filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Dall'esperienza della piattaforma Rousseau un vademecum per la sicurezza informatica di blog e siti web

25 Aprile 2019
Marco Dettori

Gli episodi di *data breach* (violazione di dati personali) che tra il 2017 e il 2018 hanno colpito il **sistema informatico del Movimento 5 Stelle** – la piattaforma Rousseau – oltre che una forte risonanza mediatica, hanno innescato l'**attività ispettiva del Garante Privacy** che, all'esito della verifica istruttoria, ha emesso il provvedimento n.548 del 21 dicembre 2017, con il quale ha prescritto ai titolari della piattaforma l'adozione di una serie di **misure e accorgimenti per conformare il trattamento dei dati personali degli utenti** alla normativa sulla *data protection* e ad **innalzare il livello di sicurezza** della piattaforma.
Da un punto di vista **esclusivamente operativo**, risultano interessanti le **misure di sicurezza** prescritte dal Garante per arginare il rischio di violazione di dati personali.

> **L'elenco delle seguenti attività ha un rilievo pratico per chiunque gestisca (o intenda gestire) un blog o un sito web che consenta agli utenti: la registrazione, la creazione di un account, la successiva autenticazione informatica per l'accesso e l'esecuzione di determinate azioni (come, ad esempio, l'espressione di un voto digitale).**

Pertanto, alla luce del citato provvedimento, **il titolare di un blog o un sito web**, sotto il profilo della sicurezza, **dovrebbe adottare** le seguenti misure:
a) in conformità all'approccio basato sul rischio che permea la normativa sulla protezione dei dati personali, si rende necessaria l'esecuzione di "[…] *adeguante azioni di* ***vulnerability assessment*** *attuate precedentemente alla messa in esercizio* – del blog o del sito web – *allo scopo di* ***individuare e correggere eventuali vulnerabilità nei servizi*** *prima di renderli fruibili al pubblico*";
b) con riferimento al **sistema di autenticazione informatica** degli utenti: *(i)* le password devono avere una **lunghezza non inferiore agli otto caratteri** e dovrebbero essere "[…] *sottoposte a un* ***controllo automatico di qualità*** *che impedisca l'uso di password deboli, costituite, ad esempio, in parole reperibili in dizionari o comunque facilmente individuabili*"; *(ii)* il sistema dovrebbe **limitare "**[…] ***il numero dei tentativi di accesso con password erronea****, per impedire attacchi brute force interattivi*";

c) sotto il profilo dei **protocolli di rete**, dovrebbe essere **adottato il protocollo *https*** (*secure hyper text transport protocol*), in modo tale che l'accesso ai contenuti del blog o del sito web sia "*basato su un **certificato digitale emesso da una Certification Authority** riconosciuta* […]";

d) il ***software*** scelto dal titolare del blog o del sito per la **gestione dei contenuti** (CMS, *content management system*), dovrebbe essere adeguatamente aggiornato dal punto di vista tecnico e dotato di **sistemi crittografici per la conservazione e registrazione delle password** degli utenti, senza consentirne il salvataggio in chiaro;

e) per quanto riguarda il tema della **riservatezza delle operazioni compiute dagli utenti** mediante il blog o il sito web, dovrebbero essere adottate **misure di auditing** che consentano di verificare gli **accessi e le operazioni effettuate dagli amministratori di sistema** sulle piattaforme informatiche. La **registrazione e la successiva verifica dei *log***, infatti, consentono al titolare del blog o del sito di dimostrare un elevato grado di sicurezza del sistema e la tutela della riservatezza dei dati personali degli utenti interessati.

TAG: *data breach, GDPR, Misure di sicurezza, Movimento 5 Stelle*
