PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3882 di mercoledì 26 ottobre 2016

La protezione dei dati personali: manca ancora una cultura aziendale

La gran parte delle aziende non ha una soddisfacente cultura in termini di protezione dei dati personali: l'incremento del rischio di perdita di dati, che con il nuovo regolamento 679/2016 può comportare gravi sanzioni. Di Adalberto Biasiotti.

I risultati di un recente studio europeo sul livello di preparazione dei dipendenti, nei confronti della tutela dei dati personali e, più in generale, dei dati aziendali, ha portato a risultati molto preoccupanti.

Ad esempio, il 78% delle aziende intervistate sviluppa un percorso di formazione per i dipendenti, con relativi aggiornamenti, non più di una volta all'anno.

Nella formazione, il tema della protezione da frodi e da violazioni non è trattato in maniera soddisfacente. Addirittura il 28 % delle aziende intervistate ha dichiarato di non aver mai sviluppato un programma di addestramento aziendale sui requisiti di congruità con i regolamenti europei e con le procedure di sicurezza interne aziendali.

Solo il 22 % delle aziende intervistate mette a punto programmi specifici di formazione sulla sicurezza.

Dal momento che gli esperti sono tutti d'accordo nel ritenere che il 90 % dei dipendenti dimentica quanto ha appreso in un corso di formazione entro una settimana dall'ultimazione, appare evidente che un percorso di aggiornamento, a scadenza annuale, è del tutto insufficiente e non ci si deve stupire se poi i risultati pratici sono del tutto inidonei a consentire all'azienda di raggiungere un livello soddisfacente di sicurezza nella protezione dei dati.

Ecco perché, al termine di questa ricerca, i consulenti offrono cinque spunti di meditazione per l'alta direzione aziendale e per i responsabili della sicurezza, anche informatica, e del trattamento di dati personali.

L'azienda deve assumere un atteggiamento costruttivo nei confronti della security-quando il vertice aziendale si dimostra convinto sostenitore di questa politica, è ben più facile che i dipendenti la adottino e la condividano. Tutti i dipendenti devono assumere un impegno personale a migliorare il livello di sicurezza del loro posto di lavoro e questo impegno deve essere ricordato da appositi cartelli, distribuiti in tutto l'ambiente di lavoro. La direzione aziendale deve individuare dei soggetti particolarmente convinti, inserendoli in programmi di formazione che potranno essere condivisi con i colleghi.

Occorre impostare un programma di formazione e aggiornamento frequente e costruttivo-la formazione e l'aggiornamento non devono essere fatti soltanto una volta all'anno, ma devono essere distribuiti lungo l'intero anno, includendo moduli sulle politiche di sicurezza adottate dall'azienda. La adozione di tecniche miste di formazione, come ad esempio formazione a distanza e formazione in aula, dimostra di essere la forma più incisiva di trasmissione di concetti di sicurezza ai soggetti interessati.

In particolare, deve essere ripetutamente inculcato il concetto di protezione dei dati aziendali, anche personali, custoditi sotto forma cartacea o digitale; una politica di regolare cancellazione e distruzione dei supporti sostiene concretamente questo atteggiamento di sicurezza, riducendo il rischio di perdita di dati.

Impostare un programma di formazione per i dipendenti che operano spesso all'infuori dell'azienda-oggi un numero crescente di dipendenti passa un tempo relativamente contenuto del proprio mese lavorativo all'interno dell'azienda. Il programma di formazione deve tener conto di questi fattori e deve consentire a tutti di poter essere inseriti in programma di formazione iniziale ed aggiornamento. La mobilità di questi dipendenti accresce il rischio di perdita dei dati ed occorre quindi rendere tali dipendenti particolarmente sensibile a questo problema.

Collegamenti a distanza con la rete informativa aziendale, non sufficientemente protetti, possono rappresentare un rischio significativo di perdita dei dati, direttamente dipendente dalla mobilità dei soggetti coinvolti. Infine, la adozione di supporti di memoria mobili costituisce un rischio che deve essere preso in considerazione e sul quale tutti i dipendenti devono essere adeguatamente sensibilizzati.

Adottate una politica di "clean desk" -una politica diffusa a tutti i livelli aziendali, che vede coinvolti tutti i dipendenti nel garantire un soddisfacente livello di sicurezza nell'ambito di lavoro, non solo durante il giorno, ma anche al termine dell'orario di lavoro, rappresenta uno strumento efficiente ed efficace di incremento del livello complessivo di sicurezza. Controlli occasionali, effettuati con spirito costruttivo e non antagonistico, possono contribuire ad accrescere la sensibilità di dipendenti sulla necessità di rispettare queste politiche, perché del tutto congrue con una più sicura operatività aziendale. Nessun terminale aziendale dovrebbe essere privo di salva schermo, protetto da password, che si attiva automaticamente ogni volta che il terminale viene abbandonato per qualche minuto.

Adalberto Biasiotti

Regolamento (Ue) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

www.puntosicuro.it