



di VALERIO ROSANO

**T**utti parlano di “BYOD” (Bring Your Own Device), ovvero la tendenza a lasciare che i dipendenti di un’azienda utilizzino i propri dispositivi tecnologici anche per scopi professionali e per il raggiungimento degli obiettivi aziendali. Molte organizzazioni contano su una forza lavoro variegata, composta da personale a tempo pieno, agenzie a contratto esterne, consulenti e professionisti indipendenti e personale part-time, pertanto le divisioni IT non hanno più l’assoluto controllo sugli strumenti che vengono impiegati per l’accesso ai dati aziendali ed ai sistemi informatici. L’utenza si è allargata includendo fornitori, clienti e impiegati e un’ampia gamma di parti interessate. Non è più possibile sviluppare applicazioni su una base utenti esclusiva sulla quale si può esercitare controllo e imporre standard.

#### **Ma a questo punto la sicurezza è garantita?**

Una proliferazione di dispositivi che rendono gli individui iperconnessi e mettono, o dovrebbero mettere, in allerta le aziende, dal momento che molte delle applicazioni aziendali sono accessibili da remoto. Da una recente indagine risulta che quasi il 58% degli intervistati ha dichiarato che l’azienda in cui lavora ha adottato una policy di sicurezza per il BYOD, vietando l’uso dei dispositivi mobili. In effetti BYOD è stato visto come una minaccia per la sicurezza delle imprese, ma

l’uso dei dispositivi personali in azienda per scopi di business è molto più che una moda temporanea o un differente sistema di approvvigionamento della tecnologia. Le divisioni IT devono rispondere adeguatamente, considerandolo un’opportunità per un mercato che sta cambiando.

“Il fenomeno rappresenta un’indicazione che l’IT interno non sta fornendo un supporto adeguato ad una parte degli utenti, i quali stanno cercando alternative. È importante riconoscere che BYOD, BYOA (Bring Your Own Application) e l’adozione del cloud sono gli indicatori principali di un cambiamento strutturale di lungo termine che sta avvenendo nel settore, non la richiesta di una parte del personale che vuole il proprio brand tecnologico preferito” ha commentato Darryl Carlton, research director di Gartner. In realtà il dipendente si è evoluto prima del suo reparto IT e quindi usa strumenti personali, mentre quelli aziendali sono spesso visti come rigidi e complessi. Molti vendor stanno impostando il loro modello di business verso questa tendenza, come Apple e Microsoft, favorendo un’adozione della mobilità che tuteli le esigenze di sicurezza e privacy delle organizzazioni. Il BYOD e la mobility andranno ad “invadere” aziende di settori come l’hospitality e il finance, che saranno “obbligate” a dotarsi sempre più di prodotti informatici per la sicurezza e la crescita della propria azienda. Nascerà così l’era del “Bring Your Own Collaboration”, pane per il nostro business. ■

# SICUREZZA PANE PER IL BUSINESS