PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 23 - numero 4976 di Mercoledì 14 luglio 2021

Privacy: una una sanzione di 3 milioni di dollari

Le sanzioni per le violazioni in tema di dati personali possono essere assai elevate in Europa, ma anche gli Stati Uniti non scherzano!

Ormai i lettori vengono frequentemente aggiornati sulle sanzioni, talvolta estremamente elevate, che vengono applicate quando vengono violati alcuni dettati del GDPR. Anche se gli Stati Uniti non hanno un documento equivalente, le sanzioni, che vengono determinate dalle varie agenzie coinvolte, possono essere di importi estremamente elevati. Vediamo le ragioni dell'applicazione di una sanzione di 3 milioni di dollari.

Il 14 aprile 2021 il Dipartimento dei servizi finanziari di New York ha annunciato che una compagnia di assicurazione ha concordato una sanzione di 3 milioni di dollari, per ripetute violazioni in tema di sicurezza informatica e protezione dei dati, nel periodo dal 2018 al 2020.

Ricordo ai lettori che il regolamento violato è entrato in vigore negli Stati Uniti nel 2017. Questo regolamento prevede che tutti coloro che sono dotati di una licenza per svolgere servizi finanziari devono utilizzare una autentica a più fattori, per garantire l'accesso sicuro dei clienti al sistema informativo aziendale.

Inoltre, il regolamento impone che una violazione informatica venga riferita entro 72 ore da quando si è verificata.

Infine, il regolamento prevede che una volta all'anno venga effettuato un audit, per verificare la corrispondenza tra le indicazioni del regolamento e le misure effettivamente utilizzate.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0143] ?#>

Tutto è cominciato il 23 ottobre 2019, quando l'istituzione finanziaria segnalò una violazione informatica. L'ufficio personale aveva ricevuto un messaggio di posta elettronica, alquanto sospetto, inviato da un dipendente che chiedeva assistenza per cambiare alcuni parametri del suo deposito. Venne avviata un'indagine interna, che mise in evidenza come il conto corrente del dipendente fosse stato violato più volte. L'ente finanziario provvide a informare i soggetti potenzialmente coinvolti, cambiare le loro credenziali e attivare un sistema di monitoraggio delle transazioni svolte sui conti a rischio.

L'indagine ha permesso di accertare che la ragione della violazione era dovuta al fatto che l'ente finanziario non aveva ancora attivato la autentica a più fattori.

Ricordo ai lettori che la autentica a più fattori consente l'accesso a un sistema informativo non solo digitando la parola chiave, ma introducendo anche ulteriori elementi di garanzia, come ad esempio la ricezione di un codice inviato tramite SMS sullo smartphone di chi richiede l'accesso, od altre tecniche similari.

Una nuova violazione si verificò il 12 maggio 2020, con uno movimento di 200.000 $ apparentemente non autorizzato. Ancora una volta, i dati misero in evidenza come una delle ragioni alla base della violazione era da attribuire alla mancanza di una autentica a due fattori.

A questo punto il Dipartimento dei servizi finanziari di New York attivò un'indagine approfondita e scoprì altre due violazioni informatiche, che non erano state segnalate.

Nel documento, che applicava la sanzione, l'ente di controllo ha riconosciuto che l'ente finanziario aveva offerto una valida collaborazione e stava mettendo a punto misure di correzione, anche se in ritardo.

L'accordo, relativo al pagamento di una sanzione di 3 milioni di dollari, è condizionato dal rispetto dei seguenti impegni:

- l'illustrazione, entro 120 giorni, di un dettagliato piano di risposta a possibili incidenti informatici,
- La conduzione di una valutazione di rischio informatico e
- la messa disposizione di tutti i dipendenti di documentazione necessaria per l'addestramento e il monitoraggio dei comportamenti.

Illustro questo documento ai lettori perché sia possibile tracciare un parallelo con quanto avviene in Europa, dove pure l'ammontare delle sanzioni è legato non solo al tipo di violazione, ma anche al comportamento assunto dal "peccatore", in fase di indagine sulla violazione e di messa punto di misure di contrasto.

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.