Dal data breach Federprivacy: cosa possiamo imparare

Un altro schiaffo alla famosa Associazione che si occupa di privacy, collegata alla nota vicenda del cyberattacco subìto, arriva proprio in prossimità di un evento in corso sulla privacy e cybersecurity. Senza lasciarci andare ad ulteriori commenti agilmente intuibili, spostiamo l'attenzione e chiediamoci cosa possiamo imparare da un data breach di questa portata, una volta per tutte.

Eccoci alla seconda puntata. Ci eravamo infatti lasciati offrendo alcuni spunti di riflessione sull'accaduto. Oggi, ci vogliamo soffermare non tanto sull'onda della prevedibile notizia, quanto su cosa possiamo imparare, e una volta per tutte, da un data breach che colpisce proprio chi lavora nel settore della protezione dei dati, e si impegna a diffonderne cultura. Intendiamoci, non vuole essere una "battuta di spirito", ma un insegnamento per tutti.

D'altronde, come in ogni evento critico che può accadere nel corso di un'esistenza in qualunque campo, si può scegliere o di concentrarsi su quell'evento con il rischio di finire (nella filosofia) del "criceto in una ruota" o essere resilienti, imparando dagli eventi avversi, come "casi scuola" utili per crescere nella propria preparazione. Del resto, **Alfred Sheinwold** (noto campione di bridge) amava ripetere che occorre imparare tutto ciò che ci è possibile dagli errori degli altri, perché non avremo tempo a sufficienza per farli tutti.

E ciò che sorprende di quanto successo, non possiamo non rilevarlo, è il silenzio assordante intorno alla spiacevole vicenda da parte proprio dei professionisti della protezione dei dati personali. Ma forse il motivo è intuibile e, in qualche modo, tanto racconta del nostro Sistema Paese.

Comunque veniamo a noi. Nel concreto, infatti, poiché la pubblicazione di "circa 15 GB di dati, appartenenti ai 26.000 utenti di Federprivacy e ai 2.500 soci membri dell'associazione italiana di professionisti della privacy e della protezione dei dati, sono stati pubblicati, in modo gratuito, su un forum pubblico. Ossia scaricabili da tutti" si è ormai verificata (nonostante fosse stato promesso il contrario), volgiamo l'attenzione sulla lezione per tutti che ne deriva.

Partendo dal presupposto che in questa vicenda come in altre – ma qui a maggior ragione con palmare evidenza – nulla sia stato lasciato al caso, è emblematica sia la sua drammaticità e sia i toni surreali. Da qui, non possiamo non riflettere – e non dovremmo essere gli unici (o quasi) tra gli studiosi della materia a farlo – pensando ovviamente anche alle istituzioni preposte alla tutela di privacy e security nel nostro Paese. Ma siamo certi che un'istruttoria sia stata doverosamente avviata.

Quindi, in ottica costruttiva, quanto successo deve essere da insegnamento e monito a chiunque, in particolare su come occorra gestire un data breach: possibilmente al meglio, stante il contesto.

In primis, a livello comunicativo.

La comunicazione, infatti, deve essere – se è utile e doveroso effettuarla, ricorrendone i presupposti – quanto mai efficace e tempestiva, oltre che in linea con quanto prescritto dal GDPR (artt. 33 e 34). Le comunicazioni post data breach devono essere corrette e ineccepibili (in modo da non rischiare di dare poi adito a interpretazioni distorte proprio da parte dei criminali informatici, come è successo nel nostro caso di studio).

A volte, in occasione di violazioni di un certo rilievo con quanto per conseguenza anche in termini di responsabilità, occorre avere l'autorevolezza e la freddezza di chiedere venia ai danneggiati/interessati della violazione e spiegare in trasparenza, con pazienza, le ragioni dell'evento, nonché le azioni fatte e da fare per minimizzare i danni.

Un data breach, per quanto poi nell'immaginario comune si tenda ad associarlo prevalentemente a una sottrazione di dati personali, non dimentichiamo che è anche altro. A stabilirlo è il GDPR stesso, all'art. 4, n. 12, fornendo un'espressa definizione di "violazione dei dati personali", quale "...violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione,

la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Quindi, un data breach è ben più ampio di quanto comunemente percepito come tale e le sue conseguenze possono andare ben oltre ciò che si possa immediatamente percepire (pensiamo solo alla possibilità teorica di prendere possesso, attraverso credenziali in chiaro, di comunicazioni confidenziali inoltrate vie e-mail da migliaia di ignari utenti interessati); e, se vogliamo guardare alle note circostanze o a quelle più in generale pensando ad altri data breach che si sono verificati negli anni, è innegabile che nel pieno dell'era digitale, l'esigenza di una costante attenzione e una piena consapevolezza si imponga prepotentemente. D'altronde, l'accountability è anche da leggersi in questa accezione.

Così, passiamo dalla teoria alla pratica, pensando alle misure di sicurezza da adottare, implementare e rafforzare, affinché eventi del genere siano sempre più rari o isolati. Anche se i dati purtroppo ci dicono che al momento tali eventi siano in netta crescita nel nostro Paese.

Evitiamo, quindi, password deboli e soprattutto se disponiamo di un data base non poniamole in chiaro, custodendole in altro modo con cifrature o altri strumenti che le proteggano. Inoltre, va assolutamente evitato l'invio di e-mail con ID e PW in chiaro, perché notoriamente tali protocolli di comunicazione non sono sicuri.

È utilissimo, inoltre, acquistare programmi di aggiornamenti della sicurezza strutturati ed estesi (ad esempio, Extended Security Update – ESU). Così come devono essere necessariamente adottati modelli organizzativi robusti con revisione di politiche/procedure.

Ma tali modelli e procedure vanno concepiti e vissuti non solo come dei documenti formali all'interno di un sistema più o meno elaborato di gestione, ma vanno testati e aggiornati periodicamente. Grazie a simulazioni, ad esempio, proprio di data breach. Il tutto a vantaggio, peraltro, di un buon modo di formare, informare e sensibilizzare coloro (autorizzati/designati) che trattano dati a più livelli in un'organizzazione.

Effettuiamo audit e controlli periodici, non solo ai fini del rinnovo di una certificazione (ad esempio ISO 27001) ma a tenuta del sistema di gestione, vieppiù se integrato tra privacy e security in considerazione del contesto che potrebbe, per ragioni di opportunità, averlo costruito.

Questi, sono soltanto alcuni dei tanti suggerimenti che potrebbero mettersi in atto. Per il resto poi, come abbiamo già scritto, nessuno può dirsi davvero al sicuro, né possiamo permetterci di giudicare. Saranno solo le competenti Autorità a poterlo fare.

Andrea Lisi e Chiara Ponti

30 Novembre 2023

già pubblicato su www.key4biz.it