L'anno nero dei data breach: tutte le principali violazioni del 2018

Redazione - 11/01/2019

ROMA 11 GENNAIO - Si configura un “data breach” quando un’azienda o un'organizzazione di altro tipo subisce un attacco informatico e le vengono sottratti i dati dei suoi utenti, o si verifica comunque un accesso alle loro informazioni non autorizzato. È purtroppo un fenomeno che capita sempre più spesso, tanto è che Business Insider ha stilato una classifica dei peggiori attacchi registrati nel 2018. Riportiamo di seguito quelli principali che potrebbero aver coinvolto anche utenti italiani.

British Airways - La compagnia aerea britannica ha subito il furto dei dati di 380mila clienti, con informazioni

che comprendono nome, numero di telefono, indirizzo e dati di pagamento. I clienti coinvolti sono stati contattati direttamente dall'azienda.

Cathay Pacific - Il numero di account compromessi sale a 9,6 milioni nel caso di Cathay Pacific, compagnia aerea che si guadagnò gli onori della cronaca lo scorso 25 ottobre. Anche in questo caso sono stati trafugati dati di identificazione, oltre che informazioni sui viaggi effettuati. Le carte di credito dovrebbero essere rimaste al sicuro, ma non è certo.

Facebook - Tra luglio e settembre 2018 un bug ha permesso di estrarre i token di accesso, e di conseguenza i dati personali degli utenti coinvolti. In risposta Facebook resettò gli accessi di 90 milioni di account, anche se poi si scoprì che quelli effettivamente messi a rischio erano un po' meno.

Google+ - Google+ ha fatto parlare di sé in due diverse occasioni. La prima per l'esposizione di 500mila account, la seconda per 52,5 milioni. In entrambi i casi si è trattato di bug i cui effetti negativi sembrano essere solo potenziali, ma l'azienda ha fatto sapere in entrambi i casi di non aver trovato segni di furto o abusi. Non che sia una garanzia totale, ma è meglio di niente. Google ha deciso di chiudere il social network, anche perché non ha mai davvero preso piede, entro aprile 2019.

Cambridge Analytica - Il caso di Cambridge Analytica è forse quello più famoso del 2018. Ne hanno parlato i notiziari in prima serata, sono state fatte indagini (alcune ancora in corso), e il dirigente Mark Zuckerberg è stato chiamato a parlare davanti a una commissione parlamentare. In pochissime parole, Facebook ha permesso a società esterne di raccogliere i dati dei suoi utenti, che poi li hanno rivenduti o usati per comunicazioni politiche – sono note azioni mirate anche a turbare le operazioni elettorali in diversi paesi, compresi Stati Uniti e Gran Bretagna.

Quora - Quora non è molto usato in Italia ma la sua presenza non è del tutto trascurabile. È un servizio di domande e risposte, che lo scorso novembre ha subito un'intrusione nei propri sistemi e il furto di circa 100 milioni di utenze. I dati includevano nome, indirizzo email, password (crittografata) e attività sul sito, cioè le domande e le risposte pubblicate.

MyFitnessPal - MyFitnessPal è un servizio piuttosto diffuso anche nel nostro paese, usato sia da chi si allena intensamente sia da chi cerca un piccolo aiuto per mantenersi in salute. L'app contiene informazioni personali come nome o email, abitudini alimentari, attività sportive e altro. Lo scorso febbraio ha subito il furto di 150 milioni di account, che sembra non aver esposto dati particolarmente sensibili.

Marriot Hotel - La notizia è recente: la catena Marriot si è fatta rubare i dati di 500 milioni di persone, che si erano registrate ai servizi della sua controllata Starwood. I dati rubati sono particolarmente sensibili e includono anche le carte di credito, ma non è tutto. Secondo il New York Times infatti si tratta di un'operazione sponsorizzata dal governo cinese.

Vale inoltre la pena di citare l'attacco ad Aadhar. Probabilmente il nome non dice nulla, a meno che non abbiate un qualche rapporto con l'India. Sono i residenti in questo Paese le vittime dell'attacco, ed è il numero degli account compromessi a far girare la testa: 1,1 miliardi di persone coinvolte, quasi l'intera popolazione.

Aadhar è infatti un database pubblico gestito dalle autorità indiane, su cui sono conservati i dati delle carte d'identità e quelli biometrici – come impronte digitali o scansioni dell'iride. È usato per accessi ad altri sistemi, usato anche da terzi come per esempio Amazon. A quanto pare chi lo gestiva non ha fatto le cose a regola d'arte quanto a sicurezza informatica; anzi, i reporter di ZDNet riportano di aver segnalato ripetutamente i problemi rilevati, senza ottenere risposte per oltre un mese.
Ovviamente, questa lista è un parziale di un vero e proprio bollettino di guerra del 2018, che potremmo definire

un "annus horribilis" per la sicurezza informatica.

Forse è però una triste realtà a cui dobbiamo abituarci: anzi, visto che con l'entrata in vigore del GDPR le aziende e tutte le altre organizzazioni che subiscono un data breach devono obbligatoriamente comunicare questi eventi all'Authority per la privacy e nei casi più gravi anche a tutti i diretti interessati che sono coinvolti, non è da escludere che nel 2019 la lista si allunghi ulteriormente.
onte (Federprivacy.)