Fideuram
www.fisac-fideuram.net
info@fisac-fideuram.net

StrongAuth: tanti punti da chiarire

Riteniamo vada fatta chiarezza sull'iniziativa aziendale che punta a sostituire l'attuale sistema di identificazione dell'utilizzatore per la connessione da remoto alle infrastrutture informatiche della banca, requisito basico per il lavoro flessibile. Intesa intende adottare il sistema a tripla chiave, in linea con le linee guida in tema di sicurezza informatica, sistema già in uso ad esempio per l'accesso della clientela al conto corrente su internet (codice titolare, pin, one-time-password).

Il problema si pone ora rispetto al lavoro flessibile, misura adottata estensivamente per la gestione dell'emergenza coronavirus, nel momento in cui si vuole imporre l'adozione dell'applicazione StrongAuth da installare sullo smartphone, aziendale per chi lo ha o personale per chi non lo ha, al fine di consentire l'accesso alla rete aziendale tramite il computer portatile.

Ora se è pacifico che sugli smartphone aziendali si procederà d'ufficio, non è chiaro cosa accade a chi, privo di smartphone aziendale, non fornirà il consenso a ricevere l'installazione di StrongAuth sul proprio dispositivo personale: non potrà più accedere alla VPN aziendale e quindi da remoto potrà utilizzare solo Skype e Outlook? oppure avrà preclusa la possibilità di svolgere smart working? quindi? non potrà lavorare a meno di dover rientrare fisicamente sul posto di lavoro?

E per chi fornirà il consenso, comunicando il proprio numero di cellulare privato, come funzionerà il tutto? Da parte aziendale è stata fornita un'informativa striminzita dando garanzia che StrongAuth non può accedere ad altri dati presenti sullo smartphone e che il numero personale non verrà utilizzato per nessun'altra finalità se non quella di autenticare in modalità sicura l'utilizzatore. Il documento "**Informativa dipendenti per StronghAuth**", scaricabile sulla intranet di Gruppo, però parla espressamente di "*conferimento dei Suoi Dati Personali*".

Va fatta chiarezza, quindi. Concretamente quali garanzie ha il dipendente in merito al livello di controllo che StrongAuth (come qualunque altro software simile) consente all'azienda rispetto a informazioni, dati, operatività sullo smartphone privato legati alla sfera personale? Ad esempio, in caso di eventi anomali, incidenti informatici, accessi illeciti o non autorizzati al patrimonio informativo della banca (d'altronde stiamo parlando di questo, di misure in adozione per il contrasto alla pirateria informatica) le autorità, le funzioni di sicurezza informatica e audit della banca, la funzione IT, tutti i soggetti deputati quali verifiche ed analisi andranno ad effettuare?

La questione è molto delicata, deve essere affrontata e chiarita anche e soprattutto dal punto di vista sindacale, vista la giurisprudenza in materia di controlli a distanza (dallo Statuto dei Lavoratori in poi). La prima questione da porre riguarda le alternative… l'azienda fornisca smartphone aziendale a chi non lo ha, oppure si utilizzino notifiche via SMS eventualmente verso smartphone privati ma senza installare StrongAuth o altro... come avviene per l'accesso internet al conto corrente. Viceversa, se l'Azienda intende imporre questo sistema, riteniamo vadano inquadrate in un accordo sindacale le garanzie per i dipendenti, dato che siamo in ambito al controllo "a distanza".

22 aprile 2020 **Fisac Cgil** Divisione Private