Anche la stampa nella privacy by design

Author : Francesco Maldera

Date : 18 Dicembre 2019

Partiamo dagli eventi sfavorevoli

Esistono eventi sfavorevoli difficili da intercettare. *Low and slow* è un tipico esempio di approccio d'attacco che amano i malintenzionati più furbi: "ti rubo denaro poco alla volta (*low*) e una volta ogni sei mesi (*slow*), così tu non te ne accorgi". Oppure quando qualcuno se ne accorge, è passato troppo tempo e la violazione, ormai, ha colpito centinaia di migliaia di persone e ha causato molti danni.

Esistono, tuttavia, eventi ancora più subdoli che, peraltro, non sono neanche legati ad attacchi di malintenzionati. Parliamo di malfunzionamenti del software che producono in stampa[1] un documento dai contenuti diversi da quelli presenti nel sistema informativo e, comunque, differenti da quelle che erano le intenzioni del soggetto che detiene e tratta i dati personali (sia esso titolare o responsabile).

L'esempio più classico è la polizza assicurativa che, in Italia, viene fornita insieme alla Carta Internazionale di Assicurazione Veicoli a Motore (la cosiddetta Carta Verde): questo è il documento che garantisce all'estero la copertura assicurativa. Supponiamo che, per un **errore di stampa**, nel punto dove deve essere indicata la targa, venga riportato un carattere sbagliato; per esempio, venga riportato uno spazio bianco al posto della prima lettera. Nessun utente se ne accorgerebbe anche perché nessun utente controlla la propria Carta Verde! Tuttavia, questo errore potrebbe, in caso di controllo da parte delle forze di polizia all'estero o di sinistro, creare molte difficoltà al conducente e, in qualche caso, anche gravi compressioni dei diritti e delle libertà della persona.

Dal punto di vista del Regolamento UE 2016/679 (GDPR) questo "evento negativo" è una **violazione di integrità** ovvero è avvenuta (seppur in stampa) una modifica non autorizzata di un dato personale. Non è detto che sia un *data breach* ai sensi dell'art. 33 del GDPR: per capirlo, conviene affidarsi alle linee guida del WP 29 n. 250rev.01 riviste ed adottate il 6/2/2018[ii]. In ogni caso, è un evento negativo che, spesso, passa inosservato perché collegato a "nuove versioni" di software che "ha sempre funzionato bene".

Insomma, la sicurezza informatica e la protezione dei dati personali deve occuparsi anche degli eventi più inattesi e, forse, più banali ma, potenzialmente, molto dannosi: le nuove *release* del software e le relative assicurazioni di compatibilità con l'ambiente nel quale devono operare.

La privacy by design del GDPR

Come già osservato, anche un errore nella stampa può costituire un *data breach* ai sensi dell'art. 33 del GDPR: deve esserci un rischio per i diritti e le libertà degli interessati. E se un referto sanitario è stampato senza un termine che il medico aveva, invece, inserito nel suo sistema di gestione delle diagnosi? Se il medico aveva scritto la frase "Senza tracce di lesioni dell'arteria..." e la stampa viene prodotta con la frase "tracce di lesioni dell'arteria...", **che succede?** Quali sono le possibili conseguenze? È un *data breach*? Probabilmente sì: certamente c'è una violazione di integrità del dato personale ed è anche possibile che ci siano conseguenze piuttosto serie per il paziente (nel lessico del GDPR l'"interessato"). Intanto, il referto è formalmente "normale" nel senso che non presenta elementi che possano apparire strani e, quindi, generare la reazione di chi lo legge: è una frase sensata rispetto alla fattispecie refertata e, quindi, non è suscettibile di una specifica richiesta di chiarimenti.
Quindi, per esempio, a fronte di quel referto, il medico di famiglia (o un altro sanitario che dovesse leggerlo successivamente) potrebbe prescrivere un ulteriore esame invasivo (una coronografia o una risonanza) che, sulla base del "vero" contenuto del referto, non sarebbe stato necessario.

Per difendersi dai comportamenti improvvisamente "strani" del software, il GDPR mette in campo **un principio determinante:** la *privacy by design*. Ricordiamo che il primo paragrafo dell'articolo 25 prevede che:

"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati".

Il titolare (o il suo responsabile del trattamento), quindi, deve prevedere, preliminarmente (*al momento di determinare i mezzi del trattamento*) e correntemente (*all'atto del trattamento stesso*) meccanismi tecnici e organizzativi che riducano al massimo i rischi per gli interessati. E un meccanismo che ha caratteristiche sia tecniche sia organizzative è il **test del software**.
In particolare, i meccanismi correnti di testing devono garantire che le nuove *release* del software:

- funzionino correttamente cioè svolgano le attività per le quali sono state progettate e realizzate;
- non presentino vulnerabilità che possano essere sfruttate da minacce note.

A questo, sia per la versione iniziale sia per le nuove versioni del software, il produttore - che normalmente è diverso dal titolare - deve aggiungere la chiara esplicitazione degli ambienti (sistemi operativi, browser, librerie di corredo, ecc.) nell'ambito dei quali è stato testato affinché chi lo utilizza (ovvero lo stesso titolare) possa adeguare i propri apparati ai requisiti corretti.

Anche quest'ultima misura, soprattutto quando il titolare è una grande organizzazione che non ha adottato alcun meccanismo simile a un *Configuration Management Database*, può non essere sufficiente e richiede un'ulteriore fase di test sul campo. Pensiamo a un ospedale nel quale sono presenti decine di postazioni di lavoro che, nel tempo, possono aver assunto, per varie ragioni, configurazioni del software di base (soprattutto librerie) differenti: occorre verificare direttamente sul campo che la stampa non subisca alterazioni così lievi da non essere notate ma potenzialmente molto dannose come quelle descritte in precedenza.

E se si applicasse ITIL v3 2011?

Abbiamo accennato al *Configuration Management Database* (CMDB) che è uno degli elementi fondanti del framework ITIL v3 2011 (talvolta impropriamente denominato ITIL v4) e, in particolare, delle linee guida sulla Service Transition ovvero di quella fase che prepara all'introduzione in esercizio di nuovi servizi o nuove release di servizi già in uso. L'implementazione di un CMDB potrebbe essere un buon punto di partenza nell'applicare il principio di privacy by design anche se, ad essere corretti, sarebbe necessario percorrere tutti i processi previsti dalla Service Transition e, in particolare, i processi di *Release and deployment management* e *Service testing and validation*.

Questo consentirebbe di dormire sonni un po' più tranquilli anche su possibili violazioni subdole come quelle che possono verificarsi in fase di stampa di un documento che viene consegnato all'interessato.

Oppure ISO 27001?

L'alternativa metodologica, non meno impegnativa di ITIL, per garantire una *privacy fin dalla progettazione* potrebbe essere quella di dotarsi di un Information Security Management System (ISMS) conforme allo standard ISO?IEC 27001. Certamente, i puristi direbbero che non possiamo far coincidere la sicurezza informatica con la protezione dei dati personali: hanno ragione, ma la privacy ha molto da imparare dai princìpi dell'*information security.*

E, quindi, per introdurre qualche misura che riduca il rischio di essere colti da un *data breach* da "stampa tagliata", è possibile ispirarsi ad alcuni dei **controlli**, tra i più sottovalutati, presenti nell'Allegato A dello standard ISO 27001:

- *A.12.1.2 Change management*: ogni cambiamento nell'organizzazione riguardante i processi, i sistemi e le infrastrutture deve essere controllato;
- *A.14.2.7 Outsourced development*: l'organizzazione deve supervisionare e monitorare le attività di sviluppo dei sistemi in outsourcing;
- *A.14.2.8 System security testing*: durante lo sviluppo devono essere condotte specifiche

attività di test riguardanti la sicurezza;
- *A.14.2.9 System acceptance testing*: piani di test ed i relativi criteri di accettazione devono essere stabiliti per nuovi sistemi, upgrade e nuove versioni.

Conclusioni

Ogni realtà potrà decidere di programmare il percorso più utile e, in fondo, più proficuo rispetto ai propri obiettivi. Basta non dimenticarsi di due cose:

- il *data breach* (in *condominio* con il diavolo) si nasconde nei dettagli;
- non serve inventarsi nulla, è quasi già tutto scritto nei framework e negli standard internazionali.

Note

[1] Quando si parla di stampa, si intendono i formati elettronici PDF o le stampe cartacee.

[2] https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827.

Articolo a cura di **Francesco Maldera**