lexant
STUDIO LEGALE

FOCUS ON

SMART WORKING, SICUREZZA DELLE INFORMAZIONI E FRODI INFORMATICHE SU COVID- 19

Strumenti e cautele da adottare

SMART WORKING, SICUREZZA DELLE INFORMAZIONI E FRODI INFORMATICHE SU COVID- 19

Per limitare il rischio contagio dettato dal Covid-19, molte Società, stanno optando per il cd smart working.

Emanuele Madini, Associate Partner di P4I-Partners4Innovation ed esperto di Smart Working ed HR Transformation, ha sottolineato come «*lo Smart Working è un modello organizzativo che interviene nel rapporto tra individuo e azienda. Propone autonomia nelle modalità di lavoro a fronte del raggiungimento dei risultati e presuppone il ripensamento "intelligente" delle modalità con cui si svolgono le attività lavorative anche all'interno degli spazi aziendali, rimuovendo vincoli e modelli inadeguati legati a concetti di postazione fissa, open space e ufficio singolo che mal si sposano con i principi di personalizzazione, flessibilità e virtualità*».

Tale metodologia di lavoro, al di là della cogente necessità, rappresenta, anche per il futuro, quindi, una grande opportunità sia per rendere il lavoro più agile sia per limitare i costi.

Giova evidenziare, per una miglior gestione di tale fenomeno, la necessità di prevedere da parte delle aziende, un regolamento volto a disciplinare lo smart working, utile anche per stabilire regole precise per i dipendenti. Tale fenomeno, quindi, richiede, anche un'evoluzione dei modelli organizzativi aziendali.

Il tema dello smart working è, tuttavia, strettamente connesso al tema della sicurezza delle informazioni.

Giova, infatti, evidenziare come, lavorare da casa, non equivale, nella maggior parte dei casi, sotto il profilo della sicurezza delle informazioni, a lavorare in azienda.

Rappresentano, infatti, nel contesto italiano, un'eccezione, le aziende dotate di un vero e proprio sistema di smart working, con applicativi sicuri, caratterizzati dalla possibilità di una fruizione da remoto, di rilevazione presenze etc.

La maggior parte delle aziende italiane, infatti, ha deciso di utilizzare tale modalità operativa solo per rispondere ad una situazione di emergenza, senza tuttavia, prendere in considerazione, il fondamentale tema della sicurezza delle informazioni, inteso non solo come sicurezza di dati personali, bensì, della più ampia compagine di dati aziendali, compreso, quindi, il Know - now di ogni Società.

Ad oggi, il maggior nemico della sicurezza delle informazioni, è rappresentato dall'utilizzo, da parte dei dipendenti, di dispositivi personali per accedere alle reti aziendali, inclusa la connettività di rete (ADSL, WIFI).

Invero, spesso, tali dispositivi personali, sono privi di antivirus aggiornati, malware e firewall sufficientemente adeguati.

Pur ribadendo la necessità di utilizzare dispositivi aziendali per una maggior sicurezza delle informazioni, di seguito viene indicato qualche suggerimento per porre, in sicurezza, i dispositivi personali dei dipendenti utilizzati per finalità aziendali:

- verificare che dispositivi abbiano un sistema supportato dalla casa madre per quanto riguarda le patch di sicurezza (pc quindi dotati di Windows 10 e non 7);
- verificare che i dispositivi siano aggiornati alle ultime patch di sicurezza sia del sistema operativo sia degli applicativi installati sugli stessi;
- prevedere software antivirus che protegga il sistema anche da malware;

- sistemi di login sicuri: se non si usano adeguati sistemi di protezione -come protocolli sicuri e software di protezione adeguati- è possibile che le utenze e le password digitate vengano carpite;
- vietare il salvataggio della password sul dispositivo, bensì, inserirla tutte le volte sul pc personale.

Una volta messo in sicurezza il dispositivo del dipendente è necessario volgere l'attenzione alle modalità con cui connettersi ai sistemi aziendali.

In merito a ciò vi sono molteplici possibilità:

- creare un secondo account sul pc personale, protetto da password con i parametri classici (8 caratteri, etc) predisponendo una guida ad hoc per il personale al fine di consentire la connessione con la rete aziendale. Così facendo vengono minimizzati i rischi di intrusione di virus, di esecuzione automatica di programmi nella fase di accensione del sistema etc. Per di più, mediante la predisposizione di tale secondo account i dati personali del dipendente rimarranno sull' account personale e, quindi, "protetti" nel caso in cui un tecnico dell'azienda debba collegarsi da remoto per installare: antivirus, programmi aziendali, etc sul pc personale del dipendente. Ed invero il tecnico non avrà la possibilità di accedere agevolmente ai dati personali riservati, evitando, quindi, eventuali contestazioni, da parte di dipendenti, al datore di lavoro;
- accessi remoti "terminalizzati", ad esempio con strumenti Microsoft o Citrix o Rdp al fine di evitare interazioni dirette tra il sistema remoto ed il sistema Informativo aziendale.

In entrambi i casi si consiglia di prevedere VPN ossia, canali di comunicazione sicuri tra il dispositivo remoto e l'azienda, attraverso il quale si accede direttamente agli applicativi ed ai dati aziendali.

Le Vpn per quanto sicure, impongono controlli periodici e mirati ai dispositivi, in quanto, pongono in diretta connessione tali dispositivi con l'azienda, con il rischio che un software malevolo infettando il dispositivo personale infetti anche l'intero sistema aziendale.

Per tale ragione si consiglia di:

- creare un registro contente tutte le utenze VPN create in tale situazione di emergenza;
- impostare un blocco dell'utenza VPN, qualora, venga inserita una password errata per più di 3/5 volte consecutive.

Come ha sottolineato Mariano Corso, Responsabile Scientifico dell'Osservatorio Smart Working del Politecnico di Milano, «Lo Smart Working non può essere la soluzione per "bloccare" l'epidemia ma, con l'impegno di tutti, può rappresentare una misura per ridurre rischi, attenuare disagi e contenere gli enormi danni economici e sociali che questa emergenza rischia di causare. I lavoratori, e soprattutto coloro che sono già Smart Workers, devono restituire il credito di fiducia dimostrando autonomia, impegno e senso di responsabilità».

Nonostante, l'emergenza, lo smart working deve essere, infatti, visto come una grande opportunità per il nostro Paese. Ed invero, "L'adozione di un modello "maturo" di Smart Working può produrre un incremento di produttività pari a circa il 15% per lavoratore, secondo le più recenti rilevazioni dell'Osservatorio Smart Working del Politecnico di Milano. Volendo proiettare l'impatto a livello di Sistema Paese, considerando che il lavoratori che potrebbero fare Smart Working sono almeno 5 milioni (circa il 22% del totale degli occupati) e che gli Smart Worker ad oggi sono 305mila, l'effetto

dell’incremento della produttività media in Italia si può stimare intorno ai 13,7 miliardi di euro, ipotizzando che la pervasività dello Smart Working possa arrivare al 70% dei lavoratori potenzial ” .

In ultimo, si ritiene necessario informarVi sul diffondersi di frodi informatiche legate al Covid-19.

Si tratta di falsi messaggi inviati via mail che, con la scusa di dare aggiornamenti sul virus, invitano ad aprire allegati infetti, i quali mirano a impossessarsi dei dati dei destinatari.

E’ essenziale, quindi, non aprire tali messaggi ed allegati. In particolare, l’ultima frode ha ad oggetto l’inoltro di email da parte di una sedicente dottoressa Penelope Marchetti, presunta "esperta" dell’Organizzazione mondiale della sanità in Italia. I falsi messaggi invitano gli utenti ad aprire un allegato contenente presunte precauzioni per evitare il coronavirus. In realtà, si tratta di un malware che cattura dati personali. Vi sono, tuttavia, altre truffe che stanno circolando a mezzo web, in particolare: una invitava ad aprire un file zip, contente documenti excel, che diffonde un pericoloso virus e consente agli hacker di assumere il pieno controllo del dispositivo dell'utente. Un'altra, simile alla precedente, nascosta dietro un file chiamato CoronaVirusSafetyMeasures.pdf, assume il controllo del dispositivo infettato, trasformandolo, all’insaputa della vittima, in un computer zombie, gestito da remoto da un computer principale per effettuare successivi attacchi informatici in tutto il mondo.

Alla luce di quanto sopra, Vi invitiamo alla massima attenzione.

Avv. Costanza Mottino — Data Protection lawyer

Roberto Bozzano — Manager It

.

Avv. Giorgia Barberis