29 dicembre 2016 16:25

Biglietto aereo e dati personali a rischio pirateria informatica

di Redazione

Le politiche europee si dedicano da anni alla questione della condivisione dei dati dei passeggeri aerei. Senza dubbio non sanno che questi sono gia' accessibili al primo venuto. Con qualche click e' facile accedere alle informazioni personali di centinaia di milioni di passeggeri aerei -ed anche modificare o annullare il loro volo in alcuni casi- in ragione del deficit di sicurezza, se non una totale inesistenza della stessa, del sistema di prenotazione.

E' la constatazione allarmante fatta da Karste Nohl e Nemanja Nikodijevic, due specialisti di sicurezza informatica, che hanno presentato i loro lavori lo scorso 27 dicembre ad Amburgo nel quadro della 34ma edizione del Chaos Communication Congress (CCC), la kermesse degli hacker.

I due esperti si sono interessati ai Global Distribution Systems (GDS): delle aziende che collegano i venditori di biglietti aerei e le compagnie aeree. Queste ultime forniscono il prezzo di ogni volo che propongono, nonche' la loro disponibilita', che i GDS collegano ai venditori di biglietti -i siti Internet di viaggi, per esempio.

Ma i GDS trattengono ugualmente in memoria le prenotazioni effettuate presso le compagnie, e archiviano quindi un gran numero di dati personali: indirizzo, E-mail, numero di telefono, numero di carta di fedelta', e talvolta numero della carta di credito. Questi dati, chiamati in gergo "dati dei dossier passeggeri" (piu' conosciuto sotto il nome di PNR – Passeger name record) sono talvolta duplicati da diversi GDS.

"Nessun hackeraggio e' necessario"

"La questione della protezione dei dati dei passeggeri aerei e' oggetto di diversi dibattiti in Europa. Si puo' pensare che questo sistema, agli avamposti di questi accordi, sia reso sicuro", spiega Karsten Nohl, un habitué del CCC, che dirige l'azienda Security Research Labs. In realta' "nessun hackeraggio e' necessario" per accedere a questi dati.

In effetti, i GDS e tutto il sistema che vi gira intorno sono stati resi pubblici da alcuni decenni e nessun provvedimento significativo di protezione dei dati che essi contengono sembra sia stato organizzato.

Primo problema. Le informazioni personali archiviate dai GDS sono accessibili a molti e numerosi dipendenti che lavorano per i siti delle agenzie di viaggi e delle compagnie aeree, secondo i due esperti. Nello specifico e' sufficiente il riferimento di una prenotazione e del nome del passeggero.

Secondo i due esperti, le procedure di sicurezza che stanno alla base di questi accessi sono molto insufficienti: una password molto spesso uguale per tutti gli impiegati dell'agenzia o del sito di viaggi, cosi' come nessuna password per i dipendenti delle compagnie aeree. "Alcune protezioni ridicolmente deboli", dice Nohl.

Dati accessibili quasi a tutti

Ci sono cose ancora piu preoccupanti: queste informazioni non sono solo accessibili ai dipendenti del settore in virtu' di una debolezza strutturale. Gli habitué delle prenotazioni di volo lo sanno bene: per trovare il dettagli del proprio volo e conoscerne le varie modalita', per esempio sul sito della compagnia aerea, e' sufficiente munirsi di un numero di prenotazione a 5 cifre e lettere e del nome del passeggero.

E’ molto raro che un’informazione supplementare (una password, per esempio) sia necessaria per accedere a queste informazioni. Questo significa che, muniti solamente di un numero di prenotazione e del cognome del passeggero, chiunque puo' accedere ai dati personali di quest’ultimo. E’ relativamente facile procurarsi queste due informazioni: in alcuni casi, il numero di prenotazione e’ sulla carta d’imbarco e puo’ quindi essere recuperato tra quelle che sono state gettate. Senza contare che migliaia di internauti, quotidianamente, postano foto delle loro carte d’imbarco sui social network.
E anche quando questi dati e il nome del passeggero non sono direttamente visibili, e’ possibile ritrovarli grazie al codice a barre presente sulla carta d’imbarco. Alcuni siti Internet permettono di leggere, molto facilmente, questi codici.
La caratteristica molto poco discreta delle carte d’imbarco era gia’ parzialmente conosciuta. Ma i due ricercatori hanno ugualmente scoperto un mezzo per ottenere facilmente un numero di prenotazione, anche senza accedere a queste carte. Per diverse ragioni, questi numeri non sono generati in modo cosi’ abbastanza casuale, e testando molto rapidamente migliaia di possibilita’, e’ possibile ottenere il numero di prenotazione associato ad un nome. Karsten Nohl ne ha dato dimostrazione sul canale televisivo tedesco WDR: e’ riuscito a trovare il biglietto di un giornalista ed a modificarlo.

3 miliardi di passeggeri aerei

I pericoli variano in base ai meccanismi di protezione organizzati sui siti e permettono di recuperare i dati personali con il numero di prenotazione e il nome (compagnie aeree, siti dei GDS…). Ma e’ possibile cambiare il nome di un passeggero, la E-mail e la data del volo, e dunque viaggiare al posto della propria vittima.
E’ ugualmente possibile farsi rimborsare il volo, per esempio in punti fedelta’. I due ricercatori, durante la loro presentazione, hanno avuto accesso al fascicolo di un passeggero che viaggiava da Monaco a Seattle e che aveva avuto l’imprudenza di postare la sua carta d’imbarco su Instagram.
In seguito ai rilievi dei due ricercatori, diversi siti di aziende gestiti dai GDS e di compagnie aeree hanno organizzato in questi ultimi giorni dei meccanismi per rendere piu’ difficile l’accesso ai dati dei passeggeri, senza che questo pero’ cambiasse la logica di funzionamento del sistema.
Nel frattempo, il carattere sensibile e la quantita’ di dati ai quali e’ permesso accedere, necessitano di piu’ ampia protezione, ha spiegato Nohl, per esempio introducendo una password, necessaria al viaggiatore per accedere alla sua prenotazione e modificarla.
Secondo la Banca Mondiale, piu’ di 3 miliardi di passeggeri sono stati trasportati per via aerea nel 2015. Il sistema GDS e’ di fatto una delle basi di dati di informazioni personali piu’ ricche che sia mai stato creata, e probabilmente una delle meno messe in sicurezza.

(articolo di Martin Untersinger, pubblicato sul quotidiano Le Monde del 29/12/2016)