PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4559 di Lunedì 14 ottobre 2019

La sicurezza informatica delle reti elettriche di distribuzione

Il responsabile della sicurezza delle reti elettriche non deve preoccuparsi solo di attacchi terroristici, che colpiscano le infrastrutture fisiche, come trasformatori e tralicci: anche gli attacchi informatici possono essere estremamente pericolosi.

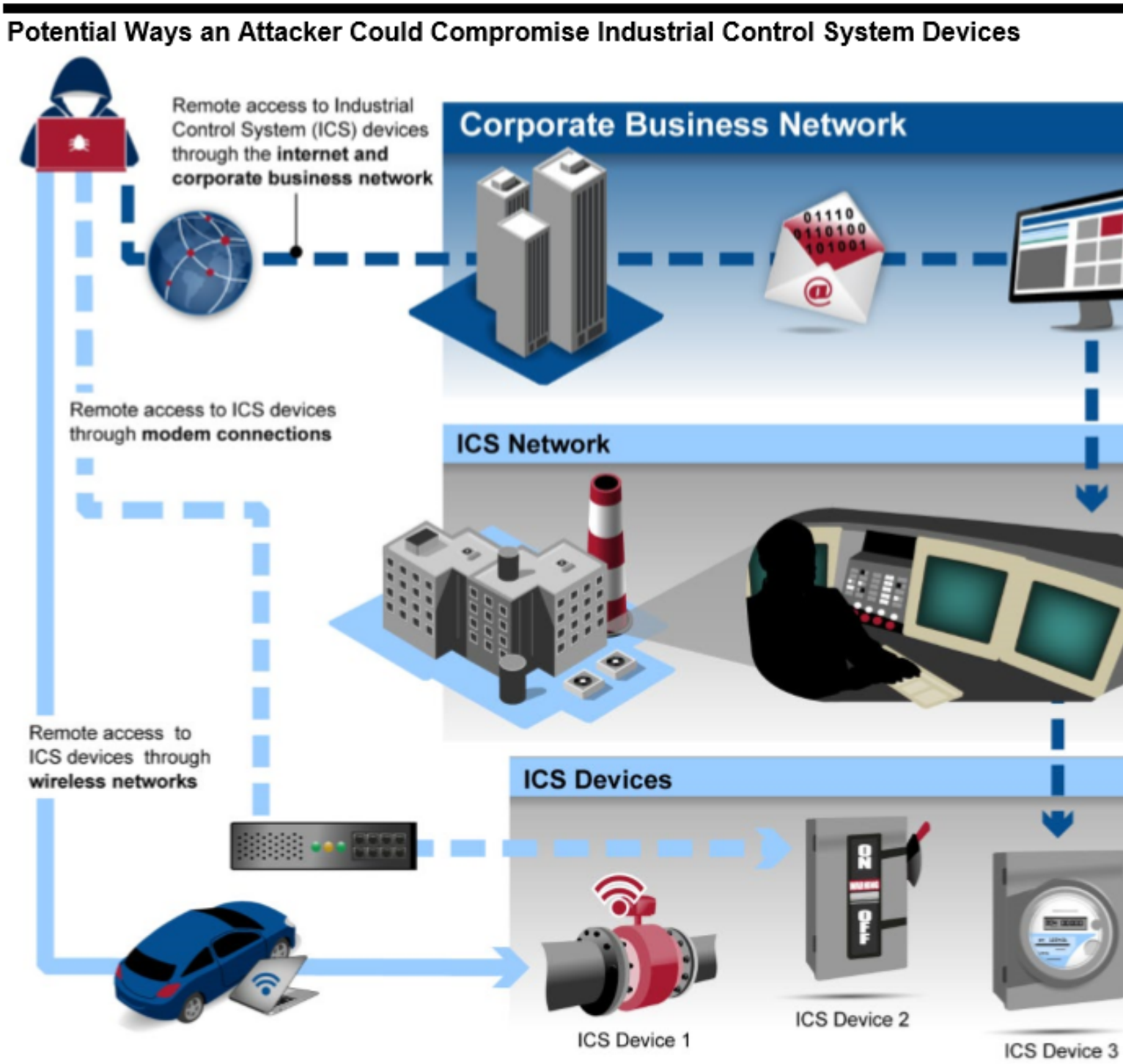
Il General accounting Office, che si occupa anche della protezione di infrastrutture critiche, ha recentemente esaminato, negli Stati Uniti, lo stato della sicurezza anticrimine delle reti elettriche di distribuzione.

Appare evidente a tutti che una rete elettrica nazionale di distribuzione, tenuta in piena efficienza, rappresenta un aspetto fondamentale per la serenità e la sicurezza di tutti i cittadini. Ecco perché un attacco a queste reti può destare preoccupazioni significative; non per nulla, la rete elettrica di distribuzione rientra fra le infrastrutture critiche nazionali, che debbono essere assoggettate a particolari valutazioni di rischio e messa a punto di idonea protezione.

Oggi più frequentemente l'attenzione degli addetti alla sicurezza si concentra sulla difesa delle strutture fisiche, come appunto le centrali di produzione, le sottostazioni di trasformazione, i tralicci e via dicendo. In realtà lo studio sviluppato dal General accounting Office ha messo in evidenza come gli attacchi informatici possano essere assai più letali, soprattutto perché possono colpire contemporaneamente un gran numero di strutture. Il fatto poi che oggi molti gestori delle reti elettriche, tra cui anche i gestori italiani, utilizzino le tecniche chiamate "smart grid", vale a dire tecniche che permettono di predire l'assorbimento energetico nelle varie parti della nazione e provvedere tempestivamente allo smistamento dell'energia elettrica presso le utenze più significative, non fa altro che sottolineare l'importanza della protezione informatica di queste reti.

L'analisi di rischio ha messo in evidenza come molte reti siano vulnerabili ad attacchi informatici, soprattutto quando l'attaccante è in grado di compromettere i sistemi industriali di controllo.

L'immagine che accompagna questo articolo mette in evidenza quali siano le aree di rischio, cui bisogna prestare particolarmente attenzione.



Ad oggi si sono già verificati alcuni incidenti informatici, che hanno coinvolto le reti elettriche, ma questi incidenti erano perlopiù di origine accidentale e non deliberata. In altri paesi, invece, questi attacchi hanno portato a una compromissione allargata delle reti e alla indisponibilità di alimentazione elettrica per gli utenti.

Gli esperti che hanno valutato a questa situazione hanno preso contatto con il Dipartimento dell'energia, che ha sviluppato dei piani per mettere a punto una strategia federale, in grado di inquadrare e mettere sotto controllo il rischio informatico, legato alle reti intelligenti, ma siamo ancora uno stato di pianificazione, più che di pratica attuazione.

Una grave limitazione, in questa strategia, sta nel fatto che mancano informazioni aggiornate sulla rete e l'analisi sin qui effettuata si basa addirittura su informazioni risalenti al 1980. Ciò significa che l'evoluzione della rete non è stata tenuta sotto sufficiente controllo, da parte dei responsabili della sicurezza informatica.

È ben vero che oggi sono disponibili delle norme che stabiliscono dei livelli di protezione da attacchi informatici, ma c'è una bella differenza tra l'avere a disposizione una norma e applicarla in pratica. Un altro problema è legato al fatto che queste norme si applicano solo a porzioni significative di rete, in termini di potenza elettrica coinvolta. Un attacco informatico distribuito potrebbe compromettere un gran numero di insediamenti, dove la quantità di potenza elettrica gestita risulta inferiore a quella, cui la norma si applica. L'impatto sarebbe comunque drammatico su tutte le utenze connesse a questi insediamenti.

Metto a disposizione dei lettori queste indicazioni, non tanto perché la maggioranza dei lettori sia coinvolta, ma soprattutto perché questo studio mette in evidenza come l'analisi dei rischi informatici debba essere oltremodo evolutiva e deve tenersi pronta a fronteggiare rischi, in precedenza non pesati in modo appropriato. Se un'azienda deve garantire la continuità di esercizio del proprio sistema informativo, deve quindi prendere considerazione possibili periodi di assenza di energia di rete, che potrebbero essere ben più lunghi di quei periodi, che oggi si danno per scontati. Un'assenza di energia elettrica primaria dell'ordine di 24 ore è ritenuto un evento abbastanza remoto, mentre questo periodo potrebbe estendersi in maniera significativa, se l'attacco informatico fosse portato con modalità tali da rendere oltremodo difficile il ripristino delle normali condizioni di funzionalità.

Adalberto Biasiotti
