ATTUALITÀ

Cosa possiamo imparare dal data breach della SIAE?

di **Fondazione AIDR** · 3 novembre 2021, 12:43

di Federica De Stefani, avvocato e responsabile Aidr Regione Lombardia

Ogni qualvolta si sente parlare di data breach dovremmo fermarci e approfondire l'argomento perché dalle vicende negative altrui si possono trarre preziosi insegnamenti.

Gli attacchi informatici aumentano, ormai, in maniera esponenziale, ma i problemi che si devono affrontare rimangono gli stessi.

Si passa dalla mancanza di adeguate misure di prevenzione alla gestione non corretta dell'evento, dalle informazioni non veritiere riferite agli interessati ai tentativi di imputare la colpa a soggetti determinati.

L'ultimo data breach salito agli onori della cronaca è quello occorso alla SIAE.

La cronistoria dell'attacco informatico inizia il 20 ottobre con la violazione delle infrastrutture IT della SIAE ad opera della organizzazione di cybercriminali denominata Everest. I dati sono stati esfiltrati, è stato richiesto un riscatto in bitcoin e i dati sono stati messi in vendita nel dark web.

Si aggiunga inoltre che alcuni artisti iscritti alla SIAE sono stati contattati direttamente dai cybercriminali per il pagamento di un riscatto per la cancellazione dei dati personali in loro possesso.

I dati personali esfiltrati

Ecco il punto cruciale di ogni data breach: i dati personali, la gestione, l'esatta valenza che attribuiamo agli stessi.

Il GDPR, da questo punto di vista, è chiaro, l'art. 33 espressamente impone che "*In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è*

venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche".

La SIAE, correttamente, notifica l'esfiltrazione al Garante per la protezione dei dati personali, che secondo la procedura apre un'istruttoria, ma poi il presidente in un'intervista al TG1 afferma testualmente che "*per fortuna non sembrerebbero esserci dati economici, cioè relativi a iban bancari, iban e cose di questo genere, solo dati anagrafici relativi a carte d'identità, codici fiscali e dati di molti nostri dipendenti...*"

Emerge in tutta la sua dimensione la mancanza di consapevolezza che ancora oggi abbiamo con riferimento ai dati personali.

I dati anagrafici vengono considerati meno importanti dei dati bancari molto probabilmente perché non si percepisce cosa si possa fare con questi dati, quali reati e quali truffe possano essere realizzate.

Smentiamo quindi questa falsa credenza: i dati anagrafici hanno la sessa importanza di altre tipologie di dati, anzi, la loro combinazione può portare ad un livello di pericolosità superiore rispetto ad un "semplice" dato bancario.

Ciò che varia è la percezione che ha l'utente della potenzialità negativa che possono avere i dati che finiscono nelle mani dei cybercriminali.

Non è mai *"solo"* un numero di telefono, non è mai *"solo"* un codice fiscale, non è mai *"solo"* un nome e cognome. È ciò che si può fare con quei dati, è questo il pericolo che si deve valutare.

La tipologia di attacco

L'attacco informatico messo a segno da Everest avrebbe sfruttato il basso livello di protezione delle infrastrutture IT di SIAE. Niente ransomware, quindi niente crittografia dei dati, ma semplice penetration test ed esfiltrazione dei dati dovuti, appunto, alle scarse protezioni adottate dalla società.

Si accendono, ancora una volta, i riflettori sulla necessità, per le aziende, di investire nelle misure di prevenzione e di sicurezza proprio per far fronte all'aumento esponenziale delle minacce cyber.

La cybersecurity deve rientrare di diritto tra le priorità aziendali poiché non è possibile, considerando i danni, economici e reputazionali, ai quali espone un incidente informatico, rimandare il rafforzamento delle misure in questo senso.

Articolo pubblicato su Istituzioni24: https://www.istituzioni24.it/2021/11/03/cosa-possiamo-imparare-dal-data-breach-della-siae/

© 2026 Istituzioni24