







Come proteggere la forza lavoro remota



GFITM

Aurea SMB Solutions

Indice

	Introduzione	3
<hr/>		
Problemi di sicurezza relativi al lavoro a distanza che gli amministratori informatici devono valutare		
	Aumento sostanziale della comunicazione online	4
<hr/>		
	Scansione e applicazione di patch a dispositivi remoti	5
<hr/>		
	Sicurezza della rete di casa	7
<hr/>		
	Salvataggio crittografato di tutti i dati	10
<hr/>		
	Quanto è difficile proteggere la forza di lavoro remota?	11
<hr/>		
	Proteggi la tua azienda con Senza Limiti Rete Sicura	12

Introduzione

La tua piccola impresa è cambiata in modi insospettabili. Anche se non opera in una località dove vige l'ordinanza di restare a casa, è necessario garantire la sicurezza dei tuoi dipendenti.

Di conseguenza, la tua attività potrebbe adesso operare parzialmente o completamente online.

Questo rende più complessa la necessità di mantenere la sicurezza di tutti i documenti e comunicazioni. I dispositivi di cui si serve la tua azienda potrebbero non trovarsi più esclusivamente nei vostri uffici.

Che fare adesso? Il tuo budget è ridotto al minimo. Non ci sono esperti informatici remoti tra i tuoi dipendenti. Nel tuo piano aziendale probabilmente non era previsto come garantire la sicurezza in caso di un evento catastrofico in cui tutti i dipendenti fossero costretti a restare a casa.

Molte aziende hanno iniziato la transizione al lavoro in remoto prima della pandemia da COVID-19. Per altri, questo significa che ci sono delle procedure consigliate consolidate e software efficienti in termini di costi per semplificare le operazioni e garantire la sicurezza aziendale.

Problemi di sicurezza relativi al lavoro a distanza che gli amministratori informatici devono valutare

Aumento sostanziale della comunicazione online

Ora che così tanta interazione e comunicazione si svolge online, è necessario garantire una solida sicurezza della posta elettronica e della comunicazione.

Mentre la sicurezza in video chat si basa generalmente solo sulla scelta del software con protezione dei dati personali più adatto alle tue esigenze, nel caso della posta elettronica le possibilità sono più sfumate. La posta elettronica deve essere tenuta al sicuro da numerose minacce, tra cui l'accesso non autorizzato o la perdita dei dati.

Le intrusioni attraverso la posta elettronica possono prendere la forma di phishing, spam o malware, con oggetti, contenuti, allegati o collegamenti ingannevoli che adescano gli utenti. È necessario avere a disposizione un servizio antispam completo associato alla formazione dei dipendenti sulla natura e l'aspetto di questi attacchi.

Gli attacchi di phishing mirati ai lavoratori in remoto probabilmente aumenteranno poiché i malintenzionati sanno che ci saranno sempre più lavoratori in questa nuova posizione potenzialmente meno protetta.

Si verificano numerosi attacchi ai lavoratori in remoto, oltre ad altri attacchi che possono avere un impatto finanziario, porre a rischio informazioni vitali e rendere l'azienda vulnerabile ad altri attacchi. I potenziali tentativi di hacking possono essere riconosciuti se gli utenti sanno cosa cercare. Offri un corso di aggiornamento ai dipendenti per metterli al corrente delle attuali truffe relative alla posta elettronica e phishing.



I malintenzionati possono ancora utilizzare la posta elettronica non protetta come punto di accesso alla rete. Per evitare ciò, bisogna assicurarsi che tutti abbiano una password complessa e che sia implementata l'autenticazione a più fattori (MFA).

Come pratica consigliata, la tua azienda dovrebbe anche valutare l'adozione di una soluzione di crittografia automatica della posta elettronica che analizzi il traffico di posta elettronica in uscita per riconoscere il materiale sensibile e crittografare i messaggi ritenuti sensibili.



Se stai già utilizzando un grande programma di posta elettronica basato su browser come Gmail, ogni messaggio di posta elettronica è già criptato con Transport Layer Security (TLS). Questo tipo di crittografia non è sicura come la crittografia end-to-end, quindi è comunque necessario utilizzare un servizio diverso per i dati sensibili. Se tutti nella tua azienda seguono i consigli sopra elencati per mantenere la sicurezza dei loro profili, evitando collegamenti malware e riconoscendo attacchi di phishing, le tue comunicazioni nell'ambiente di lavoro remoto dovrebbero essere protette.

Strumento/i necessari per questo problema di sicurezza

-  Antivirus con scansione della posta elettronica integrata
-  Strumenti di protezione da phishing e sicurezza Internet (generalmente integrati nel browser)

Pratiche consigliate

- Educare i tuoi dipendenti su tutti i comuni attacchi di phishing e spam
- Prestare molta attenzione a tutti i collegamenti e allegati inviati tramite posta elettronica, in particolare da mittenti sconosciuti
- Far rispettare correttamente le norme sulle password
- Implementare l'autenticazione a due fattori
- Utilizzare metodi di crittografia end-to-end, più sicuri per l'invio di dati sensibili



Scansione e applicazione di patch a dispositivi remoti

In circostanze normali, il tuo gruppo di lavoro informatico segue un calendario e una routine, emettendo immediatamente patch vitali e con tempi tali da inviare patch non vitali durante la notte o durante le ore non lavorative per ridurre le interferenze con il personale. Ora, la tua rete include dispositivi che non si trovano più solo in ufficio.

Per proteggere tutti coloro che lavorano da casa, è necessario un software che scansioni e applichi patch a tutti i dispositivi remoti. **Una violazione su tre** è causata da vulnerabilità prive di patch. Queste violazioni della sicurezza possono essere prevenute semplicemente assicurandosi che ai tuoi dispositivi siano applicate tutte le patch.

Questo è più difficile quando si passa al lavoro in remoto, ma non è impossibile. Ci sono opzioni software create proprio per questo scopo. Il tuo gruppo di lavoro informatico può seguire lo stesso piano di sicurezza applicato in ufficio con lievi modifiche. I dispositivi del tuo personale possono essere aggiornati e protetti, anche se sono remoti.

Strumento/i necessari per questo problema di sicurezza

- ✓ Monitor di rete
- ✓ Software di gestione remota

Pratiche consigliate

- Analizzare la tua rete e sviluppare un inventario completo. Effettuare regolarmente la scansione della rete per individuare patch mancanti
- Assicurarsi che tutti i sistemi operativi nella tua rete siano protetti (preoccupazione che non c'è quando non si lavora in remoto, ad esempio qualora tutti i dispositivi del tuo ufficio utilizzassero solo Windows)
- Pianificare il tempo necessario per inviare le patch, tenendo sempre presente gli aggiornamenti vitali che devono essere inviati immediatamente
- Eseguire un test dopo l'implementazione e prepararsi a ripristinare le patch che causano problemi finché non viene trovata una soluzione o viene emessa una nuova patch
- Identificare tutte le vulnerabilità con scansioni remote, anche quelle non dovute a patch mancanti



Sicurezza della rete di casa

Un altro passo importante per la protezione dei lavoratori in remoto è garantire che il loro sistema di sicurezza della rete di casa sia pronto e solido.

Crittografia dei dati in transito

Quando si lavora da casa, è importante che i dati dei lavoratori siano crittografati. Per garantire la riservatezza dei dati, tutti i lavoratori devono utilizzare una VPN a casa quando accedono a informazioni sensibili.

Una VPN fornisce un tunnel crittografato che protegge il tuo traffico web disconnettendosi dallo specifico indirizzo IP. Ciò garantisce alla tua azienda e ai dipendenti una maggiore riservatezza.

A seconda della tua VPN, i dipendenti possono porre a rischio la tua rete attraverso connessioni a dispositivi potenzialmente non protetti. È necessario assicurarsi che i dipendenti siano consapevoli di questo rischio e utilizzino la VPN solo quando accedono ai dati relativi al lavoro.

Wifi crittografato

Sebbene sia raro che un wifi personale venga compromesso, qualora si verificasse, l'attaccante può intercettare tutto ciò che viene inviato o inserito online: informazioni bancarie, profili di posta elettronica, credenziali di accesso aziendali e altro.

È necessario assicurarsi che la rete sia configurata correttamente e che la connessione sia crittografata. WPA2 oppure, oggi, WPA3 sono generalmente considerate le opzioni migliori per la crittografia wifi. È necessario anche assicurarsi che la parola chiave del wifi sia forte.

Modifiche al router

È necessario modificare l'accesso e la parola chiave del router. Gli standard predefiniti (come "admin") potrebbero essere deboli o facili da indovinare. I malintenzionati ne approfittano per prendere il controllo del router, trasformarlo in un bot o spiarti mentre le tue informazioni online vengono inviate attraverso il router. È necessario assicurarsi

che gli aggiornamenti del firmware vengano installati automaticamente per risolvere le vulnerabilità della sicurezza.

A seconda del livello di sicurezza richiesto dalla tua azienda, è possibile implementare altri passaggi aggiuntivi per limitare il traffico in entrata e in uscita ai dipendenti, selezionare il livello più alto di crittografia offerto nelle impostazioni del router e disattivare WPS. Questi passaggi sono complessi, quindi si consiglia di implementarli solo se assolutamente necessario.

Aggiustamenti del firewall

Ricontrollare le impostazioni del firewall per rafforzare la sicurezza della tua rete di casa. I firewall creano una barriera per prevenire le minacce che tentano di penetrare il sistema in due modi: impedendo a programmi dannosi di penetrare la tua rete e impedendo la fuoriuscita di dati dai dispositivi di casa.



In genere, i firewall sono già integrati nei tuoi dispositivi. È necessario assicurarsi che siano abilitati nelle tue impostazioni. Potrebbe risultare necessario per le piccole imprese un piano di sicurezza più completo tramite un fornitore terzo per rafforzare il firewall.





Implementare soluzioni antivirus per i dispositivi personali

Sebbene i dispositivi che si trovano in ufficio possano già disporre di protezioni antivirus, molti dipendenti ora utilizzano dispositivi personali che potrebbero invece non disporre. Anche seguendo le raccomandazioni precedenti, i dispositivi non adeguatamente protetti rappresentano un rischio significativo per la sicurezza.

È necessario assicurarsi che i computer che i tuoi dipendenti utilizzano a casa includano potenti protezioni antivirus. Date le circostanze, ciò potrebbe implicare l'acquisto di una protezione antivirus affidabile per i dispositivi dei tuoi dipendenti, quanto meno fintanto che devono accedere a dati aziendali private su di essi.

È fondamentale proteggere tutte le informazioni aziendali, inclusa la protezione dei dispositivi personali e la garanzia di aggiornamenti puntuali per queste soluzioni.

Strumento/i necessari per questo problema di sicurezza

-  VPN
-  Gestione della larghezza di banda
-  Migliori strumenti firewall
-  Protezione antivirus

Pratiche consigliate

- Utilizzare sempre una VPN con reti non affidabili
- Tenere presente le funzionalità relative alla larghezza di banda della VPN remota di un'azienda
- Scaricare la VPN remota della tua azienda solo sui dispositivi utilizzati per lavorare
- Assicurarsi che il metodo di autenticazione VPN e la crittografia siano il più potente possibile
- Monitorare costantemente le comunicazioni di rete in entrata e in uscita per rilevare attività sospette
- Impostare una parola chiave complessa per la rete wireless
- Utilizzare un router di proprietà personale anziché uno fornito dall'ISP e cambiare il nome utente e la parola chiave predefinita
- Utilizzare le funzionalità firewall più potenti a disposizione, tali che consentano comunque l'accesso a Internet come desiderato
- Implementare WPA2 o WPA3 sulla tua rete wireless
- Mantenere aggiornato il tuo router
- Mantenere aggiornata la tua protezione antivirus

Salvataggio crittografato di tutti i dati

I dati non sono adeguatamente protetti senza salvataggi regolari e crittografati. Questo è sempre vero, indipendentemente dal fatto che i tuoi dipendenti lavorino da casa, ma è ancora più importante quando si tratta di lavoratori in remoto.



C'è un minor controllo sui dispositivi dei lavoratori in remoto, quindi c'è mai la certezza che tutto sia perfettamente funzionante e protetto. Anche una cosa banale come versare caffè su un dispositivo potrebbe provocare la perdita di lavoro o dati, se il salvataggio non viene eseguito correttamente.

Un sistema ben protetto garantisce che tutti i dati aziendali vengano crittografati, caricati e salvati su una fonte centralizzata (spesso sul cloud, ma non necessariamente), eliminando il rischio di perdere importanti informazioni a causa di errori umani o attacchi.

Strumento/i necessari per questo problema di sicurezza

 Software di archiviazione abilitato alla crittografia

Pratiche consigliate

- Eseguire salvataggi frequentemente e regolarmente
- Crittografare i dati durante l'archiviazione
- Determinare per quanto tempo sia necessario conservare i dati salvati in base alla tua azienda e alle normative di conformità
- Valutare la possibilità di archiviare i dati più importanti in più di un luogo (assicurandosi che siano sempre crittografati e adeguatamente protetti)



Quanto e' difficile proteggere la forza di lavoro remota?

La maggior parte di quanto suggerito richiede piccole modifiche alle pratiche già in atto o in corso, come un servizio di gestione automatica delle patch o il salvataggio regolare dei tuoi dati.

Alcune modifiche potrebbero richiedere un adattamento iniziale, ma esistono molti prodotti per supportare le aziende che passano alla modalità di lavoro parzialmente o completamente in remoto. Seguendo alcune semplici pratiche consigliate e con l'aggiunta di alcuni necessari strumenti, la tua azienda e i tuoi dipendenti saranno in grado di lavorare in remoto e in sicurezza.



Proteggi la tua azienda con la gamma di soluzioni di sicurezza di GFI

Unlimited | Network Security

Sicurezza multilivello per prevenire e affrontare le minacce alla tua rete

Secure Network with **Firewall & Intrusion Prevention**

Secure Traffic with **Web & Email Antivirus**

Secure Endpoints with **Vulnerability Monitoring & Patching**

[Scopri di più](#)



Aurea SMB Solutions

Tutti i nomi di prodotti e le società citati possono essere marchi o marchi registrati dei rispettivi proprietari. Tutte le informazioni contenute in questo documento erano valide al meglio delle nostre conoscenze al momento della pubblicazione. Le informazioni contenute in questo documento possono essere modificate senza preavviso.