti, oggi, l'associazione mentale immediata porta ai social network.

È intuibile comprendere l'esposizione al rischio cyber che ogni connessione internet, complessa a piacere, presenta, meno immediato immaginare un rischio cyber su reti fisiche o su reti fisiche automatizzate, che apparentemente non sembrerebbero così facilmente raggiungibili ed esposte al mondo virtuale di internet; l'introduzione e la continua evoluzione delle tecnologie digitali, anche nel perimetro delle reti elettriche, invece, sta amplificando il livello di interconnessione. L'uso sempre più spinto dell'ICT e l'introduzione delle reti di nuova generazione espongono le infrastrutture che forniscono energia elettrica a seri rischi di attacchi cibernetici, facendole diventare bersaglio del cybercrime.

Ne consegue che l'attraversamento del confine tra digitale e fisico, in un mondo così interconnesso, è diventato un rischio non solo reale ma molto possibile.

Se da un lato l'automazione rappresenta la nuova debolezza di queste reti, dall'altro è il punto di forza su cui poter agire per potenziare e controllare meglio proprio la sicurezza intrinseca, attraverso l'attuazione di modelli e politiche cyber che possono essere estese in maniera rapida ed efficace.

Il contesto e le infrastrutture elettriche critiche

L'energia elettrica, neanche a dirlo, è data per scontata, ma è bene sottolineare quanto sia fondamentale per le società umane, così tanto dipendenti da essa che anche un'interruzione breve della fornitura genera impatti sulla disponibilità di altri servizi, come le telecomunicazioni, il trattamento ed erogazione dell'acqua o i servizi sanitari; molti, ma non tutti, possono sopperire a questa inattesa carenza energetica con sistemi ausiliari di generazione per un po' di tempo, ma non per molto, e il pericolo di un blackout non appare poi così remoto.

L'uso crescente delle risorse rinnovabili ha comportato, inoltre, una decentralizzazione della rete, una moltiplicazione dei dispositivi interconnessi ed un aumento degli stakeholder; la stessa separazione tra il mondo dell'*Information Technology* (IT) e quello dell'*Operational Technology* (OT), così fortemente mantenuta tradizionalmente in un contesto fisico, viene ad essere riconsiderata, il tutto per favorire una gestione più informatizzata.

I sistemi di controllo industriale (*Industrial Control Systems*, per brevità a seguire, ICS) nel settore energetico sono ora esposti non solo ai tradizionali problemi di sicurezza e disponibilità, ma anche ai nuovi rischi cibernetici, dovuti principalmente al gran numero di nuove vulnerabilità e debolezze architetturali introdotte dall'uso sempre più ampio delle tradizionali Information and Communication Technologies.

Oggi, la rete trasmissiva degli ICS di molte centrali elettriche è integrata con sistemi informativi più ampi, compresi i sistemi aziendali/corporativi e con sistemi di comunicazione, compresa la rete aziendale. Spesso i servizi di manutenzione su apparecchiature di controllo del processo sono fatti da remoto e negli ultimi anni c'è stato il salto di qualità degli attacchi ai sistemi di processo e d'effetto l'esigenza di salvaguardarli da attività malevole in senso lato, proprio per l'uso sempre più intensivo delle TLC che ha aperto a nuove possibili vie d'attacco.

Le moderne "Architetture di controllo di processo" vedono tre diversi livelli di controllo:

- il livello fisico, composto da tutti gli attuatori, sensori e, in generale, dai dispositivi che ese-

guono fisicamente le azioni sul sistema (es. aprire una valvola, misurare la tensione in un cavo, ecc.);
- il livello Cyber o cibernetico, composto da tutti i dispositivi IoT e dai software che acquisiscono i dati, elaborano strategie di processo di basso livello e forniscono i comandi al livello fisico;
- il livello Decisionale, generalmente composto da operatori umani e dalle loro organizzazioni, che, sulla base delle informazioni fornite dal Cyber Layer, decidono quale strategia di alto livello implementare per gestire al meglio il sistema infrastrutturale, soddisfacendo gli obiettivi operativi e gli obiettivi di sicurezza.

Le infrastrutture che consideriamo critiche in ambito elettrico sono sia le classiche centrali idroelettriche, sia gli impianti idroelettrici medio-piccoli distribuiti sul territorio e gli impianti delle fonti rinnovabili più recenti come l'eolico e il fotovoltaico, a cui si aggiungono certamente i sistemi di trasmissione e distribuzione dell'energia, per intenderci le centinaia di cabine primarie e migliaia di cabine secondarie.

Le centrali termiche a combustibile fossile non sono escluse dal rischio cibernetico, ma la superficie d'attacco in prospettiva è da ritenersi in riduzione con l'avanzare della transizione energetica.

Siamo consapevoli da anni che nella IT classica gestionale prevale l'interesse della integrità e confidenzialità delle informazioni sulla loro disponibilità benché ogni elemento del trittico abbia medesima importanza; nel contesto dell'informatica OT, quella dei sistemi elettrici, è stata fino a tempi recenti solo la disponibilità ad essere privilegiata, ma i rischi cibernetici e gli attacchi occorsi nel recente passato ci insegnano che anche l'integrità e la confidenzialità del dato debbano essere opportunamente protette e garantite.

Cosa intendiamo per sicurezza cibernetica o Cyber Security?

La sicurezza cibernetica è quella branca dell'informatica che implementa la sicurezza passiva ed attiva, valutando i rischi, le minacce potenziali ed analizzando le vulnerabilità dei sistemi in uso, rendendo i dati accessibili solo agli autorizzati e "oscurandoli" con la cifratura, nonché garantendo lo scambio sicuro su canali protetti; inoltre adotta le misure organizzative e tecnologiche per la sicurezza attiva, al fine di proteggere i sistemi dagli attacchi dei software malevoli.

I sistemi di controllo industriale devono quindi soddisfare requisiti di prestazione e sicurezza diversi dai sistemi IT, che vedono nel trittico della riservatezza, integrità e disponibilità delle informazioni il loro focus; nei requisiti dei sistemi di controllo industriale, le priorità sono di fatto invertite, ovvero concentrate in primis sulla disponibilità e successivamente su integrità e riservatezza, proprio in quest'ordine. Inoltre è necessario porre attenzione all'affidabilità operativa, alla sicurezza fisica degli impianti, alla salute dei lavoratori e non ultimo alla mitigazione di eventuali impatti ambientali.

I sistemi IT di solito non hanno un impatto diretto sulla salute pubblica o la sicurezza umana e possono usare strategie, come il riavvio dei sistemi, che per gli apparati SCADA sono di solito time-critical, permettendo interruzioni solo se strettamente necessarie, pianificate con settimane di anticipo.

Moltissime persone sono ancora poco sensibili alla cyber sicurezza ed alle sue pratiche, così utenti dei sistemi aziendali ed appaltatori esterni spesso usano password simili se non uguali a prescindere dall'applicazione in uso o trasferiscono informazioni con chiavette USB o, peggio, "appoggiano" temporaneamente informazioni aziendali su servizi cloud personali.

Per prevenire ciò, le postazioni di lavoro all'interno del perimetro OT non dovrebbero consentire l'uso di tali dispositivi di archiviazione oppure consentire quelli specifici autorizzati dall'end point protection.

Come in altre discipline ed ambiti, il fattore culturale è parte integrante delle difese tecnologiche adottate, nonché rilevante a mitigare se non eludere i rischi cibernetici.

È pertanto con la formazione continua che si favorisce e consolida la cyber-awareness nella popolazione, sia essa interna all'azienda che esterna, così da evitare quegli errori involontari che potrebbero essere lo *starting point* di azioni di social engineering o data gathering, propedeutici ad attacchi ai sistemi industriali.

Elementi determinanti la protezione informatica

Per vagliare quali interventi sul parco tecnologico dell'azienda debbano essere fatti più o meno celermente, il punto di partenza è l'analisi del rischio.

Normalmente si opera su tre livelli, quello normativo, tecnologico e procedurale: è bene infatti che il comparto OT sia conforme alle norme del legislatore, ma anche alle direttive e best practice frutto di esperienze degli altri player internazionali.

Aver contezza del rischio sugli asset comporta la valutazione delle vulnerabilità, che può avere come effetto l'esclusione di alcune tecnologie software o certi sistemi operativi e la declinazione delle contromisure a protezione, come l'applicazione di correttivi software, il cosiddetto *patching*.

Non è da trascurare infine l'aspetto procedurale, mappando i processi e facendoli evolvere e migliorare periodicamente in funzione delle esigenze dell'azienda, degli aggiornamenti tecnologici e normativi.

Oggi questo tris di elementi, normativo, tecnologico e procedurale è sempre più interdipendente, ed è la chiave che le aziende possono imparare ad usare per proteggersi ed evolversi in un contesto sicuro.

La diffusione di dispositivi smart e IoT (*Internet of Things*) non si limita alla dimensione del mercato consumer, ma sta penetrando sempre di più anche in campo industriale, nonostante la cautela degli operatori renda più lungo il tempo d'introduzione di tali tecnologie.

La moltitudine di tali tecnologie favorisce le possibilità d'attacco, poiché sostanzialmente ne aumenta la cosiddetta superficie, ovvero la sfruttabilità delle vulnerabilità intrinseche dei prodotti, che, nonostante gli sforzi dei costruttori, non saranno mai completamente sicuri.

La *smartification* in ambito OT e IoT stimola preoccupazione e grande attenzione, poiché gli attacchi alle infrastrutture critiche sono e saranno motivati da fattori economici e geo-politici; basti immaginare il blocco di un sistema controllore della rete elettrica sferrato per mezzo di ransomware, che dietro compenso economico tiene sotto scacco un determinato territorio.

Anche la manipolazione fraudolenta di dati è tecnica utilizzata dai criminali informatici che lanciano sniffer, denial-of-service (DoS) con lo scopo di raccogliere le informazioni, intercettando e indirizzando il traffico verso altre destinazioni, senza bloccarlo. Nel *Man-in-the-Middle attack* (MiTM) i criminali si interpongono tra la persona che invia e quella che riceve.

Il caso SolarWinds [1]

Alla fine del 2020 abbiamo appreso che è stato orchestrato, durante tutto l'anno, un cyber attacco alla catena di approvvigionamento energetica statunitense, infiltrandosi nell'infrastruttura digitale di SolarWinds e del suo software Orion, per ottenere l'accesso ai dati sensibili di una serie di dipartimenti governativi ed organizzazioni tramite aggiornamenti software infestati da malware.

È uno dei più grandi e sofisticati incidenti informatici nella storia degli Stati Uniti che ha spinto molte aziende a rivedere seriamente i rischi di sicurezza derivanti dai loro fornitori di software.

Nello specifico del caso [2], a conclusione dell'analisi dell'incidente, si è compreso che tutto iniziò nel settembre del 2019, quando i criminali informatici ebbero accesso non autorizzato all'infrastruttura di SolarWinds, iniettando un malware chiamato Sunburst nel software di SolarWinds; durante questo lungo periodo, gli hacker sono rimasti silenti all'interno dell'infrastruttura digitale dell'azienda, secondo la tecnica "osserva e non toccare".

SolarWinds, ignara della presenza di malware, ha rilasciato gli aggiornamenti del software Orion a quasi 20.000 clienti, diffondendo il malware dannoso nelle loro tecnologie ed infrastrutture, ICS compresi, consentendo imperturbata l'attività degli hacker fino al dicembre 2020, quando FireEye - società di Cyber Security nonché cliente di SolarWinds - ha rilevato e segnalato il malware sia a SolarWinds che alla SEC (*U.S. Securities and Exchange Commission*).

Questo caso tanto grave quanto eclatante ha impatti importanti su larga scala, dai costi di recupero (stimati in oltre 100 milioni di dollari) ai danni alla reputazione della stessa SolarWinds, ma anche delle varie agenzie ed entità preposte a controllo; ciò ha innescato ripercussioni legali contro la stessa SolarWinds da parte delle società e organizzazioni danneggiate, che si sono riverberate sulla quotazione economica del titolo, provocando una flessione di oltre il 40%.

Tre problemi significativi nella Cyber Security degli ICS [3]

Lo scontro culturale tra gli operatori IT e OT è passato in secondo piano rispetto a tre problemi di sicurezza emergenti per la comunità dei sistemi di controllo industriale (ICS). "Questo non funzionerà per l'OT" era un mantra comune nei giorni precedenti a SolarWinds e agli snafus (*a situation in which nothing has happened as planned*) del codice sorgente dei dispositivi intelligenti. Il personale esperto IT, che va da un singolo dipendente a robusti team 24 ore su 24, si sta riconciliando con le incognite emergenti piuttosto che correre per mettere al sicuro le vulnerabilità di Windows XP e affrontare l'overshare tecnico dei fornitori di sistemi. I leader della sicurezza e i centri operativi di sicurezza devono oggi fronteggiare tre ostacoli principali: i dibattiti sugli strumenti di sicurezza proprietari rispetto a quelli open source, le battaglie per la gestione della catena di fornitura e un panorama sempre più fosco di vulnerabilità dell'Internet delle cose (IoT).

Proprietario Vs. Open Source

I venditori di software fanno affidamento sulla natura proprietaria dei loro prodotti nelle vendite per convincere i clienti che sono più affidabili del software open source che può essere modificato praticamente da chiunque. Questa pratica è rafforzata dagli *Original Equipment Manufacturer* (OEM), che

acquistano società di software di sicurezza da offrire strategicamente insieme ai loro sistemi e prodotti. I budget per la Cyber Security in media sono incredibilmente piccoli, secondo quanto riferito tra lo 0,2% e lo 0,9% delle entrate nette. Una porzione ancora più piccola è diretta all'ICS. Questa realtà, unita alla criticità di operazioni sicure e affidabili 24 ore su 24, 7 giorni su 7, crea un'atmosfera spietata per la scelta dei giusti strumenti di sicurezza.

I programmi open source sono gratuiti ed essenzialmente crowd-sourced, e quindi anche potenzialmente debuggati piuttosto che manipolati da molti. Allo stesso tempo, l'utilità di qualsiasi software va solo fino a quando gli esseri umani sanno come estrarre valore dai suoi risultati. Per ottenere la piena utilità, gli utenti finali di solito forniscono dati, a volte confidenziali, che devono essere parte del calcolo del rischio prima dell'acquisto. Gli utenti finali hanno una visibilità limitata sul codice proprietario nel software che si basa sull'accesso e lo scambio dei loro dati. Lo stesso vale per i servizi gestiti. Un team di sicurezza potrebbe decidere su uno strumento open source per il monitoraggio della rete, ma acquistare un software di terze parti come soluzione di servizio, come SolarWinds, per la gestione e l'orchestrazione. È sempre più difficile pesare i costi e i benefici da entrambe le parti quando entrambe le opzioni presentano rischi unici e imprevisti.

Gestione della catena di approvvigionamento

L'attacco SolarWinds è stato nuovo per due motivi principali. In primo luogo, è passato inosservato dalle principali aziende di sicurezza per diversi mesi e, in secondo luogo, il suo preciso targeting ha permesso agli autori di colpire molte organizzazioni contemporaneamente. Potrebbe passare come il più grande evento di Cyber Security del 2020 ma gli attacchi alla catena di approvvigionamento sono destinati a continuare. Progettare il malware per mascherarsi come traffico legittimo sarà probabilmente una regola piuttosto che un'eccezione in futuro, come evidenziato da questo approccio all'invio di pacchetti legittimi da fonti di codice pubbliche ad applicazioni aziendali interne o private con strumenti automatizzati.

La catena di approvvigionamento per ICS è un ulteriore fattore di stress per le reti di comunicazione che già mancano della visibilità necessaria per generare un programma di Cyber Security defense-in-depth. Molti protocolli e processi statici di dati OT vivono in fogli di calcolo, con versioni software obsolete che girano su macchine industriali che hanno da 10 a più di 30 anni. L'hardware e il software ICS in un singolo ambiente provengono da decine di fornitori diversi. Tra gli switch, i firewall, i gateway e i dispositivi di mirroring delle porte, il traffico di rete potrebbe essere segmentato, ma gli incidenti recenti rivelano connessioni internet sconosciute sui dispositivi OT e sui sistemi e sottosistemi forniti da terze parti. Per garantire l'integrità del software in futuro, una distinta dei materiali del software richiesta potrebbe fare molta strada in termini di prevenzione e integrità. Sfortunatamente, catalogare ICS per tracciare retroattivamente i metadati e la provenienza della catena di fornitura è un compito costoso, dispendioso in termini di tempo e arduo.

Vulnerabilità IoT

La promessa di rivoluzionare l'industria fornendo livelli senza precedenti di interconnettività e ottimizzazione dei dati spinge molte aziende a continuare a portare nuovi prodotti IoT sul mercato ogni giorno. Nelle case, nelle fabbriche e nelle città, le cose intelligenti connesse sono progettate per servire funzioni specifiche. Creati per essere distribuiti in grandi numeri a basso costo in ambienti industriali, questi dispositivi spesso mancano di sicurezza di base e di protezione dei dati. Possono essere attaccati per ottenere l'accesso a un obiettivo più grande, per raggiungere obiettivi più profondi all'interno di una rete aziendale. Possono anche essere utilizzati per una semplice ricognizione e spionaggio. Oppure possono essere dirottati e reindirizzati su scala per armare il codice e il traffico overflow per colpire obiettivi critici.

Anche se la sicurezza degli endpoint nelle operazioni industriali sta guadagnando trazione, non tratterà le cause sottostanti che rendono l'IoT insicuro. Più feed di dati, connettività e strumenti di gestione dei dati offrono un "cerotto" per password deboli, protocolli di autenticazione e crittografia, meccanismi di aggiornamento insicuri e protezioni della privacy banali. Un attore minaccioso alle prime armi può trovare dispositivi connessi a Internet sul sito web Shodan e imparare come aggirare la segmentazione della rete e penetrare in reti IoT isolate utilizzando strumenti open source come Nmap e Ncrack. La gestione delle intrusioni sarà una battaglia costante tra il rilevamento e la risposta, con poca attenzione per affrontare i problemi di fondo dopo che i prodotti IoT sono stati acquistati e distribuiti dai fornitori.

I prossimi passi per le parti interessate

Con queste sfide in mente, è il momento di fare sul serio sulla sicurezza ICS. Approcci frammentari alle patch di vulnerabilità e al controllo della conformità non impediranno il sabotaggio da parte di un attore minaccioso. I settori critici devono prendere nota e pianificare l'indagine e l'azione per eseguire valutazioni bottom-up delle operazioni, dei sistemi e delle informazioni critiche. Ci sono diversi utili quadri di gestione

della raccolta ICS, guide all'inventario delle risorse e risorse di intelligence delle minacce. Per costruire uno slancio reale, le organizzazioni devono fare una ricognizione sulle loro operazioni e iniziare a testare le loro ipotesi.

Un nuovo standard della serie ISA/IEC 62443, ISA/IEC 62443-3-2: Security Risk Assessment for System Design, definisce una serie di misure ingegneristiche per guidare le organizzazioni attraverso il processo di valutazione del rischio di un sistema ICS o IIoT nuovo o esistente. Stabilisce anche come identificare e applicare contromisure di sicurezza per ridurre quel rischio a livelli tollerabili.

Un'altra nuova metodologia dagli esperti dell'Idaho National Laboratory (un membro dell'ISA Global Cybersecurity Alliance), *Consequence-Driven, Cyber-Informed Engineering* (CCE), si concentra sulla pianificazione dello scenario peggiore di accesso e sfruttamento. CCE procede dal presupposto che l'unico modo per capire gli attacchi prima che si verifichino è quello di pensare come un attaccante e stress-testare la vostra rete e le politiche di sicurezza.

Questi approcci sono individualizzati e permettono agli esperti di affrontare il rischio di sicurezza nei sistemi critici per iniziare ad affrontare e mitigare i principali punti critici nel 2021.

La progettazione *security by design*

La sicurezza cibernetica è stata per troppo tempo considerata solo un add-on delle soluzioni digitali, un task finale da smarcare frettolosamente prima della messa in esercizio di una soluzione e raramente integrata nei contratti come requisito *sine qua non*.

Anche per i sistemi OT e nelle reti elettriche, la Cyber Security non può più essere considerata una commodity o un *nice to have*, ma deve essere inserita come elemento pervasivo nella progettazione di un sistema, considerandola parte dell'insieme ed allo stesso tempo elemento di dettaglio necessario; quindi è fondamentale che i requisiti siano chiari ed auto-consistenti, che si operi in un contesto di laboratorio per testare le tecnologie di prossima adozione dal punto di vista cyber oltre che funzionale, per poi identificare quegli elementi specifici che andranno a comporre una dashboard di controllo ed alerting.

La security by design richiede la partecipazione attiva di molte anime aziendali, dall'interessato alla protezione degli asset, cioè il Business, al Risk Manager, al Auditor interno, dalla Corporate Security all'ufficio legale, senza mancare le unità di risposta attiva come il CERT operativo in Enel dal 2019.

La security by design prevede, sin dalle prime fasi del ciclo di vita di una soluzione, di garantire l'adozione dei principi di Cyber Security e di mantenerli durante l'intero ciclo di vita delle soluzioni IT/OT e delle infrastrutture a perimetro.

Le azioni messe in campo da Enel

L'organizzazione e i processi

Enel si è dotata di un'unità di esperti di Cyber Security all'interno del Global Digital Solution con la missione di proporre la strategia di Cyber Security al relativo Comitato Esecutivo del Gruppo, definendo e attuando il programma di Cyber Security e i piani di implementazione, in collaborazione con gli stakeholder aziendali rilevanti, definendo budget obiettivi e priorità.

L'unita di cyber definisce e presidia le architetture di Cyber Security di Gruppo su information (IT), industrial (OT) e *Internet of Things* (IoT) in sintonia con le specificità ambientali, garantendo la compliance alla normativa, alle policy, ai processi e ai controlli in materia di Cyber Security e data protection per tutte le iniziative all'interno del Gruppo, facendo leva sui Digital Hub.

Ha inoltre il compito di garantire la valutazione dello stato della sicurezza informatica attraverso test di conformità, test di penetrazione, valutazione della vulnerabilità, hacking etico, assegnazione della responsabilità per azioni correttive e verifica dell'effettivo completamento delle stesse.

Gestisce inoltre il *Cyber Emergency Readiness Team* (CERT) del Gruppo e supervisiona il processo di Identity Management e Access Control per garantire un flusso di informazioni adeguato e tempestivo su eventi significativi di sicurezza informatica alle parti interessate, in conformità con le leggi e i regolamenti sulla sicurezza interna.

Nell'organizzazione sono inoltre identificati i Cyber Security Response Manager e i Cyber Security Risk Manager come declinazione della sicurezza all'interno delle linee di sviluppo e di processo di business in conformità al Cyber Security Framework del Gruppo.

Il CERT

Un approfondimento rispetto l'organizzazione dell'unità di Cyber Security, la merita il CERT.

Enel nel suo cammino verso la trasformazione digitale presta grande attenzione alla sicurezza informatica. Con il proprio *Cyber Security Framework* ha indirizzato in modo accurato principi, organizzazione e processi operativi per un efficace presidio del cyber risk.

Uno degli elementi strategici contemplati è la ca-

pacità di prevenire e gestire eventi ostili *Cyber Security Incidents*, come attacchi informatici intenzionali e malevoli, che potrebbero danneggiare la *Constituency* di Enel, cioè l'insieme di risorse umane, dati e sistemi informatici, asset industriali e infrastrutture critiche.

È questa la missione del CERT, il Cyber Emergency Readiness Team, colleghi dell'unità di Cyber Security della Global Digital Solutions dedicati a rispondere ad attacchi informatici con attività di prevenzione, rilevamento, risposta e ripristino a incidenti cyber.

Il team opera secondo un rigoroso processo di *Cyber Emergency Response and Management*, in stretta collaborazione con tutte le altre unità di Enel, dal Business ai Digital Hub, dal Legale alle Security e alla Comunicazione, per citarne solo alcune.

I *CERT* non lavorano in modo isolato ma condividono le informazioni in un ambiente fidato, per fronteggiare con maggiore efficacia i pericoli cyber.

Nei paesi in cui il Gruppo ha infrastrutture critiche importanti, come Italia, Spagna, Romania, Sud America, il CERT di Enel - ha spiegato Francesco Perna, head of Cyber Security Risk Monitoring and Response - ha già stabilito diverse relazioni strutturate con i CERT nazionali, impegnati proprio a garantire la protezione cibernetica del Paese in cui operano. Il CERT di Enel è inoltre attivo nei circuiti internazionali come membro accreditato del Trusted Introducer, che comprende oltre 300 CERT in più di 60 Paesi, e, nelle prossime settimane, del FIRST (*Forum of Incident Response and Security Teams*) che è la comunità più estesa e importante con oltre 400 iscritti in più di 80 Nazioni.

Procedure e Policy

In ambito Enel è stata definita una specifica **Policy** che definisce il **Cyber Security Management Framework** adottato da Enel, dettagliando ruoli, responsabilità e processi.

Esso è istituito per guidare e gestire la sicurezza informatica, sulla base delle esigenze aziendali, promuovendo la sicurezza informatica attraverso l'approccio progettuale e collegando strettamente tecnologie, processi e persone.

Il Cyber Security Framework stabilisce il modello operativo e i relativi processi per la gestione della sicurezza informatica IT/OT/IoT e mira a:

- definire una strategia di Cyber Security risk based, in termini di iniziative, per l'intero Gruppo Enel;
- guidare un modello di protezione *Cyber Security by design* per applicazioni e infrastrutture, integrando funzionalità di Cyber Security a partire dalle primissime fasi del loro ciclo di vita;
- potenziare la resilienza delle infrastrutture e delle applicazioni per far fronte alle minacce e ai rischi informatici, costruendo una difesa coerente con il rischio - livello di tolleranza definito.

Inoltre, una specifica Istruzione Operativa, ***Cyber Security Risk Management Methodology***, descrive la metodologia di gestione del rischio di sicurezza informatica da un punto di vista operativo ed è applicabile a infrastrutture/sistemi/processi già in produzione, progetti in fase avanzata del ciclo di vita o nuovi progetti.

Questa metodologia include i seguenti passaggi principali:

CYBER RISK ANALYSIS initiation

❑ Business Impact Analysis (BIA) execution:

- Viene eseguita un'analisi dei rischi per ogni Centro Rischi selezionato. Un centro di rischio è un insieme di risorse fisiche, logiche e organizzative che supportano un processo aziendale o parte di esso. L'obiettivo dell'analisi è valutare gli impatti aziendali sul Centro Rischi, derivanti da perdite di riservatezza, integrità e disponibilità dei dati e per identificare il livello di impatto.
- L'Istruzione Operativa fa riferimento al tool di BIA per l'esecuzione di questa analisi di impatto.

CYBER RISK ANALYSIS completion

❑ Threat, Vulnerability and Risk Evaluation:

- Identificazione delle minacce applicabili che potrebbero avere un impatto sul centro di rischio, con relativa probabilità di accadimento e valutazione per ogni minaccia del suo livello di minaccia;
- Valutazione del livello di Vulnerabilità (considerando le misure di protezione già attuate, se presenti), una debolezza intrinseca del Centro Rischi che possono essere sfruttate da una o più minacce per arrecare danno all'organizzazione. Questa valutazione è complementare alle attività di Assurance e/o Audit.

L'output di questa fase è l'identificazione del livello di rischio per ciascuna minaccia applicabile (basata sulla combinazione del livello di impatto da BIA, livello di minaccia e livello di vulnerabilità).

❑ Cyber Security Risk Treatment Analysis and Selection:

- Identificazione delle azioni di trattamento appropriate per far fronte ai rischi di sicurezza informatica, che significa selezionare i controlli di sicurezza informatica da attuare per raggiungere il livello di rischio residuo accettabile (controlli di base, definiti all'interno delle linee guida di Cyber Security, sono sempre obbligatori).

L'Istruzione Operativa collega lo strumento di

Risk Management per valutare minacce, vulnerabilità e rischi e consente diverse simulazioni al fine di verificare come si evolve il rischio residuo in base alle diverse strategie di trattamento.

Le azioni di trattamento e il rischio residuo sono soggetti alla decisione di accettazione del Cyber Security Response Manager e devono essere formalmente registrate, insieme al livello di rischio misurato.

Il quadro regolatorio attuale nazionale e internazionale

Data la crescente sofisticazione delle minacce informatiche contro le reti elettriche, il settore dell'approvvigionamento energetico si è dotato di una vasta gamma di standard e norme per gestire questi rischi e nel tempo è diventato uno dei comparti più regolamentati in materia di sicurezza informatica.

La sicurezza cibernetica è stata sino a ora, possiamo dirlo, materia squisitamente tecnica, tenuta lontana dai tavoli regolatori e vissuta nella sua manifestazione nel mondo fisico, più quale eclatante e sporadico evento di cronaca, che una sentita esigenza difensiva; ebbene, il DL 105 del 21 settembre 2019, ne sancisce la presenza nel campo regolatorio, definendo la sicurezza nazionale cibernetica come linea di base difensiva e non più un *nice-to-have* da sbandierare come fiore all'occhiello agli stakeholders.

Il comparto elettrico, ed in particolare Enel, è fra gli operatori inclusi nel Perimetro di sicurezza nazionale cibernetica (PSNC) [4], esercitando ed assicurando il servizio essenziale di fornitura di energia alle attività fondamentali e d'interesse pubblico e privato della nazione.

In particolare, il decreto del 30 luglio chiarisce che:

- un soggetto esercita una funzione essenziale dello Stato, di seguito funzione essenziale, laddove l'ordinamento gli attribuisca compiti rivolti ad assicurare la continuità dell'azione di Governo e degli Organi costituzionali, la sicurezza interna ed esterna e la difesa dello Stato, le relazioni internazionali, la sicurezza e l'ordine pubblico, l'amministrazione della giustizia, la funzionalità dei sistemi economico e finanziario e dei trasporti;
- un soggetto, pubblico o privato, presta un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato, di seguito servizio essenziale, laddove ponga in essere: attività strumentali all'esercizio di funzioni essenziali dello Stato; attività necessarie per l'esercizio e il godimento dei diritti fondamentali; attività necessarie per la continuità degli approvvigionamenti e l'efficienza delle infrastrutture e della logistica; attività di ricerca e attività relative alle realtà produttive nel campo dell'alta tecnologia e in ogni altro settore, ove presentino rilievo economico e sociale, anche ai fini della garanzia dell'autonomia strategica nazionale, della competitività e dello sviluppo del sistema economico nazionale.

I soggetti suddetti sono individuati tra gli operatori dei vari settori: interno, difesa, spazio e aerospazio, energia, telecomunicazioni, economia e finanza, trasporti, servizi digitali, tecnologie critiche ed enti previdenziali/lavoro.

Il PSNC prevede anche per il nostro settore, quattro macro-azioni:

- ha identificato il settore energia come servizio essenziale che dipende da reti e sistemi informatici la cui interruzione può compromettere la sicurezza nazionale con ricadute economiche e impatti sul territorio e utenti, con conseguente perdita di disponibilità del servizio ed integrità e riservatezza dei dati efferenti;
- ci indica di predisporre un piano di mitigazione degli impatti e di ripristino del servizio;
- indica fra i servizi essenziali per i quali, in caso di interruzione o compromissione, il pregiudizio per la sicurezza nazionale è massimo e le possibilità di mitigazione sono minime;
- ci individua quali soggetti svolgono le funzioni indicate dalla terza direttiva.

La quota di competenze tecnico-scientifica necessaria al CISR (Comitato interministeriale per la sicurezza della Repubblica), è definita nel decreto stesso all'art.6, il quale istituisce che il Tavolo sia costituito da due rappresentanti per ciascuna amministrazione, di cui almeno il 50% sia in possesso di competenze tecnico-specialistiche nella materia della sicurezza cibernetica; questo elemento evidenzia la rilevanza che rivestono le capacità tecniche in questo ambito, nonostante ci sia una sofferenza di persone con tali skill.

Nello specifico della nostra realtà, gli obblighi dell'inclusione nel Perimetro comportano:

- predisporre e aggiornare annualmente la lista dei beni ICT di nostra pertinenza;
- individuare i beni ICT necessari a svolgere la funzione o il servizio essenziale, per valutare l'impatto sull'operatività del bene ICT, la sua compromissione della disponibilità e dell'integrità o riservatezza dei dati (CIA triad);
- valutare le dipendenze con altre reti, sistemi informativi, servizi informatici o infrastrutture fisiche di pertinenza di altri soggetti.

Dobbiamo individuare i beni ICT che, in caso di

incidente, causerebbero l'interruzione totale dello svolgimento della funzione essenziale o del servizio essenziale.

Quindi è importante trasmettere queste informazioni agli organi di Stato competenti per permettere le attività di prevenzione, preparazione e gestione delle crisi cibernetiche affidate al *Nucleo per la Sicurezza Cibernetica* (NSC), dipendente dal DIS.

Sarà necessario qualche anno per constatare gli effetti concreti di questo impianto normativo, che tenta di stabilire un framework cibernetico, per una materia sfuggente ed impalpabile come la Cyber Security.

In Europa, le aziende che operano nel settore energetico sono soggette alla direttiva sulla sicurezza delle reti e delle informazioni (NIS) quali infrastrutture critiche. In termini di standard, tra i più comuni figurano, per esempio, IEC 62645 (misure per prevenire, rilevare e rispondere ai cyber attacchi ai sistemi informatici nelle centrali nucleari), IEC 62859 (gestione delle interazioni tra sicurezza fisica e Cyber Security), ISO 27019 (raccomandazioni di sicurezza per i sistemi di controllo dei processi dell'industria degli operatori energetici) e IEC 61850 (uno standard di comunicazione per i dispositivi di protezione delle sottostazioni di alimentazione).

Due esempi di cyber sicurezza applicata

Negli ultimi 5 anni i casi di cyber attacco alle utility sono cresciuti in frequenza e soprattutto in gravità degli impatti oltre alla sofisticazione dell'attacco stesso.

Questi fenomeni hanno indotto un parziale ripensamento sulla importanza della cyber sicurezza ed aumentato in generale la sensibilità degli stakeholders.

I fattori che concorrono ad un buon livello di cyber resilienza od alla sua inefficacia, sono sempre più identificabili in aree specifiche.

La superficie di attacco

Specificatamente per gli ambienti OT, la riduzione della superficie di attacco è una strategia da percorrere, l'accesso alle stazioni di telecontrollo dovrebbe essere garantito da un sistema di identity management e dal repository degli utenti autorizzati, tuttavia questi ambienti hanno dispositivi piuttosto "statici" proprio per favorire la disponibilità dell'impianto, quindi non sempre sono integrabili, anche per intrinseca obsolescenza dei device che hanno una vita molto più lunga che in IT.

Possono essere così adottate altre misure, come il controllo network dei MAC address autorizzati a connettersi alla rete di processo (la intranet OT) oppure implementare il filtraggio a livello di IED (*Intelligent Electronic Device*) per consentire accessi temporalmente limitati.

Per proteggere opportunamente gli ambienti industriali, i comandi e le informazioni scambiate sulla rete operativa dovrebbero essere monitorati, soprattutto ora che i sistemi di sottostazione, una volta indipendenti, risultano sempre più interconnettersi condividendo informazioni; isolare le varie reti l'una dall'altra attraverso un'adeguata segmentazione diventa una possibilità di protezione e limitazione del terreno d'attacco in caso di evento.

Controllo remoto e tele-manutenzione

Oggi le connessioni remote ai sistemi OT non possono più essere fatte se non con tunnel VPN o connessioni con protocollo TLS, questo per garantire la riservatezza dei dati scambiati.

Il rischio da prevenire è quello di azioni di *sniffing* dentro la rete remota che l'attaccante può fare per analizzare ciò che passa in rete, evincere quanti device siano connessi ed i comandi lanciati per poi al momento opportuno inviarne di manipolati per attaccare.

Abbiamo sonde industriali IDS (*Intrusion Detection System*) o IPS (*Intrusion Prevention System*), per verificare coerenza delle informazioni scambiate tra i dispositivi e i livelli network superiori e proteggere adeguatamente i meccanismi di controllo delle apparecchiature elettriche.

Conclusioni

Chi ha avuto la pazienza di leggere fino a qui si sarà reso conto della vastità e della criticità del tema della Cyber Security delle infrastrutture critiche e in particolare delle reti elettriche.

Da una parte la loro progressiva digitalizzazione le rende capaci di prestazioni inimmaginabili o dai costi proibitivi senza poter contare su una intelligenza distribuita fornita dal SW.

Dall'altra l'instrumentazione delle reti con dispositivi digitali le rende potenzialmente vulnerabili in maniera proporzionale al livello di digitalizzazione implementato.

Il messaggio che vorremmo lasciare qui è che non si tratta di dover scegliere il minore dei mali tra i due (reti non digitalizzate o reti digitalizzate vulnerabili) ma di acquisire la consapevolezza che la Cyber Security è una necessità ineludibile che con la giusta attenzione e preparazione può essere adeguatamente trattata in modo da non costituire un ostacolo allo sviluppo digitale delle reti elettriche.

bibliografia

[1] https://www.cyberscoop.com/solarwinds-hack-dragos-ics-breach

[2] https://ollisakersarney.com/blog/cyber-case-study-solarwinds-supply-chain-cyberattack/

[3] https://gca.isa.org/blog/the-top-3-cybersecurity-issues-for-industrial-control-systems-in-2021

[4] https://www.cybersecurity360.it/cybersecurity-nazionale/perimetro-di-sicurezza-nazionale-cibernetica-regole-e-criteri-di-attuazione/