FORTINET

La segmentation traditionnelle échoue face à l'expansion actuelle de la surface d'attaque

Pourquoi les responsables de l'ingénierie et de l'exploitation des réseaux sont-ils concernés ?

Table des matières

FORTINET

Synthèse

Une surface d'attaque en expansion et en fragmentation — qui résulte de la mobilité et de l'adoption du multi-cloud — compromet la capacité des responsables de l'ingénierie et de l'exploitation des réseaux à maintenir les performances, la sécurité, la fiabilité et la disponibilité du réseau. La segmentation traditionnelle basée sur le réseau et les techniques de micro-segmentation encore plus récentes, sont insuffisantes dans la mesure où elles ne permettent ni de détecter, ni de prévenir les menaces. Contraintes par l'architecture du réseau, elles sont tactiques plutôt que stratégiques et axées sur la logique commerciale. Elles sont également généralement statiques, laissant les utilisateurs, les appareils et les applications autrefois fiables libres dans leurs segments autorisés. Enfin, elles manquent de visibilité globale en matière de sécurité, sur l'ensemble du réseau et dans les flux cryptés, ce qui est essentiel à une gestion efficace des risques.

Introduction : Vous avez des difficultés à gérer des réseaux disparates : La segmentation est-elle la réponse ?

La base des utilisateurs du réseau d'entreprise typique est de plus en plus dispersée géographiquement, tout comme les appareils et les applications qui se connectent aux ressources informatiques de l'entreprise. Comme les réseaux d'entreprise ont intégré les technologies mobiles et de l'internet des objets (IoT) et adopté des applications SaaS (Software-as-a-Service) dans de multiples clouds publics, leurs surfaces d'attaque sont devenues de plus en plus difficiles à protéger, même avec un périmètre de sécurité élevé.

L'un des défis de ces surfaces d'attaque en expansion et en fragmentation est qu'elles créent un ensemble de nouveaux chemins par lesquels les criminels peuvent attaquer. Un autre problème est que les menaces sont de plus en plus sophistiquées, recherchant et exploitant automatiquement toute vulnérabilité. La situation est encore compliquée car les activités de fusion et d'acquisition (M&A) peuvent aboutir à une infrastructure diversifiée avec une coordination ou une visibilité limitée entre les différentes parties de l'organisation. Dans de nombreuses organisations, la sécurité est devenue un exercice réactif, car les technologies de l'information sont incapables d'empêcher le mouvement latéral des intrusions sur les dispositifs et les applications connectés au réseau et le traversant.

Depuis des années, les responsables de l'ingénierie et de l'exploitation des réseaux ont relevé ces défis en segmentant leurs réseaux. Les techniques traditionnelles de segmentation basées sur les adresses IP ont été complétées par la segmentation des VLAN et la segmentation VMware NSX pour les charges de travail virtualisées. Les réseaux basés sur des équipements Cisco reposent sur la segmentation Cisco ACI utilisant des commutateurs physiques et des VXLAN. Ces techniques de micro-segmentation permettent de définir des politiques de contrôle d'accès par charge de travail et application ou par attributs architecturaux telles que les machines virtuelles (VM) sur lesquelles résident les applications, les données et les systèmes d'exploitation.

Dans ces approches de segmentation, des pare-feux sont utilisés pour séparer les ressources du réseau pour chaque groupe. Cela interdit à tout trafic non autorisé de passer d'un segment à l'autre. Ainsi, lorsqu'une attaque viole la sécurité du réseau dans une zone, cette approche devrait empêcher la propagation des attaques latéralement vers d'autres zones du réseau — du moins en théorie.

Malheureusement, la micro-segmentation n'est pas la panacée dont on parle parfois. Les idées sous-jacentes ont du sens, mais si une infrastructure de réseau qui implique la micro-segmentation n'est pas conçue correctement, elle pourrait en fait entraver la sécurité. La division d'un réseau d'entreprise complexe en un grand nombre de petits segments peut limiter la visibilité des menaces et de réduction des risques des attaques sur le réseau.[1]

La division d'un réseau d'entreprise complexe en un grand nombre de petits segments peut limiter la visibilité des menaces et de réduction des risques des attaques dans l'ensemble du réseau.[2]

Les trois raisons pour lesquelles le statu quo de la segmentation augmente le risque

Les techniques de segmentation actuelles posent trois problèmes principaux :

1. Le contrôle d'accès aux segments de réseau interne est conçu à partir de l'architecture, une approche tactique qui ne peut pas facilement s'adapter aux besoins changeants des entreprises.
2. Les évaluations de confiance sur lesquelles sont basées les politiques d'accès ont tendance à être statiques et à devenir rapidement dépassées.
3. Les politiques de contrôle d'accès ne peuvent pas être appliquées efficacement en raison d'un manque de composants de sécurité avancés (couche 7), du datacenter à la périphérie du réseau et, de plus, sont incapables de voir et de contrôler ces composants avec efficacité.

Ces problèmes proviennent souvent du fait que le personnel chargé de l'ingénierie et de l'exploitation des réseaux planifie l'architecture de segmentation sans accorder une attention suffisante à la sécurité. La compréhension de chacun de ces problèmes et de leur impact global peut conduire à une approche plus prudente de la segmentation.

« Trop souvent, le réseau est conçu sans tenir compte de la conception de la sécurité et de son fonctionnement. Les équipes informatiques n'intègrent pas le plan de sécurité dans le plan du réseau alors qu'en fait, les deux vont de pair. En conséquence, les deux fonctionnent comme un leader et un suiveur, plutôt que comme des partenaires égaux dans l'hélice informatique. Ce désalignement se multiplie dans des environnements de réseau très segmentés et complexes ».[3]

Une approche tactique ascendante du contrôle d'accès

On peut supposer que la conception du réseau d'entreprise est dictée par les besoins de l'organisation au fur et à mesure de son évolution. Les règles régissant qui et quoi peut accéder à telles ressources du réseau sont déterminées par les politiques de l'entreprise, les normes industrielles et les réglementations gouvernementales. En suivant ces règles, l'équipe chargée de l'exploitation du réseau configure les paramètres de contrôle d'accès dans les routeurs et les commutateurs, qui permettent aux utilisateurs, aux appareils ou aux applications d'accéder à des ressources réseau spécifiques.

Les responsables de l'ingénierie et de l'exploitation des réseaux reconnaîtront immédiatement deux inconvénients à cette approche. Premièrement, les processus opérationnels, les exigences de conformité et les besoins d'accès au réseau d'une organisation sont beaucoup plus complexes que la structure de son réseau. Par conséquent, il est très difficile d'utiliser l'architecture du réseau pour définir des segments sécurisés pour les ressources du réseau qui seront simultanément accessibles à tous les utilisateurs et applications autorisés et totalement inaccessibles à tous les autres. Dans la pratique, il y aura des failles de sécurité — des scénarios d'accès que les architectes du réseau n'ont pas envisagés — dont les mauvais acteurs pourront tirer parti. Ils le font déjà avec des logiciels malveillants sophistiqués et avancés.

Deuxièmement, tout processus, toute réglementation ou toute structure organisationnelle est susceptible de changer. Ainsi, même si la conception d'un réseau parfaitement sécurisé était réalisée, il faudrait la modifier. Une fois de plus, il existe de nombreuses possibilités de failles de sécurité, sans parler du temps et du coût de la reconfiguration, que peu d'équipes de réseau peuvent se permettre.

Il est très difficile d'utiliser l'architecture du réseau pour définir des segments sécurisés. Dans la pratique, il y aura des failles de sécurité — des scénarios d'accès que les architectes du réseau n'ont pas envisagés — dont les mauvais acteurs pourront tirer profit.

Les évaluations de confiance ont tendance à être statiques

Pour gérer efficacement les risques, les responsables de l'ingénierie et de l'exploitation des réseaux doivent disposer d'informations actuelles et précises sur la fiabilité des utilisateurs, des applications et des actifs du réseau. Leurs firewalls internes ou autres mécanismes de contrôle d'accès qui permettent ou interdisent le flux de trafic entre les segments de réseau doivent toujours fonctionner à partir de données de confiance actualisées. Si les évaluations de confiance sont obsolètes, les technologies de segmentation deviennent inutiles pour empêcher les menaces éventuelles de se déplacer latéralement dans le réseau.

La qualité des données de confiance devient une question pressante dans la sécurité de la segmentation des réseaux, car la fiabilité réelle des ressources du réseau peut changer de manière inattendue. En effet, de nombreuses organisations ont été surprises par des attaques provenant des rangs de leurs employés et sous-traitants de confiance. Plus d'un tiers des violations signalées concernent des utilisateurs internes, et 29% concernent des données d'identification volées.[4]

Certaines organisations ont réagi à ces dangers en verrouillant pratiquement leurs réseaux, en ne faisant confiance à aucun utilisateur ni application et en créant des niveaux de vérification avant d'autoriser tout accès. Les responsables de l'ingénierie et de l'exploitation des réseaux doivent protéger les biens sensibles, mais sans imposer de charges inutiles à ceux qui ont légitimement besoin d'accéder à ces biens.

« La confiance n'est pas absolue, binaire ou statique. C'est une indication du niveau relatif de force de l'assurance de la croyance. De plus, le niveau de confiance est dynamique et change avec le temps. L'accès aux capacités doit donc être adapté ».[5]

Le contrôle d'accès ne signifie pas grand-chose sans exécution

Les politiques de contrôle d'accès ne peuvent pas fonctionner comme prévu si le réseau est dépourvu des éléments clés d'une infrastructure de sécurité efficace. Les approches traditionnelles de la segmentation supposent que tous les éléments de sécurité du réseau sont en place pour exécuter les politiques de contrôle d'accès définies par l'équipe informatique. Cependant, cette hypothèse peut ne pas être valable, pour plusieurs raisons.

Le coût total de possession (CTP) est une raison majeure pour laquelle les organisations ne disposent pas toujours d'une sécurité avancée omniprésente. Par exemple, une équipe d'ingénierie et d'exploitation de réseau chargée de la segmentation peut décider que certains segments du réseau présentant des surfaces d'attaque plus petites sont correctement protégés sans application du niveau 7 de sécurité avancée. Pour des raisons budgétaires ou simplement parce que le déploiement et la gestion nécessitent trop de ressources, les équipes d'ingénierie et d'exploitation des réseaux peuvent hésiter à déployer des pare-feux de nouvelle génération (NGFW) et d'autres solutions avancées de protection contre les menaces partout où elles sont nécessaires — dans l'entreprise, dans chaque cloud dans lequel elles opèrent et sur chaque point d'extrémité et dispositif IoT.

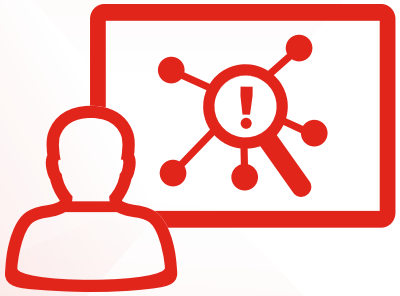
Les éléments de sécurité qui sont en place peuvent ne pas être pleinement opérationnels. Certaines équipes réseau pourraient intentionnellement désactiver l'inspection de la couche des sockets sécurisés (SSL)/la sécurité de la couche transport (TLS) dans leurs NGFW afin d'optimiser les performances du réseau. En handicapant ainsi les solutions de sécurité, on peut aider le trafic légitime à passer plus rapidement d'un segment de réseau à l'autre, mais on ouvre en même temps la porte au trafic illégitime. Et comme 72 % du trafic réseau est désormais crypté et que les cybercriminels l'utilisent pour infiltrer les réseaux et exfiltrer des données, cela est très préoccupant.[6]

L'efficacité globale des composants de la sécurité est réduite s'ils ne sont pas étroitement intégrés. Le manque d'intégration a plusieurs implications. Tout d'abord, lorsqu'un pare-feu détecte un paquet suspect, il peut s'écouler plusieurs heures, voire davantage, avant que l'administrateur de la sécurité ne saisisse l'information et ne la diffuse au reste du réseau.

Deuxièmement, les solutions de sécurité disparates ne peuvent pas facilement partager les renseignements sur les menaces, ni les renseignements acquis au niveau mondial sur les menaces connues et émergentes, ni les renseignements sur les menaces zero-day. C'est peut-être l'une des raisons pour lesquelles le délai moyen d'identification d'une brèche reste élevé, à 197 jours.[7]

Troisièmement, les organisations ne peuvent pas réagir efficacement pour atténuer l'impact des infractions qui sont détectées. Sans une technologie intégrée de Sandboxing pour mettre automatiquement en quarantaine et tester tous les paquets suspects, des dommages importants peuvent se produire avant que l'équipe de sécurité ne traite la menace manuellement.

Dans ces conditions, les responsables de l'ingénierie et des opérations réseau qui pensent que leur réseau segmenté est bien protégé peuvent travailler sous un faux sentiment de sécurité. Une évaluation continue de la sécurité de bout en bout leur permettrait de savoir comment leur plate-forme de sécurité fonctionne et si leurs politiques de contrôle d'accès atteignent leurs objectifs commerciaux. Malheureusement, sans une sécurité étendue et une visibilité de bout en bout, une évaluation fiable n'est pas possible, ce qui empêche de nombreux responsables de l'ingénierie et des opérations réseau de rendre compte avec précision de la sécurité globale de leur entreprise.



Des solutions de sécurité disparates ne permettent pas de partager facilement les renseignements sur les menaces connues ou nouvellement découvertes. C'est peut-être l'une des raisons pour lesquelles le délai moyen d'identification d'une brèche reste élevé, à 197 jours.[8]

Conclusion : Les principales préoccupations en matière de segmentation

La segmentation des réseaux est nécessaire, mais le statu quo est insuffisant. Les entreprises qui n'intègrent pas d'évaluations dynamiques de confiance dans le contrôle d'accès entre les segments laissent leurs utilisateurs et leurs actifs vulnérables. Les réseaux dans lesquels l'architecture de segmentation limite l'intention de l'entreprise ne favorisent pas la progression vers des objectifs organisationnels. Dans le même temps, si les priorités en matière de performances l'emportent sur les préoccupations de sécurité, la segmentation peut entraîner une réduction réactive et inefficace des risques des menaces. En outre, les réseaux qui n'ont pas une visibilité adéquate de la posture de sécurité peuvent ne pas intégrer la sécurité de la couche 7, qui est cruciale pour prévenir les menaces avancées.

Il appartient aux responsables de l'ingénierie et des opérations réseau de s'assurer que les politiques de contrôle d'accès aux segments internes du réseau sont adéquates en cette ère d'expansion et de fragmentation perpétuelles des surfaces d'attaque. Ce n'est qu'en accordant une attention particulière à la conception de la segmentation qu'une entreprise peut être sûre de sa capacité à déjouer les attaquants qui cherchent à se déplacer latéralement sur le réseau.

[1] Keith Townsend, « Get a Quick Primer on How Microsegmentation Can Improve Network Security (Découvrez comment la microsegmentation peut améliorer la sécurité des réseaux) », BizTech, 26 mai 2017.

[2] Idem.

[3] « Friction in the IT Helix: How to Create Harmony between Network Design and Security (Friction dans l'hélice informatique : comment créer une harmonie entre la conception du réseau et la sécurité) », Masergy, 8 août 2018.

[4] « 2019 Data Breach Investigations Report (Rapport d'enquête sur les violations de données de 2019) », Verizon, consulté le 8 juillet 2019.

[5] Neil MacDonald, « Zero Trust Is an Initial Step on the Roadmap to CARTA (La confiance zéro est une première étape sur la feuille de route de CARTA) », Gartner, 10 décembre 2018.

[6] John Maddison, « More Encrypted Traffic Than Ever (Plus de trafic crypté que jamais) », Fortinet, 10 décembre 2018.

[7] « 2018 Cost of a Data Breach Study (Coût d'une étude sur les violations de données en 2018) », Ponemon, juillet 2018.

[8] Idem.

www.fortinet.fr

361475-0-0-FR

septembre 24, 2020 3:08 PM

eb-traditional-segmentation