I consigli di un hacker su come proteggere le reti VPN collegandosi da remoto

Author : Redazione

Date : 10 Aprile 2020

In questo momento di emergenza sanitaria, rispettare le normative è fondamentale ed un gran numero di aziende si è dovuto adattare sperimentando per i propri dipendenti la modalità di lavoro da casa. Mentre i **responsabili delle risorse umane e quelli finanziari** stanno avendo numerose difficoltà a capire come gestire la situazione dei vari dipendenti, tra cui PTO e i relativi benefici per chi è in malattia, i responsabili delle aziende stanno facendo i salti mortali per capire come avere a disposizione il più alto numero di dipendenti e come gestirli dai loro **nuovi uffici domestici**, tenendo conto di come siano sostanzialmente mal equipaggiati.

Anche se alcune aziende sono preparate per affrontare **problematiche anche importanti**, sono ben poche le organizzazioni che sanno esattamente come gestire tutto ciò che deriva da una simile pandemia mondiale. Di conseguenza, dai vertici dell'azienda è abbastanza facile intuire come arrivi una sola direttiva, ovvero quella di **far lavorare da remoto i vari dipendenti**. È vero, però, che il passaggio dall'ufficio normale a quello domestico deve essere fatto con grande cura, oppure la situazione potrebbe peggiorare in men che non si dica, aspettando ovviamente la fase 2 della ripresa, durante la quale alcune aziende e fabbriche potrebbero riaprire seguendo condizioni specifiche di sicurezza.

Una forte pressione sulle aziende

C'è ovviamente una **grande pressione** che porta a dover prendere decisioni nel più breve tempo possibile, ma è fondamentale assicurarsi di agire evitando che la curva di rischio aumenti, altrimenti il proprio business potrebbe finire in un tunnel senza luce, lasciando campo libero ai propri competitor. Come reagire quindi? In modo sicuro, con **azioni metodiche, mirate e ben determinate**. Ed ecco che uno dei problemi principali da risolvere è quello di capire come proteggere adeguatamente le reti aziendali. Ci sono strategie adatte? In che modo si collegheranno i dipendenti? Scopriamone insieme alcune.

Come lavorare da remoto in sicurezza

Quindi, quello che ogni azienda deve chiedersi è come poter controllare la concorrenza,

gestendo comunque la sopravvivenza della propria realtà. Ecco i passi che si dovrebbe seguire o da cui trarre ispirazione.

Il primo passo è chiaramente quello di ottenere il buy-in delle parti coinvolte per puntare su un **approccio che sia equilibrato e metodico**, in modo tale da gestire nel migliore dei modi il rischio nel passaggio verso un ambiente di lavoro che inevitabilmente funziona da remoto. Meglio prendere tutte le dovute precauzioni piuttosto che ritrovarsi problematiche che derivano dal fatto di aver sottovalutato qualche rischio. Tutte le parti coinvolte in tale processo devono essere informate e messe a conoscenza dei rischi di spostare tutti su una VPN, chiedendo loro di stabilire delle priorità sulle azioni e sui gruppi che hanno urgenza e, invece, quanti possono comunque aspettare ancora un po'. Di conseguenza, è chiaro che avere a disposizione una guida alle Virtual Private Network (VPN) da inviare ai propri dipendenti è un'ottima soluzione, soprattutto per chi non ha grandissima esperienza con un utilizzo costante in situazioni di emergenza.

Dopo aver messo le mani su tale buy-in, bisogna concentrarsi su come risolvere le vulnerabilità note della VPN. Esistono sempre dei punti deboli e delle problematiche su cui gli hacker possono fare presa per infiltrarsi pericolosamente nella rete aziendale. Per questo motivo, le aziende devono concentrarsi il più possibile su alcuni temi di base.

Come in qualsiasi altro scenario critico, è fondamentale ottenere una VPN, ma ricordandosi ad esempio di cambiare la password predefinita. La **segmentazione della rete** è un altro passo importante in ottica protettiva. Se gli utenti effettuano il remoting su un pc desktop non hanno di sicuro la necessità di eseguire l'accesso ad un database oppure a delle infrastrutture back-end.

Lo standard dovrebbe essere considerato il **privilegio minimo**. Con ogni probabilità, giusto per fare un esempio, un marketer non ha la necessità di eseguire l'accesso all'infrastruttura.

Visibilità e controlli. Nel momento in cui le credenziali che vengono usate da parte di un dipendente sono compromesse, allora c'è l'intenzione di prevenire certe situazioni e svolgere tutti i possibili controlli che si possono mettere in atto.

L'educazione dei dipendenti. Tutto passa anche dal trasmettere le giuste informazioni ai dipendenti dell'azienda che lavorano da remoto: è fondamentale, infatti, che capiscano alla perfezione quelli che sono i nuovi rischi ed evitare operazioni inutili che potrebbero creare problematiche ben più gravi.

Ottenendo il blocco dei privilegi, la segmentazione di base e una certa visibilità, quantomeno ci sono possibilità maggiori che il proprio team abbia la capacità di tagliar fuori potenziali azioni di malintenzionati. Ovviamente, visto che si tratta di una situazione veramente estrema, anche le misure di sicurezza devono esserle. Le reti VPN sono fondamentali, ma vanno usate in modo corretto. La continuità dell'attività aziendale può necessitare dei compromessi per quanto concerne particolari procedure di sicurezza, ma è sempre meglio fare in modo che la sicurezza della propria organizzazione venga preservata, riducendo il più possibile i vari rischi.