FERRAGUTI Engineering

059 7125536
INFO@FERRAGUTI-ENGINEERING.IT

SICUREZZA IN MICROSOFT 365

PERMESSI, CONDIVISIONE SICURA, COMPLIANCE E NUOVE SOLUZIONI DI PROTEZIONE

La sicurezza informatica nel cloud è diventata una priorità assoluta per ogni azienda.

Microsoft 365 offre potenti strumenti di collaborazione e produttività, ma senza un'adeguata configurazione di sicurezza il rischio di violazioni di dati rimane elevato. Basti pensare che l'errore umano incide nella maggior parte degli incidenti: circa l'88% dei data breach è causato (direttamente o indirettamente) da sbagli o disattenzioni umane.

In questo post esploriamo cinque aspetti chiave, dalla gestione dei permessi alla Data Loss Prevention, fino a una nuova funzionalità di Microsoft Teams per aiutare la tua azienda a proteggere i dati in Microsoft 365.

GESTIONE CORRETTA DEI PERMESSI E ACCESSI

Un controllo rigoroso dei permessi di accesso è fondamentale per limitare l'esposizione dei dati aziendali.

Le configurazioni errate nel cloud (come permessi troppo aperti o utenti con privilegi eccessivi) sono responsabili di circa il 41% delle violazioni di dati.

Molti utenti dispongono di privilegi non necessari: oltre il 90% delle identità cloud utilizza meno del 5% dei permessi loro assegnati.

Ciò significa che applicando il principio del minimo privilegio ossia assegnare a ciascun utente solo le autorizzazioni indispensabili si può drasticamente ridurre la superficie di attacco e il rischio di accessi non autorizzati.

Implementare politiche di Identity and Access Management (IAM) adeguate e controllare periodicamente chi ha accesso a cosa aiuta a prevenire abusi, soprattutto se un account dovesse essere compromesso.

CONDIVISIONE SICURA DEI FILE

La condivisione dei documenti deve avvenire in modo controllato e tracciabile.

In Microsoft 365 è buona norma utilizzare gli strumenti aziendali come OneDrive, SharePoint e Teams per condividere file, impostando con cura chi può accedervi (internamente ed esternamente) ed evitando link pubblici non protetti.

OneDrive for Business, ad esempio, crittografa i file sia in transito sia a riposo, e permette di monitorare le attività sui documenti condivisi – mostrando chi vi ha avuto accesso e quando.

Grazie a queste funzionalità è possibile collaborare in modo sicuro con colleghi e partner, mantenendo il controllo su informazioni riservate.

Assicurati inoltre di utilizzare opzioni come scadenza dei link di condivisione, password per l'accesso ai file condivisi e notifiche di accesso: sono accorgimenti che riducono il rischio di diffusione non autorizzata dei dati.

COMPLIANCE NORMATIVA (GDPR)

Oltre a essere una buona pratica di business, la protezione dei dati personali è un obbligo di legge.

Il Regolamento GDPR impone alle aziende misure adeguate a tutelare i dati dei cittadini UE, con sanzioni pesantissime in caso di violazione: fino a 20 milioni di euro o al 4% del fatturato globale annuo dell'azienda.

Microsoft 365 è progettato per supportare la conformità ai requisiti GDPR, mettendo a disposizione strumenti di compliance e audit (come il Centro sicurezza e conformità, registri di controllo, eDiscovery, conservazione dei dati, etc.).

Tuttavia, spetta all'azienda configurare correttamente tali strumenti e definire policy interne in linea con la normativa. Ciò significa, ad esempio, gestire bene i consensi e le autorizzazioni, controllare i flussi di dati (specialmente quelli sensibili) e garantire che solo chi ne ha diritto possa accedere a informazioni personali.

Un approccio proattivo alla compliance non solo evita sanzioni, ma rafforza la fiducia di clienti e partner nella vostra gestione dei dati.

DATA LOSS PREVENTION (DLP)

Tra le tecniche più efficaci per prevenire fughe di dati c'è la Data Loss Prevention (DLP).

La DLP è una soluzione di sicurezza che identifica e blocca la condivisione, il trasferimento o l'uso non appropriato di informazioni sensibili.

Microsoft 365 permette di definire criteri DLP che riconoscono dati riservati (come numeri di carta di credito, dati personali, informazioni finanziarie, ecc.) e impediscono che escano dall'azienda senza autorizzazione. Ad esempio, se qualcuno tenta di inviare via e-mail un elenco di clienti contenente dati personali, la DLP può intercettare il messaggio e bloccarlo o segnalarlo.

Queste policy si applicano trasversalmente ai servizi Microsoft 365 da Exchange Online (e-mail) a SharePoint/OneDrive, fino a Teams, monitorando e proteggendo automaticamente i dati sensibili ovunque essi risiedano.

Oltre a prevenire perdite accidentali o intenzionali, la DLP aiuta l'organizzazione a rispettare le normative di settore e il GDPR, evitando che informazioni riservate finiscano in mani sbagliate.

Implementare correttamente la Data Loss Prevention significa quindi aggiungere un livello di controllo fondamentale per la sicurezza dei dati aziendali.

NOVITÀ IN MICROSOFT TEAMS: PREVENT SCREEN CAPTURE

Microsoft continua a rafforzare la sicurezza anche nelle piattaforme di collaborazione.

Una novità importante è in arrivo su Teams: a partire da luglio 2025, verrà introdotta la funzionalità Prevent Screen Capture, pensata per bloccare screenshot e registrazioni non autorizzate durante le riunioni online.

In pratica, se un partecipante tenterà di catturare lo schermo in una riunione protetta, il risultato sarà uno schermo nero.

Questo significa che documenti riservati, slide confidenziali o informazioni sensibili condivise durante le riunioni non potranno essere "fotografate" di nascosto via software.

Si tratta di un ulteriore strato di protezione della privacy nelle videoconferenze, ideale per le aziende che discutono dati critici su Teams. Naturalmente resta sempre valido il buon senso (es.: evitare di condividere schermo con contenuti sensibili se non necessario) e la prudenza generale, ma questa nuova feature dimostra l'attenzione di Microsoft nel proteggere la riservatezza delle comunicazioni aziendali: *"Ciò che accade in Teams, resta in Teams"*

MIGLIORA LA SICUREZZA DEI TUOI DATI – CHECK-UP GRATUITO

La tua azienda sta sfruttando al massimo queste funzionalità di sicurezza di Microsoft 365? Spesso una configurazione non ottimale può lasciare porte aperte a rischi evitabili.

Ferraguti Engineering, in qualità di partner IT specializzato, offre un check-up gratuito della tua attuale configurazione Microsoft 365 per individuare eventuali vulnerabilità e opportunità di miglioramento nella protezione dei dati aziendali.

Contattaci per prenotare il tuo check-up gratuito: i nostri esperti ti aiuteranno a mettere al sicuro il tuo business, garantendo che permessi, condivisioni e policy di sicurezza siano impostati correttamente.

Non aspettare che accada un incidente investi oggi qualche ora in prevenzione per dormire sonni tranquilli domani.