

La Sicurezza dei Dati in Azienda è nella loro Storia



La Sicurezza in Azienda

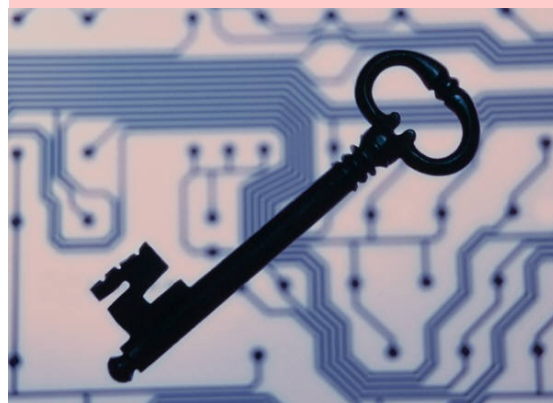
Il fluido vitale in un'Azienda sono i dati e le informazioni oggi sono sempre gestite con apparecchiature informatiche. La sottrazione o la cancellazione di un dato può costituire il fallimento di un progetto e mettere a repentaglio la sopravvivenza stessa di un'Impresa esattamente come se si verificasse un'emorragia. Potere supervisionare tutte le attività svolte su un file o su una cartella e potere stabilire chi e quando vi ha avuto accesso può essere vitale e attrezzarsi con un efficace protocollo di criptazione, irrinunciabile.

Gli Obblighi di Legge

Il 15 Dicembre 2009 è entrata in vigore una Legge che impone alle Aziende interessate di raccogliere traccia di tutti gli accessi svolti dagli Amministratori di Sistema sulle apparecchiature che possano essere interessate alla custodia di dati Sensibili. E' un obbligo di legge e le sanzioni per chi si dovesse far trovare inadempiente sono molto elevate.

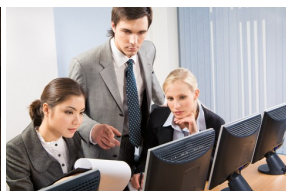
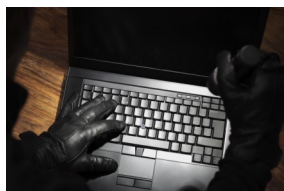
La soluzione indispensabile per riuscire a ricostruire la vita di un file, capire dove sia stato spostato e chi siano gli artefici di tutte le operazioni svolte sulla rete.

- Protegge l'Azienda da operazioni svolte sui file e sulle cartelle es. spostamenti
- Tutela il Lavoratore da accuse infondate di manomissioni o copie abusive di file
- Migliora produttività e organizzazione
- Migliora lo sfruttamento delle risorse aziendali
- Mette in regola con la Legge 196/03 sulla raccolta dei file di Log degli AdS

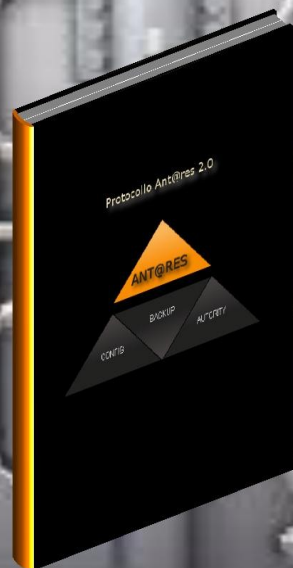


PROTEGGIAMO

**i
NOSTRI DATI**



La Storia dei Dati di un'Azienda Deve essere Protetta



PROTEGGERE LA PROPRIA AZIENDA RISPETTANDO LA LEGGE

LA LEGGE : Provvedimento del Garante (estratto)

Devono essere adottati sistemi idonei alla registrazione degli accessi logici ai sistemi ed agli archivi elettronici da parte degli Amministratori di sistema. I log derivanti devono rispondere alle caratteristiche quali completezza, invariabilità e possibilità di verifica dell'integrità. Le registrazioni devono comprendere i riferimenti temporali e descrizione dell'evento e conservate per un periodo non inferiore ai sei mesi. Adottando il Protocollo Ant@res si raggiunge la certezza assoluta che in qualsiasi momento si potranno dimostrare le effettive attività degli AdS ben oltre rispetto a quanto offerto da firma digitale.

IL RAGIONAMENTO : La tutela del proprio Know-How

Dove la Legge non impone, come es. nel caso delle Banche, deve essere la tutela del proprio bene a consigliare la migliore strategia da attuare per difendersi da fughe o smarrimenti di informazioni vitali. Tracciare le attività svolte sulla propria rete dai propri collaboratori non solo non è vietato, ma è auspicato. Condizione indispensabile è il potere utilizzare le informazioni raccolte quali probatorie nel corso di un eventuale Giudizio. Il Protocollo Ant@res rende questo possibile, i Log comprovanti tutte le attività sono conservati in un formato inattaccabile da chiunque, quindi spendibile per comprovare un illecito.

Il Protocollo Ant@res 2.0

Con il deposito di questo Brevetto Europeo Antares srl ha dato soluzione al problema di potere dimostrare che l'autore di un eventuale illecito nell'utilizzo delle apparecchiature aziendali è inconfutabilmente uno tra coloro che a determinati dati può avere accesso.

Oggi i Log file comprovanti gli accessi impropri a determinati file o cartelle da parte di un Utente non autorizzato spesso non erano sino ad oggi spendibili davanti ad un Giudice in quanto troppo facilmente modificabili con la conseguente possibilità che fossero stati trattati ad arte per costruire un castello accusatorio volto a perseguire un dipendente indesiderato.

Con l'applicazione del Protocollo Ant@res le informazioni raccolte non potranno essere manipolate da alcuno e giungeranno inalterate agli organi giudicanti.

L'effetto di questa soluzione è anche quello di rendere i Log file raccolti per ottemperare alla D.Lgs.196/03 effettivamente immutabili così come chiaramente chiede il Garante non limitandosi ad apporre una semplice firma digitale come fa la stragrande maggioranza delle soluzioni ma offrendo alle Autorità Investigative l'esatto tracciato delle attività effettivamente svolte sulla rete aziendale da parte degli Amministratori di Sistema.