Il decalogo della Privacy Compliance

Convergenza tra compliance alle norme e soluzioni tecnologiche

Premessa: qualunque genere di controllo (generalizzato e/o specifico, diretto o indiretto) sul lavoratore e sull'uso di pc/internet/risorse informatiche di ogni genere, deve essere esplicitato e previsto in apposito regolamento informatico come disciplinato dal Provvedimento del 1 marzo 2007, emanato dall'Autorità Garante in materia di privacy, nonchè tenuto conto delle vigenti nome sulla tutela del lavoratore (vedasi a titolo esemplificativo e non esaustivo l'art. 4 L. 300/70).

Navigazione web e Conservazione dei log di connessione

Le Norme

Navigazione web: al fine di ridurre il rischio di navigazioni improprie (ovvero estranee all'attività lavorativa), il datore di lavoro deve adottare misure atte e prevenire tali fenomeni, operando i controlli sul lavoratore solo in casi di necessità defensionali (vedasi riscontro di accesso a siti illeciti da parte dell'IP aziendale). Tale obiettivo potrà essere raggiunto individuando:

- categorie di siti correlati o meno con la specifica attività lavorativa;
- adozione di black-list aventi ad oggetto siti o spazi web contenenti determinate parole;
- configurazione di sistemi che limitino, monitorino o escludano download di file o programmi aventi particolari caratteristiche.

Il datore di lavoro non provvederà dunque ad un controllo diretto dei log di navigazione, ma ad un controllo generico delle navigazioni effettuate dalla rete aziendale, ricorrendo ad un controllo diretto nel caso in cui si verifichino episodi di particolare gravità (a titolo meramente esemplificativo e non esaustivo: download di materiale pedopornografico, violazione della legge sul diritto d'autore mediante download di opere musicali o cinematografiche protette).

Conservazione dei log di connessione: la conservazione dei log di connessione costituisce un aspetto prettamente tecnico con risvolti peraltro giuridici. In ottemperanza ai principi di necessità e correttezza, basilari nella normativa privacy, la conservazione di tali dati dovrà essere strettamente limitata al perseguimento di quelle che sono finalità organizzative, produttive e di sicurezza, individuando limiti anche di tipo temporale per il mantenimento di tali dati presso la struttura aziendale.

Individuazione procedure e soggetti preposti per verifica navigazione singola postazione : nel caso in cui il datore di lavoro verifichi che condotte illecite sono state assunte da un dipendente per il tramite della navigazione nonostante le misure adottate, il datore di lavoro potrà procedere all'individuazione della singola postazione di navigazione e della relativa identità del navigatore, costituendo la condotta di quest'ultimo una grave violazione della policy aziendale e primariamente una violazione di legge. Sussistendo a carico del datore di lavoro un obbligo di controllo dell'utilizzo delle risorse, tale evento straordinario potrà essere già previsto nella policy aziendale specificando la procedura adottabile in tale ipotesi nonché i soggetti preposti al controllo (a titolo meramente esemplificativo e non esaustivo: controllo generalizzato che si concluderà con un primo richiamo a lavoratori di una determinata area coinvolta nella navigazione non autorizzata, successiva individuazione e conservazione dei log di connessione indispensabili all'esercizio o alla difesa di un diritto in sede giudiziaria).

Le Soluzioni Tecnologiche

Navigazione web: Microsoft ISA 2006 permette di gestire la navigazione verso Internet utilizzando delle Policy. Le Policy possono permettere o negare la navigazione a seconda:

- Del Sito destinazione (es: voglio impedire la navigazione verso un sito di gioco online: www.poker.it)
- Dell'utente che ha effettuato la ricerca (voglio impedire agli utenti di scaricare contenuti, ma voglio permettere agli amministratori di scaricare driver o aggiornamenti)

- Dell'ora di connessione (Posso permettere la navigazione verso i siti dei quotidiani nazionali, ma solo durante la pausa pranzo)
- Della tipologia di contenuto richiesto (voglio impedire il download di certe tipologie di contenuti, es filmati, audio, ecc.)

E' possibile configurare una regola utilizzando tutti gli elementi citati sopra.

Per la funzione specifica di gestire la navigazione degli utenti tramite le blacklist è possibile usare due approcci:

Blocco della navigazione degli utenti salvo verso i siti esplicitamente permessi. Si crea una lista di siti permessi e gli utenti possono accedere solo a quei siti. Se un utente ha bisogno di accedere a un sito, per particolari esigenze lavorative, deve fare esplicita richiesta e la regola viene modificata. E' l'approccio più sicuro, è praticamente impossibile che gli utenti navighino verso siti non permessi, se gli utenti utilizzano Internet solo per specifici compiti e il numero di siti che devono usare è circoscritto è anche un approccio pratico e realizzabile facilmente. Da un altro punto di vista è un approccio poco flessibile se il numero di siti a cui gli utenti devono accedere varia spesso, e quindi in certe tipologie di aziende non è praticabile.

La navigazione è permessa, salvo i siti esplicitamente proibiti, contenuti in specifiche Blacklist. Le Blacklist possono essere create

manualmente, scaricate gratuitamente da specifici siti (molti utenti condividono le Blacklist che creano) oppure è possibile acquistare prodotti specifici che estendono le funzionalità di ISA e forniscono delle blacklist aggiornate automaticamente. Ovviamente i livelli di sicurezza e efficacia delle due tipologie sono diversi

Le Blacklist create manualmente o scaricate gratuitamente sono meno affidabili e sicure.

Queste blacklist sono generate da utenti che le mettono a disposizione sul Web quindi non c'è nessuna garanzia né della loro rispondenza al vero (magari identificano come sito porno un sito che non è porno o non individuano un sito di gioco on line) né della loro efficacia (non è detto che contengano tutti i siti porno possibili, per esempio). Le blacklilst vanno aggiornate manualmente, operazione onerosa e poco efficace: è praticamente impossibile tenerle aggiornate con tutti i siti contrari alle policy aziendali. Quindi utilizzando le Blacklist gratuite (o create manualmente dall'utente) non si riesce a impedire ma solo a limitare l'uso improprio.

Utilizzando dei prodotti specifici a pagamento (Websense, per esempio,ma ci sono parecchi partner che ne hanno a catalogo), si hanno maggiore garanzia di affidabilità e efficacia.

Questi prodotti hanno il vantaggio di fornire blacklist aggiornate che il prodotto utilizza per tenersi aggiornato (il concetto è analogo all'elenco delle tracce virali scaricate dagli antivirus)

Conservazione dei log di connessione e Individuazione procedure e soggetti preposti per verifica navigazione singola postazione: In Isa Server i log di connessione vengono conservati in un database (Microsoft SQLExpress o Microsoft SQL Server Standard). E' possibile rimuovere i log utilizzando degli script per ripulire il Database.Tramite i log di connessione e i Report di ISA è possibile individuare l'utente (lo Username con cui si autentica alla propria postazione o in rete) e la postazione da cui ha effettuato la navigazione. E' possibile configurare ISA in modo che solo i soggetti preposti al controllo possano accedere ai log di connessione ai Report.

Registrazione degli accessi degli amministratori

Le Norme

Devono essere adottati sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema. Le registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.

Le Soluzioni Tecnologiche

Nei sistemi operativi Microsoft, da windows NT in poi, è possibile registrare gli accessi al computer e agli oggetti (file, cartelle) nel computer. Per attivare la registrazione è necessario usare le Groupo Policy.

Se i computer fanno parte di un dominio, è possibile usare Group Policy a livello di dominio, valide per tutti i computer del dominio o della Organisational Unit.

Se i computer fanno parte di un Workgroup è possibile utilizzare le Group Policy locali. Bisogna configurare le Group Policy locali per ogni computer.

E’ possibile registrare varie operazioni, tra cui:

- Accesso al computer (evento di logon)
- Accesso agli oggetti
- E’ possibile registrare i tentativi di accesso che hanno avuto successo o quelle che sono state bloccate

ACS (Audit collection service) è il servizio di Operations Manager che permette di raccogliere i log di sicurezza in tempo reale dai vari serve e postazioni di lavoro distribuiti in azienda e collezionarli in un unico database (SQl Server) sul quale possono essere mantenuti e acceduti da persone identificate e diverse dagli amministratori dei sistemi.

Posta elettronica

Le Norme

Per contemperare le esigenze di accesso ai contenuti della posta elettronica aziendale da una parte, ed il diritto alla tutela della segretezza della posta, dall'altra, la policy interna potrà evidenziare l'obbligo di utilizzo della posta elettronica per esclusivi fini aziendali. La pratica quotidiana ci dimostra come siano spesso necessari accessi a e-mail o file allegati ad e-mail, in assenza del personale o per condivisione da parte di più aree della medesima azienda.

Sarà dunque opportuno che il datore di lavoro ponga a disposizione dei lavoratori:

- indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio: areacommerciale@azienda.it) con affiancamento – se operativamente necessario – ad indirizzi aziendali individuali (mario.rossi@azienda.it);

- messa a disposizione di funzionalità di sistema che in caso di assenza del lavoratore (ad esempio in caso di ferie) consentano l'invio automatico di messaggi di risposta contenenti i recapiti di posta elettronica o telefonici di altro contatto della struttura. È opportuno sottolineare che in casa di assenza di un lavoratore per malattia, qualora lo stesso non possa attivare il servizio da remoto, il datore di lavoro o chi preventivamente designato, potrà accedere alla casella di posta elettronica del lavoratore assente, per impostare la funzione sopra descritta;

- allocazione posta elettronica su apposito server: l'allocazione della posta elettronica su server è una scelta opportuna e coerente con l'obbligo normativo di effettuare copie di salvataggio dei dati con una specifica cadenza, consentendo un ripristino dei dati che non necessita di alcun accesso al pc in dotazione al lavoratore e che non sottopone lo stesso all'onere di backuppare in locale

Le Soluzioni Tecnologiche

Microsoft Exchange Server 2007 consente all'interno delle organizzazioni aziendali di supportare I requisiti di conformita' per i sistemi di messaggistica ed in particolare di e-mail. questi criteri di conformita' includono il data retention e la ricerca , il controllo dell'accesso ai dati e piu' in generale la possibilita' di creare regole e procedure di forzatura sull'utilizzo della mail. Sono sempre piu' importanti i criteri di sicurezza nello scambio delle informazioni che organizzazioni come quelle nell'ambito finanziario, farmaceutico ed altre, sono tenute ad implementare. Microsoft Exchange Server 2007 abilita nativamente questo tipo di scenari che supportano I requisiti richiesti.

In dettaglio i criteri di conformita' dei moderni sistemi di posta elettronica devono essere in grado di gestire l'uso improprio della e-mail aziendale diventata in certi casi documentazione paritetica ai documenti cartacei. La comunicazione aziendale quindi deve seguire le linee guida legislative, governative, legali, ma anche di attenzione nei riguardi delle proprietà intellettuali dei contenuti della posta elettronica (protezione del contenuto e non solo del contenitore) salvaguardando cosi' tutti gli aspetti legati ai vantaggi che una azienda puo' avere sul mercato. In questo modo e' possibile, mediante i sistemi di controllo di accesso alla posta, identificare e autorizzare gli utenti che accedono alle caselle, consentire a particolari gruppi di utenti di impersonificare ruoli aziendali oltre che essere a loro volta fruitori come Identita'

aziendali degli stessi servizi, garantendo cosi' la ricostruzione totale del percorso che ogni singola mail compie dalla sua creazione alla sua archiviazione nei sistemi di gestione a lungo termine dei documenti.

Microsoft Exchange Server 2007 gestisce regole di inoltro, controllo e journaling delle mail in modo nativo consentendo agli amministratori di effettuare questo tipo di configurazione mediante wizard centralizzati e a livello di organizzazione. Diventa quindi piu' semplice consentire il disegno di regole definite dagli uffici legali, di Human resources, delle divisioni vendite, delle divisioni acquisti di una azienda in modo da coprire i diversi livelli di attenzione richiesti a questo tipo di implementazione.

Individuazione requisiti minimi di complessità e criteri di conservazione per le password e gestione credenziali di autenticazione

Le Norme

Individuazione requisiti minimi di complessità per le password: secondo quanto previsto dalla vigente normativa privacy (vedasi il *Disciplinare tecnico in materia di misure di sicurezza, Allegato B al Decreto Legislativo n. 196/2003*), ciascuna password deve essere composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; la password non deve contenere riferimenti agevolmente riconducibili all'incaricato (pertanto non si devono utilizzare nome e cognome o date particolari) e deve essere modificata con cadenza almeno semestrale (a titolo meramente esemplificativo e non esaustivo: dati amministrazione, dati commerciali) o trimestrale (a titolo meramente esemplificativo e non esaustivo: dati del personale dipendente, dati di utenti strutture sanitarie).

Individuazione criteri di conservazione delle password: una volta individuata/e la/e password, la/e stessa/e dovrà/anno essere conservata/e al fine di:

- evitare accessi ai contenuti del pc da parte di lavoratori non autorizzati al trattamento di dati o informazioni di competenza del titolare della password;
- evitare accessi ai contenuti del pc da parte di soggetti terzi estranei alla struttura.

L'azienda potrà individuare dei criteri di conservazione direttamente nella policy interna, specificando le modalità mediante le quali potranno essere ridotti i rischi di conoscibilità delle password (a titolo meramente esemplificativo e non esaustivo: non scrivere le password su post-it affissi al pc, non comunicare la password via telefono o via mail in caso di mancanza di assoluta certezza circa l'identità della controparte).

Disattivazione credenziali di autenticazione non utilizzate: come per il precedente punto, tale operazione è obbligatoria ai sensi di legge.

Difatti, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica, le credenziali di autenticazione non utilizzate da almeno sei mesi devono essere disattivate.

***Individuazione procedure di disattivazione*:** il datore di lavoro dovrà preventivamente individuare delle procedure di disattivazione delle credenziali di autenticazione, qualora un lavoratore venga allocato in altra area o concluda il rapporto lavorativo.

Difatti, oltre ad essere obbligatorio per legge, appare un importante misura di salvaguardia delle informazioni aziendali, avere una procedura di disattivazione che consenta pressoché nell'immediatezza dell'evento, di negare l'accesso dell'ex lavoratore ai dati ed alle informazioni disponibili sino a quel momento per lo svolgimento delle attività.

***Istruzioni in ipotesi di assenza temporanea o permanente del lavoratore dal pc*:** la policy aziendale dovrà prevedere espressamente le istruzioni affinché non sia lasciato incustodito o accessibile il contenuto del pc su cui il lavoratore opera; a tal fine le politiche relative alla gestione dello screen server,consentiranno di evitare rischi di accessi da parte di personale interno non autorizzato, o soggetti esterni, ai dati ed alle informazioni gestite.

Esiste uno specifico attributo dell'utente nel dominio (Active Directory) in cui è salvata la data dell'ultimo accesso. E possibile utilizzare degli script, schedulandoli con una frequenza predefinita, per analizzare tutti gli utenti che non hanno fatto accesso da più di 6 mesi e spostarli in un repository appositi e/o disabilitarli

Le Soluzioni Tecnologiche

Individuazione requisiti minimi di complessità per le password: Se la rete aziendale è basata su un dominio, è possibile utilizzare le Group Policy di dominio, presenti da Windows 2000 Server in poi. Le Group Policy sono applicate a tutti gli utenti e i computer che fanno parte del dominio e permettono di definire:
Criteri per le password utente

- Lunghezza minima della password
- Scadenza della password
- Tempo minimo prima di poter cambiare la password
- Numero di password che vengono registrate (e che non è possibile utilizzare quando si cambia la password)
- Criteri di alta complessità (lettere-numero, maiuscole, caratteri non alfanumerici)

Individuazione criteri di conservazione delle password* e *Disattivazione credenziali di autenticazione non utilizzate:
Policy di blocco delle password in caso di tentativo di accesso falliti

- Numero di tentativi sbagliati dopo il quale l'utente viene bloccato
- Intervallo di tempo dopo il quale viene azzerato il contatore degli errori di inserimento della password
- Tempo di blocco dell'utente (è possibile bloccare l'utente per un intervallo di tempo, oppure bloccarlo indefinitamente fino all'intervento dell'amministratore

Se la rete aziendale non è basata su un dominio ma è un semplice workgroup è possibile definire le stesse Policy, solo che vanno configurate manualmente su ogni computer
Se i computer fanno parte di un dominio è possibile:

- impedire l'accesso ai computer della rete se non a utenti autorizzati tramite credenziali di accesso (username/password)
- Gestire l'autorizzazione alle risorse (File, Cartelle, Stampanti, Cartelle condivise) usando le credenziali di accesso

***Istruzioni in ipotesi di assenza temporanea o permanente del lavoratore dal pc*:**

Se la rete aziendale è basata su un dominio, è possibile utilizzare le Group Policy di dominio, presenti da Windows 2000 Server in poi. Le Group Policy sono applicate a tutti gli utenti e i computer che fanno parte del dominio e permettono di definire:

- L'utilizzo di Screen Saver protetto da Password
- Il tempo attivazione dello Screen Saver (dopo un certo numero di minuti di inutilizzo del computer)

Se la rete aziendale non è basata su un dominio ma è un semplice workgroup è possibile definire le stesse Policy, solo che vanno configurate manualmente su ogni computer. Se i computer fanno parte di un dominio è possibile configurare ogni utente perché salvi il profilo di accesso (contiene tutte le configurazioni usate durante l'accesso utente, dai preferiti di Internet, alla cartella My Documents, a quello che è salvato sul Desktop) su un server centrale. E' anche possibile definire delle HomeDirectory per gli utenti, sono delle cartelle condivise su un server centrale, gli utenti le vedono come un disco mappato e possono salvare dati o documenti. Sia ai profili che alle home directory possono accedere solo i proprietari.

Segmentazione della rete

Le Norme

Nel rispetto delle previsioni di cui al Decreto Legislativo n. 196/2003, occorre che ciascun lavoratore tratti (e quindi acceda) dati accedendo esclusivamente all'ambito del trattamento consentito (art. 30, II comma Decreto Legislativo n. 196/2003). La segmentazione della rete consentirebbe evidentemente di razionalizzare l'accesso per aree e gruppi di lavoro, consentendo di adempiere al dettato normativo con il minimo impatto organizzativo.

Le Soluzioni Tecnologiche

Sia per i domini di grandi dimensioni che per i piccoli gruppi di lavoro, implementare IPSec significa trovare un equilibrio tra la disponibilità delle informazioni al maggior numero di utenti possibile e la protezione delle informazioni riservate dall'accesso non autorizzato. In sostanza, l'isolamento di server e domini consente agli amministratori IT di limitare le comunicazioni TCP/IP dei membri di dominio che sono computer attendibili. È infatti possibile configurare tali computer in modo da consentire solo le connessioni in ingresso provenienti da altri computer attendibili o da un determinato gruppo di computer considerati attendibili. Il controllo degli accessi viene gestito centralmente tramite Criteri di gruppo per Microsoft® Active Directory®, che controlla i diritti di accesso alla rete. È possibile garantire la protezione di gran parte delle connessioni alla rete TCP/IP senza apportare modifiche all'applicazione, in quanto IPsec interviene a livello di rete, inferiore al livello applicazione, fornendo protezione end-to-end tra computer per l'autenticazione e a livello di pacchetto. Il traffico di rete può essere autenticato, o autenticato e crittografato, in diversi scenari personalizzabili.

Adozione procedure di back-up centralizzato

Le Norme

Tale aspetto è di particolare rilievo su più fronti: dal punto di vista del lavoratore, per consentirgli di avere consapevolezza circa la sussistenza delle risorse che eviteranno la perdita di dati, informazioni e quindi lavoro; dal punto di vista del datore di lavoro, per evitare inutili perdite e per adeguarsi all'obbligo normativo che in particolare sul fronte dei dati, dispone un obbligo di ripristino di alcune tipologie di dati, con tempi molto ridotti.

Le Soluzioni Tecnologiche

Usando le funzionalità di NTBackup (strumento presente in tutti i sistemi operativi da Windows 2000 in su) è possibile eseguire un backup centralizzato dei dati utente presenti nel profilo centralizzato e nelle home directory. Ovviamente i dati salvati localmente sul computer dell'utente non vengono salvati.

Protezione da rischi di intrusioni esterne e da rischi di danneggiamento dell'integrità delle risorse e dei loro contenuti

Le Norme

Questo aspetto combina un obbligo normativo con un interesse aziendale, ovvero quello di ridurre le vulnerabilità della rete aziendale rispetto agli accessi dall'esterno. Gli strumenti elettronici acquisiti devo essere aggiornati con cadenza semestrale; la policy interna avrà l'obiettivo di istruire i lavoratori su come operare evitando di alterare tali protezioni e provvedendo ad incrementarle laddove opportuno. Nell'ottica del legislatore che nel citato Allegato B ha inserito questo obbligo normativo, le intrusioni esterne sono atte a compromettere integrità e riservatezza di dati ed informazioni, ecco la ratio dalla quale nasce l'obbligo di adozione degli strumenti elettronici idonei a ridurre i rischi.

L'adozione di antivirus – centralizzati o meno – consente di ridurre i rischi di danneggiamento parziale o totale, dell'integrità di dati/informazioni/risorse informatiche.

Le Soluzioni Tecnologiche

E' possibile utilizzare le funzionalità di Firewall di ISA server. Per proteggere dai virus i server e i client è possibile utilizzare Forefront client security. Microsoft® Forefront™ Client Security è uno strumento unificato di facile gestione per la protezione dal malware dei sistemi operativi di computer desktop, portatili e server aziendali.

Protezione da rischi di salvataggio interno non autorizzato

Le Norme

Partendo dal presupposto che sulla base della normativa privacy, è onere del datore di lavoro organizzare la gestione dei dati e delle informazioni al fine di consentirne l'accesso ed il trattamento esclusivamente ai lavoratori designati, adottare dei sistemi di monitoraggio dei salvataggi delle informazioni, consente di scongiurare errori in buona fede da parte dei lavoratori, o condotte volontarie volte a carpire dati o informazioni.

Le Soluzioni Tecnologiche

Gli utenti possono salvare i file aziendali su supporti rimovibili (salvarli su Chiavi USB, dischi esterni USB, masterizzarli su un CD/DVD).

Per evitare questi comportamenti è possibile, solo per client Windows Vista, inibire l'uso di periferiche USB (dischi, Chiavi) o inibire l'uso di masterizzatori CD/DVD. Per inibire l'uso di queste periferiche si utilizzano le Group Policy (valide solo per Windows Vista) di dominio. Se i client Vista fanno parte di un workgroup è possibile definire le stesse Policy, solo che vanno configurate manualmente su ogni computer

Se i client sono Windows XP non è possibile inibire l'uso di periferiche USB o masterizzatori solo utilizzando le Group Policy, ma bisogna utilizzare degli specifici Software di terze parti a pagamento.

Protezione documenti o mail in fase di creazione

Le Norme

La protezione dati ed informazioni sancita dal legislatore può avere origine sin dalla creazione del dato o dell'informazione, eliminando alla base i rischi che potrebbero sorgere durante questa fase. Limitare pertanto la gestione del documento rispetto ad eventi esterni, consente di minimizzare il rischio di accesso o conoscibilità del dato o dell'informazione.

Le Soluzioni Tecnologiche

RMS è una tecnologia server per Windows Server 2003 che certifica le entità trusted, concede in licenza le informazioni protette con RMS, registra server e utenti e amministra le funzioni di gestione dei diritti. La tecnologia RMS agevola le fasi di installazione che permettono alle entità trusted di utilizzare le informazioni protette con RMS. È possibile ampliare RMS per supportare caratteristiche aggiuntive utilizzando il Software Development Kit (SDK) di Servizi Microsoft Windows Rights Management.

Cifratura di particolari dati o informazioni

Le Norme

La cifratura rappresenta una delle misure minime di sicurezza che il legislatore prevede in caso di trattamento dati sensibili e/o giudiziari; in realtà questa misura consente una protezione delle informazioni

aziendali che va oltre l'obbligo giuridico, consentendo di evitare rischi connessi a condotte di violazione del segreto aziendale.

Le Soluzioni Tecnologiche

Se un utente non autorizzato ma accede fisicamente a un computer (perché è incustodito o perché lo ruba o ruba l'hard disk), anche se non conosce le credenziali di accesso (username/password), può accedere al computer e ai suoi dati semplicemente installando un altro sistema operativo (ovviamente senza modificare la partizione dati e/o il disco) oppure rubando l'hard disk e connettendolo a un computer con un altro sistema operativo installato.

Per proteggersi da questa eventualità è possibile cifrare le cartelle che contengano dati particolarmente sensibili. I dati contenuti nella cartella vengono cifrati utilizzando una chiave di cifratura che viene salvata in modo sicuro nel profilo utente, anche se qualcuno ruba l'hard disk o riinstalla il sistema operativo, non ha accesso al vecchio profilo e quindi non ha la chiave per decifrare e non può accedere ai dati.

Le funzionalità differiscono a seconda dei sistemi operativi utilizzati:

Con client Windows XP è possibile cifrare i dati contenuti in una cartella, ma non tutto il disco del sistema operativo. La chiave di cifratura viene salvata nel profilo utente.

Con Windows Vista è possibile cifrare i dati contenuti in una cartella ma è anche possibile cifrare tutto il disco del computer. La chiave di cifratura può essere salvata, oltre che su disco, anche in uno specifico modulo Hardware (il modulo TPM, ormai molti laptop ne sono provvisti). Windows Vista fornisce quindi una soluzione più sicura e flessibile.