

Smart Grid e Sicurezza ICT: affrontare il problema

Questo articolo prende spunto dalla tesi "SMART GRID E SICUREZZA ICT" svolta da Andrea Gentile presso la Facoltà di Ingegneria dell'Università di Perugia – Relatori: Prof. P. Pozzi (FTI), Ing. Angelo Frascella (ENEA)

Angelo Frascella,
Andrea Gentile, Piero Pozzi



Nel corso di questa breve serie di articoli, pubblicati su Cyber Crime di Luglio-Agosto (n. 3) e Settembre-Ottobre 2011 (n. 4), dedicati al tema della sicurezza ICT per le Smart Grid (SG), si è visto come mondo della ricerca, operatori di rete, industria ed enti di standardizzazione stiano lavorando per far evolvere la rete elettrica per consentire la gestione di un sistema di generazione distribuita, integrando e interconnettendo apparati e sistemi digitali.

Questa trasformazione incrementerà l'intelligenza della rete, supportando le nuove modalità distribuite di produzione e uso dell'energia, ma, allo stesso tempo, renderà l'intero sistema vulnerabile a malfunzionamenti informatici e ad attacchi deliberati.

Alcuni dei fattori critici sono: il grande numero di dispositivi di controllo nella SG, ciascuno dei quali sarà in comunicazione con gli altri e, spesso, sarà fisicamente accessibile, l'utilizzo dei protocolli IP come standard di comunicazione fra essi, il numero crescente di attori che entreranno nel mercato elettrico e l'incremento delle informazio-

ni sensibili che circoleranno nella rete elettrica. Un malfunzionamento o un attacco a questa Infrastruttura Critica Informatizzata sarà in grado non solo di danneggiare il singolo utente o il singolo operatore energetico, ma potrà anche essere uno dei campi di battaglia delle cyberwar, con conseguenze pesantissime per il paese che subisse l'attacco.

Per tali ragioni il problema della sicurezza ICT deve essere affrontato oggi, per evitare di ritrovarsi, domani, con una rete intrinsecamente insicura.

LA BARRIERA CULTURALE

La situazione ideale sarebbe quella in cui le imprese produttrici di dispositivi per SG e del software per tali dispositivi, lavorassero in stretta collaborazione con esperti di sicurezza fin dalle fasi iniziali di progetto. Ciò assicurerebbe che le nuove tecnologie venissero implementate nel modo più sicuro, senza limitare le funzionalità originariamente progettate. Questo è il paradigma della *sicurezza fin dalla progettazione (security by design)* seguendo il quale è più facile ed economico costruire un dispositivo avendo in mente

fin dall'inizio le esigenze di sicurezza anziché dover modificare il prodotto finito ed essere costretti a sviluppare fin dall'inizio patch per chiudere le falle. In uno studio realizzato nel 2011 da J. Wheatman per Gardner, si è confermato come l'importanza strategica della sicurezza ICT non sia facilmente recepita in ambienti aziendali per la scarsa capacità degli esperti di comunicare con i vertici aziendali, ma anche per la scarsa propensione di questi nei confronti dei problemi strettamente tecnici. La "cultura" della sicurezza informatica non è "nel sangue" di molte aziende, tanto meno delle utility energetiche. In particolare queste, fino ad oggi, hanno basato la propria sicurezza sull'uso tecnologie digitali proprietarie per il controllo e l'automazione dei propri sistemi. Questa modalità di fiducia nella "chiusura" delle tecnologie proprietarie, o paradigma della *sicurezza tramite oscurità (security by obscurity)*, dà un falso senso di tranquillità all'azienda. In realtà il malintenzionato studia il protocollo proprietario "chiuso", ne trova le falle e le sfrutta per prendere il controllo dei sistemi.

Nemmeno la ricerca sulle SG sembra abbastanza attenta al problema. Nel report pubblicato nel 2011 da JRC (Joint Research Centre) di Ispra, vengono classificati i progetti europei finora svolti. Questo catalogo comprende ben 219 progetti su vari aspetti delle SG (contatori intelligenti, distribuzione, trasmissione, immagazzinamento dell'energia, applicazioni casalinghe e integrazione fra le varie parti della rete) e 30 vengono analizzati nel dettaglio. La maggior parte di questi progetti ha dato risposte abbastanza lacunose sulle tematiche della sicurezza e della privacy. L'unico che sembra aver preso seriamente in considerazione

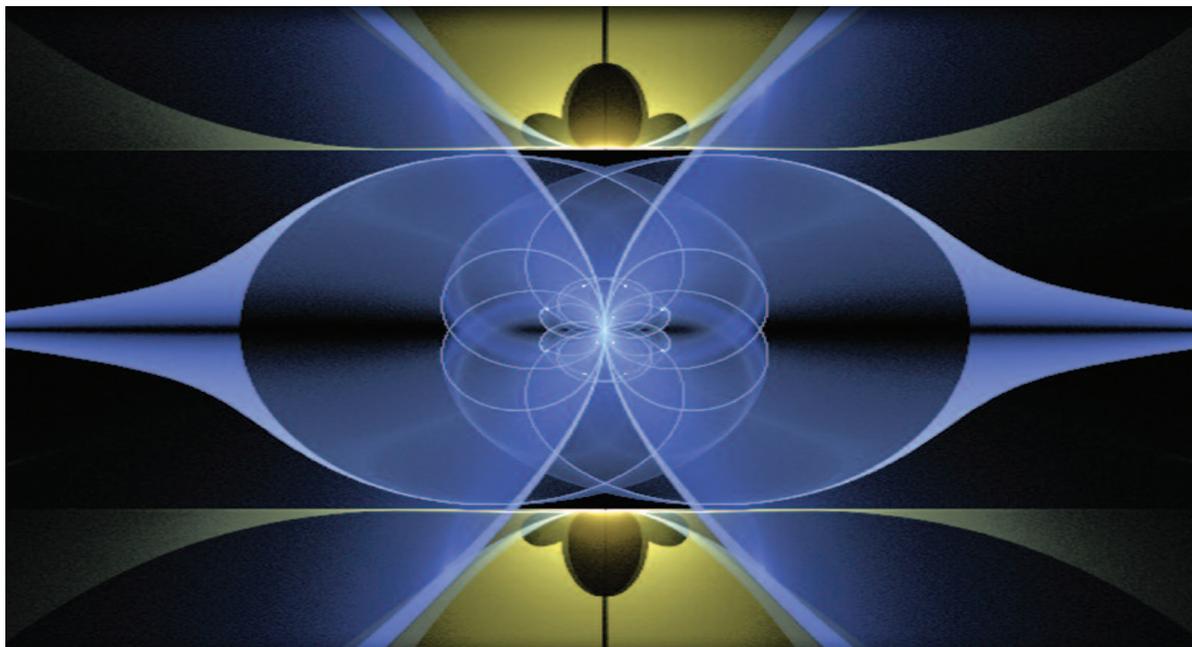
le problematiche delle cyber security è il progetto OpenMeter.

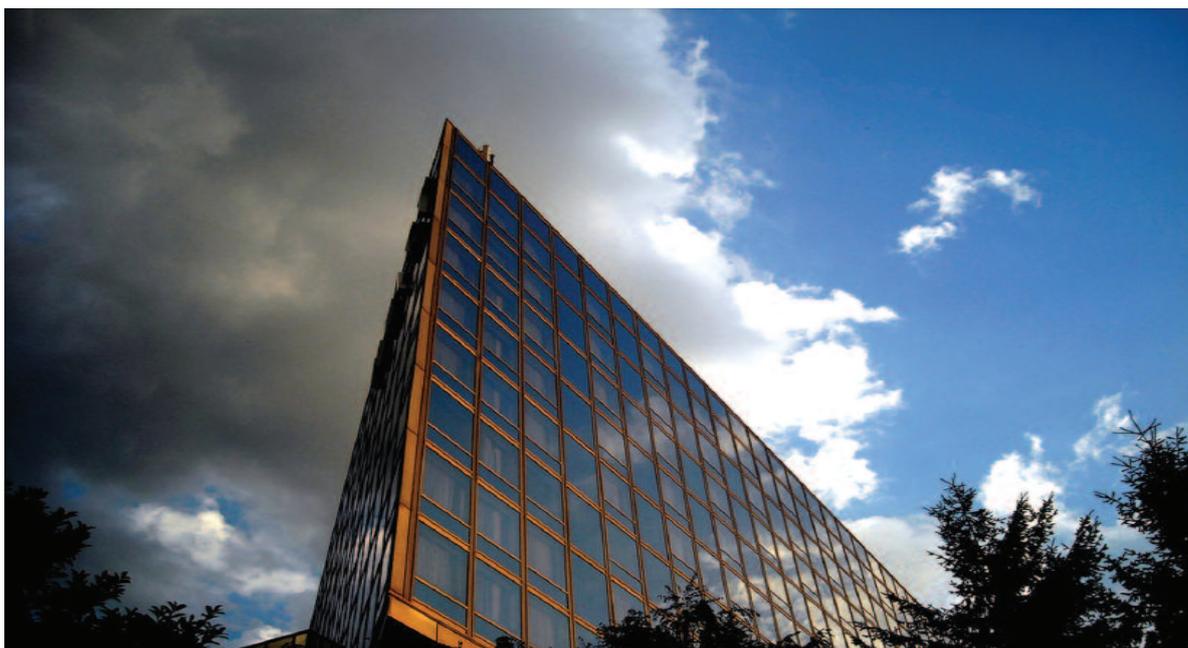
SICUREZZA E STANDARD

Il mondo della standardizzazione dimostra più sensibilità al problema. Esistono già diversi standard generali, alcuni stabili e altri in via di sviluppo, che affrontano i problemi della cyber security. Un riferimento basilare è ISO/IEC 27002:2007 che rappresenta una guida per la gestione della sicurezza ICT dei sistemi informativi e certo deve essere assunto come riferimento anche nel contesto SG.

Ve ne sono altri che coprono più direttamente i vari domini SG. Per esempio, IEC 62351 è stato realizzato con lo scopo di fornire il supporto per la sicurezza a una serie di protocolli definiti da IEC per la rete elettrica e i sistemi di gestione dell'energia, IEEE 1686 affronta la cybersecurity per i dispositivi intelligenti delle sottostazioni della rete elettrica, mentre gli standard americani NERC-CIP dà le linee guida per la cybersecurity delle infrastrutture critiche e AMI-SEC fornisce i requisiti relativi alla infrastruttura di misura (AMI, Advanced Metering Infrastructure) delle SG.

L'aspetto più rilevante è quello metodologico e strategico, che è evidente nel mandato, noto come Mandato 490, che la Commissione Europea ha dato ai principali enti di standardizzazione europei (CEN, CENELEC, ETSI). Come avvenne per lo standard GSM di telefonia mobile, l'ambizione è quella di sviluppare un insieme coerente di standard europei capaci di orientare il mercato e raggiungere obiettivi di interoperabilità, facilitando l'implementazione delle SG in Europa. In esso vi è una particolare attenzione ai temi della





cybersecurity e della sicurezza dei dati. Su questi temi vengono individuati alcuni obiettivi che vanno dallo studio degli standard esistenti allo sviluppo di una serie di servizi standardizzati per l'autenticazione, la firma digitale, la codifica dei dati in ambito SG.

Nell'ambito del Mandato 490, gli enti di standardizzazione europea hanno individuato raccomandazioni più specifiche¹¹ CEN, CENELEC, ETSI, "Standards for Smart Grids - Recommendations for smart grid standardization in Europe" (2011)

, che evidenziano la necessità di assimilare velocemente in tutti gli standard rilevanti per le SG i requisiti di sicurezza e di privacy, ma anche di collegare le funzioni e i casi d'uso delle SG con i requisiti di sicurezza e privacy, di definire meccanismi per aggiornare velocemente tali funzioni quando i requisiti cambiano e la necessità di strumenti informatici per supportare tali attività.

LE LINEE GUIDA DEL NIST

Se in Europa gli enti di standardizzazione stanno iniziando a lavorare sul tema della creazione di un quadro di riferimenti per le SG, negli Stati Uniti tale attività è già in uno stadio avanzato.

In quest'ambito il NIST (National Institute of Standards and Technology) ha definito delle linee guida sulla cybersecurity, in cui identifica sette domini di riferimento (dal grande operatore di generazione elettrica al cliente finale) e, in ciascuno di essi, un certo numero di "attori", che possono essere dispositivi, sistemi o persone, ma in ogni caso sono nodi posti in comunicazione all'interno della rete.

Uno degli obiettivi principali è quello di fornire

uno strumento di valutazione dei rischi. A tale scopo, tutte le possibili interfacce tra gli attori, intese come canali logici di comunicazione, sono individuate e raggruppate in categorie. Per ognuna, tre parametri quantificano l'impatto che avrebbe la perdita di uno dei pilastri della sicurezza (Confidenzialità, Integrità, Disponibilità).

Per esempio, nell'interfaccia fra contatore e operatore che fattura il consumo di energia, viene assegnato un impatto alto per tutti e tre i pilastri, mentre nell'interfaccia fra il sistema di controllo dell'impianto di generazione e il sistema di controllo della trasmissione, una perdita di confidenzialità è considerata poco dannosa, mentre la perdita d'integrità ha un effetto massimo. Per ogni categoria, inoltre, viene fornita una lunga lista di caratteristiche e problemi di sicurezza da affrontare. Infine vengono evidenziati i principali temi di ricerca e le classi di vulnerabilità per le SG.

Tali linee guida sono un buon punto di partenza ma non sono esaustive. Ogni implementazione, infatti, sarà molto diversa dalle altre, in quanto basata su dispositivi funzionalmente identici ma tecnologicamente diversi e avrà bisogno di uno studio specifico.

Nella guida NIST si accenna, in particolare, al problema della continua e inevitabile scoperta di vulnerabilità software. Questo rappresenta il più grande interrogativo sulla reale possibilità di una realizzazione sicura di una qualunque infrastruttura informatica e, purtroppo, anche delle SG.

IL CICLO DI VITA DELLE VULNERABILITÀ SOFTWARE

Al momento del rilascio e nell'uso di un prodotto software, è molto probabile che esso contenga

delle vulnerabilità, la cui gravità può dipendere dal contesto d'uso dell'applicazione. Il ciclo di vita di una vulnerabilità attraversa diverse fasi: dalla evidenza, al momento in cui viene rilasciata una patch software per risolverla e quindi smette di attirare l'interesse dei malintenzionati perché è stata risolta e si ritiene, anche se spesso nel concreto questo non è sempre vero, la patch è stata applicata nei sistemi in campo. Ma nuove e più "interessanti" vulnerabilità sono probabilmente state individuate e il ciclo ricomincia. Come è noto, la fase più pericolosa del ciclo è quella che si colloca fra la scoperta della vulnerabilità e la divulgazione della patch. Prima della evidenza, infatti, il fornitore non potrà iniziare a lavorare sulla correzione del problema e chi ha scoperto la vulnerabilità potrà sfruttarla direttamente o venderla sul "mercato nero".

Anche mantenendo i sistemi correttamente aggiornati alle ultime patch rilasciate dai produttori di software, non ci si può quindi ritenere al sicuro dalle minacce. In ogni caso, una corretta gestione degli aggiornamenti è doverosa.

Come si è accennato nel primo articolo della serie, il rilascio di tali patch in un contesto caratterizzato da un numero così alto di dispositivi, come sarà quello delle SG, potrà richiedere una mole di lavoro enorme e difficile da gestire.

Si potrebbero verificare situazioni in cui un numero consistente di dispositivi non venga aggiornato a quello in cui l'aggiornamento da remoto, per esempio, del firmware (software di base) di un'apparecchiatura (per esempio uno smart meter) non vada a buon fine e provochi funzionamenti anomali o addirittura il guasto del dispositivo.

La conseguenza di un simile evento potrebbe essere l'interruzione della linea elettrica.

COME RENDERE PIÙ SICURA L'INFRASTRUTTURA INFORMATICA DELLA SMART GRID

Sebbene queste osservazioni possano sembrare scoraggianti, conoscere i problemi vuol dire non farsi cogliere impreparati.

Mettendo insieme la conoscenza del contesto, le tecniche generali per la gestione della sicurezza, il lavoro fatto dal NIST e sugli standard si può fare molto per migliorare il livello di sicurezza della nascente infrastruttura e, laddove necessario, stimolare la ricerca perché trovi nuove soluzioni. A livello generale, ecco alcune prescrizioni da seguire per una progettazione accurata dell'infrastruttura informatica delle SG, che ricalcano politiche già modellate per i sistemi informativi:

- Richiedere a sviluppatori e architetti software di modellare i rischi e i potenziali vettori di attac-

co, sulla propria porzione di software. Si noti che queste figure tendono a concentrarsi più sui requisiti funzionali, che su quelli di sicurezza. Perciò dovranno essere addestrati da esperti del settore.

- Effettuare revisioni approfondite del codice sorgente. Il codice dovrà essere controllato sia dai programmatori delle utility, che dai programmatori di terze parti fornitrici di servizi o dispositivi. In tal modo si limiterà al minimo il problematico ricorso agli aggiornamenti.
- Ricorrere sempre alla cifratura, per proteggere la Confidenzialità dei dati dei propri consumatori e dei propri dati aziendali, sia per i dati in transito nelle reti che per quelli memorizzati nei database delle utility. Sebbene rappresenti un grosso onere, la crittografia computazionale dovrebbe essere implementata in ogni dispositivo, anche presso gli utenti.
- Ricorrere a firma digitale del codice e dei comandi da inviare e ricevere dai dispositivi. Senza l'uso di firme digitali, un malintenzionato potrebbe eseguire il proprio codice, per esempio in un contatore intelligente, e inviare comandi verso il resto dell'infrastruttura, che riterrebbe affidabile il contenuto della comunicazione.
- Usare più meccanismi di autenticazione (per esempio una password abbinata a una smart card). Se una delle categorie dovesse essere compromessa, l'autenticazione da parte di chi ha rubato le credenziali non sarebbe comunque possibile. Maggiore è la criticità delle azioni da svolgere, maggiori devono essere le categorie di autenticazione da richiedere.
- Applicare il concetto di "segmentazione" di rete. Nel caos di verifici un attacco, se ne potrà circoscrivere la propagazione in zone ristrette semplicemente bloccando il traffico tra segmenti di rete in cui non serve. In tal modo si potranno limitare quindi i danni ed i costi necessari per il ripristino.
- Svolgere attività di registrazione e monitoraggio di tutti gli eventi, in quanto tenerne traccia permette di avere le informazioni per identificare attacchi e ricostruire il corso degli avvenimenti in caso di incidenti.
- Utilizzare *barattoli di miele (honeypot)*, cioè dispositivi che sembrano far parte della rete e contenere informazioni preziose, ma, in realtà, sono isolati e privi di contenuti sensibili o critici, soprattutto in zone perimetrali dell'infrastruttura delle SG.
- Analizzare la propria infrastruttura con l'occhio dell'attaccante, utilizzando le stesse strategie che utilizzerebbero i malintenzionati, per testare l'infrastruttura informatica delle SG e individuare i punti deboli. ■