

## BLUE EAGLE

# Sempre connessi: ma occorre puntare su piattaforme sicure

■ Se nel XIX secolo gli uffici sembravano fabbriche, a partire dal 1960 si è prediletto un layout più aperto. È con l'inizio del XXI secolo che il design ha ancora un nuovo intento: ispirare la creatività.

Oggi, affrontiamo un terzo e più grande cambiamento che è il lavoro definito «decentralizzato».

La tendenza verso il lavoro virtuale è in forte crescita per due fattori chiave: da una parte, i rapidi progressi nelle tecnologie dell'informazione e della comunicazione e dall'altra la crescita dei paesi di recente industrializzazione.

La globalizzazione poi ha portato rapidamente all'unificazione dell'intero pianeta: oggi con un click inviamo documenti, messaggi e «videochiamiamo» o instauriamo conference calls.

Utilizziamo quindi strumenti che sono di uso comune in tutte le aziende e proprio questo lavoro da dispositivi mobili è ormai irrinunciabile; siamo sempre connessi. Due sono gli ambiti principali della virtualizzazione: la forza lavoro ed il posto di lavoro. Le persone si connettono come vogliono, quando vogliono e dove vogliono.

Le politiche aziendali volte a proteggere i dati, che tendono a reprimere l'utilizzo di piattaforme di collaborazione, spingono gli utenti ad utilizzare tecnologie di livello «consumer» e gratuite.

Il grande rischio per l'azienda si riflette sul responsabile della sicurezza informatica che perde totalmente il controllo. Dobbiamo quindi chiederci i motivi della gratuità del servizio offerto o quali sono i «guadagni» di chi ci regala il servizio.

La soluzione migliore invece è quella di fornire una piattaforma sicura per la collaborazione e la condivisione, il «sync» sicuro dei



La sicurezza informatica è sempre più importante

dispositivi, l'invio di mail protette o meglio cifrate, la rimozione dei dati nascosti nei file di office o pdf.

Una piattaforma che unisca da un lato la semplicità d'uso per l'utente e che dall'altro consenta al responsabile sicurezza di definire le policies per la protezione dei dati. Fino al decennio scorso tali soluzioni erano riservate esclusivamente a grandi realtà economiche, oggi invece sono alla portata di tutti: dal singolo professionista alla grande azienda, passando per lo studio legale e tributario associato o una piccola e media impresa.

Proteggere i propri dati e le proprie informazioni è possibile. Blue Eagle Technology, Key Partner Workshare offre la possibilità di conoscere tutti i rischi e le soluzioni disponibili sul mercato per ridurli al minimo, attraverso incontri formativi dedicati a giornalisti, professionisti, legali, aziende: [www.blueeagle.events](http://www.blueeagle.events). Informazioni sulle soluzioni offerte su [www.eaglenetworks.it](http://www.eaglenetworks.it) - [www.eaglesafe.it](http://www.eaglesafe.it)



Essere sempre connessi è un fattore positivo per un'azienda ma può anche risultare un rischio

## INFORMATICA

## Sicurezza al centro anche per i Pc

■ Il tema della sicurezza è sempre attuale anche nel mondo informatico. Infatti, è sempre più importante l'analisi delle minacce e del rischio di attacchi all'integrità di un sistema informatico e dei dati in esso contenuti o scambiati in una comunicazione con un altro utente. La sicurezza informatica comprende quindi sia la cifratura (la confidenzialità dei dati), sia l'autenticazione, ossia l'accesso fisico e logico solo ad utenti autorizzati. Non è semplice individuare quel complesso di misure preventive per annullare potenzialmente i problemi che affliggono spesso un sistema informatico.

Adottando però semplici misure preventive è possibile evitare i più frequenti problemi che attaccano i personal computer. L'utilizzo di un buon antivirus è un passo obbligatorio per qualunque pc che si connette alla rete Internet, ma ciò non basta: è importantissimo provvedere con regolarità all'aggiornamento del file delle firme. Usare poi un firewall può sembrare eccessivo, ma l'uso di dispositivi di filtraggio (come appunto i firewall), purché opportunamente configurati, è in grado di offrire un discreto grado di protezione contro attività preparatorie che un aggressore in genere compie prima di tentare un accesso non autorizzato.

Anche se può risultare scontato, è comunque importante ricordare di non aprire ingenuamente allegati di posta elettronica.