Un enorme oleodotto statunitense è stato preso in ostaggio dagli hacker

Code interminabili di automobilisti si stanno accalcando davanti a tutte le pompe di benzina della **costa est statunitense**, così da riempire i serbatoi con disperati rifornimenti d'emergenza. In una sola settimana, le richieste di carburante sono salite dal 20 al 40 per cento, un fenomeno che solitamente è riservato a quelle occasioni in cui un cataclisma meteorologico si sta per abbattere sui centri urbani, tuttavia questa volta le preoccupazioni dei cittadini hanno a che vedere con un **attacco hacker**.

Venerdì 14 maggio la **Colonial Pipeline Co.** si è infatti vista costretta a bloccare l'operatività della sua intera infrastruttura, un'infrastruttura non da poco, visto che gestisce una oleodotto di quasi 3.500 chilometri e che distribuisce circa il 45 per cento dei carburanti utili ad alimentare le autovetture e i jet della parte orientale del Paese. Il risultato è che **17 Stati sono ora in stato di emergenza** e il prezzo della benzina sta progressivamente salendo, con l'Amministrazione Biden che ha provato a intervenire approvando domenica una legge che permette il trasporto massiccio su gomme degli idrocarburi, ma la cosa non ha rappresentato che un mero palliativo.

Ciò che è noto è che il tutto **sia stato causato da un *ransomware***, ovvero da un "sequestro" di 100 GB di dati per cui, dicono persone vicine si fatti, i criminali hanno chiesto un riscatto dalla portata non meglio definita. L'FBI punta il dito contro i cybercriminali russi di DarkSide i quali, a loro volta, si sarebbero smarcati da eventuali ideologie socio-politiche per sottolineare che loro siano esclusivamente interessati esclusivamente al vil denaro.

Senza attardarsi troppo nel ginepraio rappresentato dal cyberspionaggio internazionale e dalle letture propagandistiche dei fatti, questo attacco ha reso evidenti i limiti e le vulnerabilità degli Stati Uniti, Paese che per anni non ha finanziato il rimodernamento delle proprie infrastrutture critiche, abbandonandole in uno stato di **obsolescenza**. Complici gli incalcolabili disastri informatici che hanno recentemente colpito gli USA – il caso SolarWinds e il caso Microsoft Exchange -, i sistemi legati al Governo sono sempre più un colabrodo in cui è facile per i malintenzionati infiltrarsi, ancor più perché nessuno ha intenzione di **investire adeguatamente nella cybersicurezza**.

Il settore lamenta infatti che vi sia una grave penuria di esperti, tuttavia è anche vero che le aziende hanno generalmente difficoltà a tenersi i professionisti migliori, i quali vengono reclutati direttamente dalla National Security Agency (NSA) per infiltrarsi nei server stranieri. La stessa NSA ha dunque il problema omologo, considerando che un numero considerevoli dei suoi dipendenti, fattisi le ossa, abbandona il governo per arruolarsi nelle più remunerative **ditte private di spionaggio**.

Dopo aver puntato per anni sul fomentare la competitività del mercato e sul pianificare

stratagemmi di controllo che hanno dato vita al capitalismo della sorveglianza, gli Stati Uniti si sono creati un vero e proprio campo minato in cui gli è divenuto difficile districarsi. La situazione è resa ulteriormente insidiosa dal fatto che la situazione amministrativa della cybersicurezza a stelle e strisce sia **spezzata tra due organi governativi**: il Cyber Command del Pentagono, il quale si occupa di attaccare le altre nazioni con uno schema di "difesa in anticipo", e l'Infrastructure Security Agency del Dipartimento della sicurezza interna.

Quel che è peggio, **non esisterebbero soluzioni definitive per il prossimo futuro**, almeno stando al report pubblicato nel 2020 dalla Cyberspace Solarium Commission, un corpo intergovernativo bipartisan il cui scopo sarebbe proprio quello di sviluppare strategie di difesa contro le insidie digitali. Il problema di base è infatti esterno alle mani del Governo e la sua radice la si ritrova nei modi in cui il mondo globalizzato si approccia agli affari. **L'economia spinge perché le aziende tecnologiche aggiornino i propri prodotti rapidamente**, cosa che comporta necessariamente una gestione molto leggera dei tempi di rodaggio dei software, i quali finiscono con l'essere immessi nel mercato con criticità che possono non di rado causare problemi, primo tra tutti la fuga di dati.

Alleggerire il peso dei cyberattacchi richiederebbe un uso più parsimonioso e sobrio della Rete, ma proprio la Rete rappresenta ora più che mai una miniera d'oro di introiti, causando un cortocircuito che gli USA non intendono approcciare.

[di Walter Ferri]