

MalpensaNews

Il lavoro ibrido è la normalità ma serve capire come proteggere le comunicazioni aziendali a distanza

divisionebusiness · Tuesday, March 31st, 2026

Le innovazioni tecnologiche alimentano i processi di digitalizzazione che coinvolgono anche le metodologie di lavoro e le procedure operative aziendali che si possono svolgere da remoto. Così vengono riconfigurate le attività professionali che si avvalgono di strumenti informatici all'avanguardia per lo svolgimento di determinate mansioni a distanza. Tuttavia, non mancano neppure i problemi perché le comunicazioni aziendali sono vulnerabili agli attacchi informatici e ai tentativi di data breach. Minacce che si possono fronteggiare con l'ausilio dei protocolli crittografati per le [business email](#) e le interazioni professionali da remoto.

Le prerogative operative e organizzative del lavoro ibrido a distanza

Lo smart working combina in maniera innovativa ed efficiente il lavoro in ufficio con quello svolto da remoto. Ecco il principale tratto distintivo di questo modello procedurale più flessibile, ma altrettanto redditizio e produttivo. A seconda del tempo trascorso nella sede aziendale o in un altro luogo alternativo, il lavoro ibrido è suddiviso in due categorie:

- Office First
- Remote First

In entrambi i casi, le ripartizioni tra le ore in ufficio e quelle da remoto vengono concordate in precedenza. L'attuazione dello smart working richiede un minimo di organizzazione perché le attività professionali a distanza vengono supportate da strumenti digitali, software gestionali e piattaforme di comunicazione.

Priorità strategiche: la protezione delle comunicazioni aziendali da remoto

Le imprese subiscono diverse tipologie di attacchi informatici perché i [cybercriminali](#) puntano a monetizzare il furto dei dati sensibili, dei conti correnti o delle proprietà intellettuali. Ecco i rischi che rendono essenziale la predisposizione di un protocollo difensivo avanzato ed efficace. Soprattutto quando le comunicazioni aziendali transitano attraverso le reti Wi-Fi pubbliche o vengono gestite tramite dei dispositivi mobili personali. Con la diffusione del lavoro ibrido sono aumentate anche le minacce informatiche, ma le aziende possono adottare diversi strumenti di sicurezza. Sistemi di cifratura, email crittografate e VPN (Virtual Private Network) garantiscono una maggiore protezione durante le attività a distanza che prevedono lo scambio di informazioni

riservate. Così si possono preservare tutti i dati che assicurano la continuità operativa e la stabilità dei flussi di lavoro.

Indicazioni, strumenti e sistemi di protezione per le comunicazioni aziendali da remoto

Le minacce informatiche vengono fronteggiate con degli approcci strutturati che prevedono l'integrazione tra [tecnologie avanzate](#) e prassi consolidate. Anche i dipendenti possono incrementare i livelli di sicurezza con l'adozione di comportamenti più responsabili nel corso delle sessioni di lavoro da remoto. Ecco perché le imprese devono elaborare delle linee guida per impedire l'accesso ai sistemi aziendali da reti pubbliche o non protette. Le comunicazioni a distanza si possono proteggere con delle pratiche condivise e delle risorse in grado di cifrare le connessioni provenienti da dispositivi mobili o privati. Anche gli accessi vengono verificati ogni volta con dei protocolli di autenticazione piuttosto rigidi, dati i rischi derivabili da un'eccessiva fiducia riposta nei confronti dei singoli dipendenti. Le email crittate potenziano ancor di più i sistemi difensivi sviluppati per le comunicazioni aziendali a distanza perché impediscono le intercettazioni fraudolente dei messaggi scambiati tra dipendenti, mentre i calendari crittografati rendono più complessi i tracciamenti degli appuntamenti o delle scadenze. I dati memorizzati online, infine, vengono salvaguardati con dei firewall avanzati e dei sistemi di sicurezza informatica basati sugli spazi di archiviazione remota.

This entry was posted on Tuesday, March 31st, 2026 at 7:00 am and is filed under [Lavoro](#). You can follow any responses to this entry through the [Comments \(RSS\)](#) feed. You can skip to the end and leave a response. Pinging is currently not allowed.