PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3726 di giovedì 25 febbraio 2016

Che fare, a fronte della sottrazione di dati personali di un dipendente?

Quando vengono sottratti dati personali di un dipendente, viene danneggiata l'azienda ed il dipendente. Ecco gli accorgimenti da prendere a fronte di questa particolare tipologia di reato. Di Adalberto Biasiotti.

In un recente numero della rivista abbiamo pubblicato un cenno ad una sentenza della cassazione, che ha messo in evidenza come il furto di dati aziendali interni, da parte di un dipendente, deve essere inquadrato in un profilo specifico di reato.
Vediamo invece adesso di affrontare un problema, che purtroppo ogni tanto si presenta, legato al fatto che **un malvivente sia stato in grado di sottrarre i dati personali dei dipendenti di un'azienda**.
In questo caso evidentemente il soggetto danneggiato non è soltanto l'azienda, ma anche il dipendente, e occorre inquadrare correttamente le modalità di reazione dell'azienda a questo evento, che talvolta potrebbe essere addirittura drammatico.

Ecco perché è opportuno che il responsabile del trattamento dei dati personali metta a punto un piano di mitigazione e reazione ad un'eventuale violazione di questa specifica categoria dei dati.
È noto che le risorse umane hanno a disposizione un gran numero di dati personali dei dipendenti, alcuni evidentemente assai sensibili.
Molto spesso nelle aziende è previsto un periodico ciclo di valutazione del comportamento del dipendente, magari in preparazione ad una promozione, e i dati relativi potrebbero avere un impatto significativo sulla carriera del dipendente coinvolto.
Non parliamo poi del fatto che molto spesso lo stipendio viene accreditato sul conto corrente bancario del dipendente e quindi anche questo dato delicato viene archiviato dal Dipartimento delle risorse umane.
Ma non è finita.

Nel profilo personale di un dipendente, anche se non proprio nella cartella fisica che contiene i suoi dati, sono conservati dati afferenti ai privilegi di accesso al sistema informativo, all'utilizzo di apparecchiature aziendali di vario tipo, all'autorizzazione all'uso di auto aziendali e via dicendo.
La raccolta di tutti questi elementi potrebbe perfino consentire un malvivente di creare una identità fittizia, che gli permetterebbe di comportarsi, a tutti gli effetti, come il dipendente, i cui dati sono stati violati.
Come si vede, sono molte e gravi le ragioni per le quali il responsabile della protezione dei dati deve mettere a punto un piano, in grado di tutelare innanzitutto il dipendente, e subito dopo l'azienda, ove i dati personali violati non siano afferenti a progetti , studi o attività commerciali dell'azienda, ma riguardino uno specifico dipendente.

Gli esperti sono concordi sul fatto che un approccio trasparente ed una reazione immediata sono aspetti fondamentali nel gestire in modo corretto un'eventuale violazione di questo tipo.
L'azienda deve pertanto prendere immediato contatto con il dipendente coinvolto, da quel momento in avanti, e mantenere un rapporto costruttivo e aggiornato, senza nulla celare delle proprie debolezze. Ove infatti queste debolezze venissero scoperte successivamente, la posizione dell'azienda indubbiamente ne risulterebbe aggravata.

Il fatto di informare tempestivamente il dipendente ha inoltre il vantaggio che egli viene direttamente coinvolto nella attività di reazione all'uso improprio dei suoi dati. Egli potrà prendere contatto con i propri corrispondenti, e verificare se qualcheduno ha cercato di utilizzare in modo improprio i suoi dati.
Ad esempio, il rapporto con la propria istituzione bancaria diventa estremamente importante.
Appare anche evidente che se i dati sottratti fanno riferimento a un gran numero di dipendenti, l'azienda deve immediatamente attivare una squadra di emergenza, magari attivando un numero verde, per offrire ogni possibile assistenza ai dipendenti coinvolti.
Alcune aziende, coinvolte in questo dramma, hanno addirittura allestito una hotline per i dipendenti, in modo da dare tempestive aggiornate le risposte alle loro domande.
Non dimentichiamo infine che spesso i dati personali del dipendente coinvolgono anche dati personali afferenti alla sua precedente attività ed alle aziende, in cui egli ha precedentemente lavorato.

In questo caso appare evidente che potrebbe essere opportuno prendere contatto anche con queste aziende, per evitare che il malvivente, che ha sottratto questi dati, possa prendere contatto con queste aziende simulando l'identità del dipendente.
Un altro vantaggio del coinvolgimento immediato dei dipendenti in queste situazioni di crisi sta nel fatto che è così possibile dare loro delle indicazioni sulle modalità con cui reagire a possibili domande, provenienti dai mezzi di comunicazione di massa.
Il guaio è già grosso e non c'è certo bisogno di peggiorare l'immagine dell'azienda, dando risposte che potrebbero comprometterla in misura significativa.

L'aggiornamento del piano
Anche se non sono ancora molte le aziende che hanno già messo a punto un piano di risposta ad una possibile violazione dei dati, il modesto numero tende fortunatamente a crescere, purtroppo sulla spinta di eventi delittuosi, che vengono riferiti dagli organi di comunicazione di massa.
Come sempre accade, quando si allestisce un piano di emergenza, esso deve essere continuamente aggiornato, perché lo scenario può cambiare e perché gli strumenti di attacco e di difesa possono anch'essi cambiare.
Le tecniche di gestione delle crisi, che sono illustrate da specifiche norme emesse da comitati specializzati, possono indubbiamente essere preziose.
Queste norme fanno riferimento sia ai problemi di comunicazione con l'esterno, sia di comunicazione con l'interno, sia di supporto alle persone danneggiate sia ad interventi di natura informatica, per mettere sotto controllo la situazione.
Ancora una volta uomo avvisato, mezzo salvato!

Adalberto Biasiotti