Identificazione dei requisiti di sicurezza per il supporto di una forza lavoro remota su larga scala

Progettazione di un programma di telelavoro sicuro

Sommario

Panoramica preliminare

Le organizzazioni devono supportare il telelavoro come componente del loro piano di Business Continuity, che richiede la capacità di passare rapidamente a una forza lavoro parzialmente o totalmente remota. In questo modo, l'organizzazione deve confrontarsi con nuove problematiche di rete e di sicurezza, poiché la rete aziendale viene utilizzata in modo decisamente diverso dai dipendenti in loco.

Proteggere una forza lavoro remota richiede l'identificazione e la distribuzione di soluzioni di sicurezza che soddisfino le esigenze dei dipendenti e della rete della sede centrale. La maggior parte dei dipendenti ha bisogno solo di un accesso sicuro alla rete aziendale e alle applicazioni basate su cloud, e tutto questo richiede accesso VPN e autenticazione a più fattori (MFA, Multi-Factor Authentication). Gli amministratori di rete e i dirigenti possono avere requisiti di rete aggiuntivi, come la connettività persistente e una soluzione di telefonia sicura. La rete della sede centrale dell'organizzazione deve anche essere in grado di supportare e proteggere le connessioni di rete provenienti dalla stragrande maggioranza della forza lavoro di un'organizzazione, richiedendo una robusta autenticazione degli utenti e una sicurezza perimetrale avanzata.

Introduzione

La capacità di supportare i telelavoratori può contribuire a migliorare il piano di Business Continuity di un'organizzazione. Consente all'organizzazione di adattarsi quando circostanze impreviste, come disastri naturali o pandemie, impediscono ai dipendenti di lavorare in loco.

In queste circostanze, un'organizzazione può essere costretta a passare rapidamente a una forza lavoro per lo più o totalmente remota. Quando si progetta o si implementa una soluzione di telelavoro, è importante considerare non solo i requisiti di rete, ma anche le ulteriori problematiche di sicurezza create dal lavoro a distanza.

Soddisfare i requisiti di base del telelavoro

I dipendenti possono avere requisiti diversi del loro ambiente di lavoro a distanza. Tuttavia, i telelavoratori hanno una serie di requisiti di base per garantire una connessione sicura e autenticata alla rete aziendale. Questi includono l'accesso a rete VPN (Virtual Private Network) e una soluzione di autenticazione avanzata per proteggere gli account da violazioni.

VPN

Durante il telelavoro, un dipendente tratta i dati riservati dell'azienda sulla sua rete domestica. Proteggere tali dati da violazioni richiede la capacità di garantire che la connessione di un telelavoratore alla rete aziendale sia sicura.

I telelavoratori devono avere accesso a una VPN che fornisca una connettività diretta e crittografata tra il proprio dispositivo e la rete aziendale, proteggendo non solo la riservatezza e l'integrità dei dati aziendali in transito, ma garantendo anche che tutto il traffico tra il dipendente e la rete Internet pubblica sia monitorato e protetto dall'infrastruttura di sicurezza informatica esistente dell'organizzazione.

Autenticazione a più fattori

Con i dipendenti che lavorano da casa, vi è una maggiore probabilità che le credenziali di accesso eventualmente sottratte, combinate con l'accesso a un dispositivo non presidiato, possano consentire l'accesso non autorizzato all'account di un utente. In queste situazioni, molte delle funzioni utilizzate per rilevare schemi di accesso anomali, come il luogo e l'ora del tentativo di autenticazione, potrebbero non essere applicabili in quanto gli schemi di lavoro dei dipendenti cambiano a causa del telelavoro.

La sicurezza dell'accesso alla rete aziendale, alle risorse e ai dati richiede una soluzione di autenticazione più robusta rispetto ai nomi utente e alle password tradizionali. A tutti i telelavoratori dovrebbe essere rilasciato un token di autenticazione sicura. Le opzioni per i token MFA includono dispositivi fisici come una chiave elettronica o soluzioni software-based, ad esempio un'applicazione mobile, che possono essere utilizzate per verificare l'identità di un utente prima che possa avviare una connessione VPN alla rete aziendale o accedere ad altre risorse aziendali riservate.

Le direttive PCI DSS per il telelavoro richiedono che i dipendenti che accedono ai dati di titolari di carte di credito effettuino l'autenticazione tramite una VPN e utilizzino l'autenticazione a più fattori.[1]

Supportare i power user remoti

Sebbene a molti telelavoratori possa bastare una connessione VPN e un token MFA, altri hanno requisiti aggiuntivi. I power user, compresi gli amministratori di rete e i dirigenti, hanno bisogno di un ufficio remoto più avanzato per svolgere le proprie mansioni. È possibile che tali utenti abbiano bisogno di una connettività persistente alla rete aziendale e di una soluzione di telefonia sicura.

Connettività persistente

Alcuni utenti, come gli amministratori di rete e il personale di sicurezza, richiedono un accesso più flessibile e persistente alla rete aziendale. Tali dipendenti possono avere più dispositivi che devono essere collegati alla rete aziendale o richiedono una connettività di lunga durata non limitata da timeout di sessione automatici.

Le esigenze dei power user che lavorano da un ufficio domestico possono essere soddisfatte con la distribuzione di un access point wireless, che può fornire un tunnel VPN attendibile alla rete aziendale. Al fine di garantire una connessione sicura, questo acces point wireless deve essere combinato con un Next-Generation Firewall (NGFW) basato su desktop per fornire l'ispezione del traffico, la gestione degli accessi e Advanced Threat Protection.

Telefonia sicura

Quando si lavora da remoto, è essenziale che i membri del personale, soprattutto i dirigenti, abbiano accesso a una soluzione di telefonia sicura per proteggere le comunicazioni e i dati aziendali riservati. In caso contrario, si corre il rischio di esporre i dati riservati a causa di intercettazioni su reti cellulari o dell'utilizzo di applicazioni mobili dannose.

Un modo efficace per fornire telefonia sicura ai lavoratori fuori sede è quello di sfruttare le comunicazioni VoIP (Voice-over-IP). Se un utente dispone già di accesso a una connessione Internet sicura, persistente e attendibile, l'instradamento del traffico vocale su questa connessione richiede un overhead aggiuntivo minimo. In questo modo, l'organizzazione può monitorare il traffico vocale ed eseguire un'analisi del perimetro della rete alla ricerca di contenuti potenzialmente dannosi destinati a sfruttare applicazioni software VoIP vulnerabili.

Le soluzioni di telefonia per i telelavoratori devono fornire loro tutte le caratteristiche dei loro telefoni aziendali in loco. In questo modo, è possibile ridurre al minimo la probabilità che i lavoratori utilizzino dispositivi personali per le comunicazioni aziendali. Le opzioni importanti includono la possibilità di effettuare e ricevere chiamate, accedere alla segreteria telefonica, controllare la cronologia delle chiamate e accedere alla rubrica dell'organizzazione.

Il 72% di una giornata lavorativa di un CEO è composta principalmente da riunioni. È quindi necessario rendere le telecomunicazioni sicure per i loro uffici remoti.[2]

Sicurezza e stabilità degli headend

Le soluzioni di sicurezza per una forza lavoro remota non si limitano al lato client. Un numero crescente di telelavoratori introduce nuove minacce alla sicurezza e nuovi requisiti di rete anche presso la sede centrale dell'organizzazione.

Quando si pianifica un programma di telelavoro per garantire la Business Continuity, è necessario assicurarsi che la rete della sede centrale sia in grado di autenticare gli utenti e i dispositivi che tentano di accedervi da remoto e di gestire e proteggere un numero molto maggiore di connessioni VPN in entrata.

Autenticazione di utenti e dispositivi

Un modello di sicurezza zero-trust è molto importante quando un'organizzazione supporta una forza lavoro per lo più o totalmente remota. I dipendenti possono tentare di connettersi alla rete aziendale utilizzando dispositivi sconosciuti o personali, e i sistemi collegati a reti non attendibili hanno una maggiore probabilità di essere compromessi dai criminali informatici.

La protezione della rete dell'organizzazione e dei dati e delle risorse riservati in essa contenuti richiede la capacità di autenticare gli utenti e i dispositivi che tentano di connettersi ad essa. A tale scopo, è possibile utilizzare un server di autenticazione centralizzato con connettività al servizio Active Directory dell'organizzazione: LDAP (Lightweight Directory Access Protocol) e RADIUS (Remote Authentication Dial-In User Service).

Questo server deve essere in grado di scalare per soddisfare le esigenze di una forza lavoro remota più consistente senza ostacolare la produttività degli utenti. Il supporto di SSO (Single Sign-On), la gestione dei certificati e la gestione degli ospiti garantiscono inoltre l'autenticazione degli utenti senza creare un carico significativo per i telelavoratori.

Protezione del perimetro di rete

Una differenza tra una forza lavoro in loco e una forza lavoro remota è il numero di connessioni VPN che un'organizzazione deve essere in grado di gestire. I dipendenti in loco sono collegati direttamente alla LAN aziendale, mentre i telelavoratori devono inviare tutto il loro traffico su una connessione VPN. Il firewall NGFW di un'organizzazione deve essere in grado di terminare tutte le connessioni VPN ed eseguire l'ispezione di un gran numero di connessioni di rete crittografate. Poiché l'ispezione del traffico crittografato è costosa da un punto di vista di elaborazione, è fondamentale che il firewall NGFW di un'organizzazione sia in grado di soddisfare la domanda. A tale scopo, sono necessari firewall NGFW con processori di sicurezza avanzati dedicati, che riducono al minimo la latenza e aumentano la produttività al massimo, prevenendo colli di bottiglia della rete che possono peggiorare significativamente la produttività dei dipendenti.

I firewall NGFW a livello headend devono anche eseguire l'ispezione del livello 7 di tutto il traffico. Tale aspetto è importante in qualsiasi contesto aziendale, ma con una forza lavoro remota un'organizzazione può aspettarsi una maggiore concentrazione di contenuti dannosi sulle connessioni in entrata da parte dei telelavoratori. Ciò è dovuto al fatto che i dispositivi dei dipendenti collegati alle reti personali hanno una maggiore probabilità di essere infettati da malware, che può tentare di spostarsi lateralmente attraverso di essi verso la rete aziendale. Un firewall NGFW di livello 7 può identificare l'applicazione che un pacchetto in entrata sta tentando di raggiungere e bloccare i pacchetti da applicazioni con vulnerabilità note. I firewall NGFW headend devono anche essere integrati con funzionalità di sandboxing per analizzare in modo sicuro i contenuti sospetti che non possono essere associati ad alcuna minaccia nota.

L’ispezione di TLS (Transport Layer Security)/SSL (Secure Sockets Layer) riduce in media del 60% il throughput del firewall.[3]

Conclusioni

Quando si passa al telelavoro in modo rapido e massiccio, è essenziale che un'organizzazione non sia solo in grado di sostenere le operazioni, ma anche di garantire la sicurezza dei telelavoratori e dei dati riservati da essi trattati.

A tale scopo, è necessario che un'organizzazione distribuisca soluzioni di sicurezza sia presso le postazioni di lavoro remote dei telelavoratori che sulla rete aziendale principale. In questo contesto, è necessario scegliere soluzioni in grado di soddisfare i requisiti infrastrutturali univoci e i problemi di sicurezza associati a una forza lavoro remota. Durante una situazione di emergenza, quando è necessaria una risposta immediata, la selezione di una soluzione che possa essere distribuita in tutta semplicità e rapidità garantisce un impatto minimo sulle operazioni aziendali.

[1] Emma Sutcliffe, "How the PCI DSS Can Help Remote Workers", PCI Security Standards Council, 26 marzo 2020.

[2] Michael E. Porter e Nitin Nohria, "How CEOs Manage Time", Harvard Business Review, luglio 2018.

[3] "NSS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports", NSS Labs, 24 luglio 2018.

www.fortinet.com

628535-0-0-IT

settembre 8, 2020 1:23 PM

ebook-teleworker-solutions