PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4968 di Venerdì 02 luglio 2021

Il confine sfumato fra attacchi terroristici e attacchi informatici

Talvolta è difficile individuare un confine netto fra un attacco terroristico ed un attacco informatico, con richiesta di riscatto. L'attacco di cui è rimasta vittima la Colonial pipeline negli Stati Uniti ne è un classico esempio.

Per definizione, un attacco terroristico è tale quando l'attaccante non è animato da motivi economici. Il fatto poi che le conseguenze di un attacco informatico, con finalità di terrorismo o finalità di ricatto, siano poco diverse, dimostra quanto oggi sia complessa la difesa di infrastrutture critiche.

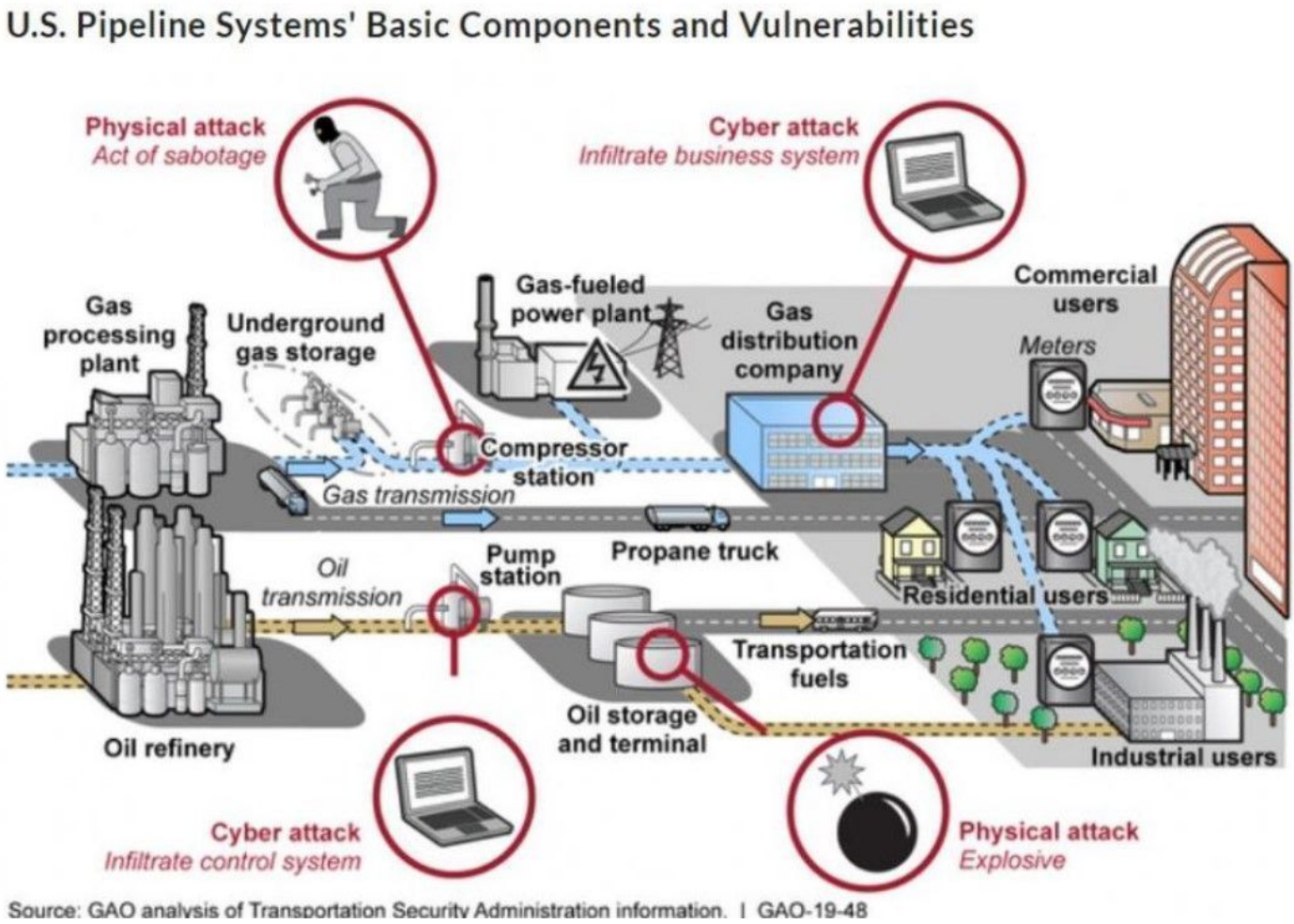
Il recente attacco informatico alla Colonial pipeline, negli Stati Uniti, che ha portato ad uno sconvolgimento temporaneo nella distribuzione di benzina ed altri prodotti petroliferi in gran parte della costa sud orientale degli Stati Uniti, ne è un tipico esempio.

L'indagine condotta dal General accounting Office, magistralmente illustrata nella infografica allegata, ancora una volta mette in evidenza come le minacce informatiche alle infrastrutture critiche richiedano una attività di prevenzione ben più incisiva di quella attualmente svolta.

Ecco il quadro della situazione.

Più di 2, 7 milioni di miglia di oleodotti trasportano e distribuiscono petrolio, gas naturale e altri prodotti critici negli interi Stati Uniti. La protezione del sistema di oleodotti è una responsabilità condivisa sia a livello di governo federale, sia a livello di aziende private, che gestiscono questi oleodotti.

Ecco una info grafica illuminante, che mette in evidenza tutti i punti deboli di questa struttura.



Anche se gli attacchi fisici, ad esempio con esplosione di un ordigno, rappresentano un rischio primario, le vulnerabilità di una rete di oleodotti sono assai differenziate, e tra questi il rischio di attacco informatico è particolarmente grave.

Secondo le informazioni fornite dalla Colonial pipeline, il 7 maggio, l'azienda viene a sapere che era vittima di un attacco informatico. Gli attaccanti hanno introdotto un ransomware nel sistema informativo dell'azienda; questo tipo di attacco rende difficoltoso l'accesso ai dati operativi, in pratica bloccando la operatività aziendale. Il ransomware utilizzato si chiama DarkSide.

La reazione dell'azienda si è articolata in due fasi:

- dapprima l'azienda ha isolato molti apparati di rete, compromettendo tuttavia la possibilità di distribuzione del carburante,
- indi si è attivata per recuperare i dati bloccati.

Alla data del 12 maggio, non vi erano però indicazioni circa il fatto che questi sistemi operativi fossero stati violati. L'isolamento di questi apparati, tuttavia, ha portato all'arresto temporaneo della movimentazione dei fluidi. Il 13 maggio l'azienda ha riferito che la rete aveva recuperato la piena operatività.

Nel frattempo, tutte le cronache nazionali hanno dato notizia di lunghe code ai distributori, dovute al fatto che gli utenti temevano di rimanere a secco, nonché del fatto che l'azienda aveva pagato un riscatto di 5 milioni di dollari.

Al proposito, vale la pena di ricordare che nel dicembre 2018 la gestione degli oleodotti, affidati alla Transportation Security Adminstration, aveva messo in evidenza delle significative debolezze informatiche, che hanno portato all'emissione di ben 10 raccomandazioni migliorative. Ad oggi, solo sette di queste raccomandazioni sono state attuate.

Ancora, a tutto il settembre 2020, il General accounting Office aveva pubblicato la bellezza di 3300 raccomandazioni, mirate al miglioramento della resistenza ad attacchi informatici della rete di distribuzione, ma ad oggi ancora molte raccomandazioni non sono state attuate.

Alcuni lettori potrebbero chiedersi: l'Italia come è messa? Ai posteri l'ardua risposta.

Adalberto Biasiotti

---

www.puntosicuro.it