Data breach: pianificare per prevenire il "panico d'organizzazione"

La simulazione: un buon modo per tenersi pronti a un eventuale data breach

Si dice che il presupposto per gestire correttamente un data breach consista nell'avere un'organizzazione preparata. Ma come? In alcuni approcci viene ad esempio proposta una simulazione di incidente per testare la procedura e individuare eventuali punti critici. Eppure, per quanto tale intervento possa avere un indubbio fascino si pone al di fuori dei margini della pianificazione bensì attiene maggiormente ad una fase di verifica e correzione. Insomma: può essere utile, ma deve quanto meno coordinarsi ad una corretta pianificazione preventiva e soprattutto all'assetto organizzativo predisposto dall'organizzazione.

A differenza di un penetration test che individua vulnerabilità di sicurezza da risolvere, una simulazione di data breach deve essere infatti in grado di individuare criticità anche di natura non strettamente tecnica ma collegate ad aspetti organizzativi e dunque – volendo approssimare – al fattore umano.

Non è infrequente, infatti, che emerga un "panico d'organizzazione" nel momento in cui si entra a conoscenza della compromissione di dati e sistemi, producendo così comportamenti non programmati e soprattutto incoerenti con gli obiettivi di sicurezza e tutela degli interessati. Uno dei fattori più rilevanti che può generare tale esito consiste in una attribuzione di ruoli e responsabilità non definita o incoerente, che ha l'effetto di impattare fortemente sulla capacità di rilevazione o reazione.

Ad esempio, se vengono compromesse tempestività o completezza d'informazione, la ricaduta riguarda tutti i processi decisionali a seguire: analisi, mitigazione, damage control, gestione delle comunicazioni (interne ed esterne) e degli adempimenti normativi. Diventa dunque necessario agire in modo preventivo andando a definire ruoli e responsabilità (anche con una matrice RACI), flussi informativi e andando ad intervenire su possibili "colli di bottiglia" decisionali. In tal senso la comunicazione interna è un elemento critico, cui devono seguire interventi di sensibilizzazione e addestramento relativi alla procedura e alle istruzioni operative fornite.

Tanto la sensibilizzazione che le istruzioni operative devono chiarire a tutti gli operatori autorizzati all'acceso ai dati cosa sia un evento di violazione dei dati personali e cosa fare, fornendo strumenti adeguati alla rilevazione e al reporting, nell'ottica di produrre in ogni caso una registrazione conforme all'obbligo di cui all'art. 33.5 GDPR. Non solo: è necessario che qualora siano o possano essere coinvolti soggetti esterni all'organizzazione si dovranno individuare e contrattualizzare le modalità operative di assistenza, fra cui la definizione di un eventuale Service Level Agreement (SLA).

Il livello logicamente successivo, riguardante invece gli snodi decisionali, richiederà una particolare attenzione nell'individuare

quali soggetti – management, consulenti o funzioni interne – vadano coinvolti perché la progressiva formazione della volontà dell'organizzazione in risposta al data breach sia rendicontabile e conforme tanto ai requisiti normativi che alle best practices di sicurezza.

Fonte: Federprivacy