WHITE PAPER

Principali considerazioni per l'implementazione del telelavoro sicuro su larga scala

Identificazione dei rischi per la sicurezza e dei requisiti avanzati di una forza lavoro remota

Sintesi preliminare

La capacità di far passare rapidamente la forza lavoro di un'organizzazione al telelavoro è una componente essenziale di un piano di Business Continuity. Tuttavia, i telelavoratori creano requisiti di sicurezza aggiuntivi e problematiche di sicurezza diversi rispetto ai dipendenti in loco.

I telelavoratori spesso si collegano alla rete aziendale tramite reti non protette o inattendibili, consentendo potenziali intercettazioni e l'utilizzo dei dispositivi in aree non protette, dove possono essere smarriti o sottratti. Gli utenti avanzati possono avere requisiti che non possono essere soddisfatti da un client VPN (Virtual Private Network) standard.

Al di là di questi requisiti di base, i telelavoratori possono utilizzare dispositivi non attendibili per accedere alle risorse aziendali ed è più probabile che cadano in preda all'ingegneria sociale durante una crisi, creando maggiori rischi per la sicurezza. Inoltre, questi dipendenti devono essere in grado di accedere alle risorse basate su cloud senza una latenza di rete significativa. È per via di questi requisiti più avanzati che i controlli di sicurezza di base non offrono una sicurezza adeguata per una forza lavoro remota.

Il 54% dei professionisti IT ritiene che i telelavoratori rappresentino un maggiore rischio per la sicurezza rispetto al personale in loco.[1]

Solo il 74% delle aziende richiede una VPN per i telelavoratori.[2]

Introduzione

Il piano di Business Continuity di ogni organizzazione deve includere la capacità di far passare rapidamente la maggior parte o tutta la forza lavoro al telelavoro. Disastri naturali, pandemie o attacchi terroristici sono solo alcuni degli eventi che possono renderlo necessario.

Una transizione sicura e senza problemi dal "business as usual" in ufficio a una forza lavoro completamente remota richiede una pianificazione e un'attenta considerazione delle esigenze dei telelavoratori, come l'accesso alle risorse di rete, un'ampia larghezza di banda e il supporto tecnico. La transizione amplifica anche i rischi per la sicurezza del telelavoro, a causa delle vulnerabilità della rete domestica e dei dispositivi personali, nonché le sfide della supervisione e dell'applicazione di una buona integrità informatica.

Problematiche correlate a connettività e produttività sicure

Il primo passo di una strategia di telelavoro sicuro è garantire che i telelavoratori abbiano la possibilità di connettersi alla rete aziendale in tutta sicurezza. Le problematiche si presentano sia nella sicurezza della connettività remota che nel mantenimento della produttività dell'utente attraverso la connessione remota. Queste hanno a che fare con le reti domestiche, gli utenti stessi e le apparecchiature di rete dell'ufficio aziendale.

Le reti domestiche sono vulnerabili

Per i dipendenti, il modo più semplice per connettersi all'impresa è tramite la loro rete domestica e le connessioni Internet pubbliche. La rete domestica del dipendente, tuttavia, è probabilmente meno sicura della rete aziendale, il che la rende più vulnerabile agli attacchi.

Il traffico tra il telelavoratore e la rete aziendale potrebbe essere intercettato, e potenzialmente modificato, da un intercettatore. Inoltre, il traffico di rete che non passa attraverso la rete aziendale non è protetto dalle soluzioni di sicurezza in loco di un'organizzazione, rendendole più vulnerabili al malware.

I telelavoratori possono non essere chi sembrano

In circostanze normali, molte organizzazioni si basano su un modello di sicurezza basato sul perimetro. Secondo questo modello, chiunque all'interno della rete è considerato attendibile, mentre i soggetti esterni sono potenzialmente malintenzionati. In questo modo, l'organizzazione ha la possibilità di identificare i tentativi di connessione anomali in base alla posizione e alla data/ora di connessione (poiché la maggior parte dei lavoratori opera durante il normale orario di lavoro).

Con una forza lavoro completamente remota, questo modello tradizionale non è più applicabile in quanto sia gli utenti legittimi che le potenziali minacce si collegano a risorse esterne alla rete e possono lavorare in orari disparati. Inoltre, quando i dipendenti lavorano da remoto, la probabilità che un utente non autorizzato abbia accesso e controlli i dispositivi di un dipendente è maggiore.

Gli headend VPN non sono scalabili

In situazioni di "business as usual", molte organizzazioni sono sprovviste di prassi consolidate di telelavoro. Infatti, solo il 41% delle aziende consente il telelavoro.[3] Di conseguenza, molte organizzazioni non dispongono delle infrastrutture necessarie per supportare una forza lavoro completamente o prevalentemente remota.

In circostanze normali, una percentuale significativa del traffico di un utente è interna alla rete, accedendo a condivisioni di file, database e altre risorse interni. Tuttavia, quando i dipendenti lavorano da remoto, tutto il loro traffico passa attraverso i firewall perimetrali, aumentando il carico su questi dispositivi.

L'uso di VPN non fa che aggravare questo problema. La crittografia e la decrittografia del traffico VPN è costosa da un punto di vista di elaborazione e può esaurire rapidamente le risorse della CPU di un Next-Generation Firewall (NGFW).

Il telelavoro a taglia unica non funziona

Per il lavoratore generico, una connessione sicura alla rete aziendale e alle risorse basate su cloud è sufficiente per svolgere le proprie mansioni. Tuttavia, alcuni dipendenti hanno ulteriori esigenze quando lavorano a distanza.

I power user, ad esempio gli amministratori di rete e il personale di sicurezza, richiedono una connettività persistente alla rete. Questi utenti possono richiedere la possibilità di connettere più dispositivi alla rete, che può essere difficile da gestire manualmente tramite client VPN, o connessioni che durano più a lungo della durata di timeout delle sessioni standard dei client VPN.

I super user, compresi i dirigenti e gli altri responsabili, trattano normalmente dati estremamente riservati e devono essere in grado di farlo anche lavorando a distanza. Questi dipendenti richiedono un livello di protezione più elevato rispetto a quello fornito dalla maggior parte dei client VPN.

Applicazione delle policy di sicurezza informatica in una crisi

Al di là delle esigenze basilari di una forza lavoro remota, il telelavoro crea ulteriori problemi di sicurezza a un'organizzazione. Tra questi si annoverano l'uso di dispositivi non sicuri per il lavoro, una maggiore probabilità di incidenti di sicurezza durante una crisi e la necessità dei telelavoratori di accedere in modo efficiente alle applicazioni basate su cloud.

La risposta agli incidenti è più complessa per i telelavoratori

Le situazioni che costringono un'organizzazione a passare a una forza lavoro remota sono spesso caotiche ed emotivamente complesse per i dipendenti. In genere, gli esseri umani sono inclini a prendere decisioni di sicurezza sbagliate in queste situazioni e i criminali informatici fanno spesso leva su questi sentimenti per sferrare i loro attacchi.

Nei periodi di crisi, è più probabile che i dipendenti siano vittime di attacchi di phishing e che un'organizzazione sia meno preparata a rispondere agli incidenti. Con una forza lavoro remota, l'assistenza tecnica in genere non ha una disponibilità immediata per un dipendente e i piani di risposta all'incidente di un'organizzazione potrebbero non coprire gli imprevisti in cui un telelavoratore subisca un incidente di sicurezza. Di conseguenza, il costo per l'organizzazione, sia in termini di produttività dei dipendenti che di sforzi di risoluzione, può essere molto più alto in situazioni in cui il telelavoro diventa la norma.

I telelavoratori potrebbero non disporre di patch di sicurezza essenziali

Le organizzazioni sprovviste di prassi consolidate di telelavoro spesso non sono dotate di dispositivi di proprietà dell'azienda in grado di supportare una forza lavoro completamente remota. Di conseguenza, i dipendenti che lavorano da casa possono utilizzare dispositivi non approvati, compresi laptop o tablet personali.

Solo il 15% delle organizzazioni ha completato la transizione verso un modello di sicurezza a zero-trust, che non considera automaticamente attendibile chiunque all'interno del perimetro della rete.[4]

Il 75% dei professionisti IT ritiene che il rischio di violazione dei dati sia maggiore per i telelavoratori.[5]

Il protocollo RDP (Remote Desktop Protocol), utilizzato dagli amministratori di sistema per la gestione dei dispositivi remoti, è il principale vettore di infezione del ransomware nel 70–80% dei casi.[6]

Il 42% dei computer remoti riceve le patch di sicurezza entro tre giorni, rispetto al 48% delle macchine in loco.[7]

La capacità di far rispettare le policy BYOD (Bring-your-Own-Device) è essenziale quando i dipendenti lavorano da casa. I dispositivi utilizzati dai telelavoratori hanno storicamente una percentuale di patch inferiore rispetto ai dispositivi in loco, anche se tutti i dispositivi sono di proprietà dell'azienda.[8] Questi ritardi nell'applicazione delle patch possono rivelarsi costosi, poiché il 60% delle violazioni dei dati è causato da una vulnerabilità per la quale era disponibile un patch che non è stata correttamente applicata.[9] Un'organizzazione deve essere in grado di eseguire analisi prima della connessione per garantire la conformità delle patch e che i telelavoratori non espongano la rete aziendale a ulteriori rischi informatici.

I telelavoratori richiedono un accesso al cloud efficiente e sicuro

Quando i dipendenti lavorano in loco, la sicurezza delle loro connessioni alle risorse basate su cloud utilizzando dispositivi di sicurezza in loco è logica, poiché il traffico è già convogliato nel perimetro della rete. Tuttavia, i telelavoratori si collegano dall'esterno della rete con il traffico correlato al cloud.

Il backhauling del traffico correlato al cloud dei telelavoratori verso la rete aziendale per le analisi di sicurezza aumenta la latenza della rete, creando potenziali problemi in termini di prestazioni per le applicazioni Software-as-a-Service (SaaS) sensibili alla latenza, oltre ad avere un impatto negativo sulla produttività dei telelavoratori.

Man mano che le organizzazioni si affidano sempre più alle soluzioni SaaS nelle attività di telelavoro, diventano un bersaglio più vulnerabile per i criminali informatici. Configurazioni errate nelle policy di sicurezza e nelle impostazioni di configurazione delle applicazioni SaaS potrebbero causare una violazione dei dati o consentire ai criminali informatici di utilizzarle come vettore di infezione per il malware.

Il 62% delle aziende consente l'utilizzo dell'approccio BYOD per i telelavoratori.[10]

Le organizzazioni che distribuiscono rapidamente soluzioni basate su cloud per supportare il telelavoro hanno maggiori probabilità di configurare erroneamente le impostazioni di sicurezza.[11]

La sicurezza di base del telelavoro non è sufficiente

Il passaggio della maggior parte o di tutti i dipendenti di un'organizzazione al telelavoro crea notevoli problemi di sicurezza. Il piano di Business Continuity di un'organizzazione dovrebbe tenere conto di queste problematiche e includere soluzioni per affrontare questi nuovi rischi.

La distribuzione di controlli di sicurezza di base per il telelavoro, come la connettività VPN e l'autenticazione dei super user, consente a un'organizzazione di supportare il telelavoro intermittente di una parte dei suoi dipendenti. Tuttavia, la Business Continuity suggerisce che un'organizzazione deve essere in grado di mantenere i normali livelli di produttività e sicurezza con una forza lavoro per lo più o totalmente remota. Per raggiungere questo obiettivo, è necessario garantire la sicurezza dell'endpoint e assicurare un accesso ad alta velocità e affidabile alle applicazioni SaaS più importanti.

[1] "Remote Work Is the Future—But Is Your Organization Ready for It?", OpenVPN, visitato il 29 aprile 2020.

[2] Ibid.

[3] "The Modern Workplace: People, Places & Technology", Condeco, maggio 2019.

[4] "2019 Zero Trust Adoption Report", Cybersecurity Insiders, novembre 2019.

[5] "Data Protection Report 2019", Shred-it, 17 giugno 2019.

[6] Lawrence Abrams, "FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips", Bleeping Computer, 27 febbraio 2020.

[7] Robert Lemos, "Patching Poses Security Problems with Move to More Remote Work", Dark Reading, 31 marzo 2020.

[8] Ibid.

[9] "Costs and Consequences of Gaps in Vulnerability Response," ServiceNow e Ponemon Institute, 29 ottobre 2019.

[10] "Remote Work Is the Future—But Is Your Organization Ready for It?," OpenVPN, visitato il 29 aprile 2020.

[11] Liam Tung, "Microsoft Office 365: US issues security alert over rushed remote deployments", ZDNet, 30 aprile 2020.

FORTINET

www.fortinet.com

settembre8,20201:40PM

668978-0-0-IT

D:\Crystal Page\Projekty 2020\Argos\Assignment A-359635-1115275\Work\clean\it-IT\Zero Trust Network Access\WP_Key Considerations for Implementing Secure Telework at Scale\wp-teleworker-A4