PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4814 di Mercoledì 11 novembre 2020

Videoconferenze e protezione dei dati personali

Ian Hulme, Direttore di Assurance del Garante britannico- ICO, fornisce consigli a imprenditori, datori di lavoro e manager su come implementare in modo sicuro le più recenti tecnologie di videoconferenza

La crisi del COVID-19 sta cambiando il modo in cui viviamo le nostre vite. Mantenere la distanza significa che molti di noi lavorano da casa per la prima volta e si adattano a nuovi modi di fare il nostro lavoro. Per fortuna, la tecnologia ci sta aiutando tutti a rimanere connessi. Il software e le app per videoconferenze sono modi preziosi per fare affari, tenere riunioni del personale e tenersi in contatto con i colleghi.

Ma con tutti coloro che lavorano in circostanze così straordinarie, è facile dare priorità alla convenienza, rispetto alla sicurezza. Questi consigli permettono di combinare l'efficienza della connessione digitale con la necessità di protezione della privacy; si raccomanda la distribuzione di questi consigli a tutti gli autorizzati coinvolti.

Hai controllato le impostazioni di privacy e sicurezza?

La tecnologia di videoconferenza deve essere trasparente. Gli utenti devono sapere come verranno elaborati i loro dati, oltre ad avere scelta e controllo su di essi. Quindi dovresti sempre attivare le funzioni di privacy e sicurezza. Queste possono includere la limitazione dell'accesso alle riunioni tramite password, il controllo del momento in cui le persone possono partecipare alla riunione o il controllo degli utenti autorizzati a condividere i propri schermi. Pensa sempre a chi e come condividi l'ID o la password della riunione. È consigliabile effettuare queste scelte prima di iniziare la riunione e prendere in considerazione la possibilità di fornire ai dipendenti consigli chiari sulle funzionalità da utilizzare e su come.

Sei a conoscenza dei rischi di phishing?

Molti di noi sono a conoscenza dei segni indicatori di attacchi di phishing, ma si sa cosa osservare, durante in una video chat? La 'funzione di chat dal vivo' può essere utilizzato da persone malintenzionate per diffondere messaggi di phishing. Sii vigile. Non fare clic su link o allegati che non ti aspettavi o provenienti da partecipanti alla riunione, che non conosci o riconosci.

Hai controllato la politica di sicurezza della tua organizzazione?

Anche se potresti avere un'app preferita, per tenerti in contatto con i tuoi amici e familiari, dovresti controllare quale strumento la tua organizzazione ha scelto di utilizzare. Le organizzazioni devono selezionare una piattaforma di videoconferenza che corrisponda ai propri criteri di sicurezza.

Ti sei accertato che tutto il software sia aggiornato?

Una delle misure di sicurezza più efficaci, che è possibile adottare con facilità, è mantenere tutto il software aggiornato, e il software di videoconferenza non fa' eccezione. Se è stata installata un'app di videoconferenza, si deve mantenerla aggiornata, applicando regolarmente tutti gli aggiornamenti software disponibili. La tua organizzazione potrebbe aver configurato l'applicativo, in modo da eseguire questa operazione automaticamente. Se si accede a un servizio di videoconferenza tramite un browser Web, assicurarsi che anche il browser sia aggiornato.

È sempre la videoconferenza lo strumento giusto per il proprio lavoro?

In un periodo di crisi, le decisioni vengono spesso prese rapidamente, per portare a termine il lavoro da svolgere. Ma, a lungo termine, le circostanze possono cambiare e il bilanciamento dei rischi potrebbe essere modificato. Non c'è motivo di rimanere impegnati a utilizzare un particolare strumento o servizio per sempre, solo perché è stato usato in condizioni di emergenza. Aggiornate periodicamente la vostra decisione di utilizzare strumenti di videoconferenza.

Adalberto Biasiotti

www.puntosicuro.it