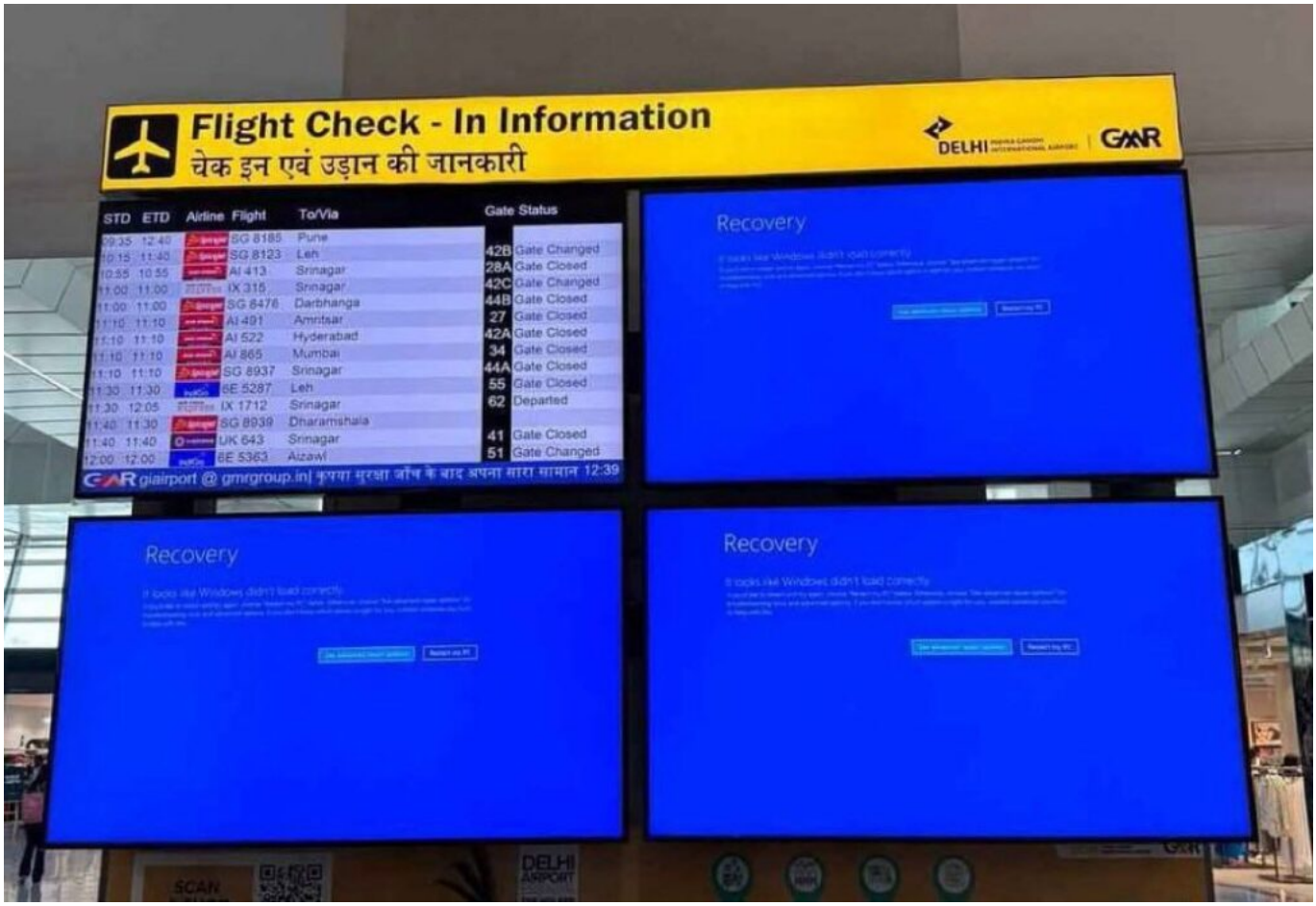
All’albeggiare del 19 luglio, il popolo australiano si è svegliato e ha scoperto che molti dei computer di aziende e istituzioni, semplicemente, non funzionavano. Al posto dei soliti programmi e finestre, i terminali presentavano quella che in gergo viene chiamata la “schermata blu della morte”, che sui dispositivi Windows segnala un errore di sistema critico che non può essere risolto autonomamente. Con il passare delle ore, sempre più nazioni si sono rese conto di star patendo lo stesso problema: Malesia, India, Olanda, Regno Unito, Germania, Spagna, Stati Uniti e molti altri. Banche, Borse, media d’informazione, ospedali e compagnie aeree stanno subendo rallentamenti o **interruzioni nei servizi**. Il danno economico è difficile da stimare. Ciò che è più chiaro, sono le cause: stando alle prime ricostruzioni, il pesante disagio sarebbe stato causato da un **aggiornamento difettoso** di un programma informatico.

A essere finito sotto accusa è infatti il *software* Falcon Sensor, prodotto e distribuito dall’impresa di cybersicurezza **Crowdstrike**. L’azienda in questione non è certamente tra le più rappresentate nella cultura di massa, tuttavia non stiamo parlando di una realtà piccola o priva di mezzi: lo scorso giugno, Crowdstrike è stata inserita nel prestigioso indice di Borsa Standand & Poor’s 500, mentre nel 2020 l’azienda avuto un ruolo rilevante nell’identificare nel Governo russo il sospettato numero uno per gli attacchi hacker subiti dagli USA durante le elezioni del 2016.

Il fatto che un’entità tanto potente possa banalmente aver messo online per errore un *update* dannoso ha indotto alcuni osservatori a pensare che Crowdstrike fosse caduto vittima di un cyberattacco di natura politica. Tuttavia, il coordinatore della National Cyber Security australiana, Michelle McGuinness, e l’Agenzia nazionale francese per la sicurezza dei sistemi informatici (ANSSI) hanno immediatamente bocciato l’ipotesi, sostenendo che non ci siano indizi che promuovano la pista del cyberterrorismo. Quali che siano le cause, gli effetti sembrano però essere ben definiti: Falcon Sensor, una volta aggiornato, sarebbe **entrato in conflitto con il servizio cloud di Microsoft**, Microsoft Azure, rendendo inoperabili i computer dei propri clienti.



L’effetto del bug sui terminali di informazione sui voli dell’aeroporto di Nuova Delhi, in India.

Un problema non da poco, se si considera l’ampio spettro di aziende che si sono appoggiate a Crowdstrike per tutelare i propri sistemi informatici da ogni forma di accesso illecito. Tra le **imprese ed entità coinvolte** figurano Sky News, Ryanair, Sisal, Wizz Air, Delta Airlines, United Airlines, American Airlines, Turkish Airlines, il sistema sanitario nazionale britannico, la Borsa di Londra. E poi gli aeroporti di Melbourne, Singapore, Vienna, Milano, Catania, Los Angeles e altri ancora. Stando ai dati diffusi da Cirium, azienda specializzata nell’analisi aviaria, **nella sola Italia si parla già di almeno 45 voli cancellati**. Alla luce di quanto sta succedendo, le quotazioni statunitensi di Crowdstrike hanno subito un tracollo di più del 20%, con una perdita di valore stimata in 16 miliardi di dollari.

Microsoft, dal canto suo, ha riferito genericamente che i disagi siano stati causati “da un aggiornamento di un software di terze parti”, ma anche che le “cause fondamentali” del problema siano state risolte. Tuttavia, riferisce cautamente la Big Tech, “l’impatto residuo”

continuerà a colpire i servizi per un tempo non meglio definito. Probabilmente giorni. Questi disagi planetari saranno comunque quasi certamente al centro di varie indagini mirate a identificare cosa abbia spinto Crowdstrike a distribuire un *update* obbligatorio tanto disastroso. Nel frattempo, **l'episodio ha ricordato ai popoli e ai legislatori di tutto il mondo come la "*cloud economy*" non sia priva di insidie**, e come anche i software più superficiali siano ormai tanto integrati nelle Reti informatiche che basta una svista per creare un disastroso effetto domino.

[di Walter Ferri]