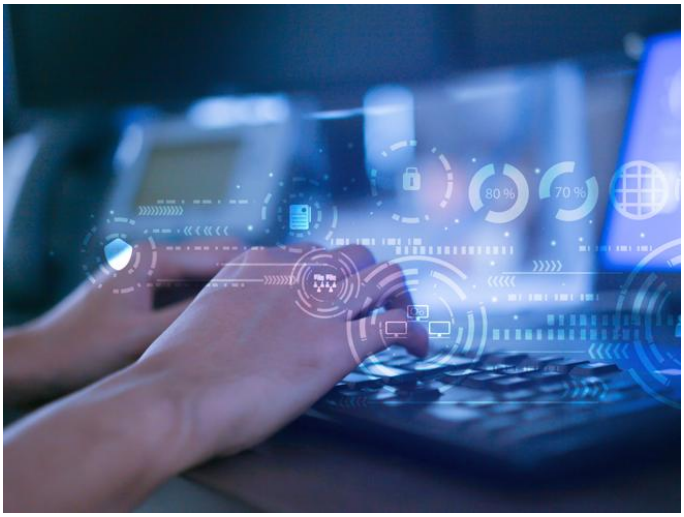
CORONAVIRUS E CYBER SECURITY

Smart working, dieci regole per proteggere i dati (e non rischiare)

di **Sergio Bocconi** | 11 mar 2020



L' emergenza coronavirus sta cambiando il nostro modo di lavorare. Ed espone le aziende a un grado di cyber-risk per certi versi non preventivato. Tutte le imprese, le banche, le compagnie di assicurazioni dotate di un'infrastruttura adeguata hanno attivato o potenziato lo smart working, cioè il lavoro a distanza o agile. E molto probabilmente questa situazione si tradurrà, una volta venute meno le condizioni che hanno portato il governo ad agevolare lo smart working, in una stabile riorganizzazione del lavoro o comunque nella previsione di modalità più flessibili accanto a quelle tradizionali. Tutto ciò però significa per le aziende anche un'attenzione molto più alta nella protezione dei dati proprietari perché il perimetro da cui è possibile utilizzarli diventa 'liquido'. Ecco quindi dieci regole un applicare subito per mettere in sicurezza il patrimonio rappresentato dai dati, ora più esposto ad attacchi esterni. Il decalogo è stato messo a punto da Yarix, divisione sicurezza digitale di Var group, società di It guidata da Francesca Moriani che fattura 343 milioni e che fa parte di First, la rete globale sulla protezione che riunisce player come Nasa, Apple e Google con l'obiettivo di contrastare le minacce emergenti.

Pc e cellulari al sicuro

La prima linea di difesa che le aziende devono mettere in campo riguarda la protezione dei propri asset: è necessario sviluppare consapevolezza sui comportamenti da adottare nella custodia dei dispositivi (mai lasciarli in auto, sul sedile in treno mentre si va in bagno, nella cassaforte degli hotel, e così via), e fornire meccanismi che consentano di inibire la possibilità di accesso ai dati a chi dovesse entrarne in possesso.

Uso accorto delle password

È indispensabile un'adeguata consapevolezza dei dipendenti riguardo alle politiche più opportune sull'uso (e riuso) della password, unita a presidi tecnici messe a punto dall'azienda per imporre un secondo (o un terzo, se necessario) fattore di autenticazione.

Dispositivi e sistemi di protezione

Soprattutto per le attività di business critiche, è meglio che i dispositivi utilizzati (pc, smartphone, tablet) siano di proprietà aziendale: è (relativamente) semplice garantire che siano protetti con adeguati strumenti (antivirus e altro). Quando sono di proprietà dei dipendenti devono essere previste adeguate misure per limitare il rischio, ma tali indicazioni possono essere viste come limitazioni troppo spinte per i propri device personali.

Attenzione all'uso delle mail

Le vulnerabilità legate a un uso non consapevole delle e-mail non sono meno gravi quando si lavora da remoto. È essenziale che si mantengano le stesse attenzioni a tentativi di phishing, spear phising e scam (cioè alle varie forme di truffa digitale) di quando si usa il pc in ufficio. Perciò è auspicabile si prevedano, e di conseguenza si metta in guardia, scenari in cui è più probabile che lo smart worker abbia un'attenzione ridotta (e sia quindi più vulnerabile ad attacchi di questo tipo).

Reti pubbliche

L'uso delle reti wifi pubbliche può essere un veicolo che consente più facilmente di condurre attacchi ai dispositivi. Diventa quindi necessario, oltre alla consapevolezza su quali siano le reti fidate e su come riconoscere eventuali tentativi di camuffamento, anche introdurre politiche che mettano in evidenza in modo chiaro quali siano le attività critiche di business alle quali non si deve (e non dev'essere possibile) accedere da parte di chi lavora da remoto ed è connesso a reti pubbliche.

Computer sconosciuti

È necessaria una formazione diffusa sui rischi che si corrono utilizzando computer di cui non sa nulla. Nel caso sia indispensabile l'uso di pc pubblici o comunque di terzi, bisogna prendere alcune precauzioni: non vanno utilizzati per scambiare informazioni sensibili; occorre usare sempre il private browsing; non vanno salvate informazioni di login; va pulita la history della navigazione e dei download prima di chiudere il browser.

Sicurezza e "spioni"

Non tutti i rischi sono di natura esclusivamente tecnica. Chi lavora da remoto e magari si trova in spazi pubblici, deve prestare attenzione a chi può osservare ciò che sta facendo. Così nelle password di accesso vanno usate le stesse precauzioni che si usa quando al bancomat si digita il pin. Attenti dunque al rischio 'spioni' che magari possono anche scattare foto quando vengono visualizzate informazioni sensibili.

Usb esterne

I dispositivi Usb esterni sono un eccellente metodo per veicolare malware (virus). Non va dunque consentito a terzi di collegarli al proprio pc. Nel caso si renda necessario l'uso di una chiavetta per condividere materiale, meglio chiedere indicazioni al servizio It aziendale.

Monitoraggio 24/7

Meglio estendere a chi lavora da remoto il perimetro di monitoraggio continuo (24 ore su 7 giorni) che prevede la raccolta di informazioni cruciali e di avvisi sugli andamenti della rete e dei sistemi It.

Attenzione ai cuccioli

Come azienda hai messo in atto tutte le azioni per garantire con i protocolli più moderni e mettere in sicurezza l'accesso dei dipendenti remoti ai tuoi dati? Bene, ora pensa ai...cuccioli

(bambini certo, ma non solo) che possono zampettare sulla tastiera mentre chi lavora da casa ha lasciato per un attimo il pc senza bloccare la sessione. Una ragione in più per applicare tutte le regole illustrate. A cominciare dalla prima. E chiedere la massima collaborazione a chi è in smart working. Il lavoro va fatto sempre in team, anche se i partecipanti sono lontani.

RCS MediaGroup S.p.A. - Divisione Quotidiani Sede legale: via Angelo Rizzoli, 8 - 20132 Milano | Capitale sociale: Euro 270.000.000,00

Codice Fiscale, Partita I.V.A. e Iscrizione al Registro delle Imprese di Milano n.12086540155 | R.E.A. di Milano: 1524326 | ISSN 2499-0485