Identifiez les besoins de sécurité d'un personnel itinérant

La mise en place d'un programme de télétravail sécurisé

Table des matières

Synthèse

Les organisations doivent soutenir le télétravail en tant que composante de leur plan de continuité d'activité, ce qui nécessite la capacité de passer rapidement à une main-d'œuvre partiellement ou entièrement distante. Cela crée pour l'organisation, de nouveaux défis pour le réseau et la sécurité, car le réseau de l'entreprise est utilisé d'une manière très différente de celle des employés sur site.

Pour sécuriser une main-d'œuvre distante, il faut identifier et déployer des solutions de sécurité qui répondent aux besoins des employés et du réseau du siège. La majorité des employés n'ont besoin que d'un accès sécurisé au réseau de l'entreprise et aux applications basées sur le cloud, ce qui nécessite un accès VPN et une authentification multifactorielle (MFA). Les administrateurs de réseau et les cadres peuvent avoir des exigences supplémentaires en matière de réseau, telles qu'une connectivité permanente et une solution de téléphonie sécurisée. Le réseau du siège de l'organisation doit également être capable de prendre en charge et de sécuriser les connexions réseau provenant de la grande majorité du personnel d'une organisation, ce qui nécessite une authentification robuste des utilisateurs et un périmètre de sécurité avancé.

Introduction

La capacité à soutenir les travailleurs distants peut contribuer à améliorer le plan de continuité d'activité d'une organisation. Elle permet à l'organisation de s'adapter lorsque des circonstances imprévues, telles que des catastrophes naturelles ou une pandémie, rendent le travail sur place impossible pour les employés.

Dans ces circonstances, une organisation peut être contrainte de passer rapidement à une main-d'œuvre majoritairement ou totalement distante. Lors de la conception ou de la mise en œuvre d'une solution de télétravail, il est important de prendre non seulement en compte les exigences réseau, mais aussi les problèmes de sécurité supplémentaires créés par le travail à distance.

Répondre aux exigences de base du télétravail

Les employés peuvent avoir des exigences différentes en ce qui concerne leur environnement de travail à distance. Toutefois, tous les télétravailleurs doivent satisfaire à un ensemble d'exigences de base pour garantir une connexion sécurisée et authentifiée au réseau de l'entreprise. Ces exigences comprennent l'accès à un réseau privé virtuel (VPN) et une solution d'authentification forte pour protéger les comptes contre tout compromis.

Réseaux privés virtuels

Lorsqu'il travaille à distance, un employé traite des données sensibles de l'entreprise sur son réseau domestique. La protection de ces données contre tout compromis nécessite la capacité de garantir que la connexion d'un télétravailleur au réseau de l'entreprise est sécurisée.

Les télétravailleurs doivent avoir accès à un VPN qui assure une connectivité directe et cryptée entre leur machine et le réseau de l'entreprise. Cela permet non seulement de protéger la confidentialité et l'intégrité des données sensibles de l'entreprise en transit, mais aussi de garantir que tout le trafic entre l'employé et l'Internet public est surveillé et protégé par l'infrastructure de cybersécurité existante de l'entreprise.

Authentification multifactorielle

Comme les employés travaillent à domicile, il est plus probable que le vol des identifiants de connexion, combiné à l'accès à une machine non surveillée, puisse permettre un accès non autorisé au compte d'un utilisateur. Dans ces situations, de nombreuses caractéristiques utilisées pour détecter des modèles d'accès anormaux, comme le lieu et l'heure de la tentative d'authentification, peuvent ne pas être applicables lorsque les habitudes de travail des employés changent parce qu'ils travaillent depuis un bureau à domicile.

La sécurisation de l'accès au réseau, aux ressources et aux données de l'entreprise nécessite une solution d'authentification plus robuste que les noms d'utilisateur et mots de passe traditionnels. Tous les télétravailleurs doivent recevoir un jeton d'authentification sécurisé. Les options de jetons d'AMF comprennent des dispositifs physiques tels qu'un porte-clés ou des solutions logicielles telles qu'une application mobile, qui peuvent être utilisés pour vérifier l'identité d'un utilisateur avant de pouvoir établir une connexion VPN au réseau de l'entreprise ou accéder à d'autres ressources sensibles de l'entreprise.

Les directives PCI DSS pour le télétravail exigent que les employés qui accèdent aux données des titulaires de cartes s’authentifient via un VPN et utilisent une authentification multifactorielle.[1]

Soutenir les utilisateurs avertis, distants

Si de nombreux télétravailleurs peuvent se débrouiller avec une connexion VPN et un jeton d'AMF, d'autres ont des exigences supplémentaires. Les utilisateurs experts, notamment les administrateurs réseau et les cadres, ont besoin d'un bureau à distance plus complet pour accomplir leurs tâches principales. Ces utilisateurs peuvent avoir besoin d'une connectivité permanente au réseau de l'entreprise et d'une solution de téléphonie sécurisée.

Connectivité persistante

Certains utilisateurs, tels que les administrateurs de réseau et le personnel de sécurité, ont besoin d'un accès plus souple et permanent au réseau de l'entreprise. Ces employés peuvent disposer de plusieurs appareils qui doivent être connectés au réseau de l'entreprise ou avoir besoin d'une connectivité de longue durée qui ne soit pas limitée par des interruptions de session automatiques.

Les besoins des utilisateurs experts travaillant à domicile peuvent être satisfaits par le déploiement d'un point d'accès sans fil qui peut fournir un tunnel VPN fiable au réseau de l'entreprise. Afin de garantir une connexion sécurisée, ce point d'accès sans fil doit être associé à un pare-feu de nouvelle generation (NGFW) pour assurer l'inspection du trafic, la gestion des accès et une protection avancée contre les menaces.

Téléphonie sécurisée

Lorsqu'ils travaillent à distance, il est essentiel que les membres du personnel, et en particulier les cadres, aient accès à une solution de téléphonie sécurisée afin de protéger les communications et les données sensibles de l'entreprise. Dans le cas contraire, une entreprise risque d'exposer des données sensibles en raison des écoutes sur les réseaux cellulaires ou de l'utilisation d'applications mobiles malveillantes.

Un moyen efficace de fournir une téléphonie sécurisée aux travailleurs hors site est de tirer parti des communications par voix sur IP (VoIP). Si un utilisateur a déjà accès à une connexion Internet sécurisée, persistante et fiable, l'acheminement de son trafic vocal sur cette connexion ne nécessite qu'une surcharge minimale. Cela permet également à l'organisation de surveiller le trafic vocal et de le scanner sur le périmètre du réseau à la recherche de contenus potentiellement malveillants destinés à exploiter des logiciels VoIP vulnérables.

Les solutions de téléphonie pour les télétravailleurs doivent leur fournir toutes les fonctionnalités de leurs téléphones professionnels sur site. Cela minimise la probabilité que les travailleurs utilisent des appareils personnels pour les communications professionnelles. Les options importantes comprennent la possibilité de passer et de recevoir des appels, d'accéder à la messagerie vocale, de consulter l'historique des appels et d'accéder au répertoire téléphonique de l'entreprise.

72% de la journée de travail d'un PDG est consacrée à des réunions, ce qui rend les télécommunications sécurisées essentielles pour ses bureaux distants.[2]

Sécurité et stabilité de la tête de réseau

Les solutions de sécurité pour une main-d'œuvre distante ne se limitent pas au côté client. Un nombre croissant de télétravailleurs introduisent de nouvelles menaces de sécurité et de nouvelles exigences en matière de réseau au siège de l'organisation également.

Lors de la conception d'un programme de télétravail visant à assurer la continuité des activités, il est essentiel de s'assurer que le réseau du siège est capable d'authentifier les utilisateurs et les dispositifs qui tentent d'y accéder à distance, et de gérer et sécuriser un nombre beaucoup plus important de connexions VPN entrantes.

Authentification des utilisateurs et des appareils

Un modèle de sécurité à vérification systématique est très important lorsqu'une organisation soutient une main-d'œuvre presque ou entièrement distante. Les employés peuvent tenter de se connecter au réseau de l'entreprise en utilisant des appareils inconnus ou personnels, et les systèmes connectés à des réseaux non fiables ont une plus grande probabilité d'être compromis par des acteurs de la cybermenace.

Pour sécuriser le réseau de l'organisation et les données et ressources sensibles qu'il contient, il faut pouvoir authentifier les utilisateurs et les appareils qui tentent de s'y connecter. Cela peut être réalisé en utilisant un serveur d'authentification centralisé avec une connectivité à l'Active Directory de l'organisation, le protocole LDAP (Lightweight Directory Access Protocol — Protocole allégé d'accès annuaire) et le RADIUS (Remote Authentication Dial-In User Service).

Ce serveur devrait pouvoir être adapté aux besoins d'une plus grande main-d'œuvre distante sans entraver la productivité des utilisateurs. La prise en charge de la signature unique (SSO), de la gestion des certificats et de la gestion des invités garantit également l'authentification des utilisateurs sans créer de charge importante pour les employés distants.

Sécuriser le périmètre réseau

L'une des différences entre une main-d'œuvre sur place et une main-d'œuvre distante est le nombre de connexions VPN qu'une organisation doit être capable de gérer. Les employés sur site sont directement connectés au réseau local de l'entreprise, mais les télétravailleurs doivent envoyer tout leur trafic sur une connexion VPN. Le pare-feu nouvelle génération d'une organisation doit être capable de mettre fin à toutes les connexions VPN et de procéder à l'inspection d'un grand nombre de connexions réseau cryptées. L'inspection du trafic crypté étant coûteuse en termes de calcul, il est vital que le pare-feu nouvelle génération d'une organisation puisse s'adapter à la demande. Pour ce faire, les NGFW doivent disposer de processeurs de sécurité avancés dédiés. Ceux-ci minimisent la latence et maximisent le débit, évitant ainsi les congestions du réseau qui peuvent dégrader considérablement la productivité des employés.

Les pare-feux nouvelle génération qui se trouvent en tête de réseau doivent également effectuer une inspection de la couche 7 de tout le trafic. Cela est important dans tout contexte d'entreprise, mais avec une main-d'œuvre distante, une organisation peut s'attendre à une plus grande concentration de contenu malveillant sur les connexions entrantes des travailleurs distants. En effet, les machines des employés connectées à des réseaux personnels ont une probabilité plus élevée d'être infectées par des logiciels malveillants, qui peuvent tenter de se déplacer latéralement à travers eux vers le réseau de l'entreprise. Un pare-feu nouvelle génération de couche 7 peut identifier l'application qu'un paquet entrant tente d'atteindre et bloquer les paquets provenant d'applications présentant des vulnérabilités connues. Les pare-feux nouvelle génération, en tête de réseau, doivent également être intégrés à des capacités de Sandboxing pour analyser en toute sécurité les contenus suspects ne peuvant être associés à aucune menace connue.

L’inspection de la couche de sécurité du transport (TLS)/couche des sockets sécurisés (SSL) réduit le débit du pare-feu de 60% en moyenne.[3]

Conclusion

Lors d'une transition rapide et massive vers le télétravail, il est essentiel qu'une organisation puisse non seulement poursuivre ses activités, mais aussi assurer la sécurité des télétravailleurs et des données sensibles qu'ils traitent.

Pour ce faire, une organisation doit déployer des solutions de sécurité à la fois sur les sites de travail distants des télétravailleurs et sur le réseau principal de l'entreprise. Ce faisant, il est essentiel de sélectionner des solutions capables de répondre aux exigences d'infrastructure et aux préoccupations de sécurité uniques associées à une main-d'œuvre à distance. En cas de catastrophe, lorsqu'une réponse immédiate est nécessaire, le choix d'une solution pouvant être déployée rapidement et facilement garantit un impact minimal sur les opérations de l'entreprise.

[1] Emma Sutcliffe, « How the PCI DSS Can Help Remote Workers (Comment le PCI DSS peut-il aider les travailleurs à distance) », Conseil des normes de sécurité PCI, 26 mars 2020.

[2] Michael E. Porter et Nitin Nohria, « How CEOs Manage Time (Comment les PDG gèrent-ils le temps) », Harvard Business Review, juillet 2018.

[3] « SS Labs Expands 2018 NGFW Group Test with SSL/TLS Security and Performance Test Reports (NSS Labs étend le test du groupe NGFW 2018 avec des rapports de test de sécurité et de performance SSL/TLS) », NSS Labs, 24 juillet 2018.

www.fortinet.fr

628535-0-0-FR

septembre 24, 2020 1:39 PM

ebook-teleworker-solutions