



Linate, check in fuori uso. Basta un tombino della Telecom per sabotare la cybersecurity?

Parlano tutti di cyberwar e mostrano i muscoli come il gigantesco Golia di biblica memoria. Primi tra questi i vettori dell'informazione che non perdono occasione per vantare iniziative futuribili, ostentare progetti avveniristici, raccontare di essere pronti a qualunque genere di attacco. Avevo pensato di lasciarmi convincere e – mentre guardavo al domani con maggiore serenità – ho scoperto che Davide aveva preso le sembianze di un tombino o, a volerlo nobilitare, di un “pozzetto” in cui vengono ospitati cavi, giunzioni e connessioni delle reti di comunicazione.

L'impari duello tra il ciclope e il minuscolo avversario c'è stato all'alba, secondo le migliori tradizioni di chi sfida qualcuno a singolar tenzone. Alle 6 di stamane le prime vittime. Niente di grave, per fortuna, perché a farne le spese sono stati solo i viaggiatori in attesa dell'imbarco all'aeroporto di Linate e il danno si è limitato ad uno spiacevole ritardo. I sistemi informatici dello scalo, infatti, sono andati in tilt e subito la preoccupazione ha lasciato briglia sciolta a chi non ha esitato a immaginare qualche azione hacker o ancor peggio un sabotaggio terroristico.

Nulla di tutto questo. Le minacce che per consuetudine vengono ipotizzate a sproposito non hanno alcuna responsabilità nell'accaduto. Il blocco dei computer adoperati per le normali operazioni di check-in è da ricondursi al banale allagamento di un pozzetto della Telecom che – finito fuori uso – ha determinato l'interruzione delle connessioni telematiche indispensabili per l'ordinario svolgimento delle operazioni a terra.

Voluminosi risk assessment e impeccabili documenti di valutazione della vulnerabilità informatica hanno palesato la loro totale inutilità e dimostrato che prima della “impermeabilità” dei sistemi, sarebbe il caso di cominciare a esaminare quella più materiale degli alloggiamenti in cui trova collocazione il tessuto connettivo digitale senza il quale è impossibile dar corso anche alle attività più elementari.

Le operazioni di registrazione hanno subito un significativo rallentamento perché – inutilizzabili i computer – è stato necessario tornare a “carta e penna” per non bloccare i voli. La compilazione manuale delle carte di imbarco e la registrazione old style del bagaglio hanno caratterizzato la giornata.

La caccia al colpevole non ha richiesto il ricorso a speciali detective o imbattibili esperti di intelligence: è bastato davvero poco per ricordare il tracciato dei delicati gangli della rete Internet aeroportuale. L'esame delle condizioni dei pozzetti con le centraline Telecom di Novegro ha lasciato intendere che la situazione poteva tornare alla normalità senza ulteriori problemi. Nessun antivirus o firewall, ma un paio di pompe idrovore sono bastate a superare l'imbarazzante impasse. Almeno fino alla prossima pioggia...

Di queste ed altre cose si parlerà domani in un convegno dal titolo wertmulleriano: “Dopo il ministero degli Esteri e le vittime del ransomware Petya, a chi tocca?”. L'evento gratuito – che si terrà all'Aula Multimediale dell'Università telematica internazionale Uninettuno alle 10 di domani, 14 luglio – è il primo di un ciclo di conferenze e seminari in materia di cyber security mirati a creare una cultura che finora è mancata e fruibile anche in streaming per chi non riesce a raggiungere la sede dell'incontro.

di Umberto Rapetto