

Telindus: la Difesa dei Dati come chiave della sicurezza. Meglio soluzioni esterne che una struttura interna

*Le applicazioni su Internet e il mercato globale consentono più informazioni, ma anche tanti pericoli in più. Telindus, società quotata sul mercato Euronext Bruxelles è oggi uno dei maggiori partner per la fornitura di servizi e soluzioni per l'Information and Communication Technology (ICT). Ci guida alla scoperta di questa realtà il suo Amministratore Delegato Mauro Cipollini.*

*Una rete di ICT nell'attuale realtà finanziaria può essere considerata un elemento da controllare per realizzare gli obiettivi aziendali?*

L'infrastruttura ICT è sempre stata un elemento critico per il raggiungimento del successo aziendale. Le società più lungimiranti da tempo hanno integrato i processi organizzativi aziendali all'evoluzione delle soluzioni It.

*Questo come è avvenuto?*

Basta considerare la rivoluzione che c'è stata nel modo di gestire la relazione con i propri clienti. L'innovazione It e Internet offrono all'azienda nuovi canali e nuovi strumenti di business. Soprattutto nel settore finanziario, l'informazione deve essere immediatamente e direttamente accessibile ai clienti. Per garantire l'esattezza e la pronta disponibilità dei dati, i sistemi e le soluzioni It non possono che complementare l'attività dei dipendenti.

*Cosa sta condizionando il mercato della sicurezza in Italia?*

Nel nostro Paese c'è un grande interesse sul tema della sicurezza accresciuto da una sempre maggiore consapevolezza di tutti gli *stakeholder* aziendali, non ultimi i clienti. Purtroppo l'adozione delle opportune misure e soluzioni di sicurezza non è sempre così immediata. Ciò anche a causa della pervasività dei sistemi e delle soluzioni, sia sulle infrastrutture ICT esistenti sia, soprattutto, sui processi di business.

*È aumentato l'interesse delle aziende verso il tema della sicurezza informatica?*

Certamente, anche perché i media si stanno occupando di questo argomento. Il Governo italiano sta definendo con maggiore attenzione gli aspetti relativi alla sicurezza informatica. Anche i convegni che vengono organizzati nel nostro Paese sull'argomento sono numerosi e con un buon livello di informazione.

*È importante per un'azienda capire a quali rischi si è esposti?*

Solo attraverso un'attenta analisi si riescono a mettere in campo progetti e azioni commisurati. Troppo spesso si parte da un approccio di tipo implementativo, senza dare la dovuta attenzione agli aspetti di valutazione del rapporto costi/benefici nell'adozione della soluzione. Occorre un'analisi a 360° che permetta di dimensionare l'investimento in sicurezza alla tipologia e alla dimensione del business e soprattutto al livello di rischio sostenibile.

*Quali possono essere le soluzioni per difendersi dagli attacchi che minacciano la propria azienda?*

Come ho anticipato è importante dimensionare gli interventi di sicurezza alla propria tipologia e ai propri processi di business. L'adozione di soluzioni di sicurezza è un processo

continuo che ruota attorno a tre attività fondamentali: *prevenzione, scoperta e reazione*. Occorre capire quale possa essere il livello di rischio accettabile per la tipologia di business e adottare le misure e le soluzioni opportune. Ma ciò non basta, il sistema va monitorato e gestito nel suo divenire.

*Altri interventi da adottare?*

Sicuramente non è irrilevante fare leva sulle esigenze normative (Basilea 2, DPS, ecc.) per far crescere continuamente il livello di sicurezza dell'infrastruttura. Sempre più le aziende saranno anche oggetto di audit e valutazioni mirate a verificare il livello di sicurezza adottato e garantito. Perché non appoggiarsi alle disposizioni normative per creare un circolo virtuoso di miglioramento della qualità dell'infrastruttura, operando non solo sulle tecnologie, ma anche su processi e risorse?

*Come agiscono solitamente gli "hacker"?*

È difficile poter delineare una unica linea di condotta anche perché la stessa può avere diverse motivazioni. Mi sembra importante sottolineare che la figura dell'*hacker* non rappresenta l'unico pericolo per l'organizzazione aziendale. Molti "danni" vengono causati dall'intrinseca debolezza degli strumenti informatici. Lo stesso dipendente può essere veicolo inconsapevole di un attacco.

*Qual è il modo migliore per affrontare il problema della sicurezza?*

È un tema complesso per l'imprenditore e di difficile soluzione. Il modo migliore è quello di affidarsi a esperti di sicurezza dei sistemi informatici. Con l'evoluzione delle tecnologie, con le competenze che il personale interno dovrebbe avere e mantenere aggiornate nel tempo, potrebbe essere difficile, oltre che poco conveniente dal punto di vista economico, dotarsi unicamente di una struttura di sicurezza interna con elevati standard.

*Si potrebbe ovviare scegliendo soluzioni integrate?*

Può essere una chiave di lettura. Secondo noi il problema della sicurezza deve essere affrontato non solo dotandosi di buone infrastrutture tecnologiche ma ricorrendo a soluzioni integrate di sicurezza e per soluzioni integrate intendiamo l'opportuna combinazione di processi, tecnologia e persone. Una soluzione potrebbe essere rappresentata anche dall'integrazione di una struttura interna con l'opportuno intervento di un *outsourcer* specializzato.

*Cosa offre Telindus ai propri clienti?*

Noi siamo un'azienda storica presente sul mercato da oltre trent'anni. Abbiamo vissuto l'evoluzione di sistemi e soluzioni di networking e sicurezza fin dai primi anni, accumulando un ricco bagaglio di esperienze, anche a livello internazionale. Per missione aziendale da sempre siamo attenti alle evoluzioni tecnologiche e a tutto quello che di nuovo c'è sul mercato.

*Ma siete anche un riconosciuto "system integrator"?*

Abbiamo sicuramente le capacità implementative adeguate, ma siamo in grado di coprire tutte le fasi fondamentali per l'adozione delle opportune soluzioni di sicurezza. Dall'analisi, allo studio di fattibilità, all'implementazione, a tutte le fasi di "follow-up" e monitoraggio del progetto e dei processi.

*Intervista a cura di Titti Acone*