PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4393 di Lunedì 28 gennaio 2019

Il segreto per proteggere bene i dati personali

Il regolamento europeo non manca di sottolineare, ad ogni occasione, come gli applicativi criptografici rappresentino un prezioso strumento di protezione dei dati personali. Esaminiamo un caso specifico.

Chi scrive non ha dubbi sul fatto che, con il passare del tempo, la criptografia rappresenterà uno dei più diffusi e preziosi strumenti di protezione dei dati personali. Ad esempio, il fatto che oggi siano disponibili, a prezzi attraenti, chiavi USB dotate di applicativo criptografico, rappresenta un esempio di capillarità di utilizzo di algoritmi criptografici. Di particolare interesse, in questo contesto è l'utilizzo di hard disk, dotati di applicativi criptografici incorporati. È uno strumento efficiente ed efficace, che permette di garantire il rispetto di precise esigenze di protezione dei dati, anche se ovviamente esiste qualche limitazione all'uso.

Ricordo ancora una volta che la responsabilità nel determinare il piano di protezione dei dati personali è in carico al titolare del trattamento, con l'ausilio del responsabile del trattamento e con il conforto del responsabile della protezione dei dati.

Un dato che sia sempre protetto da algoritmo criptografico è evidentemente un dato che è ben più difficile catturare da parte di un attaccante; se poi anche il dato viene perduto, esso è illeggibile per chi possa ritrovare questo supporto.

Ecco perché l'utilizzo di hard disk, dotati di applicativo criptografico incorporato, rappresenta una soluzione relativamente economica ed oltremodo brillante.

È bene comunque sottolineare il fatto che il dato è protetto solo finché è residente all'interno dell'hard disk ed occorre mettere a punto specifiche misure di protezione, quando il dato viene prelevato presso l'interessato e registrato sull'hard disk; altrettanto specifiche misure di protezione devono essere usate, quando il dato viene estratto l'hard disk e utilizzato in fase di trattamento.

In altre parole, il dato è protetto solamente quando è archiviato sull'hard disk e non quando viene movimentato.

Avendo chiaro questo aspetto, vediamo come funziona un disco con applicativo criptografico incorporato. Tanto per cominciare, il fatto che l'algoritmo criptografico sia incorporato in hardware rappresenta un grande vantaggio, perché la velocità di funzionamento dell'algoritmo è molto più elevata, rispetto a soluzioni software. Quando il disco viene spedito dal fabbricante, la chiave, che è incorporata nell'hardware, non è attivata. Usando una chiave di autentica, i dati possono essere letti senza nessuna difficoltà.

La decisione circa l'attivazione da algoritmo criptografico sull'hard disk è presa dall'utente, che cambia la chiave di autentica di fabbrica in una nuova chiave, che può essere archiviata su un server di gestione delle chiavi.

Nell'uso corrente, questa nuova chiave viene applicata durante l'attivazione dell'hard disk e protegge i dati registrati sull'hard disk durante tutto il periodo di funzionamento. Quando l'hard disk è a riposo, i dati sono protetti da un accesso illecito e non possono essere estratti, anche se l'hard disk viene collegato ad un'altra macchina.

Lo standard utilizzato per la chiave di cifratura è di elevato livello, appartenente alla categoria TCG-E, vale a dire Trusted Computing Group Enterprises. Questo applicativo è lo stesso che viene utilizzato anche nella protezione criptografica di dati custoditi su laptop. Questo standard fa riferimento ad un algoritmo crittografico assai evoluto, lo Advanced Encryption Standard con chiave a 256 bit. La compatibilità di questo standard è applicabile sia a dischi in tecnica SAS, sia SATA.

Come sempre, non esistono difese assolute, tanto è vero che alla recente convention di Las Vegas, chiamata Black Hat, alcuni hacker hanno presentato alcune possibili soluzioni di violazione di queste protezioni, a condizione però che la hacker abbia accesso fisico al disco rigido. Si tratta quindi di una situazione non certamente realizzabile con facilità, perché queste macchine sono di solito custodite in ambienti protetti contro l'intrusione fisica.

Adalberto Biasiotti

---

www.puntosicuro.it