NT+ Diritto
Norme & Tributi Plus

Il Sole 24 ORE

Comunitario e Internazionale 01 Febbraio 2021

EDPB, nuove linee guida sul data breach - Attacchi informatici e rischi del "fattore umano"

Stampa

di Luca Tufarelli, Giulia Maria Amato, Carola Spada*

In breve

In questo appuntamento: breach volontario, e involontario, misure organizzative e tecniche per prevenire / mitigare l'impatto dei rischi derivanti dal fattore umano , perdita o furto di dispositivi aziendali, attacchi sui siti web volti all'esfiltrazione di dati e misure organizzative e tecniche per prevenire / mitigare l'impatto degli attacchi informatici

Nel primo appuntamento del Focus abbiamo visto come le linee guida forniscono ai Titolari del trattamento un utile strumento per agevolare l'individuazione delle ipotesi in cui, a causa di un incidente di sicurezza o di altri comportamenti contrari alle prescrizioni dei sistemi di compliance aziendali, si verifichi una violazione dei dati personali appartenenti a persone fisiche. Oggi parliamo delle misure per mitigare l'impatto dei rischi derivanti dal fattore umano e le tecniche per la prevenzione degli attacchi informatici

Fonti di rischio derivanti dal fattore umano

Data breach volontario

Altra fonte di rischio per la realizzazione di violazioni di dati personali potrebbe derivare dal "*fattore umano*", per tale intendendosi i dipendenti/collaboratori del Titolare del trattamento che abbiano accesso ai dati personali per via dell'attività prestata in favore dell'azienda.

Le violazioni potrebbero essere sia involontarie, quindi causate da mero errore, ovvero volontarie. Esempio tipico di tale seconda ipotesi potrebbe essere il dipendente che, prima di lasciare la posizione lavorativa presso l'azienda effettua una copia dei dati di contatto dei clienti per contattarli successivamente ed attrarli poi presso la nuova impresa.
Queste tipologie di violazioni sono tipicamente violazioni di riservatezza, poiché la banca dati da cui si attinge viene di solito lasciata intatta, il suo contenuto "semplicemente" copiato per un ulteriore utilizzo.
Anche la quantità di dati interessati è solitamente bassa o media. Inoltre non si tratta di categorie di dati sensibili (come potrebbero essere i dati bancari) o particolari ex art 9 GDPR.
In questi casi pertanto, poiché la violazione non comporta un rischio elevato per i diritti e le libertà delle persone fisiche, sarà sufficiente la notifica all'Autorità. Tuttavia, fornire l'informazione agli interessati potrebbe essere utile per il Titolare del trattamento, essendo più conveniente che il cliente venga informato dall'azienda sulla fuga di dati piuttosto che dall'ex dipendente che cerca di contattarli.
Naturalmente valutazioni diverse dovranno essere condotte nell'ipotesi in cui i dati raccolti dall'ex dipendente siano dati particolari o sensibili o nel caso in cui si abbia contezza di intenzioni assai più pericolose circa l'utilizzo dei dati (come ad esempio furti di identità o frodi).

Data breach involontario

Un esempio tipico di errore umano dal quale derivi la violazione di dati personali potrebbe essere l'invio di una mail ad un soggetto diverso da quello cui era destinata. Anche in questa ipotesi siamo in presenza di una violazione della riservatezza, non sussiste invece una violazione dell'integrità o della disponibilità dei dati dell'interessato.
L'azione più efficace di mitigazione è quella di contattare prontamente il destinatario della mail, chiedendogli di cancellarla. In tali ipotesi il basso numero di individui interessati, l'individuazione immediata della violazione e le misure adottate per ridurre al minimo i suoi effetti rendono il caso privo di rischi. Sarà quindi sufficiente registrare la violazione ex art. 33 co 5 GDPR.

Tali considerazioni mutano nel caso in cui vengano erroneamente trasmessi dati sensibili e/o che coinvolgano un elevato numero di soggetti (es. un dipendente della pubblica amministrazione che mandi una mail contente indirizzi postali, numeri di previdenza sociale ecc. di un elevato numero di cittadini). L'aumento significativo di rischio per i diritti e le libertà degli interessati comporterà gli obblighi di cui agli artt. 33 e 34 GDPR.

Misure organizzative e tecniche per prevenire / mitigare l'impatto dei rischi derivanti dal fattore umano
-Implementare di tecniche per forzare l'autenticazione dell'utente quando accede a dati personali sensibili;
-Disabilitare dell'account aziendale dell'utente non appena la persona lascia l'azienda;
-Controllare i flussi di dati insoliti tra il file contenuti nel server e le postazioni di lavoro dei dipendenti;
-Attuare periodicamente programmi di formazione, istruzione e sensibilizzazione per i dipendenti sui loro obblighi in materia di privacy e sicurezza e sull'individuazione e la segnalazione di minacce alla sicurezza di dati personali. Sviluppare un programma di sensibilizzazione per ricordare ai dipendenti gli errori più comuni che portano alla violazione dei dati personali e come evitarli.
-Utilizzare meccanismi (ad es. token (senza fili) per l'accesso/apertura di account bloccati) per un rapido passaggio dell'utente a ambienti condivisi.

Perdita o furto di dispositivi aziendali
In caso di furto o smarrimento di dispositivi portatili aziendali (come pc, tablet, chiavette USB) il Titolare del trattamento dovrà prendere in considerazione tutte le circostanze inerenti i dati trattati sul dispositivo, come la tipologia di dati in esso memorizzati, nonché le misure adottate prima della violazione per garantire un'efficace livello di protezione e sicurezza.
L'utilizzo di sistemi di crittografia del dispositivo che rendano leggibile i dati in chiaro solo ai soggetti in possesso della chiave, nonché un'adeguata protezione dall'accesso al dispositivo (preferibilmente tramite doppia autenticazione), sono strumenti in grado di eliminare del tutto il rischio per i dati degli interessati in esso contenuti.
Inoltre, al fine di ripristinare la disponibilità persa a causa del furto/smarrimento del dispositivo, dovrebbe essere altresì garantito un idoneo sistema di backup.
In presenza di tutte le misure di sicurezza su indicate sono infatti scongiurati sia i rischi per la riservatezza e l'integrità, in quanto il soggetto che dovesse reperire il dispositivo non potrebbe avere accesso ai dati in esso contenuti, sia i rischi legati alla violazione della disponibilità, in quanto il sistema di backup evita la perdita dei dati medesimi e ne consente un rapido ripristino. (A tale proposito, se possibile e appropriato al trattamento dei dati in questione, sarebbe comunque opportuno non salvare i dati sul dispositivo, ma su un server centrale di back-end.)
Ne consegue che in tali ipotesi sarà sufficiente la registrazione della violazione ex art. 33 co 5 GDPR.

Attacchi sui siti web volti all'esfiltrazione di dati
Gli attacchi che sfruttano le vulnerabilità dei siti web commessi tramite attacchi di iniezione, es. SQL injection (1) , compromissione del sito e metodi simili, mirano in genere a copiare, esfiltrare e abusare delle informazioni in esso contenute. Si tratta quindi di violazioni della riservatezza ma anche dell'integrità dei dati.
Le potenzialità di questi attacchi sono assai pericolose, i dati captati dal sito web di un Titolare che offre servizi al pubblico possono consentire l'identificazione univoca dell'utente e contenere informazioni sensibili. Il range di danno può andare dal targeting con marketing non richiesto a furti di identità, campagne di phishing etc.
Spesso quindi ne deriva un rischio elevato per i diritti e libertà degli interessati e di conseguenza è necessario l'adempimento dell'obbligo di notifica all'Autorità, ma anche di comunicazione agli interessati.

Misure organizzative e tecniche per prevenire / mitigare l'impatto degli attacchi informatici
-Crittografia e gestione appropriata delle chiavi, specialmente quando i trattamenti riguardano password, dati sensibili o i dati finanziari, (l'utilizzo di crittografia di hashing e salt è sempre preferibile alla cifratura delle password);
-Mantenere il sistema aggiornato (software e firmware);
-Garantire che tutte le misure di sicurezza IT utilizzate siano efficaci, e mantenerle regolarmente aggiornate in caso di mutamento dei trattamenti o delle circostanze del trattamento. Tenere un registro di tutti gli aggiornamenti eseguiti;

-Utilizzare metodi di autenticazione forte come l'autenticazione a due fattori, integrato da una politica di aggiornamento password;
-Utilizzare firewall adeguati, aggiornati, efficaci e integrati e sistemi rilevamento delle intrusioni.

____
*Studio Legale Ristuccia Tufarelli & Partners
(1) *SQL injection è una tecnica di code injection, usata per attaccare applicazioni che gestiscono dati attraverso database relazionali sfruttando il linguaggio SQL. Il mancato controllo dell'input dell'utente permette di inserire artificiosamente delle stringhe di codice SQL che saranno eseguite dall'applicazione server: grazie a questo meccanismo è possibile far eseguire comandi SQL anche molto complessi, dall'alterazione dei dati (e.g. creazione di nuovi utenti) al download completo dei contenuti nel database.*