PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4198 di Venerdì 16 marzo 2018

È Smart, ma non è sicura: la nuova rete elettrica intelligente

La complessa rete elettrica che va dalla produzione alla distribuzione dell'energia elettrica viene gestita con algoritmi intelligenti, per ottimizzare la distribuzione dell'energia ed i carichi di lavoro degli apparati. Tutto molto bello, ma...

Da più parti, in giro per il mondo, si stanno alzando le voci di specialisti, che segnalano come le moderne reti elettriche intelligenti possano presentare problemi di sicurezza non indifferenti, che potrebbero essere sfruttati sia da terroristi, sia da criminali comuni.

Ad esempio, uno dei più recenti incidenti si è verificato nel dicembre 2017, in Ucraina, dove degli hacker furono in grado di intervenire sulla rete di distribuzione dell'energia elettrica, scollegando dalle reti un certo numero di sottostazioni e lasciando decine di migliaia di persone senza elettricità. In parallelo, gli attaccanti hanno anche preso di mira i call center attraverso un attacco di DDoS alla rete telefonica. Gli utenti non solo sono quindi rimasti senza energia elettrica, ma non ebbero nemmeno la possibilità di chiamare per segnalare l'accaduto.

Un problema alla base della struttura di sicurezza di una rete elettrica intelligente è legato al fatto che in normali sistemi informatici la riservatezza rappresenta un aspetto principale delle misure di sicurezza, rispetto almeno alla integrità e disponibilità dei dati. Per contro, in una rete elettrica intelligente la disponibilità e l'integrità hanno la priorità più elevata, rispetto alla riservatezza dei dati.

Questa situazione apre la porta a possibili attacchi da parte di criminali, che potrebbero essere in grado di tenere sotto controllo l'assorbimento energetico di una specifica utenza, ricavando da queste informazioni notizie in merito alla presenza o meno nell'abitazione degli occupanti.

Non parliamo poi degli attacchi terroristici che potrebbero mettere in ginocchio un paese, bloccando la rete elettrica.

Per la verità, i gestori di queste reti già da tempo si sono attivati per cercare di mettere sotto controllo questi problemi, effettuando interventi, che ad ora devono però ancora essere verificati da un soggetto terzo, come ad esempio una Tiger team.

Ad esempio, i messaggi che vengono spediti e ricevuti dai contatori intelligenti trasportano un identificatore del messaggio e un identificatore del componente. Spedendo due messaggi allo stesso contatore significa che ogni messaggio deve avere un codice

di autentica diverso, mentre spedendo lo stesso messaggio a due diversi contatori occorre associare due codici di autentica diversi. Se non vi è una coerenza in questi dati, la rete ignora i messaggi, supponendo che questi messaggi invalidi siano stati generati da malviventi.

Controllo di anomalia

Un'altra tecnica di sicurezza che utilizzano molti gestori di rete viene chiamata "controllo di anomalia", in quanto la rete è progettata in modo da mettere in evidenza comandi anomali. Si tratta di una situazione non dissimile da quella utilizzata dalle reti ferroviarie, che inviano comandi in linea per l'attivazione di scambi e passaggi a livello. Un messaggio anomalo viene tempestivamente individuato ed annullato.

Ad oggi, bisogna tuttavia riconoscere che queste tecniche di sicurezza sono più mirate a evitare delle anomalie nella distribuzione dell'energia elettrica, che non a proteggere in modo efficiente ed efficace i dati personali degli utenti.

La prossima entrata in vigore a pieno ritmo del nuovo regolamento europeo 679/2016 impone anche ai gestori di queste reti di effettuare delle valutazioni di impatto, che potrebbero mettere in evidenza debolezze strutturali, almeno per quanto riguarda la protezione dei dati personali.

Se un attaccante è in grado di sottrarre questi dati, siamo in presenza di una violazione dolosa di dati personali, che rientrano nell'ambito dell'articolo 33 del regolamento e che necessariamente prevedono la comunicazione di questi dati all'autorità Garante. Se poi l'autorità Garante riterrà che la violazione sia dovuta ad insufficienti misure di sicurezza da parte del titolare del trattamento, le sanzioni potrebbero essere estremamente elevate.

Ancora una volta, tutti gli esperti sono d'accordo che la sicurezza al 100% non esiste, ma resta comunque in capo al titolare del trattamento dimostrare che egli ha fatto quanto era ragionevolmente possibile per mettere sotto controllo la situazione.

Adalberto Biasiotti

---

www.puntosicuro.it