Il caso Almaviva (ma non solo) e la sovranità tecnologica a chiacchiere

17 dicembre 2025

2,3 terabyte di dati strategici nazionali sul dark web. Piani industriali di Ferrovie dello Stato, contratti con il Ministero della Difesa, documentazione riservata su progetti che coinvolgono Leonardo. Almaviva – 41.000 dipendenti, fornitore di servizi di cyber security al settore Difesa e Sicurezza – è stata penetrata in profondità da quello che gli analisti definiscono un'"infiltrazione profonda e prolungata".

Il danno è fatto. Le indagini sono in corso. E noi vogliamo tentare un esercizio di fantasia.

Immaginate che…

Immaginate che circa un anno fa l'amministratore di una piccolissima azienda italiana (ripetiamolo, italiana) che sviluppa tecnologie di sicurezza informatica innovative abbia incontrato i vertici di Almaviva: presentazione della tecnologia con, in risposta, l'abituale, ostentata sufficienza. Tuttavia, per effetto della presenza di "terzi" e per non mostrarsi più *snob* del dovuto, viene spedito a confrontarsi, per una valutazione tecnica preliminare, con tecnici interni di fiducia.

Qualche giorno dopo si svolge la preliminare e l'incaricato guarda, valuta, comprende. La sua reazione è netta: **"Questa roba serve ai nostri clienti"**. Non una certificazione formale, beninteso, solo il riconoscimento esplicito che la soluzione risponderebbe a bisogni concreti; diciamo "risponderebbe" perché, fino a quel momento, la valutazione non è terminata. Quest'azienda italiana (chiamiamola *Mandolino srl*, così restiamo nei luoghi comuni) ne è molto soddisfatta. Da quando, infatti, ha depositato il brevetto e si è messa sul mercato, ai potenziali clienti non chiede altro che di **testare la sua soluzione**, tant'è che il suo motto è

> *"Ve lo regaliamo per farvelo violare, ve lo vendiamo se non ci riuscite"*

Immaginate ora che da quel momento non succeda più nulla. Nessun approfondimento, nessun test, nessuna PoC, nessun *pilot* – nonostante l'offerta di verifiche approfondite e gratuite, appunto, senza impegno. Silenzio.

Passano i mesi. Un anno. Poi arriva il breach. 2,3 terabyte. Infiltrazione profonda. Dati strategici compromessi. Cosa è andato storto?

La strategia del paracadute d'oro

Parliamoci chiaro, in questo racconto ipotetico nessuno potrebbe affermare che con la soluzione della Mandolino srl il *breach* non ci sarebbe stato, e il punto è proprio questo: **nessuno può affermarlo** (tranne forse la Mandolino perché sa di cosa parla, ma ne se guarda bene perché sarebbe del tutto irrituale). Spieghiamoci meglio.

Nel mondo *IT corporate* esiste una regola non scritta:

> *"Nessuno viene mai licenziato per aver scelto IBM"*

O Fortinet. O Cisco. O Palo Alto. O qualcuno con bellissime certificazioni tutte colorate. Puoi essere bucato, ma se hai scelto un brand riconosciuto, la poltrona è salva. Hai fatto "la scelta responsabile", hai seguito la "best practice".

Il paradosso? Tutti i grandi brand sono stati violati, ripetutamente. Pensate a Fortinet stessa: ha subito un breach nel 2022 via zero-day che ha compromesso migliaia di sistemi, con accesso persistente mantenuto anche dopo le *patch* (e qui dovete immaginare una parentesi con dentro un *fottilione* di punti esclamativi).

Eppure continua a essere scelta. Perché? **Perché protegge "te", non i sistemi.** È la cultura del CYA – *Cover Your Ass*. L'alibi istituzionale conta più dell'efficacia reale. Se vieni bucato dopo aver scelto il leader di mercato, chi può biasimarti? Hai fatto tutto "secondo i canoni". Il problema era "troppo sofisticato", l'attacco "troppo avanzato", la minaccia era una "APT di livello *nation-state*". Mai, mai la scelta tecnologica in sé.

Però, se un'azienda italiana presenta una soluzione innovativa, brevettata, in tecnica non nota, con *track record* documentabile, la reazione è diversa. Troppo rischiosa per la carriera. A volte viene da pensare che non riescano a capirla.

Sia come sia, questa mentalità ha un prezzo che si misura in terabyte di dati strategici sul dark web.

L'ipocrisia della sovranità tecnologica

Quanto parlare di sovranità tecnologica, vero? Convegni, tavole rotonde, dichiarazioni solenni. Sui palchi dedicati alla *cyber security* delle infrastrutture critiche si parla di *resilienza* (altro termine completamente sbagliato ma che fa molto figo, moderno e competente), di "farsi trovare preparati", di ecosistema nazionale. Applausi, strette di mano, foto di gruppo.

Poi si scende dal palco e si riprende a mangiare groviera a colazione, pranzo e cena.

Insomma, cosa manca? Forse la competenza? Naaaaa, mica sempre. La volontà? Più probabile. Il rispetto del proprio mandato? Ecco, questo è interessante. Chi gestisce infrastrutture critiche ha (avrebbe?) un **mandato** preciso: **valutare** e **scegliere** le soluzioni **migliori** per proteggere gli asset.

Certo, "migliori" è un termine pericolosamente vago: "migliori" per chi? E in cosa? Migliori per la propria carriera? Ne abbiamo parlato. Migliori per convenienza politica o di relazione? È praticamente la stessa cosa. Migliori per la funzione che devono svolgere? Beh sì, questo sì. E come faccio a sapere se sono migliori? **Le devi provare!** Le devi provare, santo cielo, le devi provare! Devi essere disposto (e determinato) a farlo, e abbastanza competente, e libero, da decidere se sono eleggibili o no.

Bene: ma quando questo mandato viene disatteso, quali conseguenze ci sono? Se vieni bucato dopo aver scelto Fortinet, nessuna. Hai fatto "la scelta responsabile". Al massimo cambi dipartimento. Il sistema ti protegge. Se invece avessi scelto quella piccola azienda italiana (posto che te l'avessero permesso, ovvio) e fossi stato bucato? Carriera e relazioni preferenziali finite. "Come hai potuto correre questo rischio?"

Ed ecco un bel problema: l'asimmetria totale delle conseguenze. Finché questa asimmetria esisterà, il sistema non potrà cambiare. Non cambierà con i convegni sulla sovranità, non con le direttive NIS2.

Questa è la sovranità tecnologica italiana: proclamata nei convegni, ignorata nelle decisioni. Preferiamo fornitori extra-UE con le loro implicazioni geopolitiche, piuttosto che rischiare con una tecnologia italiana che funziona.

Un sistema che premia l’immobilismo

Continuate con l’esercizio di fantasia e supponete che non sia un caso isolato. Immaginate cioè che la *Mandolino srl* abbia vissuto questa dinamica decine di volte. Certo, si potrebbe sempre pensare che, in fondo, sono loro a essere delle pippe, però è indimostrabile e l’affermazione resta faziosa. Perché vedete, esiste un principio logico molto semplice. Se qualcuno ti presenta una soluzione in tecnica non nota affermando che rovescia i paradigmi, hai due opzioni razionali:

1. Pensi sia un ciarlatano e lo mandi via educatamente (o anche no, sai che novità)
2. Decidi che vale la pena verificare e lo metti alla prova

Tertium non datur. Non esiste una terza opzione logicamente coerente.

Eppure è esattamente ciò che accade: si arriva al punto in cui un tecnico interno – uno dei tuoi, pagato per valutare le soluzioni – dice esplicitamente che “serve ai nostri clienti”, “dovremmo averla tutti” ecc. (aggiungiamoci anche un bel “se fosse vera” di prima battuta, frase che la *Mandolino* potrebbe ormai mettere sulle brochure per tutte le volte in cui l’ha sentita). Ma poi non si approfondisce. Non ci si sporca le mani a verificare. Non si mette alla prova il possibile (enorme) vantaggio.

Perché? Perché farlo significherebbe assumersi una responsabilità. Significherebbe uscire dalla *zona di comfort* dei *brand* noti (un giorno dovremo decidere se bruciare sul rogo prima “zona di comfort” o “resilienza”. “Resilienza”, senza dubbio). Il problema è che nella *zona di comfort* non ci sono solo le poltrone sicure. Ci sono anche gli attaccanti, che conoscono perfettamente quelle soluzioni note, quelle vulnerabilità ricorrenti, che hanno tutto il tempo del mondo per infiltrarsi, mappare, esfiltrare.

> Zona di comfort per i decisori = zona di comfort per gli attaccanti

Gli unici a non essere comodi sono quelli i cui dati finiscono sul dark web. Insomma, nel nostro esercizio di fantasia, questo schema si ripete continuamente: sovranità tecnologica a chiacchiere e comode poltrone di pelle pregiata in attesa di un nuovo convegno con ali di folla plaudente e un occhio di bue.

Ora, per finire, una domanda piuttosto triste: secondo voi, questa storia è vera?
