Le sfide moderne della sicurezza aziendale e come affrontarle

La questione del posto di lavoro flessibile

Le aziende moderne hanno la necessità di accedere, spostare e condividere le informazioni a una velocità e su una scala sempre maggiori. I dipendenti desiderano lavorare con metodi più efficienti e collaborativi. Dato che il luogo di lavoro si estende oltre le tradizionali mura dell'ufficio, è necessario che i processi siano flessibili quanto le modalità di lavoro del personale.

Si tratta di scenari che quasi tutte le aziende di oggi devono affrontare e, nonostante contribuiscano in maniera significativa alla produttività e all'innovazione aziendale, comportano anche minacce potenzialmente gravi alla sicurezza dei dati aziendali.

Come bilanciare le aspettative dei dipendenti con la necessità di proteggere le informazioni? Questo documento analizza la sfida della realizzazione di un ambiente di lavoro digitale flessibile ma sicuro, delinea i potenziali rischi per la sicurezza e offre alcune soluzioni concrete per affrontarli.

RICOH
imagine. change.

La situazione

I dipendenti desiderano un ambiente di lavoro flessibile e una maggiore mobilità

I lavoratori di oggi confidano nella tecnologia per poter lavorare ovunque si trovino.

Anche se un'azienda non dispone di personale che lavora da remoto, la diffusione della tecnologia mobile e cloud ha esteso lo spazio di lavoro oltre i confini della scrivania. L'ideale di mobilità per i professionisti è molto più che una semplice e-mail sul telefono: è l'accesso diretto a documenti, dati, colleghi e clienti in qualsiasi momento e ovunque. Questa libertà è diventata un'aspettativa scontata, quindi limitarla non è la strada giusta se si desidera attrarre e mantenere talenti.

Tuttavia, la creazione di un luogo di lavoro realmente flessibile e mobile può esporre le aziende a una serie di potenziali minacce per la sicurezza. Cosa succede se un portatile o un telefono viene perso o rubato? Come si gestisce la sicurezza delle informazioni quando i dipendenti possono accedervi dai dispositivi personali? Come si proteggono i dati quando i dipendenti si connettono a una rete Wi-Fi pubblica?

RICOH
imagine. change.

Le sfide

Disporre di un sistema inadeguato di archiviazione e condivisione delle informazioni con i dipendenti all'interno e all'esterno dell'ufficio può avere conseguenze gravi a livello di produttività e sicurezza.

Se i dipendenti hanno la percezione di non disporre degli strumenti di cui hanno bisogno, potrebbero ricorrere a soluzioni improvvisate e non sicure. I file vengono inviati via e-mail agli account personali e consultati dai computer di casa, e i documenti vengono archiviati e condivisi tramite soluzioni cloud gratuite. L'adozione non autorizzata di diversi servizi cloud può trasformare rapidamente un sistema informativo ben progettato in una struttura disorganizzata.

Queste soluzioni alternative possono causare il pericoloso fenomeno conosciuto come "fuga di dati", che rappresenta una costante perdita di controllo sulle informazioni.

Le soluzioni alternative, seppur utilizzate secondo le migliori intenzioni, mettono a rischio la sicurezza dei dati importanti

L'84% dei dipendenti utilizza l'indirizzo e-mail personale per inviare file sensibili[1].

L'approccio "Bring your own device" (BYOD) è sempre più diffuso

Più della metà delle aziende nordamericane ed europee sta sviluppando programmi BYOD per soddisfare le richieste del personale[2].

Molte violazioni dei dati sono accidentali

Nel 2017 nel Regno Unito sono stati compromessi oltre 28 milioni di documenti. Per il 38% di questi la causa è stata attribuita a perdite accidentali[3].

Il Wi-Fi pubblico è un campo minato

Si stima che solo il 5% degli hotspot Wi-Fi pubblici sia crittografato, ma il 95% degli utenti li utilizza per lavoro almeno una volta a settimana[4].

L'entità dei rischi è spesso sconosciuta

Oltre la metà dei manager IT non ha alcuna visibilità sul trasferimento di file e dati all'interno della propria organizzazione[5].

1. Ipswitch File Transfer, 'Are Employees Putting Your Company's Data at Risk? Survey Results Exposing Risky Person-to-Person File Sharing Practices: An eBook report' www.ipswitchft.com. 2. www.forrester.com/Bring-Your-Own-Device-(BYOD). 3. www.theregister.co.uk/2017/09/20/gemalto_breach_index/ 4. gfi.com/blog/survey-95-6-of-commuters-in-the-us-put-company-data-at-risk-over-free-public-wi-fi/ 5. eBook dello studio di Ipswitch File Transfer: www.ipswitchft.com

RICOH
imagine. change.

Le soluzioni

Il primo passo verso la costruzione di un ambiente sicuro è la comprensione del flusso delle informazioni all'interno della propria organizzazione: dove sono archiviate e come vengono utilizzate. Poiché i dati circolano nell'azienda attraverso numerosi di dispositivi, questi devono essere protetti con misure di sicurezza sofisticate.

Mantieni le informazioni all'interno del sistema

Disporre del miglior sistema di sincronizzazione e condivisione dei file serve a poco se le informazioni necessarie sono conservate in un archivio cartaceo. Una soluzione di scansione su cloud è in grado di inviare i documenti direttamente al servizio scelto e garantire un'archiviazione sicura. **La soluzione software Streamline NX di Ricoh permette di eseguire la scansione su cloud in modo facile e sicuro.**

Recupera le informazioni quando ne hai bisogno

Nonostante la praticità e la flessibilità dei file digitali, in molti casi sono ancora necessarie le copie cartacee. Assicurati che le informazioni giuste finiscano sempre nelle mani corrette con **soluzioni di stampa sicure, come la funzionalità Print2Me di Streamline NX di Ricoh.**

Stampa mobile e stampa guest

In caso di urgente necessità di stampare, il personale e gli ospiti in visita inviano spesso allegati a un contatto in sede. Ciò può aumentare il rischio che virus e malware vengano trasmessi inavvertitamente. La comunicazione peer-to-peer tra il dispositivo e il cellulare e la stampa pull basata sul cloud permettono di ridurre questo rischio. **Scopri di più sulla stampa mobile MyPrint di Ricoh.**

Gestisci le informazioni

L'implementazione di una soluzione di gestione dei documenti può garantire che ciascun dipendente abbia un adeguato livello di accesso alle informazioni. Inoltre, può fornire informazioni su come, quando e da chi vengono visualizzati o modificati i documenti. **Scopri in che modo Ricoh e DocuWare collaborano per consentire una gestione dei documenti sicura ed efficiente.**

Rivolgiti a un esperto

Visita il sito **www.ricoh.it** oppure contatta il rappresentante locale Ricoh per scoprire come possiamo aiutarti a costruire un luogo di lavoro sicuro e flessibile.

Ricoh Italia Srl
Viale Martesana 12
20090 Vimodrone (MI)

+39 02 91987100

www.ricoh.it

RICOH
imagine. change.