Pillole di Sicurezza

Disclosure dei data breach

Data pubblicazione: 10 agosto 2015

Disclosure dei data breach: la spinta normativa come fattore di miglioramento

La crescente evidenza della vulnerabilità delle infrastrutture IT trova un riflesso nella altrettanto crescente attenzione, delle diverse fonti di atti legislativi o regolamentari, agli incidenti di sicurezza che possono compromettere la riservatezza dei dati, cioè ai cosiddetti *data breach*.

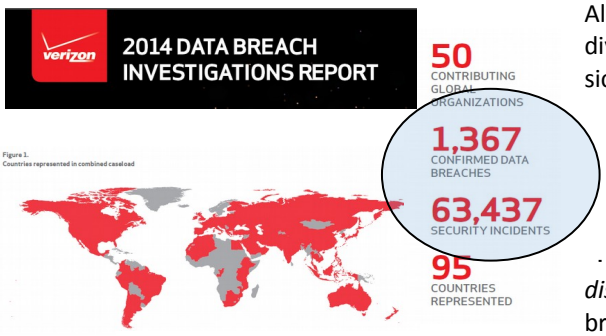

Figura 1- Numerosità dei data breach

Alcuni esempi di tale attenzione sono riportati nei box a lato: autorità diverse ed in momenti differenti, oltre a prescrivere misure e politiche di sicurezza volte a ridurre la probabilità di incidenti di sicurezza, hanno introdotto la necessità di organizzare e documentare la reazione ad una violazione avvenuta ed anche l'obbligo di notificarne l'accadimento ad un soggetto esterno ed indipendente e, in alcuni casi, anche agli interessati.

E' la cosiddetta *disclosure* dei data breach, che aiuterà, fra l'altro, a portare alla luce un fenomeno che molti interessi aziendali spingono a tenere nascosto, se non a negare.

Circolare Banca d'Italia n. 263 del 27 dicembre 2006 – 15° aggiornamento del 2 luglio 2013
La gestione degli incidenti di sicurezza informatica segue procedure formalmente definite, con l'obiettivo di minimizzare l'impatto di eventi avversi e garantire … funzionamento dei servizi e delle risorse ICT coinvolti.
…

I gravi incidenti di sicurezza informatica sono comunicati tempestivamente alla Banca d'Italia, con l'invio di un rapporto sintetico recante una descrizione dell'incidente e dei disservizi provocati agli utenti interni e alla clientela nonché i seguenti dati, accertati o presunti: …

Se si guarda con attenzione, si può notare come gli interventi normativi contengano, però, spinte contraddittorie: da un lato si introduce l'obbligo alla notifica del data breach, dall'altro si qualifica l'evento, che scatena l'obbligo di denuncia, con aggettivi qualitativi - gravi violazioni, high risk – che introducono un margine di discrezionalità che sembra andare in senso opposto.

Effettivamente ne deriva un ammorbidimento della norma - la cosa è ben evidente nelle diverse versioni del nuovo Regolamento EU sulla protezione dei dati personali - ma sarebbe sbagliato trarre la conclusione che ci si trovi di fronte alla valutazione del legislatore di una ridotta rilevanza del tema.

Più correttamente questa contraddittorietà della norma va interpretata come un prodotto della volontà di introdurre un elemento di flessibilità che lasci alle aziende un margine di valutazione utile ad escludere fatti effettivamente minori e poco rilevanti. Allo stesso tempo consente una certa progressività nella traduzione delle aspettative del legislatore in comportamenti aziendali: indica una strada che oggi lascia qualche libertà in più ma che, con l'evoluzione della normativa, è prevedibile che si farà sempre più stretta.

EU - General Data Protection Regulation (proposal)
Article 31 Notification of a personal data breach to the supervisory authority
1. In the case of a personal data breach which is likely to result in a high risk for the rights and freedoms of individuals, such as discrimination, identity theft or fraud, financial loss, … or any other significant economic or social disadvantage, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 51.

La sicurezza della informazioni aziendali sta infatti diventando un aspetto sempre più critico non solo per la tutela di diritti di terzi ma anche per la competitività delle imprese e dell'intero sistema-paese, anche su base europea.

Dai data breach derivano, infatti, alle imprese diversi ordini di danni.

Innanzitutto, un danno specifico e diretto, legato al valore delle informazioni sottratte o svelate ed alle conseguenze che ne possono derivare sull'operatività e sui contratti in essere.

Decreto legislativo del 28 maggio 2012 n. 69
In caso di violazione di dati personali, il fornitore di servizi di comunicazione elettronica accessibili al pubblico comunica senza indebiti ritardi detta violazione al Garante.
2. Quando la violazione di dati personali rischia di arrecare pregiudizio ai dati personali o alla riservatezza di contraente o di altra persona, il fornitore comunica anche agli stessi senza ritardo l'avvenuta violazione.

Soprattutto in un Paese caratterizzato da settori ad alta tecnologia basati su aziende di dimensioni medie/medio grandi, con catene di subfornitura fatte di piccole o anche piccolissime imprese, la sottrazione di know how distintivo può incidere direttamente sulla capacità di reggere la sfida competitiva di una concorrenza sleale difficilmente perseguibile sul piano giuridico in modo efficace.

Spesso, inoltre, anche in aziende eccellenti sotto molti profili, la dimensione media o medio piccola e la cultura d'impresa dominante, conducono ad una struttura organizzativa molto sottile, lontana da queste tematiche e dunque portata a risposte inadeguate che l'organizzazione fatica a gestire.

In questo senso il rischio connesso al data breach è anche un rischio-Paese.

Immediatamente dopo il danno diretto, la divulgazione della avvenuta sottrazione genera un danno reputazionale che investe l'intera catena delle relazioni aziendali sia verso i fornitori che verso i clienti.

Le conseguenze del data breach, però, non finiscono qui perché assai spesso le informazioni oggetto della violazione riguardano soggetti terzi – persone fisiche o giuridiche - legati all'impresa da relazioni diverse. I diritti di tali soggetti trovano la loro tutela nella legge (in senso lato), come è il caso, ad esempio, dei box riportati a lato, che li trasforma in sanzioni a danno dell'impresa, quando ne ricorrano gli estremi.

La sanzione, infine, stabilendo che l'impresa è venuta meno ai propri doveri nei confronti di terzi, indebolisce la posizione dell'impresa nelle eventuali cause con i partner di business ed apre la strada a contenziosi con tali soggetti, i quali, spesso, sono in numero molto rilevante, come si può vedere in Figura 2, e possono dare origine a class action potenzialmente molto onerose.

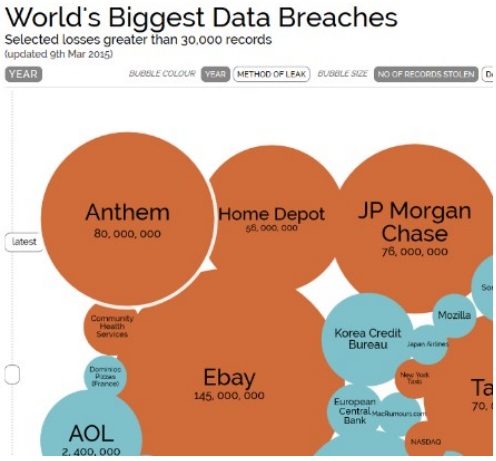

Figura 2- Numerosità dei soggetti coinvolti

Come si vede, l'obbligo di notifica è solo l'aspetto che più colpisce di normative che cercano di affrontare una tematica assai rilevante e complessivamente molto critica.

Dover ottemperare all'obbligo di notifica, fornendo tutti i dati richiesti, che documentano lo stato delle procedure e delle tecnologie al momento dell'evento ed il comportamento tenuto dall'azienda in risposta ad esso, impone di affrontare il tema con un respiro più ampio ed in tutti i suoi aspetti perché quei dati raccolti e resi pubblici potranno essere usati anche contro l'azienda.

Sarebbe, quindi, superficiale sfruttare la maggiore flessibilità della norma al fine di ridurre il costo della compliance senza guardare ai rischi sottesi che vanno ben al di là delle sanzioni potenziali, pur rilevanti. Il rischio di incidenti di sicurezza che comportino la perdita di riservatezza di informazioni rilevanti è reale, non è inventato dal legislatore, come si evince dai dati sommari riportati in Figura 1, e può comportare conseguenze gravi: è questa la principale ragione per cui è necessario porre in essere preventivamente una risposta organizzativa e tecnologica che consenta di

- intercettare la violazione al più presto, se possibile fin dal momento in cui l'attacco prende forma,
- reagire immediatamente per contrastarla e
- ridurne l'impatto, ponendo in essere in tempi brevi le contromisure necessarie, incluso il coinvolgimento dei soggetti a cui i dati violati si riferiscono, secondo piani predisposti anticipatamente
- documentare ogni evento ed ogni azione intrapresa.

Si tratta, cioè, di dedicare una rinnovata attenzione al profilo di rischio aziendale che si ottiene ponendo la probabilità della violazione uguale a 1, cioè partendo dalla considerazione che, per quanti sistemi di difesa siano posti in essere, l'evento non può essere escluso.

Figura 3

E' interessante notare, fra l'altro, come, in questo scenario a cui si riferisce la Figura 3, sia la *detection* che la *reaction* impongano spesso di coinvolgere i proprietari dei dati che, in caso di dati personali ma non solo, sono soggetti terzi: la detection perché richiede un monitoraggio continuato delle attività lavorative quotidiane di cui tutti gli interessati devono essere informati e si colloca al confine fra il diritto alla tutela degli asset aziendali ed il controllo a distanza dei lavoratori; e la reaction perché non informare prestamente gli interessati di una violazione che li riguarda può esporli ad un rischio ancora maggiore.

Porre attenzione a questi due aspetti della gestione della sicurezza e del rischio non significa trasferire gli investimenti da un tema agli altri due ma acquisire aziendalmente la consapevolezza che una risposta adeguata ai rischi insiti nelle nuove architetture digitali dell'economia e delle relazioni sociali comporta una equilibrata politica di investimento in tutti e tre gli ambiti.

Trascurare questa necessità porta allo scenario descritto in Figura 4 che rappresenta il gap fra la velocità dell'attaccante e la lentezza del difensore: è come contrapporre a Messi un cinquantenne sovrappeso sperando di non prendere goal. Spesso l'acquisizione illecita di accesso ad informazioni riservate si protrae nel tempo per giorni, settimane o addirittura mesi: al contrario di altri furti, la sottrazione di informazioni non comporta il venire meno delle informazioni ma della loro riservatezza.

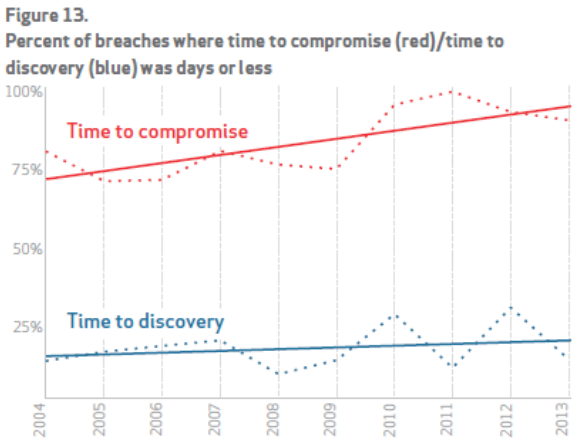

Figura 4

Il danneggiato può quindi continuare ad operare come sempre senza accorgersi di nulla se non attiva iniziative specifiche volte ad rilevare ciò che può succedere.

Costi quotidiani che non producono quasi nulla se non in presenza di un attacco che potrebbe non arrivare mai: costi, quindi, simili a quelli assicurativi che devono essere gestiti con grande attenzione ed oculatezza in modo che siano sostenibili nel lungo periodo

Non si tratta, quindi, solo di definire le pur necessarie policy aziendali, lasciandole ad invecchiare in qualche archivio, quanto di sostenerle con le tecnologie adeguate a rendere sempre meno soggetta all'errore umano e ai limiti dell'organizzazione l'azione di contrasto all'azione criminale condotta contro l'azienda.

Automatizzare il più possibile i comportamenti aziendali in fatto di sicurezza è un elemento essenziale per ottenere l'efficacia necessaria a costi sostenibili e senza presumere o pretendere di dotare l'azienda di competenze e capacità sproporzionate rispetto alla struttura organizzativa.

L'esistenza di normative che affrontano questi temi, imponendo vincoli ed obblighi, è una ragione in più che contribuisce a rafforzare la richiesta della necessaria attenzione del management e di un budget adeguato, non un impedimento burocratico allo sviluppo del business.

Gli eventuali limiti e difetti di queste normative sono aspetti marginali, spesso figli dei compromessi necessari in sede legislativa per ottenere l'obiettivo primario, a fronte delle resistenze e dei contrasti fra i diversi interessi coinvolti.

Lo sforzo posto in essere, gli investimenti effettuati in procedure, tecnologia, formazione sono essi stessi ed al di là della loro efficacia, la dimostrazione dell'attenzione aziendale nella cura dei propri asset e degli interessi di terzi coinvolti nella propria attività e potranno essere fatti valere, a difesa dell'azienda, sia rispetto alle autorità vigilanti (Garante privacy, Banca d'Italia, ….) sia nei confronti di chi avesse ricevuto un danno a causa del data breach.

E' dunque necessario che la risposta alle normative vigenti ed a quelle in arrivo non sia vista come un mero problema di compliance ma di adattamento più generale dell'azienda al nuovo scenario in cui la *digital transformation* la porterà ad operare, a prescindere dalle volontà dei singoli, dalla cultura aziendale e dalle scappatoie legali che si possono individuare nel breve periodo.

Sergio Fumagalli

sergio.fumagalli@zeropiu.it

Vice President di Zeropiu Spa, società di system integration e consulenza specializzata sui temi della sicurezza delle identità digitali e dei dati, attiva in Italia e nei Paesi Scandinavi.
Dopo un'esperienza parlamentare nella XIII legislatura, dal 2001 inizia a occuparsi professionalmente di Privacy, collaborando con il Garante della Privacy e pubblicando, come co-autore, il testo "Privacy guida agli adempimenti", IPSOA, 2004, 2005.

Partecipa, fin dal 2008 alla Oracle Community for Security: è stato co-autore dei documenti prodotti dalla Community e attualmente coordina il gruppo di lavoro sul nuovo Regolamento europeo sulla privacy.

E' membro del direttivo di Clusit.

Dal 2004 al 2012 è stato membro del Cda di Webank, la banca online del gruppo BPM.