Il dato è protetto. Dietro una maschera

UN SOFTWARE IN GRADO DI MASCHERARE E PROTEGGERE I DATI SENSIBILI TRATTATI QUOTIDIANAMENTE DAI REPARTI IT DELLE BANCHE E DAGLI OUTSOURCER NEGLI AMBIENTI DI TEST E DI PRE-PRODUZIONE. UNA SOLUZIONE PRESENTATA DA MICRO FOCUS CHE VUOLE RISPONDERE ANCHE AL DETTATO DELLA CIRCOLARE 263 DI BANCA D'ITALIA SUL RISCHIO INFORMATICO

Mascherare il dato senza perderne significato e qualità, per renderlo inaccessibile nel pieno rispetto del quindicesimo aggiornamento della Circolare 263 di Banca d'Italia: ovvero la gestione del cosiddetto "rischio informatico". Un escamotage che diventa basilare soprattutto negli ambienti di test, in cui sono tanti i dati sensibili sottoposti ad analisi di pre-produzione, con il conseguente rischio di causare, anche inconsapevolmente, una fuoriuscita dei dati e incorrere in sanzioni economiche, penali, ma anche in importanti danni di immagine. «Un caso molto recente è avvenuto in Corea – racconta Alberto Avanzi, Divisione R&D, Solution Architect Data Express di Micro Focus – dove, a seguito del furto di un pc portatile, sono stati sottratti i dati personali di 20 milioni di clienti del Korea Credit Bureau. Ogni singolo record rubato è costato all'istituto 202 dollari».

Alberto Avanzi, Divisione R&D, Solution Architect Data Express di Micro Focus

I dati sensibili con la maschera

Senza contare l'impatto in termini di immagine di eventi del genere e il pericolo di una "fuga" di clienti preoccupati per la sicurezza dei propri dati. Un rischio all'ordine del giorno, che ha portato Micro Focus a rivolgersi al mercato bancario con un software in grado di mascherare i dati che transitano dai database alle piattaforme di prova, mettendo in sicurezza tutte le informazioni sensibili che, secondo quanto richiesto dalla Circolare 263, non possono essere visibili nemmeno al personale IT e agli outsourcer che si occupano dello sviluppo degli ambienti di test. «Il 70% delle organizzazioni IT ha sempre utilizzato i dati di produzione, dove sono presenti dati sensibili, anche se spesso di bassa qualità, in quanto non aggiornati, nelle operazioni di test, appesantendo le dimensioni di storage e rallentando il time-to-market – commenta Avanzi. Con l'entrata in vigore, il primo febbraio 2015, del quindicesimo aggiornamento della Circolare, questo processo non è più compliant. Bisogna quindi mascherare il dato, creando una serie di metadati che rispecchino, per qualità di informazione, tutti i dati sensibili che le banche possiedono».

Algoritmi per mantenere la qualità del dato

Il meccanismo di mascheramento, presente da 9 anni sul mercato e già testato da alcune banche e realtà assicurative italiane, è «parametrico, ripetibile ma irreversibile», come spiega Avanzi. Si basa su "dizionari", degli algoritmi matematici capaci di trasformare il dato originale in un "alter ego": ad esempio, Mario Rossi diventerà Paolo Bianchi, «in un rapporto uno a molti che non permette di cogliere il dato originario, preservandone però il significato – prosegue Avanzi. In altre parole, si otterranno dei nomi e dei cognomi veri, anche se non associati alla identità originaria del dato. E anche per le partite IVA o i codici fiscali si avrà una trasformazione 1:1, evitando la duplicazione delle chiavi».

Stefano Arduini, Responsabile Area Internal Auditing, Certificazioni di Cedacri

Giuseppe Gigante, Regional Marketing Manager di Micro Focus

Data subsetting: estrarre i dati, senza errori

E, anche se mascherato, il dato deve affrontare diverse fasi: quella di test, il collaudo, il training e, infine, la messa in produzione. «Quattro livelli in cui bisogna riuscire a spostare il dato in modo agevole e veloce, senza fare errori di trascrizione manuale e, soprattutto, evitando l'accesso alle informazioni sensibili contenute negli archivi per garantirne la riservatezza – commenta Stefano Arduini, Responsabile Area Internal Auditing, Certificazioni di Cedacri. Per avere quindi dati consistenti e trattati nel rispetto delle disposizioni di legge, abbiamo scelto di adottare una gestione centralizzata di data masking e di subsetting del dato. Il risultato è una maggiore protezione delle informazioni sensibili e una migliore gestione dello spazio di storage occupato dai dati, in quanto gli ambienti di collaudo e di training, grazie al subsetting, non vengono popolati manualmente, ma in modo automatizzato e replicabile grazie a semplici estrazioni mirate».

Ambienti di test meno costosi e di qualità

Infine, sia per le banche sia per gli outsourcer i vantaggi sono diversi. «Oltre a essere compliant ai requisiti regolamentari, infatti, si ottimizza lo storage e la si preserva la qualità dell'ambiente di test – conclude Giuseppe Gigante, Regional Marketing Manager di Micro Focus. Inoltre, grazie a dei file guida non è necessario riscrivere i dati in ogni ambiente, riducendo i costi della gestione del dato e minimizzando i rischi di violazione o divulgazione impropria delle informazioni sensibili».

G.C.

LA CIRCOLARE DELLA BANCA D'ITALIA 263/2006 – 15° AGGIORNAMENTO

A partire dal primo febbraio 2015 tutte le banche italiane si devono conformare alle disposizioni contenute nel TITOLO V, Capitolo 8 del quindicesimo aggiornamento della Circolare 263 di Banca d'Italia. L'obiettivo della Circolare è fornire un quadro normativo organico e coerente con le raccomandazioni dei principali organismi internazionali e mettere le banche in condizione di gestire il cosiddetto "rischio informatico": ovvero il «rischio di incorrere in perdite economiche, di reputazione e di quote di mercato in relazione all'utilizzo di tecnologia dell'informazione e della comunicazione».

Le conseguenze e le sanzioni in caso di violazione

Come racconta Camilla Manfredi, avvocato di Rödl&Partners, nel caso di irregolarità riscontrate nell'attività di vigilanza, la Banca d'Italia ha il potere di applicare sanzioni amministrative a carattere pecuniario. Ma anche di sanzionare penalmente chi, all'interno del dipartimento IT, si occupa della gestione del dato, con reclusioni dai 6 mesi ai 3 anni, a seconda della gravità dell'illecito nel trattamento dei dati, e anche con il pagamento di somme che vanno dai 6mila ai 36mila euro.
Insomma, il trattamento del dato è una attività pericolosa e per questo si può incorrere nella Responsabilità civile per danni. Con ben poco scampo per la banca: «Chi ritenga di essere stato danneggiato a seguito dell'attività di trattamento dei suoi dati personali, può ottenere il risarcimento senza dover provare la colpa del Titolare del trattamento». Inoltre, «i danni cagionati alle persone per effetto di un trattamento illecito devono essere riparati dal responsabile del trattamento, il quale può essere esonerato dalla propria responsabilità se prova che l'evento dannoso non gli è imputabile, in particolare quando dimostra l'esistenza di un errore della persona interessata o un caso di forza maggiore: per provare ciò occorre dimostrare di aver seguito tutte le cautele nella scelta del responsabile e dell'incaricato [...], nonché di avergli fornito la strumentazione e le indicazioni scritte necessarie e di aver vigilato sul loro operato», ma «anche qualora si dimostri che la mancata adozione di misure di sicurezza sia imputabile al responsabile del trattamento, il titolare del trattamento può incorrere in una culpa in eligendo o in vigilando».

Camilla Manfredi, avvocato di Rödl&Partners