PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 19 - numero 4094 di giovedì 05 ottobre 2017

Avete un piano di emergenza per un data breach?

Anche le aziende di grande dimensione non hanno ancora messo a punto un piano di emergenza per fronteggiare una possibile violazione dei dati.

Pubblicità
<#? QUI-PUBBLICITA-MIM-[BIA0001] ?#>

Cominciamo ad inquadrare il problema.

Equifax è una azienda di dimensioni mondiali che utilizza tecniche avanzatissime per stabilire delle valutazioni di affidamento creditizio per aziende, anch'esse di tutto il mondo.

L'azienda organizza, raccoglie e analizza i dati su più di 820 milioni di utenti e più di 91 milioni di aziende. Il suo database raccoglie una moltitudine di informazioni oltremodo sensibili, afferenti alle valutazioni di credito dei soggetti controllati.

Le sue azioni sono contrattate alla Borsa di New York a e l'azienda impiega poco meno di 10.000 dipendenti in tutto il mondo.

Appare evidente che una azienda che svolge un'attività del genere ha un ruolo critico, perché una valutazione negativa può rendere difficilissima la concessione del credito ad un soggetto, fisico o giuridico, mentre una valutazione positiva, non adeguatamente supportata, potrebbe mettere in difficoltà chi concede il credito.

Ci si potrebbe attendere che un'azienda del genere abbia messo a punto delle tecniche di protezione raffinatissime per il proprio data base, che costituisce il vero patrimonio aziendale, insieme agli algoritmi che analizzano i dati grezzi e da essi estraggono le valutazioni di affidabilità del credito.

Orbene, questa azienda è stata recentemente vittima di un attacco per ransomware, che certamente molti nostri lettori conoscono, perché in Italia sono state già numerose le aziende colpite da questo particolare tipo di attacco.

In particolare, i due applicativi WannaCry e Petya hanno più volte dimostrato la loro capacità di sfruttare debolezze nella architettura di difesa di un database, esponendo quindi i titolari a queste richieste di riscatto, che in molti casi sono state purtroppo accettate.

L'azienda Equifax, in particolare, ha dovuto urgentemente attivare sul proprio sito, che i lettori possono consultare, una intera sezione dedicata a tutti i clienti, che potrebbero essere stati coinvolti nella violazione di questi dati.

Il fatto stesso che l'attacco abbia avuto buon fine è la prova provata del fatto che le misure di difesa non erano sufficienti, oppure gli strumenti di attacco erano troppo intelligenti!

Ricordo ai lettori che il nuovo regolamento generale europeo sulla protezione dei dati personali rende obbligatorio per il titolare del trattamento la segnalazione all'autorità nazionale Garante di qualsiasi violazione dei dati. Non è prevista nessuna esenzione, indipendentemente dalla natura dei dati perduti o sottratti.

L'autorità Garante, volta ricevuta la segnalazione, analizza la situazione, valuta la criticità dell'evento ed eventualmente dà indicazioni vincolanti al titolare coinvolto. È del tutto opportuno, e il regolamento sottolinea questo aspetto, che una notifica all'autorità Garante sia accompagnata da una descrizione non solo delle circostanze in cui si è verificata la violazione, ma anche delle misure che il titolare ha già messo in atto per prevenire il ripetersi di un simile evento.

Nel libro che ho dedicato alla illustrazione del nuovo regolamento generale europeo un intero capitolo è dedicato alle modalità, con cui è possibile affrontare questo evento, del quale si può solo stimare la probabilità che si verifichi, ma che non si può certo affermare non si possa mai verificare.

Questa è la ragione per la quale tutte le aziende dovrebbero aver già attivato un programma di emergenza, da tenere costantemente aggiornato e da utilizzare al più presto, non appena si ha notizia di una perdita di dati.

Ovviamente la disponibilità di un piano di emergenza non costituisce garanzia assoluta di pronto intervento e messa sotto controllo dell'evento, ma certamente può offrire un prezioso strumento per la limitazione dei danni.

Tanto per dare un esempio di casi concreti, recentemente accaduti, ricordo a tutti i lettori che uno dei più grandi servizi di trasporto di pacchi e corrispondenza è rimasto vittima proprio di un attacco condotto con i due software sopraelencati.

Il responsabile della sicurezza informatica ha dichiarato che l'attacco ha coinvolto non solo il sistema informativo primario, ma anche i sistemi informativi di centinaia di altre aziende, di dimensioni minori, cui questa azienda si appoggia per la raccolta e lo smistamento dei plichi. Al momento non è ancora possibile per l'azienda stabilire quale sia stato l'impatto economico e quando l'azienda potrà riprendere appieno la propria attività. Stiamo parlando di un evento che si è verificato nel maggio 2017 e ne parliamo oggi, a ottobre 2017!

Colgo l'occasione per ricordare a tutti i lettori che è bene tenersi costantemente aggiornati sulle modalità con cui si sviluppano queste violazioni dei dati, per poter costantemente aggiornare il proprio piano di emergenza, confidando nel fatto che tale piano sia stato già sviluppato e approvato dall'alta direzione!

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.