diritto&diritti dal 1996
diritto.it
fondatore Francesco Brugaletta

La comunicazione da fornire agli utenti in caso di data breach consistente nel furto delle password di un account email

Autore: Muia' Pier Paolo
In: Diritto civile e commerciale

Garante per la protezione dei dati personali: provvedimento n. 106 del 30 aprile 2019

Riferimenti normativi: art. 33, par.3, lett b), c), d); 34, par. 2 del General data protection regulation

Fatto

Una Società, operante nel campo delle soluzioni di marketing digitale e comunicazione online, aveva, nel febbraio 2019, comunicato al Garante per la protezione dei dati personali di aver subito un data breach.

In particolare, ai sensi del Regolamento europeo per il trattamento dei dati personali, la Società aveva notificato al Garante la violazione dei dati personali da essa trattati, avvenuta tramite un accesso fraudolento mediante un hot spot della rete Wifi.

Tramite le verifiche condotte sull'accesso illecito subito, la Società aveva accertato la violazione di circa 1.5 milioni di credenziali di account di posta elettronica di due portali web, riconducibili ad utenti che avevano eseguito l'accesso mediante la web mail.

La Società aveva poi reso noto al Garante che immediatamente dopo l'intrusione erano stati eseguiti i primi interventi di contenimento e mitigazione, come la predisposizione della forzatura del cambio password e la relativa informazione agli utenti mediante landing page.

In riferimento alle possibili conseguenze della violazione dei dati personali la Società ha tranquillizzato il Garante affermando che non vi era stata evidenza di accesso anomalo, in termini di volumi e connessioni, alle caselle e-mail degli interessati, e questo, secondo quanto sostenuto dalla Società, era dipeso dalla forzatura del cambio password immediatamente predisposta, che aveva reso inservibili le credenziali acquisite durante l'attacco. Infatti, solo nel caso in cui le credenziali fossero state utilizzate nel lasso di tempo tra la violazione e la forzatura del cambio password sarebbe potuto avvenire l'accesso non autorizzato a caselle e-mail.

Diritto & Diritti ISSN 1127-8579

La Società, nella sua nota destinata al Garante, aveva specificato anche le azioni messe in campo per dare avviso agli interessati dell'intrusione subita dal sistema, in ottemperanza a quanto stabilito dal GDPR, secondo cui "quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo". Secondo quanto riferito dalla Società ben presto sarebbe stata inviata una e-mail a tutti gli interessati che avevano subito la violazione dei dati personali.

La decisione del Garante

Valutate le informazioni acquisite in occasione dell'attività ispettiva condotta, **il Garante ha ritenuto di ordinare alla Società di comunicare la violazione dei dati personali a tutti gli interessati coinvolti senza ritardo, e comunque entro trenta giorni dalla data di ricezione del provvedimento**. Il Garante ha altresì specificato che la comunicazione destinata agli interessati doveva **contenere un linguaggio semplice in modo da risultare chiara la natura della violazione dei dati personali, e doveva contenere il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni**; **descrivere le probabili conseguenze della violazione dei dati personali e contenere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi**, utilizzando i mezzi di comunicazione che permettano di raggiungere il maggior numero di interessati.

Il Garante, chiamato a valutare la notizia di data breach subito dalla Società, ha in primo luogo posto l'attenzione sulle possibili conseguenze, quali il furto o usurpazione dell'identità, che potrebbero derivare agli interessati dalla violazione dei dati personali. Infatti l'acquisizione da parte di terzi di credenziali di autenticazione per l'accesso ad un servizio, come nel caso di specie al servizio di web mail, indipendentemente dal fatto che ne consegua un effettivo utilizzo per l'accesso a tale servizio, è da ritenere fonte di potenziale pregiudizio per gli interessati in considerazione della probabilità che le medesime credenziali possano essere utilizzate per accedere anche ad altri servizi online.

Nel caso di specie il Garante ha ritenuto che la violazione dei dati personali subita dagli utenti dei servizi forniti dalla Società era in grado di presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ed è da questo assunto che il Garante ha formulato la propria convinzione circa la necessità di dare una corretta, rispetto a quella già data, comunicazione agli interessati.

Infatti, secondo quanto riferito dalla Società la comunicazione dell'avvenuta violazione era stata già data agli interessati da parte della Società – attraverso l'invio di una comunicazione nelle caselle di posta elettronica, le cui credenziali di autenticazione era state oggetto di violazione - seppur in modo differente

Diritto & Diritti ISSN 1127-8579

a seconda che l'interessato avesse provveduto o meno ad effettuare il cambio della password nell'intervallo di tempo intercorso tra il momento dell'attivazione del meccanismo di enforcement del cambio della password e il momento in cui sono state inviate le comunicazioni.

Infatti per gli utenti che dopo la violazione avevano effettuato il cambio della password nelle 48 ore precedenti l'invio della comunicazione, si dava avviso che vi era stata un'attività anomala sui sistemi, senza suggerimento di alcuna azione correttiva, evidenziando che l'operazione di cambio della password aveva reso inutilizzabili le credenziali precedenti ritenute non più sicure.

Mentre per gli utenti che dopo la violazione non avevano effettuato il cambio della password nelle 48 ore precedenti l'invio della comunicazione, si dava avviso che vi era stata un'attività anomala sui sistemi, e veniva suggerito quale azione correttiva il cambio della password al fine di eliminare il rischio di accesso indesiderato alla propria casella email.

Tali comunicazioni, come detto pocanzi, erano state inviate alle stesse caselle di posta elettronica le cui credenziali di autenticazione era state oggetto di violazione, potendo in questo modo inficiare l'efficacia della comunicazione stessa. Le comunicazioni, infatti, ben potevano non aver raggiunto i reali utilizzatori delle caselle di posta elettronica, perché già violate.

Per tali ragioni, tenuto conto delle comunicazioni effettuate ad opera della Società nonché delle modalità utilizzate, **il Garante ha ritenuto necessario suggerire quale provvedimento quello di effettuare una nuova comunicazione della violazione dei dati personali agli interessati contenente una descrizione della natura della violazione e delle possibili conseguenze della stessa, nonché l'indicazioni specifiche sulle misure che gli interessati possono adottare per proteggersi da eventuali conseguenze negative della violazione**. Come ad esempio la raccomandazione di non utilizzare più le credenziali compromesse, modificando la password utilizzata per l'accesso a qualsiasi altro servizio online qualora coincidente o simile a quella oggetto di violazione, e di scegliere un mezzo di comunicazione che massimizzi la possibilità di comunicare correttamente le informazioni a tutte le persone interessate.

Volume consigliato

Diritto & Diritti ISSN 1127-8579