PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 22 - numero 4701 di Martedì 19 maggio 2020

COVID-19: smart working, videoconferenze e cybersecurity

La realtà digitale è una risorsa e un'opportunità, ma porta con sé anche vulnerabilità e criticità che non vanno sottovalutate.

Durante la Fase 1 e 2 della gestione della pandemia **Coronavirus** le risorse telematiche (dallo **smart working** all'**eLearning**, alla **videoconferenza**) sono state cruciali per permettere ai professionisti di gestire la situazione nel migliore dei modi, non fermando l'attività lavorativa o preparandosi alla ripartenza.

La realtà digitale è una risorsa e un'opportunità, ma porta ovviamente con sé anche vulnerabilità e criticità che non vanno sottovalutate. Prime tra tutte, quelle legate alla **cybersecurity** dei propri dispositivi informatici o delle piattaforme di videoconferenza main stream che, proprio grazie alla loro notorietà, appaiono spesso come completamente sicure.

Non è certo questo il momento di abbassare la guardia: una ricerca commissionata da Check Point evidenzia un aumento del rischio di attacchi informatici e furto di dati oltre l'usale, già di per sé alto. I risultati della ricerca riportano un aumento in tutto il mondo dei tentativi di attacco per il 71% delle aziende e problemi di sicurezza legati al telelavoro per il 95% a partire dallo scoppio della pandemia. In questa fase storica che scommette tutto sul digitale, i cyber criminali hanno sfruttato le paure e i meccanismi innescati dalla pandemia di covid-19.

Come detto, su un campione di 411 professionisti dipendenti di aziende di tutto il mondo, il 71% degli intervistati ha segnalato un aumento delle minacce o degli **attacchi** indirizzati alla propria azienda dall'inizio dell'epidemia: tentativi di phishing (55%), siti Web malevoli che affermano di offrire informazioni o consigli sulla pandemia (32%), incremento dei malware (28%) e dei ransomware (19%).

Per quanto riguarda lo **smart working**, il 95% degli intervistati afferma che i problemi di sicurezza informatica sono aumentati in seguito alla necessità di adottare in massa il telelavoro. Le tre sfide principali citate sono la difficoltà di garantire l'accesso remoto sicuro alle applicazioni (56%), la necessità di soluzioni scalabili per l'accesso da remoto (55%) e il proliferare di soluzioni di "shadow IT" usate dai dipendenti senza il consenso dell'azienda (47%).

La **sicurezza informatica** deve essere una priorità essenziale. Tomá? Foltýn, content writer di ESET Security Community, in un recente articolo ha spiegato come la continua richiesta di organizzare videoconferenze tra persone e tra aziende stia evidenziando molti problemi di **privacy e sicurezza**, riferendosi soprattutto a piattaforme inflazionate, in termini di sovraccarico di utilizzo, come Zoom.

Videoconferenze e criticità: il caso Zoom

"In un periodo in cui la maggior parte delle persone è confinata all'interno delle proprie mura domestiche nel tentativo di contenere la pandemia COVID-19 ? si legge nel documento dell'esperto ? la popolarità dei software di videoconferenza per il lavoro, l'istruzione e il tempo libero sta esplodendo. Tra i vari strumenti di comunicazione che sono stati improvvisamente spinti alla ribalta, probabilmente quello che spicca maggiormente è Zoom". Una piattaforma digitale molto famosa che, ultimamente, ha dovuto fronteggiare una grande richiesta da parte di privati e aziende che ha portato alla luce problematiche legate alla privacy e alla sicurezza. "Lo sviluppatore dell'app ? prosegue lo specialista di cybersecurity ? sta affrontando una tempesta di critiche da vari fronti, tra cui sostenitori della privacy, esperti di sicurezza, diversi alti funzionari US e l'FBI. Le critiche hanno continuato ad accumularsi negli ultimi giorni, tanto da spingere l'azienda a rispondere". Alcune settimane fa, infatti, il fondatore e amministratore delegato dell'azienda, Eric S. Yuan, si è scusato per i problemi emersi e ha delineato le misure per rafforzare la sicurezza e la privacy di Zoom. "Ha anche annunciato ? prosegue Foltyn ? uno stop delle attività di sviluppo per 90 giorni, precisando che l'azienda sta dedicando tutte le proprie risorse ingegneristiche alla "risoluzione dei problemi di fiducia, sicurezza

e privacy".

Quali sono le problematiche in cui Zoom è incappata? "L'informativa sulla privacy di Zoom ? evidenzia il professionista della sicurezza informatica ? non menzionava che la versione iOS della propria app inviava dati analitici a Facebook anche di utenti non in possesso di un account Facebook, secondo un rapporto di Vice della fine di marzo. L'azienda ha riconosciuto il problema e ha rimosso il Software Development Kit (SDK) di Facebook per iOS ed è attualmente alle prese con una causa collettiva in California su questa criticità. Nonostante le dichiarazioni, i video e audio meeting dell'applicazione non supportano la crittografia end-to-end, secondo una ricerca di The Intercept. L'azienda si è giustificata chiarendo che utilizza il protocollo crittografico di trasmissione TLS (Transport Layer Security). La differenza sostanziale è che quest'ultimo non garantisce che le comunicazioni degli utenti siano invisibili all'azienda. Inoltre, l'app ha anche rivelato diverse vulnerabilità nella sicurezza, anche se sono state tutte risolte in breve tempo. Sul suo client Windows è stata riscontrata una vulnerabilità UNC path injection che potrebbe esporre le credenziali di accesso a Windows degli utenti e persino portare all'esecuzione di comandi arbitrari sui loro dispositivi. Altri due bug, questa volta riguardanti il client MacOS di Zoom, avrebbero potuto consentire a un malintenzionato di prendere il controllo di un computer vulnerabile". Come se non bastasse, poi: "L'FBI ? aggiunge Foltyn ? ha anche evidenziato il fenomeno "Zoom-bombing" a seguito di molteplici segnalazioni che riportavano episodi di troll che si intrufolavano in riunioni private e lezioni scolastiche per mostrare immagini non adatte al contesto".

Il rischio è stato altissimo per un enorme numero di persone, dato che la piattaforma ha visto moltiplicato per almeno venti il numero degli utenti giornalieri negli ultimi mesi. Per ammissione dello stesso Yuan, Zoom è stato sopraffatto da un imprevisto successo. "Ora abbiamo un insieme molto più ampio di utenti che stanno utilizzando il nostro prodotto in una miriade di modi inaspettati, presentandoci sfide che non avevamo previsto quando la piattaforma è stata concepita".

La domanda dell'esperto di cybersecurity è quindi: "Come rimanere al sicuro?". Anche, e soprattutto, in questo momento di lavoro a distanza (che si tratti di smart working o di videoconferenze), non dovremmo trascurare mai l'importanza della nostra privacy e sicurezza. Per esempio, per quanto riguarda il caso trattato "Le misure più efficaci da adottare per proteggere la sicurezza e la privacy includono: la protezione con password delle riunioni e il controllo dei partecipanti alle riunioni; la limitazione della possibilità di condivisione dello schermo all'organizzatore; l'astensione dal condividere link o ID di riunione sui social media".

---

www.puntosicuro.it