Optimiser la sécurité des réseaux des entreprises au quotidien grâce à une segmentation réseau efficace

Par conséquent, les processus sous-jacents de configuration réseau augmentent en taille et en complexité, impactant les ressources mobilisées pour gérer les changements requis.

Ces changements affectent tous les environnements, des pare-feu et routeurs de multiples fournisseurs au SDN et aux plateformes de cloud hybride. L'immensité du réseau moderne fait qu'il est incroyablement difficile pour les entreprises d'en gérer la complexité. Les cybercriminels profitent volontiers de cette confusion, ce qui oblige les entreprises à se protéger des attaques ciblées et automatisées qui risquent de pénétrer leur réseau en se jouant de règles d'accès par trop permissives.

La segmentation réseau pour contenir les menaces et éviter qu'elles se propagent à d'autres zones

Une approche populaire en réponse à ces enjeux liés à la sécurité du réseau est celle de la segmentation réseau, où les applications et l'infrastructure sont divisées en segments, de façon à contenir les menaces et les empêcher de se propager à d'autres zones. Si l'attaque exploite un service existant, il est possible de donner la priorité au monitoring et d'évaluer les règles d'accès vulnérables pour diriger l'effort de réponse et d'atténuation des incidents.

Si l'approche de segmentation réseau n'est pas nouvelle, elle n'est pas pour autant obsolète. Toutefois, la définition d'une segmentation réseau efficace, sa mise en œuvre et sa maintenance à long terme constituent un challenge de taille pour de nombreuses entreprises, surtout dans le contexte d'intensification des réglementations de confidentialité et de modifications fréquentes de l'infrastructure par l'adoption du cloud. Alors, comment les entreprises garantissent-elles la mise en œuvre efficace de pratiques de segmentation réseau, tout en prenant en compte l'ensemble des complexités d'un réseau d'entreprise ? Et comment atteindre leur niveau idéal de limitation granulaire des accès ?

Commencer par les bases

La première étape consiste à évaluer la situation : qu'attendent les entreprises de leur réseau et comment le diviser ? Pour faire simple, des services individuels sont souvent enclins à contenir leurs applications dans leur propre sous-section ou unité, ce qui est parfaitement logique et constitue une étape nécessaire pour que les données sensibles ne finissent pas entre de mauvaises mains.

De plus, la segmentation est une considération cruciale pour les entreprises qui doivent démontrer l'alignement entre leurs meilleures pratiques et le Règlement général de l'UE sur la protection des données (RGPD). En vertu de ce nouveau règlement, les entreprises doivent tracer les accès aux données appartenant à des résidents de l'UE. Après avoir divisé le réseau en segments individuels

ou zones de sécurité, ou étiqueté les applications, les responsables IT devront prévoir le provisioning d'un accès minimal requis à ces zones ou applications. Surtout, les zones hautement sensibles doivent faire l'objet d'une surveillance proactive pour identifier si les accès superflus peuvent être supprimés.

Une tâche qui s'inscrit dans la durée

Comme on l'entend souvent « la sécurité est un cheminement et non un aboutissement ». La segmentation réseau s'inscrit donc dans la durée et requiert une maintenance continue. Les systèmes en réseau doivent constamment être mis à jour, dans le contexte de nouveaux besoins métier, de nouveaux dispositifs ou de nouveaux logiciels.

Pour réussir la segmentation de leurs réseaux, les entreprises ont intérêt à :

Surveiller le trafic réseau dans chaque segment pour évaluer les niveaux d'activité normaux.
Réduire l'accès à des segments particuliers via des pare-feu pour atténuer les menaces exogènes.
Séparer les données selon une approche réglementaire, pour obtenir à la clé, une plus grande visibilité sur ce que contiennent les actifs protégés et savoir quelles mesures prendre pour réduire les risques.
Assurer une surveillance continue des violations et des menaces visant le réseau, de façon à pouvoir apporter des changements en temps réel, l'analyse des risques étant intégrée au processus de gestion des changements.
Conduire régulièrement des audits internes pour vérifier que les précédents changements des règles de pare-feu n'ont pas introduit de nouveaux risques.

Un pas en avant : la microsegmentation

Selon la maturité et la complexité de l'entreprise, ainsi que ses obligations métier, la microsegmentation se pose comme une solution pragmatique de gestion des accès réseau via une approche applicative plus dynamique. Au moyen de la microsegmentation, les segments individuels sont décomposés parfois même jusqu'aux niveaux de l'application et de l'utilisateur. Dans ces cas, l'accès aux données n'est autorisé qu'à un groupe de sécurité prédéfini dont les utilisateurs sont soigneusement encadrés par l'équipe de sécurité. Ce groupe peut aisément être modifié pour refléter les changements de personnel et l'accès est établi entre le groupe de sécurité spécifique et l'application spécifique. Plutôt que de traiter les réseaux comme des segments plus larges d'utilisateurs, la microsegmentation vous permet d'embrasser d'emblée la sécurité d'une façon gérable.

La microsegmentation peut s'obtenir avec des réseaux physiques, de même qu'avec des réseaux cloud privés et publics au moyen de technologies réseau définies par logiciel pour l'administration d'infrastructures cloud avancées. Ceci suppose des solutions de segmentation complètes des réseaux de cloud hybride et hétérogènes, permettant aux équipes de sécurité IT de maintenir et gérer visuellement une politique de microsegmentation pour leur organisation.

Dans un environnement en mutation constante, il est impératif que cette volatilité n'augmente pas la surface d'attaque, au risque d'exposer l'entreprise à une compromission du réseau. Les bons outils d'automatisation peuvent permettre à la solution d'atténuer grandement les risques pour la sécurité en instaurant une culture donnant la priorité à la sécurité dans l'approche

d’accompagnement des changements et en réduisant le degré de complexité et les délais de gestion continue des changements apportés au réseau.

Ce peut être utile également pour l’efficacité de segmentation des réseaux, même si un équilibre doit être trouvé. Les entreprises doivent se méfier de la tendance à compliquer excessivement l’administration de différents groupes et à rendre le contrôle par trop granulaire.

Il peut donc être difficile de maintenir la segmentation réseau au niveau voulu compte tenu de la nature complexe des règles de sécurité et du fait que les demandes de changement constantes sont désormais la norme dans la plupart des entreprises. Toutefois, si le réseau est divisé en plus petites zones, une attaque d’une zone segmentée ne peut se propager à une autre, créant ainsi une infrastructure bien plus sûre et renforçant grandement la sécurité du réseau. Enfin, les entreprises doivent éviter de segmenter excessivement le réseau et maintenir une console centrale pour bien gérer un réseau micro-segmenté à l’échelle des plateformes physiques, cloud et de plusieurs fournisseurs.