L'Economia del CORRIERE DELLA SERA
Dir. Resp.: Luciano Fontana
www.datastampa.it Tiratura: 0 - Diffusione: 0 - Lettori: 2044000: da enti certificatori o autocertificati
23-MAR-2020
da pag. 29
foglio 1 / 2
Superficie: 54 %

LAVORARE DA CASA AL SICURO
ISTRUZIONI PER L'USO

Dalle password alle videoconferenze, una guida per chiudere le porte ai pirati informatici

di **Chiara Sottocorona**

Tutti casa, a lavorare a distanza, per difenderci dal Covid-19. Ma senza dimenticare di proteggerci da altri virus meno letali, quelli informatici. Se lo smart working è più che raddoppiato con l'emergenza epidemia, e potrebbe arrivare a coinvolgere da cinque a otto milioni di italiani, non basta improvvisare. Bisogna scegliere gli strumenti più adatti e adottare le misure di protezione giuste per evitare intrusioni o perdite di dati. Ecco il decalogo delle misure consigliate da due importanti aziende di sicurezza informatica, TrendMicro e Kaspersky.

Le reti

I dipendenti erano abituati ad arrivare in ufficio ed avere la propria postazione destktop o notebook connessa alla rete aziendale con inclusi tutti i software di sicurezza (firewall, proxy, antivirus, protezione della navigazione e delle mail). Lo smart working cambia la situazione perché le informazioni passano da un router non controllato, quello di casa, ed entrano in una rete aziendale che non era predisposta per avere quel pc all'esterno. Perciò le prime due misure consigliate da Gastone Nencini, direttore di TrendMicro, società attiva nella cybersicurezza, sono destinate a proteggere il router casalingo: la porta d'ingresso e uscita dei dati. «Per evitare intrusioni occorre che il software del router sia aggiornato all'ultima release — avverte —. Se lo abbiamo in abbonamento da una telecom avviene in automatico, ma chi l'ha comprato e installato da solo deve aggiornarlo».

Occorre anche avere la password in funzione per proteggere il wi-fi in casa, ed è raccomandato cambiarla: si tratta di modificare il codice Wep e si può farlo andando sulla propria pagina cliente nel sito dell'operatore.

«Per avere comunicazioni sicure tra i dipendenti a casa e i server aziendali è necessaria una rete Vpn (Virtual private network), che va installata sul pc o anche sullo smartphone con un'app», raccomanda Nencini. Le grandi aziende ne sono già dotate, mentre le piccole o gli studi professionali possono rapidamente ottenerla attraverso i servizi cloud. «La Vpn cripta il flusso di comunicazione, ma non protegge i contenuti, quindi è essenziale che a monte i dispositivi che si collegano alla rete aziendale siano protetti da un antivirus recente e non gratuito — precisa il direttore di TrendMicro — perché altrimenti non assicura la protezione totale né l'aggiornamento. M va protetto anche lo smartphone con un antivirus ».

I dispositivi mobili

Nel 2019 gli spyware che hanno colpito i telefonini sono raddoppiati rispetto all'anno precedente, avverte Kaspersky, che mette in guardia anche contro il phishing, sempre in agguato. «Tutte le organizzazioni dovrebbero assicurarsi, con una chiara comunicazione, che i dipendenti siano ben consapevoli dei rischi in cui possono incorrere lavorando da casa — precisa David Emm, principale security researcher di Kaspersky —. Abbiamo rilevato diversi casi di criminali informatici che cercano di sfruttare il momento nascondendo file dannosi in documenti che sembrano collegati al coronavirus».

Le raccomandazioni dei Kaspersky Lab per chi lavora da casa sono di separare i file personali da quelli di lavoro, limitare le app, tenere sempre aggiornati sistemi operativi e software, fare attenzione alle navigazioni. Senza dimenticare il back-up dei dati.

La condivisione

Perché il lavoro da casa sia veramente «smart», oltre che sicuro, meglio usare strumenti protetti che aiutano la comunicazione. Per le chiamate audio e video o le chat ci sono Skype (nel pacchetto Office di Microsoft), Zoom, che in videoconferenza permette di ospitare fino a 100 partecipanti e anche di registrare la sessione. O Hangouts Meet, con la trasmissione in streaming delle riunioni, che in questo momento Google rende disponibile gratuitamente nella versione di base. Anche Microsoft dal 5 marzo ha messo a disposizione per sei mesi gratuitamente Teams, che combina videoconferenze, chat e integrazione delle applicazioni. Mentre Cisco ha esteso a 90 giorni la gratuità di Webex Meeting che permette riunioni in audio e video fino a 100 utenti. Per l'emergenza Cisco offre anche in licenza gratuita Cisco Umbrella, che protegge le navigazioni e Duo Security, che permette alle aziende di stabilire l'affidabilità di

un dispositivo per consentirne l'accesso alla rete. C'è anche un offerta free di Slack, uno dei più usati software collaborativi, che permette di organizzare la messaggistica, il calendario e l'avanzamento di progetti per gruppi di lavoro.

«Ci dobbiamo abituare a nuove modalità e dobbiamo capire che la tecnologia ci sta dando una mano — dice Nencini — perché oggi abbiamo gli strumenti giusti e la capacità di banda che ci consente di continuare a lavorare fuori dall'ufficio». Con attenzione, però.