LINEE GUIDA PER IL LAVORO DA REMOTO PER PMI

Checklist di controllo per la sicurezza dell'accesso remoto per ogni IT manager

Quando si verifica una perturbazione nella società, abilitare un'opzione per il lavoro da casa è essenziale per la continuità aziendale. Ma nello sforzo di mantenere produttivi i lavoratori e mandare avanti il business, la messa a disposizione in modo frettoloso di un'opzione di lavoro remoto può rendere la propria organizzazione vulnerabile in termini di sicurezza. Se c'è una cosa che di cui siamo a conoscenza sui criminali informatici, è che non esitano a cogliere qualunque opportunità. Utilizza questa checklist di controllo dettagliato per aiutare a proteggere la propria forza lavoro indipendentemente dalla sua posizione.

- [ ] **Irrigidire le proprie politiche sulle password**
  Se si è stati permissivi su questo punto, ora è il momento di rafforzare le policy. Richiedere password lunghe (o meglio ancora, frasi-chiave, imporre modifiche regolari e bloccare gli account dopo un determinato numero di accessi non riusciti. Spiegare ai dipendenti che non possono riutilizzare le password di lavoro per nessuno dei propri accessi personali.

- [ ] **Richiedere autenticazione a più fattori (MFA)**
  Conosciuta anche come autenticazione a due fattori (2FA), questa è in assoluto la migliore difesa contro crimini informatici che usano tecniche coercitive, password-spray attack o credenziali rubate acquistate sul dark web per mascherarsi come dipendenti e infiltrarsi nelle reti aziendali. Se vengono utilizzate posta elettronica, suite di produttività o altre applicazioni basate su cloud, è necessario attivare la MFA se è disponibile. Se gli utenti devono accedere alla rete interna, occorre mettere in campo una soluzione MFA.

- [ ] **Richiedere una VPN per accedere alla rete interna**
  Una VPN crittografa il proprio traffico aziendale mentre attraversa la rete Internet pubblica in modo da non poter essere spiato. Inoltre, una connessione VPN consente al team IT di estendere ai dispositivi remoti una gamma più ampia di soluzioni di sicurezza della rete interna. Se per alcuni lavoratori si sta già utilizzando una VPN, è necessario assicurarsi di disporre di licenze e capacità sufficienti per coprire i nuovi utenti. Se i dipendenti accederanno alle risorse sulla rete interna, la combinazione di VPN e MFA è indispensabile.

- [ ] **Se possibile, utilizzare un'interfaccia di desktop virtuale**
  Con questo tipo di soluzione, il dipendente accede a una macchina virtuale che si trova nel cloud o nel data center aziendale e la controlla da remoto. Può essere configurata per apparire esattamente come un sistema di ufficio. Il vantaggio è che i dati o i file sensibili esistono solo sulla macchina virtuale e non sono mai residenti nel sistema domestico del dipendente.

- [ ] **Ricordare ai lavoratori di essere consapevoli della rete e di diffidare del Wi-Fi**
  Una cosa che è completamente fuori dal controllo aziendale è la loro rete domestica e altri dispositivi che si connettono ad essa. Specificare di disattivare qualsiasi tipo di file-sharing sul sistema che useranno per lavoro e di controllare il loro router di casa o l'access point Wi-Fi per essere sicuri che la sicurezza WPA2 sia abilitata. Ricordare loro di non collegarsi mai a un access point Wi-Fi non protetto o aperto che non richieda una chiave di sicurezza.

Investire nella sicurezza completa degli endpoint per i lavoratori a domicilio

Non ci si può fidare che l'antivirus fornito con un sistema domestico o un dispositivo personale sia all'altezza della situazione. Una soluzione completa protegge da ogni tipo di minaccia con molteplici livelli di difesa, incluso un firewall personale, protezione da siti Web malevoli e protezione da malware su unità USB portatili. L'opzione migliore in questo caso è una suite di sicurezza endpoint di livello aziendale che il reparto IT possa gestire da remoto.

Richiedere la crittografia quando i dipendenti lavorano su file sensibili

Se i dipendenti scaricano file aziendali sui propri dispositivi personali, fornire loro una soluzione di crittografia. Insistere sul fatto che mantengano i propri file personali separati dai documenti aziendali e salvino i documenti aziendali in una cartella crittografata. Inoltre, applicare una politica che salvi i documenti revisionati nell'archivio dati aziendali, in modo da non doversi preoccupare del backup remoto.

Trasmettere l'abitudine di fare il log-out

Quando i lavoratori si fermano per la pausa pranzo, terminano la giornata di lavoro o ogni volta che si allontanano dal dispositivo per più di un minuto o due, devono disconnettersi dalla rete aziendale. È una buona pratica in qualsiasi momento. È d'obbligo se il computer è condiviso, o se altri a casa possono accedervi.

Promuovere patch e aggiornamenti

Dire ai propri lavoratori a domicilio di abilitare gli aggiornamenti automatici su tutti i loro sistemi, per assicurarsi che siano aggiornati con tutte le misure di sicurezza. Controllare attentamente se anche il proprio ambiente interno è aggiornato, in particolare strumenti e sistemi critici per la sicurezza che potrebbero non essere senza patch perché in esecuzione 24 ore su 24, 7 giorni su 7. Prestare particolare attenzione alle macchine connesse da casa con in esecuzione Windows 7, che non viene più aggiornato. Potrebbe essere necessario semplicemente bloccare l'accesso fino a quando non è stato aggiornato a una versione supportata.

Fornire ai dipendenti formazione sulla sicurezza informatica

Non importa quanta tecnologia venga messa in campo, un'altra importante protezione è tra le orecchie dei dipendenti. Falsi avvisi dal lavoro per confermare le credenziali di accesso, visitare siti Web aziendali, gestire le richieste del capo per facilitare un pagamento o un trasferimento di fondi e altre truffe saranno in aumento man mano che i truffatori informatici tentano di lucrare sui lavoratori a domicilio. Gli impiegati consapevoli e vigili hanno meno probabilità di caderci. Soprattutto quando lavorano da remoto, un programma regolare di formazione manterrà alta la guardia.

Ecco le buone notizie

Le suite di produttività basate su cloud, la collaborazione online tramite chat e conferenze e altre tecnologie connesse a Internet e all'accesso remoto possono rendere i lavoratori a domicilio produttivi come se fossero in ufficio, anzi spesso anche più produttivi. Quando portano a casa il lavoro con sé, assicurarsi di fornirgli anche le giuste misure di sicurezza.

Per ulteriori informazioni sulle soluzioni di sicurezza ESET, visitare la nostra PAGINA WEB dedicata.