

L'azienda rischia con un lavoratore in remoto

a cura di Marianna Di Iorio

Come dimostra un recente studio pubblicato da Vanson Bourne, molti manager IT hanno paura che i dipendenti in remoto possano compromettere la sicurezza aziendale

Nove manager IT su dieci hanno paura dei rischi alla sicurezza causati dalle azioni dei **lavoratori in remoto**.

La preoccupazione più forte è che gli hacker possano utilizzare le connessioni in remoto come una porta d'ingresso alla Rete aziendale.

Lo rivela l'ultimo studio condotto da **Vanson Bourne**, specializzata in ricerche di mercato nel mondo della tecnologia.

In particolare, l'indagine, condotta su un campione di 200 imprese del Regno Unito con un numero massimo di dipendenti pari a 250, ha mostrato che l'87% dei lavoratori in remoto usano i loro PC personali per accedere ai dati della propria azienda.

Questa azione pone in serio **rischio l'organizzazione**, in quanto l'azienda stessa non è in grado di gestire i PC dei lavoratori in remoto e quindi non può installare adeguati sistemi antivirus.

Come dimostra lo studio, si tratta di un problema molto sentito perchè è in continuo aumento il numero di dipendenti che richiede al proprio datore di lavoro di poter lavorare da casa.

Alla base di questa richiesta, come dichiara il 59% del campione intervistato, ci sarebbe la possibilità simultanea di incrementare la produttività aziendale e trovare un giusto equilibrio tra la sfera lavorativa e quella privata.

Ad ogni modo, ci sono anche aziende che non concedono questa possibilità ai loro impiegati.

Come nel caso di quasi la metà degli intervistati (46%) che ha dichiarato di non aver ottenuto il permesso di lavorare da casa.

Versione originale: <http://www.pmi.it/sicurezza/news/1490/lazienda-rischia-con-un-lavoratore-in-remoto.html>