dal sito Fisac Intesa Sanpaolo
4 maggio 2020

SMART WORKING, SICUREZZA E STRONG AUTHENTICATION: E' TEMPO DI FARE CHIAREZZA

Sin dal primo momento dell'emergenza sanitaria le OO.SS. del Gruppo hanno ritenuto che uno dei più importanti fattori di tutela della salute per i colleghi fosse il ricorso al Lavoro Flessibile.

L'aver già provveduto fin dal 2015 ad un accordo sindacale che ne definiva il quadro normativo, in netto anticipo su tutto il resto del Settore, ha consentito di mettere da subito in sicurezza tutti i lavoratori della Sede Centrale, che ne erano già destinatari. **Abbiamo insistito in questi due mesi affinché il Lavoro Flessibile fosse rapidamente esteso anche a tutte le altre realtà per le quali non era originariamente stato previsto quali Filiali, Direzioni Regionali e di Area BdT, Divisione Private, FOL e Pulse.**

Quello in corso è indubbiamente un importante "esperimento" di Lavoro Flessibile e monitoreremo gli sviluppi che vi potranno essere nella cosiddetta Fase 2, che vede al momento abilitati:

- circa 23.700 colleghi di Strutture Centrali e Staff;
- oltre 13.000 colleghi della Rete Banca dei Territori;
- circa 1.500 colleghi della Rete Private e Fideuram.

La situazione di emergenza ha nel contempo esposto colleghi e clienti a maggior rischio di frodi ed attacchi degli hacker, per questo motivo la Banca ha deciso di rafforzare i presidi di cyber security attraverso una serie di interventi quali:

- attività di intellligence su phishing e malware
- nuove regole per intercettare gli attacchi ai clienti
- collaborazione con le Forze dell'Ordine
- sistemi di verifica automatizzati dei sistemi informatici
- verifica approfondita circa la possibilità di accesso fraudolento ai sistemi interni aziendali.

In quest'ottica l'Azienda ha deciso di adottare una modalità di autenticazione a doppio fattore per l'accesso ai propri sistemi in modo da migliorare la sicurezza delle informazioni che sono gestite quotidianamente dai colleghi. Analogamente a quanto è stato adottato per l'accesso al sito della Banca da parte della clientela, è prevista una autenticazione basata su password unitamente all'utilizzo dello smartphone: per fare questo l'Azienda ha scelto di utilizzare la App StrongAuthh.

Per i colleghi in possesso di smartphone aziendale occorre semplicemente scaricare la app seguendo le istruzioni del video tutorial.

Dato però che moltissimi colleghi sono stati abilitati allo smart working in tempi molto ristretti, non tutti erano ancora dotati di cellulare aziendale. La App può essere scaricata anche su telefoni personali, per questo motivo l'Azienda ha inoltrato nei giorni scorsi un sondaggio in cui chiedeva al lavoratore la disponibilità ad utilizzare il proprio numero personale per configurare l'applicazione.

L'azienda ha dichiarato che il numero personale non sarà pubblicato e che sarà utilizzato unicamente per il fine in questione, in modo da garantirne la sicurezza e la riservatezza ed in ottemperanza delle norme in

materia di Privacy. Nelle attuali condizioni, qualora il collega decidesse di non utilizzare il proprio numero personale per scaricare l'App StrongAuthh di fatto renderebbe impossibile l'accesso in sicurezza al lavoro flessibile, in quanto non potrebbero essere utilizzate le procedure aziendali ma unicamente Skype e Outlook.

L'iniziativa su StrongAuth – che l'Azienda ha dichiarato essere necessaria per un maggior livello di sicurezza – è stata veicolata in modo piuttosto confuso, creando apprensione e malcontento nei colleghi e, ad oggi, perdurano dubbi e quesiti:

- Se non fornisco il mio numero di telefono personale non potrò dunque più svolgere Lavoro Flessibile? E perché sino ad ora è stato possibile? E se non potessi più svolgere lo smart working quale sarebbe la decorrenza?
- La App StrongAuth ha qualche forma di invasività/conflittualità nei confronti delle altre App e dei dati presenti nel mio smartphone? Scaricando la App si potrebbe rischiare la perdita di dati personali?

Nelle ultime riunioni in call abbiamo già posto tutte queste domande all'Azienda e attendiamo risposte coerenti e complessive.

Abbiamo da subito richiesto all'Azienda di garantire ai colleghi la massima tutela in termini di sicurezza e di procedere celermente alla fornitura di telefoni aziendali anche se in questo momento di emergenza l'approvvigionamento è difficile, analogamente a quanto già accaduto per la fornitura dei pc alle strutture che hanno avuto, solo ora, accesso allo smart working.

Riteniamo tuttavia che l'Azienda debba attivarsi per arrivare in tempi congrui alla consegna di cellulari aziendali in modo da evitare il rischio di decadenza dallo smart working proprio in concomitanza con la Fase 2 che prevede un rientro in Sede Centrale con progressività e nel rispetto del 20% degli spazi e soprattutto qualora l'utilizzo di StrongAuth possa in prospettiva divenire, come sembrerebbe dalla lettura di alcuni documenti circolanti all'interno dell'Area Digita la nuova modalità di accesso a tutte le postazioni di lavoro, non solo per il lavoro flessibile**.**

Oltre alla sicurezza dei sistemi, riteniamo invece che occorra intervenire efficacemente sulle procedure informatiche in modo da permettere ai colleghi -in particolare alle task force- di poter lavorare bene e in "sicurezza".

Milano, 4 maggio 2020

Delegazioni Trattanti Gruppo Intesa Sanpaolo
FABI – FIRST/CISL – FISAC/CGIL – UILCA – UNISIN