LIVRE BLANC

Quels éléments prendre en compte dans la mise en place d'un télétravail sécurisé à grande échelle

Identification des risques de sécurité et des exigences avancées d'une main-d'œuvre distante

Résumé

La capacité à faire passer rapidement le personnel d'une organisation au télétravail est un élément essentiel d'un plan de continuité d'activité. Cependant, les télétravailleurs ont des exigences de sécurité supplémentaires et des défis de sécurité différents de ceux des employés sur site.

Les télétravailleurs se connectent souvent au réseau de l'entreprise sur des réseaux non sécurisés ou non fiables, ce qui peut permettre d'écouter aux portes et d'utiliser des dispositifs dans des zones non sécurisées où ils peuvent être perdus ou volés. Les utilisateurs avertis peuvent avoir des besoins qui ne peuvent être satisfaits par un client de réseau privé virtuel (VPN) standard.

Au-delà de ces exigences de base, les télétravailleurs peuvent utiliser des dispositifs non fiables pour accéder aux ressources de l'entreprise et sont plus susceptibles d'être victimes d'ingénierie sociale en cas de crise, ce qui crée davantage de risques pour la sécurité. En outre, ces employés doivent pouvoir accéder aux ressources basées sur le cloud sans latence importante du réseau. C'est pour ces exigences plus avancées que les contrôles de sécurité de base n'offriront pas une sécurité adéquate pour une main-d'œuvre majoritairement distante.

54% des professionnels IT estiment que les télétravailleurs présentent un risque de sécurité plus important que le personnel sur site.[1]

Seulement 74% des entreprises exigent un VPN pour les télétravailleurs.[2]

Introduction

Le plan de continuité d'activité de chaque organisation doit prévoir la possibilité de faire passer rapidement la plupart ou la totalité de la main-d'œuvre au travail à distance. Les catastrophes naturelles, les pandémies ou les attaques terroristes ne sont que quelques-uns des événements qui peuvent rendre cette transition nécessaire.

Une transition sûre et sans heurt du « business as usual » au bureau à une main d'œuvre totalement distante exige de la planification et une prise en compte attentive des besoins des télétravailleurs, tels que l'accès aux ressources du réseau, une large bande passante et un support technique. La transition amplifie également les risques de sécurité du télétravail, en raison des vulnérabilités du réseau domestique et des appareils personnels, ainsi que les défis liés à la supervision et à l'application d'une bonne cyber-hygiène.

Défis en matière de connectivité sécurisée et de productivité

La première étape d'une stratégie de télétravail sécurisé consiste à s'assurer que les travailleurs distants ont la possibilité de se connecter de manière sécurisée au réseau de l'entreprise. Il y a des défis à relever tant pour sécuriser la connectivité à distance que pour maintenir la productivité des utilisateurs sur la connexion à distance. Ces défis sont liés aux réseaux domestiques, aux utilisateurs eux-mêmes et à l'équipement réseau du bureau de l'entreprise.

Les réseaux domestiques sont vulnérables

Pour les salariés, le moyen le plus simple de se connecter à l'entreprise est le réseau domestique et l'Internet public. Toutefois, le réseau du domicile de l'employé est probablement moins sécurisé que le réseau de l'entreprise, ce qui le rend plus vulnérable aux attaques.

Le trafic entre le télétravailleur et le réseau de l'entreprise pourrait être intercepté, et éventuellement modifié par un tiers. En outre, le trafic qui ne passe pas par le réseau de l'entreprise n'est pas protégé par les solutions de sécurité sur site de l'entreprise, ce qui la rend plus vulnérable aux logiciels malveillants.

Les télétravailleurs ne sont peut-être pas ce qu'ils semblent être

Dans des circonstances normales, de nombreuses organisations s'appuient sur un modèle de sécurité basé sur un périmètre. Selon ce modèle, toute personne à l'intérieur du réseau est considérée comme fiable, alors que les parties extérieures sont considérées comme potentiellement malveillantes. Cela permet à une organisation d'identifier les tentatives de connexion anormales en fonction du lieu et de l'horodatage (puisque la plupart des travailleurs travaillent pendant les heures habituelles de bureau).

Avec une main-d'œuvre entièrement distante, ce modèle traditionnel n'est plus applicable puisque tant les utilisateurs légitimes que les menaces éventuelles se connectent à des ressources extérieures au réseau et peuvent travailler à des heures irrégulières. En outre, lorsque les employés travaillent à distance, la probabilité qu'un utilisateur non autorisé accède aux appareils d'un employé et les contrôle est plus élevée.

Les têtes de réseau VPN manquent d'adaptabilité

Dans le cadre du « business as usual », de nombreuses organisations n'ont pas de politique de télétravail. En fait, seulement 41% des entreprises autorisent le travail à distance.[3] Par conséquent, de nombreuses organisations ne disposent pas de l'infrastructure nécessaire pour soutenir une main-d'œuvre entièrement ou principalement à distance.

Dans des circonstances normales, un pourcentage significatif du trafic d'un utilisateur est interne au réseau, accédant aux partages de fichiers internes, aux bases de données et à d'autres ressources. Cependant, lorsque les employés travaillent à distance, tout leur trafic passe par les pare-feux périmétriques, ce qui augmente la charge de ces dispositifs.

L'utilisation des VPN ne fait qu'exacerber ce problème. Le cryptage et le décryptage du trafic VPN sont coûteux en termes de calcul et peuvent rapidement épuiser les ressources CPU d'un pare-feu de nouvelle génération (NGFW).

Le télétravail « applicable à tout le monde » ne fonctionne pas

Pour l'employé standard, une connexion sécurisée au réseau de l'entreprise et aux ressources dans le cloud suffit pour accomplir ses tâches professionnelles. Toutefois, certains employés ont des exigences supplémentaires lorsqu'ils travaillent à distance.

Les utilisateurs avertis, tels que les administrateurs réseau et le personnel de sécurité, ont besoin d'une connectivité permanente au réseau. Ces utilisateurs peuvent avoir besoin de pouvoir connecter plusieurs appareils au réseau, ce qui peut être difficile à gérer manuellement via des clients VPN, ou des connexions qui durent plus longtemps que la durée standard de la session des clients VPN.

Les super-utilisateurs, y compris les cadres et autres membres du personnel de direction, traitent régulièrement des données très sensibles et doivent pouvoir le faire tout en travaillant à distance également. Ces employés ont besoin d'un niveau de protection plus élevé que celui fourni par la plupart des clients VPN.

Appliquer les politiques de cybersécurité en cas de crise

Au-delà des besoins fondamentaux d'une main-d'œuvre à distance, le télétravail crée des défis supplémentaires en matière de sécurité pour une organisation. Il faut notamment tenir compte de l'utilisation de dispositifs non sécurisés pour le travail, d'une probabilité accrue d'incidents de sécurité en cas de crise, et du besoin des télétravailleurs d'accéder efficacement aux applications basées sur le cloud.

La réponse aux incidents est plus difficile pour les travailleurs distants

Les situations qui obligent une organisation à faire la transition vers une main-d'œuvre distante sont souvent chaotiques et émotionnelles pour les employés. Les humains sont en général enclins à prendre de mauvaises décisions de sécurité dans ces situations, et les cybercriminels capitalisent régulièrement sur ces émotions pour réaliser leurs attaques.

En temps de crise, les employés sont plus susceptibles de tomber dans le piège d'attaques de phishing, et une organisation est probablement moins préparée à réagir à l'incident. Avec un personnel distant, le service d'assistance est moins immédiatement disponible pour un employé, et les plans de réponse aux incidents d'une organisation peuvent ne pas couvrir les éventualités où un télétravailleur subit un incident de sécurité. Par conséquent, le coût pour l'organisation peut être beaucoup plus élevé en cas de travail distant, tant en termes de productivité des employés que d'initiatives d'assainissement.

Les télétravailleurs peuvent manquer de patchs de sécurité vitaux.

Les organisations qui n'ont pas de politique de télétravail établie disposent souvent d'un nombre insuffisant d'appareils appartenant à l'entreprise pour prendre totalement en charge une main-d'œuvre distante. Par conséquent, il est possible que les employés qui travaillent à domicile utilisent des appareils non approuvés, notamment des ordinateurs portables ou des tablettes.

15% des organisations seulement ont effectué une transition vers un modèle de sécurité à vérification systématique, ce qui ne suppose pas automatiquement que l'on fasse confiance à quiconque se trouvant dans le périmètre du réseau.[4]

75% des professionnels IT estiment que le risque de violation des données est plus élevé pour les télétravailleurs.[5]

Le protocole de bureau distant, utilisé par les administrateurs système pour la gestion des appareils distants, est le principal vecteur d'infection des rançonslogiciels dans 70 à 80% des cas.[6]

42% des ordinateurs distants reçoivent des correctifs de sécurité dans un délai de trois jours, comparé à 48% des machines sur site.[7]

La capacité à faire appliquer les politiques de « bring-your-own-device » (BYOD — Apportez votre équipement personnel) est essentielle lorsque les employés travaillent à domicile. Les appareils utilisés par les télétravailleurs ont historiquement un taux de correctifs plus faible que les appareils sur site, même si tous les appareils appartiennent à l'entreprise.[8] Ces retards dans l'application des correctifs peuvent être coûteux, puisque 60% des violations de données sont causées par une vulnérabilité non corrigée pour laquelle un correctif était disponible.[9] Une entreprise doit être en mesure d'effectuer des analyses avant connexion pour vérifier la conformité des correctifs, afin de s'assurer que les travailleurs distants n'exposent pas le réseau de l'entreprise à un risque cyber supplémentaire.

62 % des entreprises autorisent le BYOD pour les travailleurs à distance.[10]

Les organisations déployant rapidement des solutions basées sur le cloud pour soutenir le travail à distance sont plus susceptibles de mal configurer les paramètres de sécurité.[11]

Les télétravailleurs ont besoin d'un accès efficace et sécurisé au cloud

Lorsque les employés travaillent sur place, il est logique de sécuriser leurs connexions aux ressources dans le cloud à l'aide d'appareils de sécurité sur place, puisque le trafic passe déjà par le périmètre du réseau. Cependant, les télétravailleurs se connectent de l'extérieur du réseau avec du trafic à destination du cloud.

Le transfert du trafic des télétravailleurs vers le réseau de l'entreprise à des fins d'analyse de sécurité augmente la latence du réseau. Cela peut créer des problèmes de performance pour les applications SaaS (Software-as-a-Service) sensibles à la latence et avoir un impact négatif sur la productivité des télétravailleurs.

Comme les organisations dépendent de plus en plus de solutions SaaS dans le cadre du travail distant, elles deviennent une cible de plus en plus importante pour les cybercriminels. Les erreurs de configuration des politiques de sécurité et des paramètres de configuration des applications SaaS pourraient être la cause d'une violation de données ou permettre aux cybercriminels de les utiliser comme vecteur d'infection pour des logiciels malveillants.

La sécurité de base du télétravail ne suffit pas

La transition de la plupart ou de la totalité des employés d'une organisation vers le télétravail crée des défis importants en matière de sécurité pour une organisation. Le plan de continuité d'activité d'une organisation doit tenir compte de ces défis et inclure des solutions pour faire face à ces nouveaux risques.

Le déploiement de contrôles de sécurité de base pour le télétravail, tels que la connectivité VPN et l'authentification forte des utilisateurs, permet à une organisation de prendre en charge le travail distant intermittent avec une fraction de ses employés. Toutefois, la continuité d'activité signifie qu'une organisation doit être capable de maintenir des niveaux normaux de productivité et de sécurité avec une main-d'œuvre principalement ou entièrement distante. Pour ce faire, il faut sécuriser le point d'extrémité et garantir un accès fiable et à haut débit aux applications SaaS essentielles.

[1] « Remote Work Is the Future—But Is Your Organization Ready for It? (Le travail à distance est l'avenir — mais votre organisation est-elle prête pour cela ?) », OpenVPN, consulté le 29 avril 2020.

[2] Idem.

[3] « The Modern Workplace: People, Places & Technology (Le lieu de travail moderne : les personnes, les lieux et la technologie) », Condeco, mai 2019.

[4] « 2019 Zero Trust Adoption Report (Rapport sur l'adoption de la confiance zéro en 2019) », Cybersecurity Insiders, novembre 2019.

[5] « Data Protection Report 2019 (Rapport sur la protection des données 2019) », Shred-it, 17 juin 2019.

[6] Lawrence Abrams, « FBI Says $140+ Million Paid to Ransomware, Offers Defense Tips (Le FBI affirme avoir versé plus de 140 millions de dollars à Ransomware et donne des conseils de défense) », Bleeping Computer, 27 février 2020.

[7] Robert Lemos, « Patching Poses Security Problems with Move to More Remote Work (Les correctifs posent des problèmes de sécurité en cas de déménagement vers un lieu de travail plus éloigné) », Dark Reading, 31 mars 2020.

[8] Idem.

[9] « Costs and Consequences of Gaps in Vulnerability Response (Coûts et conséquences des lacunes dans la réponse aux vulnérabilités) », ServiceNow et Ponemon Institute, 29 octobre 2019.

[10] « Remote Work Is the Future—But Is Your Organization Ready for It? (Le travail à distance est l'avenir — mais votre organisation est-elle prête pour cela ?) », OpenVPN, consulté le 29 avril 2020.

[11] Liam Tung, « Microsoft Office 365: US issues security alert over rushed remote deployments (Microsoft Office 365 : les États-Unis lancent une alerte de sécurité pour les déploiements à distance précipités) », ZDNet, 30 avril 2020.

FORTINET®

www.fortinet.fr

septembre 24, 2020 1:34 PM

668978-0-0-FR