PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5724 di Mercoledì 30 ottobre 2024

In Italia ci sono troppi spioni: occorre intervenire con urgenza

Sulla base delle notizie di stampa degli ultimi giorni, il ministro Nordio ha sottolineato la urgenza di stanziare fondi per migliorare il livello di sicurezza dell'accesso alle banche dati governative. Ecco qualche considerazione in merito.

Certamente tutti i lettori sono rimasti profondamente colpiti dalle notizie afferenti ad un banchiere di Bitonto, che ha avuto accesso pressoché libero ai conti correnti di numerosi VIP, clienti dell'istituto cui egli apparteneva. Risale al 25 ottobre 2024 la notizia, apparsa su tutti i giornali, di una azienda privata che catturava dati personali, presenti in banche dati statali, per venderli a privati.

Per dare un'idea del giro di affari che può essere collegato a questa attività, ecco le tariffe esposte da questa società:

- per il pacchetto di base, chiamato Tips, 1000 ?,
- per il pacchetto avanzato, chiamato KYC, 5000 ?,
- per il pacchetto ancora più avanzato, chiamato Eidd, 15.000 ?.

Ovviamente all'aumento di prezzo corrispondeva una maggiore quantità di informazioni, molte delle quali oltremodo sensibili.

Le banche dati cui gli operatori potevano accedere erano svariate, tra le quali Sid (sistema di indagine delle forze dell'ordine), Serpico (sistema informatico dell'agenzia delle entrate), Siatel (acronimo di Sistema interscambio anagrafe tributarie enti locali), Anagrafe, INPS, Sos (acronimo di segnalazioni operazioni sospette) e via dicendo.

Di particolare interesse il fatto che i malviventi accedevano a queste banche dati utilizzando i profili di accesso di soggetti autorizzati, che erano riusciti in qualche modo a carpire o a farsi cedere, forse a fronte di appropriate remunerazioni. In altre parole, i malviventi accedevano non entrando nel cuore del sistema, ma lavorando dai terminali periferici.

Ecco motivo per cui il ministro della giustizia ritiene che si debbano con urgenza attivare sistemi assai più raffinati di identificazione degli utenti, che richiedono l'accesso ai sistemi. La banale autorizzazione, basata su un user ID ed una password, è ormai da tempo ritenuta insufficiente da tutti gli esperti di sicurezza ed ecco perché occorre passare al più presto ad autorizzazioni a due livelli, magari accompagnati da un OTP (one time password), che venga rilasciato ad ogni accesso.

Occorre inoltre introdurre dei sistemi di monitoraggio degli accessi, che mettano tempestivamente in evidenza accessi ripetuti, provenienti da uno stesso profilo di accesso. La mancanza di questi sistemi di monitoraggio, ad esempio, non ha permesso alla banca, il cui sistema informativo era stato saccheggiato dall'operatore di Bitonto, di rendersi conto tempestivamente della quantità e tipologia di accessi effettuati dal dipendente stesso.

Ci permettiamo di ricordare a tutti i lettori un prezioso documento, che nasce da una iniziativa congiunta dell' Agenzia per la cybersicurezza nazionale (ACN) e del Garante per la protezione dei dati personali, centrata sull'importanza della crittografia. Le linee guida si rivolgono a tutte quelle imprese e amministrazioni che, in qualità di titolari o responsabili del trattamento dei dati, conservano sulle proprie piattaforme le password degli utenti (vedi allegato).

Questo documento si accompagna ad altre linee guida, che sarà bene che i responsabili della sicurezza informatica aziendale studino attentamente tali linee guida, che sono disponibili sul sito dell'agenzia per la cybersicurezza nazionale.

LINEE GUIDA FUNZIONI CRITTOGRAFICHE - Conservazione delle Password (pdf)

Adalberto Biasiotti