Microsoft 365

INFORMATION WORKERS GROUP

E-book

Come gestire la tua attività in modo sicuro sempre e ovunque

Quali sono le 4 insidie più comuni per la sicurezza nell'ambiente di lavoro ibrido e come evitarle?

Microsoft 365

INFORMATION WORKERS GROUP

Sicurezza nell'ambiente di lavoro ibrido

La pandemia ha accelerato il lavoro da remoto, inducendo le organizzazioni di tutto il mondo ad adottare il principio del lavoro da qualsiasi luogo. E non si tratta di un fenomeno passeggero. Il lavoro ibrido è la nuova normalità. Con i dipendenti che lavorano da più sedi utilizzando una serie di dispositivi personali e mobili, molte PMI devono affrontare sfide legate alla sicurezza. Hanno difficoltà a favorire la produttività e a garantire la sicurezza dei dati mentre gestiscono una forza lavoro sparsa in più luoghi. Da un lato, devono agevolare l'accesso remoto e favorire una collaborazione continua in tempo reale. Dall'altro, devono proteggere le identità, prevenire minacce informatiche e perdita di dati, nonché rendere sicuri i dispositivi.

È un lavoro complesso. Quando accedono ai dati di lavoro da casa, i dipendenti possono essere esposti a vulnerabilità della sicurezza. Ad esempio, possono utilizzare soluzioni gratuite o consumer con funzionalità di sicurezza minime. Gli hacker lo sanno e cercano di cogliere l'occasione: i criminali informatici hanno sfruttato la pandemia inviando a PMI, grandi organizzazioni e singoli individui e-mail sul COVID-19 contenenti raggiri e tentativi di phishing. Un esempio è l'OMS, che segnala un aumento di cinque volte degli attacchi informatici.

Ora più che mai, è fondamentale valutare la sicurezza degli ambienti di lavoro ibridi. Diamo ora un'occhiata più da vicino alle quattro insidie più comuni per la sicurezza nell'ambiente di lavoro ibrido e parliamo di come evitarle.

Microsoft 365

INFORMATION WORKERS GROUP

Perché la sicurezza è importante: problemi attuali

Microsoft 365

INFORMATION WORKERS GROUP

Al giorno d'oggi, le aziende non possono permettersi di non prendere sul serio la sicurezza. Le ricerche dimostrano che il costo medio di un attacco alla sicurezza per le piccole imprese è di circa 149.000 dollari. Si tratta di un impatto finanziario significativo, soprattutto se si considera il fatto che il 55% delle PMI subisce attacchi ogni anno.

E gli attacchi ransomware non sono una passeggiata: il 43% delle aziende impiega più di una settimana per risolvere il problema. L'interruzione che ne risulta ha un costo per le organizzazioni. Solo il 35% delle PMI tornano produttive dopo un attacco ransomware prolungato.

Ciò che è ancora più preoccupante è che gli autori degli attacchi possono decifrare addirittura il 90% delle password in meno di sei ore. Significa che la minaccia di compromissione è costante, in particolare nel mondo ibrido, dove i dipendenti lavorano da remoto e spesso cambiano le password a proprio piacimento.

Pertanto, è fondamentale che le aziende valutino le proprie misure di sicurezza e si adeguino se necessario. Come proteggere le password dal furto? Come si garantisce che i dispositivi utilizzati dai dipendenti siano sicuri? I dipendenti possono accedere in modo semplice e sicuro alle applicazioni di lavoro in ufficio, a casa e in viaggio, proteggendosi al contempo da utenti non autorizzati? È possibile garantire che i dati di lavoro riservati non vengano memorizzati su dispositivi personali, soprattutto se un dipendente lascia l'azienda? Infine, come si fa a rendere un lavoro ibrido sicuro riducendo al minimo i costi e la complessità?

Per porre tutte le domande giuste e rispondere, dovresti prima essere informato sulle minacce alla sicurezza più importanti.

Microsoft 365

INFORMATION WORKERS GROUP

Impara a difenderti dalle 4 insidie più comuni per la sicurezza

Prevenire è meglio che curare. Con questo in mente, parleremo delle quattro insidie più comuni per la sicurezza, compresi i modi per evitarle.

Insidia per la sicurezza n. 1: phishing

Di cosa si tratta?

Il phishing è una forma di frode in cui un utente malintenzionato invia un messaggio tramite e-mail o altri canali di comunicazione elettronica fingendo di essere una persona o un'azienda rispettabile. Una tattica comune di phishing è quella di inviare un'e-mail con un indirizzo del mittente falso, il che suggerisce che il messaggio proviene da una fonte attendibile. In questo modo, è più probabile che il destinatario lo apra.

Gli attacchi di phishing sono popolari tra i criminali informatici, poiché è abbastanza facile indurre qualcuno a fare clic su un link dannoso in una e-mail apparentemente legittima.

Qual è l'insidia?

Supponiamo che un dipendente ignaro apra un'e-mail dal CEO della propria azienda. Richiesta: acquistare carte regalo elettroniche per un evento imminente con cui omaggiare i clienti presenti. Poiché il tempo stringe, il dipendente effettua rapidamente l'acquisto e invia i numeri delle carte regalo al CEO. Una settimana dopo si scopre che il CEO non ha mai effettuato la richiesta.

È solo uno dei tanti esempi di attacco di phishing riuscito. Il problema è che il phishing è molto comune e i criminali informatici prendono spesso di mira le PMI. Dal 90 al 98% di tutti gli attacchi informatici inizia con il phishing. Inoltre, stanno diventando sempre più avanzati. Sono ormai lontani i giorni in cui gli attacchi di phishing erano facilmente individuabili. Oggi, sono studiati così perfettamente che possono ingannare persino gli esperti addestrati a individuarli. Inoltre, il malware è spesso progettato in modo così perfetto che gli antivirus o gli strumenti di sicurezza tradizionali non riescono a individuarlo. Questi programmi possono nascondersi e riscrivere se stessi. Una volta penetrati nel sistema, copriranno le loro tracce.

Cosa puoi fare per evitarlo?

Per prevenire gli attacchi di phishing, è possibile utilizzare una soluzione che offre quanto segue:

Protezione in tempo reale e scansione degli allegati

La protezione in tempo reale impedirà ai criminali informatici di reindirizzare link apparentemente sicuri a siti Web non sicuri. Ogni volta che si fa clic su un link, questo viene controllato in tempo reale. Se la destinazione è nota per essere dannosa, viene bloccata.

Scegli una soluzione che esegua anche la scansione degli allegati e-mail, in modo da poter rilevare il malware prima che sia troppo tardi.

Detonazione di URL

Ogni volta che un utente fa clic su un link che ha una reputazione sconosciuta, il sistema controlla la destinazione. Se rileva un comportamento sospetto o identifica il link come dannoso, avvisa l'utente di non aprirlo.

Tecnologia anti-spoofing

Utilizzando l'apprendimento automatico e tecniche di analisi avanzate, il sistema identifica i segnali per cui un mittente di posta elettronica potrebbe non essere chi afferma di essere. Se viene rilevata la rappresentazione, l'e-mail viene bloccata o spostata nella cartella della posta indesiderata.

Autenticazione a più fattori

Con questo metodo, puoi tenere gli utenti malintenzionati fuori dal tuo ambiente, anche se un attacco di phishing causa la compromissione di una password. Coloro che desiderano configurare posizioni attendibili (come una rete aziendale) e bloccare l'accesso dai paesi in cui non operano possono optare per l'autenticazione avanzata a più fattori.

Insidia per la sicurezza n. 2: ransomware

Di cosa si tratta?

Il ransomware è un software dannoso che blocca l'accesso a un sistema informatico o ai file a meno che non venga pagata una somma di denaro.

In genere, la crittografia protegge dati e file personali. Il ransomware però la usa per prendere i file in ostaggio. Questo significa che non puoi accedere ai tuoi documenti, a fogli di calcolo, immagini, video e altri file importanti. Inoltre, un PC infetto può diffondere ransomware ad altri computer della rete.

Qual è l'insidia?

Il ransomware penetra nelle reti in modo discreto. Ad esempio, un dipendente può ricevere da un amico un'e-mail su un video divertente che mostra come creare uova sode a forma di cuore. Il dipendente deve solo seguire il link e fare clic su "Esegui". Più tardi quello stesso giorno, i colori sullo schermo cambiano e appare una finestra per informare l'utente che tutti i file sul computer sono stati dirottati e criptati.

Il dipendente non potrà accedere a nulla a meno che non paghi un riscatto. Se sceglie di non farlo, probabilmente non avrà mai più accesso ai file.

Cosa puoi fare per evitarlo?

Sono diverse le misure che puoi adottare per individuare i tentativi di ransomware quando il danno non è ancora stato fatto:

Adottare precauzioni contro il malware e altri contenuti dannosi inviati tramite e-mail

È possibile intercettare e sottoporre a scansione i messaggi con allegati sconosciuti. Opta per una soluzione che non consegna l'allegato se rileva attività sospette. Inoltre, assicurati di utilizzare una funzione per il controllo dei collegamenti ipertestuali ogni volta che fai clic su di essi e che blocca la destinazione se è ritenuta dannosa.

Proteggere i dispositivi dei dipendenti

Usa una soluzione che impedisca l'accesso non autorizzato alle cartelle comuni, come Desktop e Documenti. In questo modo, i tentativi del ransomware di crittografare i file in queste posizioni saranno bloccati.

Assicurarsi di poter recuperare i file in caso di attacco ransomware riuscito

Indipendentemente dalla quantità di misure adottate, è importante prevedere l'ipotesi più sfavorevole. Cosa succede se la tua azienda diventa vittima di un attacco ransomware? In tal caso, dovresti essere in grado di recuperare le versioni dei file precedenti all'attacco con pochi clic.

Microsoft 365

INFORMATION WORKERS GROUP

Insidia per la sicurezza n. 3: Bring Your Own Device

Di cosa si tratta?

Bring Your Own Device (BYOD) si riferisce a una politica che consente ai dipendenti di utilizzare i propri dispositivi (laptop, tablet e smartphone) per accedere alle informazioni e alle applicazioni aziendali. Nel mondo ibrido, il BYOD è sempre più popolare tra le aziende, poiché contribuisce a ottimizzare la produttività ovunque e riduce le spese per l'hardware.

Qual è l'insidia?

I dispositivi personali sul posto di lavoro possono aumentare la probabilità di virus, hacking e perdite di dati. Ogni dispositivo che accede alle informazioni aziendali è un ulteriore endpoint che gli hacker possono tentare di violare.

Inoltre, i dispositivi sono facili da perdere o rubare. Se un dipendente lascia un laptop incustodito in aeroporto per un minuto, qualcuno potrebbe afferrarlo e scomparire. Inoltre, le persone dimenticano costantemente i propri telefoni sugli aerei e nei taxi. Tuttavia, ogni volta che un dispositivo scompare, le informazioni aziendali al suo interno sono a rischio.

Eppure molte aziende scelgono di accettare queste insidie, perché è difficile implementare il lavoro ibrido senza una politica BYOD. Consentire alle persone di "utilizzare i propri dispositivi" aumenta la soddisfazione, il coinvolgimento e la produttività dei dipendenti. Le persone possono lavorare in modo efficiente e rimanere sempre al passo con il proprio lavoro da qualsiasi luogo.

Cosa puoi fare per evitarlo?

Per offrire una politica BYOD e mitigare i rischi, è necessario:

Controllare quali app sono autorizzate ad accedere ai dati aziendali

Assicurati di richiedere agli utenti di accedere ai dati di lavoro dalle app essenziali e configura politiche che mantengono i dati protetti (esempi includono la crittografia o la protezione dei dati con un codice PIN).

Impedire agli utenti di spostare i dati in un'app non protetta

Talvolta, gli utenti copiano e incollano il testo dalle e-mail aziendali nel proprio telefono o in un altro luogo non protetto. In alternativa, potrebbero salvare un foglio di calcolo dei dati dei clienti nell'archiviazione cloud personale (ad esempio Dropbox). Si consiglia di utilizzare una soluzione che impedisca loro di farlo.

Essere in grado di eliminare i dati aziendali da un dispositivo

In alcuni casi, è necessario eliminare i dati aziendali da remoto, ad esempio se un dispositivo viene perso o rubato, o se un dipendente lascia l'azienda. Scegli pertanto una soluzione che ti consenta di farlo senza influire sui dati personali sul dispositivo.

Insidia per la sicurezza n. 4: dati sensibili

Di cosa si tratta?

Nel nostro mondo ibrido e collaborativo, i file contenenti informazioni aziendali sensibili non rimangono all'interno delle quattro mura del tuo ufficio. I dipendenti possono scaricare un file su una chiavetta USB in modo da poterci lavorare a casa. Oppure potrebbero inviare informazioni finanziarie al tuo contabile.

Naturalmente, ci sono informazioni che non vuoi che siano esposte online. Che si tratti di dettagli sui clienti, trascrizioni di riunioni o registri finanziari, hai l'obbligo di proteggere i dati sensibili.

Qual è l'insidia?

Chiunque può essere in grado di scaricare un documento riservato e lasciare l'azienda. Devi quindi assicurarti che solo i dipendenti e gli ospiti invitati possano accedere a file o e-mail. Tuttavia, è più facile a dirsi che a farsi. Gestire ogni parte della sicurezza dei dati è un lavoro a tempo pieno. Per soddisfare tutte le tue esigenze in materia di sicurezza, dovrai gestire un catalogo di prodotti diversi.

È possibile utilizzare soluzioni di più fornitori per proteggere i dati sensibili, ma ciò presenta uno svantaggio: la protezione end-to-end può diventare molto complessa e dispendiosa in termini di tempo.

Cosa puoi fare per evitarlo?

Ecco cosa dovresti fare per gestire correttamente i dati sensibili in modo efficiente in termini di tempo:

Controllare l'accesso alla posta elettronica

Per assicurarti che solo il destinatario previsto di un'e-mail possa accedere alle informazioni, utilizza controlli come "Non inoltrare" o "Non stampare". Se vuoi realmente ottimizzare la sicurezza, puoi crittografare un messaggio di posta elettronica (inclusi eventuali allegati), in modo che solo il destinatario possa leggerlo. Ciò è particolarmente utile quando i dipendenti devono inviare dati sensibili a un partner o cliente al di fuori dell'organizzazione.

Controllare l'accesso a documenti e file

Alcuni file, ad esempio un foglio di calcolo contenente i nomi e le informazioni di contatto dei clienti, non possono finire nelle mani sbagliate. Ecco perché è necessario utilizzare una soluzione che consenta di limitare l'accesso ai file, controllare se i dipendenti possono modificare i documenti e impedirne la stampa.

Limitare l'accesso, anche se il file viene salvato all'esterno dell'azienda

Cosa succede se un dipendente invia un file tramite e-mail a qualcuno al di fuori dell'azienda o lo salva sul proprio PC? Devi sempre mantenere il controllo dei tuoi dati. Assicurati quindi che tutte le misure protettive e restrittive adottate siano valide sempre e ovunque.

Microsoft 365

INFORMATION WORKERS GROUP

È giunto il momento di gestire la tua attività in modo sicuro: passaggi successivi

Microsoft 365 è una soluzione completa e intelligente che consente ai dipendenti di essere creativi e di collaborare in modo sicuro nel mondo ibrido di oggi. Utilizzando l'intelligenza artificiale, identifica e protegge dalle minacce emergenti in tempo reale. Con Microsoft 365, puoi affrontare in modo semplice ed efficace le insidie discusse in questo e-book, abilitando un ambiente di lavoro ibrido sicuro.

Vuoi gestire la tua attività in modo sicuro sempre e ovunque?

Microsoft 365 ti consente di:

✔ **Proteggere i dispositivi**
Controlla quali dispositivi e utenti possono accedere alle informazioni aziendali, applica politiche di sicurezza per proteggere i dati su qualsiasi dispositivo e rimuovi i dati aziendali dai dispositivi persi o rubati.

✔ **Proteggere i dati aziendali**
Crittografa le e-mail sensibili, blocca la condivisione di informazioni sensibili (come i numeri delle carte di credito) e limita la copia e il salvataggio dei dati aziendali.

✔ **Utilizzare un antivirus avanzato**
Applica la protezione da malware su tutti i dispositivi, utilizzando funzionalità di gestione che forniscono informazioni dettagliate sulle minacce attive nel tuo ambiente.

✔ **Proteggersi dalle minacce informatiche**
Difenditi da allegati non sicuri, link sospetti, phishing e ransomware. La soluzione consente inoltre di rilevare malware negli allegati e-mail e abilitare l'autenticazione avanzata a più fattori.

✔ **Abilitare l'accesso remoto sicuro**
Consenti ai dipendenti di accedere in modo sicuro alle app aziendali da qualsiasi luogo, aiuta a proteggere da password perse o rubate e fornisci il giusto livello di accesso alle persone giuste tenendo a bada gli hacker.

Microsoft 365

Chi Siamo

Siamo un’azienda di IT consulting, Partner Gold Microsoft. Grazie all’esperienza maturata in oltre 15 anni di attività a supporto delle organizzazioni (aziende private e PA) e alla capacità di evolverci costantemente, forniamo soluzioni tecniche e organizzative per soddisfare le esigenze in termini di collaborazione, connessione e comunicazione all’interno dei moderni ambienti di lavoro.

Siamo parte di Altea Federation, con la quale condividiamo la necessità di dare seguito alla rivoluzione digitale ormai inevitabile, ridefinendo la collaborazione in ottica smart e l’ufficio, inteso come luogo fisico, evolutosi in digital workplace a forte personalizzazione. È il nostro Human Workplace.

IWG INFORMATION WORKERS GROUP

Viale Avignone, 94
00144 Roma
Mail: info@iwgroup.it
Tel: +39 0687450063