



MASSIMO BECCHERLE
Direzione
Commerciale

LA PROTEZIONE DEL KNOW-HOW AZIENDALE

Secondo voi, nel mercato odierno, basato su concorrenza, globalizzazione e conoscenza, cos'è che rende un'Azienda sufficientemente sicura? Partendo dal presupposto che la domanda è legittimamente discutibile visto che ognuno di noi ha una propria considerazione ed attribuisce uno specifico valore al concetto di Sicurezza, possiamo tuttavia affermare, generalizzando, che esso riguarda persone, ambienti, strutture o informazioni, in modo indistinto. Nonostante ciò, sarebbe ipocrita non riconoscere che fino a questo momento l'impiego di misure di sicurezza aziendale si sia concentrato maggiormente sulla security fisica, intesa proprio come accesso ad un building, vigilanza contro intrusioni, ingressi non autorizzati o furti.

E' noto infatti che ogni attività aziendale, è caratterizzata anche da uno specifico patrimonio informativo, conosciuto come know how, che rappresentando l'asset attraverso il quale le Aziende e le organizzazioni perseguono i propri obiettivi e producono valore, diventa quindi bene da sottoporre a tutela.

La segretezza di un'informazione prevede un enorme vantaggio soprattutto per chi la possiede: eleva il detentore infatti in una posizione privilegiata rispetto ai concorrenti. Ed ecco perché il know how per essere proteggibile non deve essere accessibile

a tutti: se si diffonde si "volgarizza" e perde di conseguenza il proprio valore. Eccoci arrivati quindi al nocciolo della questione, che come un dubbio amletico pone le aziende moderne a riflettere e ponderare sulla questione: "tutelare o non tutelare, questo è il problema". Il passo più difficile, che precede il vero e proprio impiego di strumenti atti a difendere il patrimonio informativo aziendale, è riuscire a valutare secondo quale entità e livello di importanza tali informazioni siano suscettibili di tutela. Il problema è che spesso non ci si rende conto che le misure di sicurezza a protezione del proprio know how richiedono altrettante policies che coinvolgano anche il fattore umano, imponendo comportamenti corretti e leali da parte dei dipendenti, dei collaboratori o dei vari consulenti. Un atto di concorrenza sleale da parte di un ex dipendente si potrebbe manifestare per esempio, molto semplicemente, nella sottrazione di segreti aziendali o acquisizione di dati relativi a prove, studi o analisi – come un elenco di clienti o un procedimento di produzione – valendosi direttamente o indirettamente di ogni altro mezzo non conforme ai principi della correttezza professionale, con l'obiettivo di danneggiare l'altrui azienda. Oggi, a causa del difficile clima in cui si ritrova ad annaspere l'intero mercato italiano, episodi di questo tipo non sono così impensabili anzi: si verificano più spesso

e con un grado di problematicità sempre maggiore.

Trattandosi quindi di comportamenti molto pericolosi, in quanto i dati in questione rappresentano, per chi li detiene, un'importante risorsa anche di valore economico, le alternative di tutela per un titolare aziendale sono sostanzialmente due: prevenire i danni tramite patti di riservatezza per via contrattuale, il cui limite sta però nella validità temporale del suddetto atto; od anticipare una qualsiasi forma di rischio attraverso una soluzione IT. Attualmente esiste infatti sul mercato una soluzione disponibile in

sua funzione di repository aziendale, SCS procede in modo automatico e diretto a soddisfare questa esigenza, attraverso un flusso automatico delle informazioni. Ciò significa che una volta stabilita la disattivazione o sospensione di un soggetto, tale informazione giunge a conoscenza di tutti i dipartimenti aziendali, automaticamente e senza nessun intervento manuale. In questo modo è chiaro che le informazioni personali del soggetto rimarranno comunque presenti nella memoria del software, anche se per l'Azienda non risulteranno più attive. Il concetto di base

Il Sig. Rossi per esempio, una volta concluso il proprio rapporto di lavoro con l'Azienda, non solo necessiterà di uno specifico pass per entrare nuovamente in essa, ma qualora desiderasse accedervi tramite web utilizzando la propria password aziendale, ne sarà assolutamente impossibilitato. Lo stesso concetto può essere benissimo applicabile anche a figure esterne all'Azienda, come interinali, consulenti o fornitori che intrattengono con la stessa rapporti di collaborazione brevi o comunque non duraturi.

Riassumendo, questa applicazione dà la straordinaria possibilità ad un'impresa di definire chi, come, quando e per quanto tempo è abilitato all'accesso ad una determinata struttura. Automaticamente, al termine della scadenza predefinita, sarà lo stesso software a procedere alla disattivazione delle credenziali del soggetto senza nessun altro tipo di intervento. Concludendo, sulla base delle informazioni elaborate, possiamo ora rispondere con più chiarezza alla domanda che ci eravamo posti inizialmente, e cioè quali sono gli elementi che concorrono a rendere un'azienda sicura al giorno d'oggi. Senza alcun dubbio essi si manifestano in un connubio ed una giusta integrazione tra la Sicurezza Fisica e quella Logica (espressa in questo caso nella gestione del know how aziendale); ma Sicurezza significa anche riuscire a valutare e scegliere la strada più efficace e meno impervia per il raggiungimento dei propri obiettivi. Se poi, come in questo caso, il fine è la disabilitazione delle credenziali di un nominativo, fino ad ora utente attivo per l'Azienda, la soluzione ci viene posta su un piatto d'argento: appare chiaro a tutti infatti, come sia più problematico, incerto e dispendioso provvedere a tali procedimenti per via manuale, rischiando banali errori, probabili ritardi o dimenticanze (questo anche a causa dei gravi problemi di asincronismo tutt'ora presenti fra i vari Dipartimenti di un'Azienda). Se assieme alla tecnologia poi, si sono evoluti anche i rischi connessi alla tutela del patrimonio informativo aziendale, la risposta software è quella che offre i maggiori vantaggi e minor rischi, perché si avvale di una piattaforma web che opera in modo automatico e diretto, senza intoppi e in piena sicurezza. ■

Quando Sicurezza significa disabilitare l'accesso fisico e logico ad un utente in modo veloce, certo ed automatico.

piattaforma web, che punta ad ottimizzare le risorse aziendali provvedendo indirettamente anche alla protezione del patrimonio informativo. Si tratta di un software presente nella suite di prodotti di Digitrónica.IT. La piattaforma web è denominata Security Core System, (SCS) e nasce formalmente come strumento di gestione centralizzata del controllo degli accessi a garanzia di maggiore sicurezza per le aziende italiane, grazie alla gestione di tutti i più importanti processi autorizzativi interni ed esterni al building. In riferimento al problema specifico posto in questa sede, SCS viene pensato come la soluzione ideale per garantire un maggior e continuo allineamento delle informazioni relative alla relazione Azienda-Dipendente (o ex Dipendente), soprattutto nella delicata fase di fine rapporto lavorativo.

L'obiettivo è infatti quello di tutelare l'impresa e il suo patrimonio informativo procedendo alla sospensione momentanea (o disattivazione definitiva) delle diverse autorizzazioni in possesso ad uno specifico nominativo. Grazie alla

è molto semplice e non serve pensare ad episodi straordinari per avere un'idea delle potenzialità di tale prodotto. Si pensi molto semplicemente a quando avviene un cambio di ruoli all'interno di una struttura aziendale. Equilibri, autorizzazioni, licenze o permessi subiscono inevitabilmente delle modifiche. SCS risolve il gravoso lavoro di provvedere a nuove registrazioni o aggiornamenti dei dati sensibili dei soggetti interessati, modificando in modo autonomo ed indipendente le informazioni e ripristinando automaticamente congruenza e stabilità nell'attività aziendale. Ciò significa che verranno subito rilasciate le nuove autorizzazioni per l'accesso ai dati o alle risorse fisiche, secondo quanto stabilito dalle relative policies.

Questo può perciò dirsi al momento uno dei modi più professionali, sicuri e veloci di provvedere al controllo del proprio building, non solo per quanto riguarda l'accesso fisico di soggetti alla struttura, ma anche il loro contatto con l'azienda sotto qualsiasi altro punto di vista, anche tecnologico se vogliamo.