

“Sicuri di essere sicuri?”

Letizia Maria Ferraris: “Data Breach ... se lo conosci... lo eviti... e difendi te stesso”

Viviamo nell’era digitale dove la maggior parte delle informazioni personali e professionali sono archiviate *online*.

Non è un caso che la normativa (europea e interna) sia più esigente sugli obblighi di attuazione di misure di sicurezza per il trattamento dei dati e che le autorità di controllo abbiano a loro volta un approccio più rigoroso, contrastando le violazioni con sanzioni significative.

Le aziende pubbliche e private si trovano così a implementare programmi di compliance completi, seguendo *best practices*, anche per poter contrastare l’aumento significativo di quelle violazioni di dati personali, meglio conosciute come *data breach*.

Dicasi *data breach* un incidente in cui informazioni sensibili, confidenziali o protette vengono rese accessibili (a seguito di furto, interferenze illecite o altri reati equipollenti) a terzi o modificate o distrutte o rese indisponibili creando un rischio per i diritti e le libertà degli interessati, a cui appartengono i dati raccolti.

Il fenomeno è molto diffuso e trova spesso origine nella vulnerabilità nei sistemi di sicurezza o nell’errore umano.

Per sottrarre dati, gli hacker (o criminali informatici) utilizzano raffinate metodologie, come l’invio di *Phishing* (email o messaggi ingannevoli che inducono le vittime a fornire informazioni personali o a cliccare su link infetti) o il ricorso a *Malware* (*software* dannosi che possono infettare i sistemi e permettere agli hacker di accedere ai nostri dati).

Gli errori o le fragilità dei *software* sono spesso accompagnati da comportamenti umani, facilitatori inconsapevoli di condotte non lecite: l’uso di credenziali deboli, impostazioni di sicurezze non corrette che lasciano i dati esposti, perdita di dispositivi, tablet, smartphone o chiavette usb.

Quando un’azienda piccola o grande o un ente pubblico viene a conoscenza di una violazione di dati che riguarda i propri dipendenti o i clienti o terzi, diventa fondamentale agire rapidamente per individuare il livello di gravità e i rischi per le persone “interessate” (cioè coloro i cui dati trafugati fanno riferimento) e mettere in atto (tempestivamente) tutte le misure per contenere tali danni, in base alle normative nazionali e internazionali.

Se poi le violazioni comportano rischi per gli interessati, il Regolamento Generale sulla Protezione dei Dati (GDPR) dell’Unione Europea richiede che esse siano segnalate entro 72 ore. Quando i rischi sono di maggiore gravità, tutte le persone coinvolte dovranno essere informate dell’accaduto.

Questa è anche la ragione per cui in un tempo di formazione ed educazione all’uso consapevole delle varie forme di digitalizzazione nei rapporti economici e sociali, appare urgente la consapevolezza dei *data breach*.

In un sistema economico illuminato, infatti, prima ancora delle sanzioni, si deve temere il danno reputazionale.

Ogni qual volta i nostri dati finiscono nelle mani sbagliate, le attività fraudolente (primo tra tutti, il furto

d'identità o la compromissione delle informazioni finanziarie) possono avere conseguenze devastanti sulla vita di ciascuno e sulla sua onorabilità (come accade in ambito sanitario, con la diffusione di diagnosi, trattamenti di cura o altre informazioni riservate sulle patologie).

Conoscere le minacce che possono causare un *data breach* e adottare misure di sicurezza appropriate, permette inoltre di monitorare le transazioni e adottare misure preventive per evitare perdite economiche (e le sanzioni annesse).

Venendo alle tutele, le prime linee di difesa contro i *data breach* sono costituite dall'uso di password forti e complesse (evitando l'uso di parole comuni e preferendo la combinazione di lettere, numeri e caratteri speciali) ovvero l'uso di 'autenticazione a due fattori (2FA, che aggiunge un ulteriore livello di sicurezza richiedendo due passaggi di verifica prima di concedere l'accesso ai dati) con l'aggiornamento software e dispositivi.

Seguendo il quadro normativo (art. 83, 58, 5, 6, 12-14 GDPR), è però possibile delinearne di più complesse: **misure preventive** idonee a ridurre il rischio; **misure correttive** per mitigare gli effetti delle violazioni e prevenire quelle future; **misure rafforzative**, per 'bloccare' gli accessi informatici non autorizzati; **misure valutative**, per monitorare lo stato dei rischi.

Per intercettare le attività illecite di cui fossimo destinatari, sarà insomma auspicabile la costante formazione sulle tecniche utilizzate dai cybercriminali, partecipare a corsi in materia di sicurezza cyber, ricorrere a riviste specializzate, affidarsi a fornitori affidabili, applicare sempre il principio di minimizzazione (ovvero mettere a disposizione solo i dati che devono essere "trattati" per ottenere un servizio) o anche solo leggere attentamente le informative.

Tutto ciò potrà fare la differenza nel monitorare chi intende offrire servizi digitali falsi o dannosi.

In un mondo sempre più connesso proteggere noi stessi rimane esclusiva nostra responsabilità!

© 2024 CIVICO20NEWS – riproduzione riservata

Data di pubblicazione: 28/10/2024

Salvato in PDF in data: 23/10/2026

Link all'articolo: <https://civico20-news.it/la-tutela-dei-dati-personali/csi-ferraris/28/10/2024/>