PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4919 di Venerdì 23 aprile 2021

Siamo certi che la rete elettrica italiana sia sufficientemente protetta?

Alcuni problemi che sembra si siano manifestati nella sicurezza informatica della rete di distribuzione di energia elettrica, affidata a Terna, meritano di essere approfonditi, approfittando delle avanzate esperienze degli Stati Uniti.

L'affidabilità della rete elettrica degli Stati Uniti, che rappresenta una componente essenziale della vita dei cittadini, è sempre un tema, che richiede un'attenzione tutta particolare.

La rete elettrica per solito è articolata in tre parti:

- la generazione di energia elettrica,
- la trasmissione ed infine
- la distribuzione.

Il fatto che recentemente nel Texas si sia verificata una drammatica situazione, che ha impedito l'erogazione dell'energia elettrica a milioni di cittadini, dimostra come l'affidabilità della rete, sia a fronte di eventi accidentali, sia a fronte di attacchi fisici od informatici, rappresenti un aspetto fondamentale per la salvaguardia della salute e della operatività della cittadinanza.

Questo è il motivo per cui General accounting Office, GAO, negli Stati Uniti, ha riesaminato tutti gli aspetti afferenti alla sicurezza della rete elettrica, prestando particolare attenzione:

- agli attacchi informatici, con una valutazione delle conseguenze potenziali di questi attacchi,
- alla descrizione delle iniziative prese dai soggetti coinvolti per migliorare la sicurezza informatica della rete di distribuzione,
- ed infine a quali particolari iniziative sono state attivate dalle strutture militari, che potrebbero essere più gravemente compromesse dalla mancanza di energia elettrica.

Il motivo per cui il General Accounting Office ha prestato particolare attenzione ad attacchi informatici, è legata al fatto che oggi la gestione della rete, dalla produzione dell'energia fino alla distribuzione a livello residenziale, è basata su strutture informatiche.

Gli attacchi informatici, cui può essere soggetta la rete, sono di varia natura.

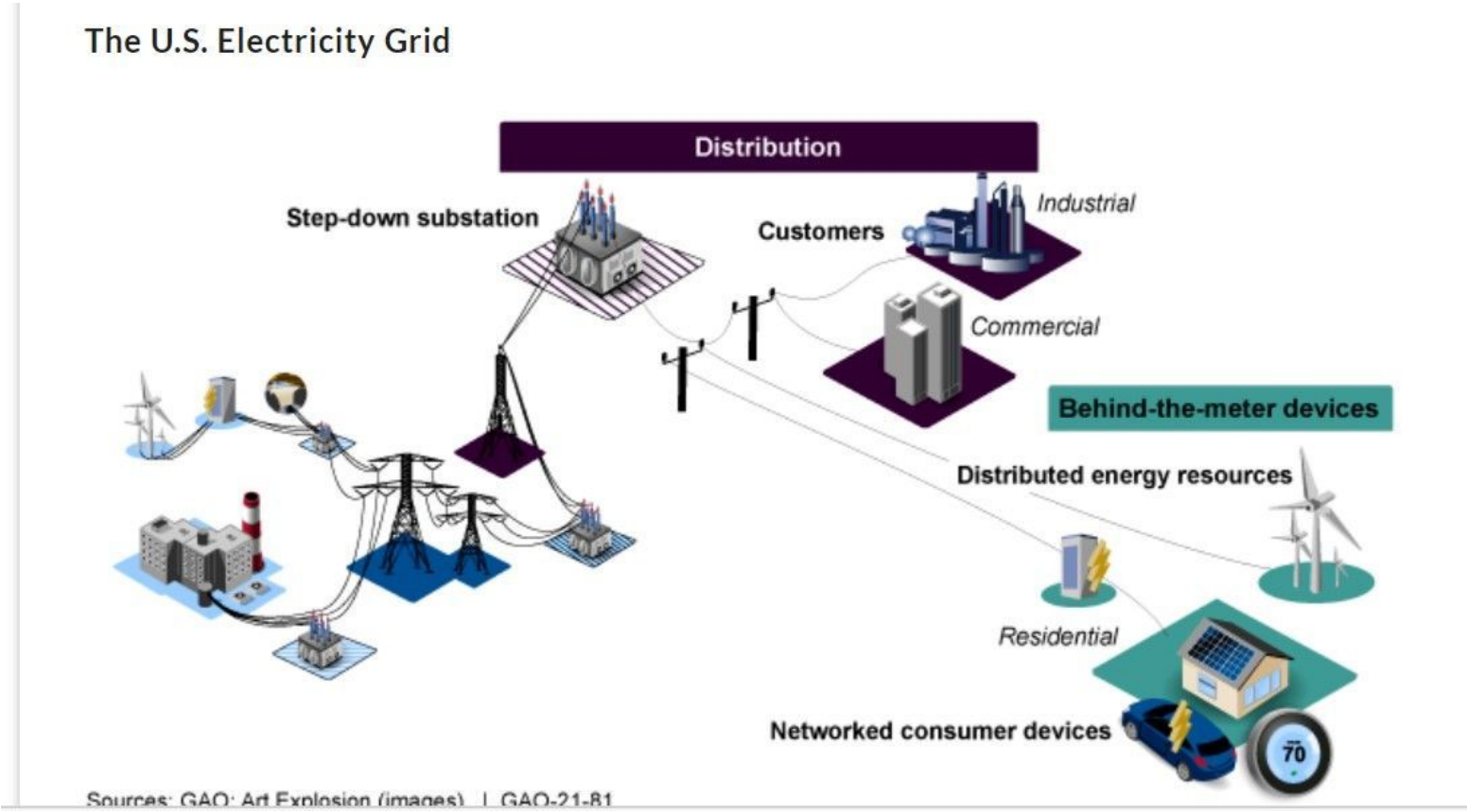
Gli attaccanti, ad esempio, possono compromettere la catena di rifornimento dei sistemi di controlli industriali, manipolando prodotti hardware e software, prima che essi vengano utilizzati presso l'utente.

Oggi moltissime aziende utilizzano dei sistemi di controllo industriali accessibili via Internet e, in assenza di adeguate protezioni, è possibile comprometterli in modo drammatico.

L'esperienza collegata all'attacco che è stato indirizzato alle centrifughe, utilizzate dall'Iran in fase di arricchimento dell'uranio, ne è una prova evidente.

Gli attacchi possono anche essere diretti verso le reti che permettono agli utenti aziendali di collegarsi alla rete, tramite una rete privata virtuale. Gli attaccanti possono usare queste possibilità di collegamento per assumere il controllo delle reti e dei sistemi di controllo industriale.

Infine, l'intera rete può essere soggetta agli attacchi ormai chiamati correntemente "spearphising", costituiti da messaggi di posta elettronica, con allegati o link, che possono consentire ad applicativi dolosi di accedere alle reti aziendali o addirittura alle reti virtuali private.



È ben vero che il Dipartimento dell'energia, a livello federale, ha sviluppato dei piani per attuare una strategia di sicurezza informatica a livello nazionale, applicata alla rete elettrica, ma sembra che ad oggi questi piani non prenda conto figurano in

considerazione tutte le varie modalità di attacco, che i malviventi continuano a mettere a punto.

Adalberto Biasiotti

---

www.puntosicuro.it