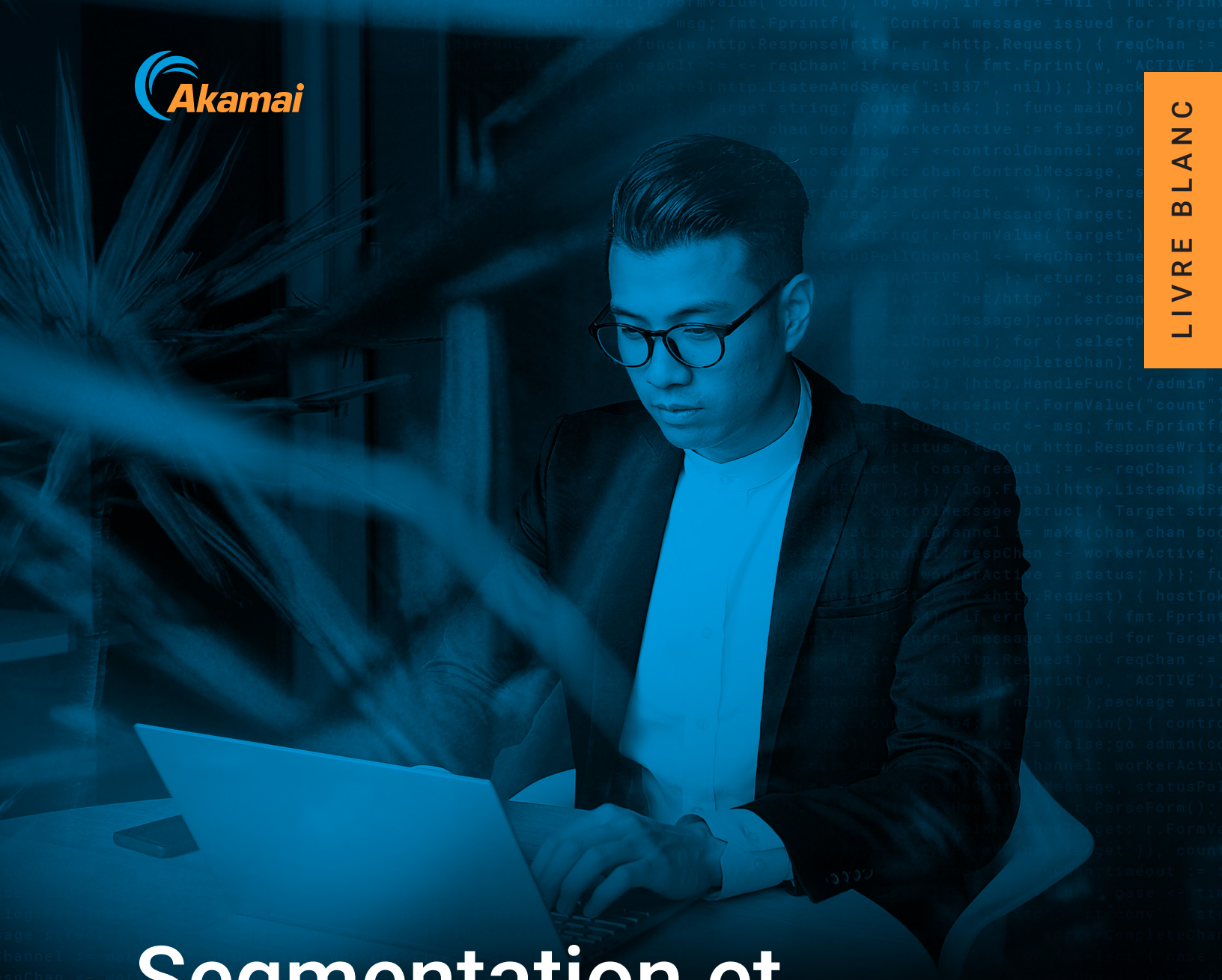
Akamai

LIVRE BLANC



Segmentation et microsegmentation du réseau dans les environnements d'entreprise actuels

Présentation

L'idée de segmentation n'est pas nouvelle en matière de sécurité. Les pare-feu de périmètre, ainsi que les VLAN et listes de contrôle d'accès, sont les moyens traditionnellement utilisés par la plupart des entreprises pour segmenter et protéger leur infrastructure informatique. Cependant, les temps changent. L'augmentation de la conteneurisation, la mise en réseau logicielle, l'utilisation d'une infrastructure publique et multicloud, et l'expansion des terminaux connectés à Internet ont créé un nouvel ensemble de problèmes de sécurité à traiter, qui nécessite une solution conçue pour un environnement informatique hétérogène avec différents ensembles d'exigences de sécurité. De plus, les ransomwares et les acteurs malveillants affiliés à des États nationaux représentent désormais un risque pour toute entreprise. Les attaques deviennent de plus en plus sophistiquées, alors même qu'il est de plus en plus difficile d'obtenir une visibilité sur votre environnement informatique. Les mesures de sécurité périmétrique traditionnelles, ainsi que les pare-feu de nouvelle génération basés sur l'inspection approfondie des paquets ou la détection basée sur les signatures, peinent à faire face au volume de trafic que connaît aujourd'hui le centre de données d'une entreprise. Voyons comment les bonnes techniques de microsegmentation constituent la meilleure technologie pour pallier les insuffisances des autres approches alternatives de segmentation du réseau.

> Les environnements de cloud hybride étant devenus la norme, ils requièrent un ensemble d'exigences spécifiques allant au-delà de la sécurité périmétrique traditionnelle

Les pare-feu traditionnels sont inadaptés au trafic est-ouest

Lorsqu'elle cherche à segmenter ses environnements informatiques, une entreprise peut d'abord se tourner vers les terminaux de sécurité périmétrique existants. Malheureusement, ces terminaux ont été conçus pour surveiller le trafic qui se déplace du nord au sud, du client au serveur. Cela inclut l'ensemble du trafic qui arrive dans le centre de données à partir d'une source externe. Plus récemment, le volume de trafic au sein du centre de données se déplaçant d'un serveur à l'autre, généralement appelé trafic est-ouest, a augmenté de manière exponentielle. Cela est en grande partie dû à la croissance de la virtualisation et de l'infrastructure convergente, notamment l'hyperviseur, le VPC et l'informatique basée sur les conteneurs.

Les mesures de sécurité périmétrique comme les pare-feu traditionnels ne protègent pas votre entreprise des terminaux infectés et n'empêchent pas les attaquants d'étendre leur emprise sur le trafic est-ouest. Avec l'essor du cryptage TLS et la facilité avec laquelle le trafic malveillant se dissimule dans les ports d'application légitimes ouverts, de nombreuses attaques peuvent passer même à travers les pare-feu. Vous n'êtes donc pas en mesure de repérer les violations existantes et de les résoudre ou de les déjouer. Cela signifie également que vous ne pouvez pas facilement limiter le temps de présence des attaquants sur votre réseau. Plus ce temps est long, plus la violation est catastrophique. L'Active Adversary Playbook 2022 de Sophos a révélé que, bien que la durée moyenne de présence soit de 15 jours, les petites entreprises et certains secteurs d'activité ont connu des durées moyennes de présence beaucoup plus longues, allant jusqu'à 34 jours.[1] Plus un attaquant peut passer inaperçu au sein de votre réseau, plus les dommages qu'il peut causer sont importants.

Il n'est tout simplement pas possible d'utiliser suffisamment de pare-feu virtualisés pour protéger des milliers d'applications ou de charges de travail. Même s'il était possible de créer une solution virtualisée, il serait impossible de la gérer ou de la contrôler, compte tenu des environnements dynamiques en constante évolution dans lesquels nous travaillons aujourd'hui. En matière de cloud hybride, par exemple, les pare-feu traditionnels sont encore plus difficiles à utiliser, car ils doivent fonctionner dans différents environnements, suivre les charges de travail dans différents clouds et être contrôlés à partir d'un point unique. Pour tenter de résoudre ces problèmes, plusieurs approches de segmentation du réseau ont vu le jour.

Trois approches de segmentation à envisager

Sachant que les pare-feu, même virtualisés, ne suffisent pas à protéger les centres de données du cloud hybride, les entreprises cherchent à appliquer la segmentation au sein de l'infrastructure est-ouest selon trois méthodes principales. Comme nous l'avons vu, en l'absence de règles de segmentation et de mesures de sécurité solides, n'importe quel port ou serveur peut communiquer avec n'importe quel autre. Cela signifie que si un pare-feu de serveur fait l'objet d'une violation, l'attaquant peut facilement se déplacer vers n'importe quel autre dans le réseau. Le moyen le plus efficace de limiter la connectivité entre les serveurs est de segmenter le réseau. Il existe trois grands types de segmentation du réseau, la microsegmentation étant la technologie que les entreprises peuvent utiliser pour appliquer des règles et un contrôle de plus en plus granulaires. Les utilisateurs peuvent combiner les trois types de règles de segmentation énumérés ci-dessous, afin d'élaborer des règles plus granulaires pour les applications critiques ou à risque.

Segmentation de l'environnement

Cette approche permet de séparer les différents environnements les uns des autres. Ainsi, les entreprises peuvent séparer la branche développement de leur société de l'environnement de production, par exemple. Il s'agit de la première étape cruciale de toute règle de segmentation, qui peut être suivie par la création de règles plus granulaires.

Segmentation de l'application

En approfondissant la segmentation, le « cloisonnement » des applications à forte valeur ajoutée permet de séparer chaque application critique spécifique du reste du réseau. Les meilleures solutions de microsegmentation permettent même de contrôler cette séparation au niveau du processus.

Segmentation de niveau

La forme la plus étroite de segmentation se trouve dans l'application elle-même. Dans ce cas, vous pouvez créer une règle de gestion des communications entre les différents niveaux du même cluster d'applications, en contrôlant le trafic entre les serveurs Web, les serveurs d'applications et les serveurs de bases de données, par exemple. Ce contrôle peut également être effectué au moyen d'une application au niveau du processus, si vous le souhaitez.

Méthode de segmentation du réseau — segmentation du réseau au moyen de VLAN

La plupart des entreprises commencent par employer des VLAN. Ces réseaux locaux virtuels permettent aux entreprises d'attribuer à chaque segment son propre chemin de communication, par l'intermédiaire d'un pare-feu ou de listes de contrôle d'accès (ACL) sur le routeur lui-même. Si le VLAN est un choix courant pour la segmentation du réseau, il n'en reste pas moins que de nombreux problèmes se posent en filigrane. Examinons plus en détail les raisons pour lesquelles les VLAN ne répondent pas aux besoins actuels en matière de sécurité.

Il est facile de comprendre pourquoi de nombreuses entreprises choisissent les VLAN comme méthode de segmentation. Il est possible de le faire avec l'architecture existante, ce qui rend leur déploiement peu coûteux et simple. Cependant, il s'agit d'une approche de segmentation très rigide et complexe, dont la maintenance peut s'avérer coûteuse et dont la mise en œuvre nécessite des temps d'arrêt.

Pour commencer à utiliser les VLAN, vous devrez vous familiariser avec les serveurs et dépendances de chaque segment, puis créer la configuration que vous souhaitez pour le ou les commutateurs du réseau que vous segmentez. Comme cette opération est réalisée par des ingénieurs réseau et qu'elle concerne souvent plusieurs sites, elle peut prendre plusieurs jours et coûter beaucoup de temps et d'argent. Le trafic peut être interrompu ou ralenti pendant la durée de la configuration.

À une époque où l'agilité est un avantage concurrentiel majeur, voire un impératif, des coûts élevés et une lenteur en matière d'évolution sont synonymes de résultats désastreux pour l'entreprise. Selon Forbes, la capacité d'adaptation est la clé de la survie : « La rupture n'est pas nouvelle, mais sa vitesse, sa complexité et sa dimension mondiale sont d'une ampleur inégalée jusqu'à présent. ... Ce ne sont pas les entreprises les plus grandes ou les plus stables financièrement qui survivront, mais celles qui parviendront à s'adapter à l'accélération exponentielle du rythme du changement. »[2]

Il est important de reconnaître que les VLAN n'ont pas été créés dans une optique de segmentation. Initialement conçus pour réduire la congestion, leur utilisation pour contrôler les communications n'est pas une façon intelligente de tirer parti de cette technologie existante. C'est à bien des égards une mauvaise utilisation. Il n'est donc pas surprenant que la segmentation à l'aide de VLAN comporte des limites.

- **Technologie cloud :** les VLAN et autres règles traditionnelles de segmentation du réseau ne peuvent pas être étendus au cloud. Si vous utilisez des pare-feu segmentés internes (ISFW) ou des listes de contrôle d'accès (ACL) pour déterminer quels utilisateurs peuvent accéder aux segments du réseau, vous devrez probablement vous appuyer sur le SDN (mise en réseau logicielle) pour le cloud. Cette méthode est généralement mise en œuvre par des fournisseurs de logiciels tiers qui utilisent des pare-feu ou des sous-réseaux virtualisés.
- **Conteneurs :** la sécurité reste une préoccupation majeure compte tenu de l'adoption généralisée des conteneurs dans les environnements informatiques. Comme chaque conteneur est exécuté sur le même noyau, un exploit pourrait mettre tous les conteneurs en danger. L'isolation est un combat permanent et ne peut être résolue par les méthodes habituelles de segmentation du réseau.
- **Restrictions de protocole :** la limite des VLAN est de 4 096 segments, ce qui limite la capacité à assurer une segmentation adéquate dans les grands centres de données. Les approches de segmentation plus granulaires ne présentent pas cette limitation.

De la segmentation du réseau à la segmentation des applications : introduction des contrôles de la couche 4

Bon nombre de ces problèmes ont été résolus en adoptant la segmentation des applications à l'aide de groupes de sécurité dans les environnements cloud et de pare-feu basés sur hyperviseur pour les environnements virtualisés sur site. La segmentation traditionnelle des applications met en œuvre des contrôles de niveau 4, ce qui permet d'isoler les niveaux de service les uns des autres, de sorte qu'une application dispose d'une limite sécurisée. Chaque niveau est limité au niveau d'accès dont il a besoin pour fournir toutes ses fonctionnalités, mais pas plus. La séparation entre les niveaux d'une application individuelle est claire, et la menace de compromission potentielle est réduite au minimum.

Imaginez les niveaux que vous pourriez trouver dans une entreprise standard, depuis les équilibreurs de charge et les bases de données jusqu'aux serveurs d'application à l'intérieur et à l'extérieur de votre propre zone démilitarisée (DMZ). La séparation de ces niveaux permet à chacun d'entre eux de disposer de ses propres règles et fonctionnalités de sécurité. La segmentation des applications permet aux entreprises de mettre en place les contrôles appropriés pour chaque niveau, en limitant les informations et communications sensibles, tout en autorisant un large accès des utilisateurs lorsque cela est nécessaire. Par exemple, une entreprise peut empêcher certaines bases de données de communiquer avec Internet ou s'assurer que si un attaquant s'introduit dans un simple équilibreur de charge, il ne peut pas se déplacer pour accéder à des informations plus sensibles sur le niveau de la base de données.

Lorsque la solution devient plus granulaire, la segmentation des applications permet à une entreprise de séparer un cluster d'applications entier des autres secteurs de l'entreprise. Comme nous l'avons vu, cela réduit la surface d'attaque et la capacité des attaquants à effectuer des mouvements latéraux d'un niveau à l'autre.

Les limites des contrôles de la couche 4

La segmentation traditionnelle des applications peut manquer de profondeur, ce qui a un impact direct sur votre visibilité. La couche réseau, où s'effectue le routage, déplace les données entre les systèmes, en attribuant des adresses IP et des protocoles qui détaillent le chemin emprunté par les segments de données jusqu'à leur destination. La segmentation des applications utilise souvent les contrôles réseau de la couche 4, en se concentrant sur la manière dont les données elles-mêmes sont acheminées. Les grands segments de données sont divisés en segments ou blocs plus petits, prêts à être reconstitués à leur destination. Le contrôle des flux permet d'accélérer ou de ralentir ce processus de manière dynamique, en fonction des besoins des terminaux qui envoient ou reçoivent les informations.

Dans l'écosystème actuel des menaces, les contrôles de ces couches sont essentiels, mais dans certains cas, il peut être souhaitable de pouvoir définir une règle à un niveau encore plus granulaire. Les attaquants ont démontré leur capacité à usurper des adresses IP et à utiliser des techniques de talonnage (piggybacking) sur les ports autorisés pour pénétrer dans un réseau. En outre, la protection de couche 4 ne limite pas les mouvements latéraux au sein d'une application ou d'un niveau, ce qui pourrait vous laisser avec une surface d'attaque plus grande que vous ne le souhaiteriez.

L'un des meilleurs exemples de la nécessité de contrôles plus granulaires que la simple couche 4 est celui des initiatives de mise en conformité. Les techniques traditionnelles de segmentation des applications ont, dans une certaine mesure, permis aux entreprises de satisfaire à certaines réglementations spécifiques en matière de conformité, comme la séparation du CDE pour PCI-DSS ou la protection des données personnelles pour HIPAA. Toutefois, si les techniques relatives à la couche 4 ont été acceptées par le passé comme des moyens efficaces de démontrer la conformité, la réalité a montré qu'elles n'étaient peut-être pas suffisantes. Selon le Verizon 2022 Payment Security Report, seuls 43 % des entreprises sont « entièrement conformes ».[3] Pire encore, une conformité à 100 % ne signifie pas pour autant une sécurité à 100 %. Bien que les contrôles de la couche 4 puissent vous couvrir en termes de conformité, ils ne réduisent pas suffisamment la surface d'attaque pour avoir un effet significatif sur la sécurité. Point final. Les attaquants peuvent utiliser un port ouvert de la couche 4 entre deux niveaux avec un processus distinct (couche 7) et s'emparer de tout ce qu'ils veulent.

Segmentation à l'aveugle : le manque de visibilité dans la segmentation du réseau et des applications

Comme le constatent les entreprises, s'il ne fait aucun doute que la segmentation des applications est un pas dans la bonne direction, elle ne va pas assez loin pour résoudre tous les problèmes inhérents à une approche de segmentation rudimentaire. Un autre défi à relever est celui de la visibilité. Il est essentiel de pouvoir disposer d'une vue d'ensemble précise et en temps réel de votre réseau à chaque étape de votre processus de segmentation, ce qui constitue une limitation de nombreuses approches.

Avant de commencer, vous devez visualiser les dépendances des applications afin de pouvoir élaborer des règles précises. Une fois la segmentation établie, vous devrez prouver qu'elle fonctionne comme prévu, non seulement pour confirmer la solidité de votre dispositif de sécurité, mais aussi pour apporter la preuve de votre conformité aux réglementations, le cas échéant.

Sans visibilité en temps réel et historique, vous ne disposez d'aucune preuve, ni pour vous, ni pour les parties prenantes tierces et les organismes de réglementation. La collecte manuelle de ces preuves est longue et coûteuse à gérer, et il y a toujours un risque d'erreurs de configuration. Une solution de segmentation qui ne peut pas fournir ce type de visibilité n'est tout simplement pas suffisante.

Microsegmentation jusqu'à la couche 7, la couche applicative

En revanche, la segmentation au niveau de la couche applicative (couche 7) est très efficace pour limiter les mouvements latéraux, même au sein d'un cluster d'applications. La couche 7 est celle où les services de réseau s'intègrent au système d'exploitation. Les protocoles tels que HTTP, FTP, TFTP et SMTP sont tous des protocoles de la couche 7. Les dernières avancées en matière de technologie de microsegmentation sont capables de segmenter cette couche avec beaucoup plus de profondeur que les autres solutions, ce qui permet à votre entreprise de visualiser et de contrôler l'activité au niveau de la couche 7 ainsi qu'au niveau de la couche 4 traditionnelle. Cela signifie qu'au lieu de s'appuyer sur les adresses IP et les ports, les entreprises peuvent utiliser des processus et des flux spécifiques lors de la configuration de leurs règles. Les avantages de la segmentation vont ainsi bien au-delà d'un niveau spécifique ou même d'un cluster d'applications. Elle permet également de repérer les menaces à l'aide d'un simple hachage erroné, même si l'attaquant reproduit un processus ou une voie d'accès autorisé.

En ce qui concerne la création de règles, la segmentation de la couche 7 permet d'établir des règles d'autorisation ou des exceptions très spécifiques, où seuls des processus ou flux précis sont autorisés et où toutes les autres communications sont bloquées par défaut. Cela permet de renforcer l'isolation des données entre les systèmes, tout en autorisant la communication pour les flux de données nécessaires ou critiques pour l'entreprise.

Les meilleures solutions de microsegmentation offrent la visibilité dont les entreprises ont besoin pour gagner en agilité

Avec des agents sur chaque charge de travail, basée sur un hyperviseur ou un VPC, des conteneurs, des serveurs bare-metal ou même des systèmes IoT/OT, une solution de microsegmentation holistique permet à votre entreprise de disposer d'une carte visuelle complète de l'ensemble de votre infrastructure informatique. Avec les solutions véritablement intelligentes, cela inclut les environnements de centre de données, de cloud, de multicloud et de cloud hybride, ainsi que les terminaux distants. Les solutions traditionnelles de segmentation des applications peinent à obtenir cette vue d'ensemble, généralement parce qu'elles utilisent une combinaison de technologies centrées sur le réseau.

Une carte visuelle complète de votre environnement devrait également vous indiquer quelles règles de sécurité sont en place et appliquées en temps réel. En un clin d'œil, vos ingénieurs et professionnels de la sécurité devraient être en mesure de voir les lacunes potentielles à combler dans la couverture de vos règles, ou les règles supplémentaires qu'ils doivent mettre en œuvre ou créer de toutes pièces.

Cette visibilité permet également à votre entreprise de se préparer aux nouveaux logiciels ou aux mises à jour des systèmes existants, en créant les règles de segmentation des applications mises à jour ou nouvelles avant qu'elles ne soient prêtes à être déployées. Une fois les mises à jour effectuées, vos équipes de sécurité disposent des informations en temps réel dont elles ont besoin pour détecter et résoudre les activités d'application sortant de la norme, en veillant à ce qu'aucun risque de sécurité ne passe inaperçu ou ne devienne un exploit actif. Après coup, votre entreprise dispose d'outils contextuels pour comparer un incident aux données historiques et comprendre l'environnement exact qui a permis à l'anomalie de se produire. Vous pouvez renforcer les règles, adapter la segmentation et détailler l'incident en vue d'une mise en conformité ou d'une étude plus approfondie.

Le choix du Zero Trust

Un autre avantage de la microsegmentation est sa capacité à adopter le modèle de sécurité Zero Trust. Bien que le principe de Zero Trust ait été lancé par Forrester en 2010, des technologies comme la microsegmentation contribuent à faire de ce concept une réalité, et les chercheurs et experts en sécurité continuent à en vanter les mérites.[4]

L'idée est simple : Aucun trafic ou utilisateur n'est fiable tant qu'il n'a pas été vérifié et approuvé, qu'il provienne d'une source externe ou interne, et ce à chaque tentative de connexion. Les trois grands principes de Zero Trust de Forrester[5] sont tous soutenus par des règles de microsegmentation solides et granulaires :

- Par défaut, aucune entité n'est considérée comme fiable
- Une surveillance complète de la sécurité est mise en œuvre
- L'accès de moindre privilège est appliqué

Le concept de Zero Trust est à l'opposé de la sécurité périmétrique, qui consiste à protéger les entrées de son château par des douves profondes et à supposer que tout ce qui se trouve à l'intérieur est autorisé à y pénétrer. Comme la plupart des entreprises ne disposent plus d'un réseau ou d'un centre de données confiné, l'idée d'un « château » est obsolète, et une stratégie du moindre privilège comme celle du Zero Trust est le seul moyen de s'assurer que vous pouvez savoir et contrôler qui se trouve à l'intérieur à n'importe quel moment.

Pérennisez votre entreprise avec la microsegmentation

La segmentation du réseau peut assurément aller au-delà de la sécurité périmétrique. La segmentation de l'environnement et des applications jusqu'à la couche 4 sont des étapes importantes dans l'élaboration de votre stratégie. Mais comme les environnements informatiques deviennent de plus en plus complexes, il vous faudra peut-être une solution de segmentation offrant encore plus de granularité avec la segmentation par niveau et la mise en œuvre au niveau des processus jusqu'à la couche 7 aux stades de l'application et du niveau.

Les entreprises actuelles ont dépassé le stade de l'infrastructure autonome. Elles s'appuient souvent sur des technologies comme le SDN dans le cloud, les conteneurs ou les hyperviseurs bare-metal. Elles travaillent dans différentes zones géographiques et dans des centres de données physiques.

Le seul moyen de se protéger des menaces externes et internes est d'utiliser une solution qui inspecte et contrôle l'ensemble du trafic, d'est en ouest comme du nord au sud, et qui, pour les applications cruciales ou à risque, offre une visibilité supérieure à celle que permet la seule couche 4. La microsegmentation jusqu'à la couche 7, au stade de l'application ou du niveau, vous permet d'avoir une vision précise de l'ensemble de votre environnement informatique et de créer et d'appliquer facilement des règles de sécurité granulaires suivant le modèle Zero Trust. Une bonne solution de microsegmentation ne vous demandera pas de choisir entre la sécurité et l'agilité, alors faites le choix qui vous offre la meilleure posture de sécurité globale dans toute votre organisation.

Pour plus d'informations, consultez le site akamai.com/guardicore.

1 Shier, John. 2022. « The Active Adversary Playbook 2022. » Sophos. 7 juin.

2 Gonda, Rob. 2018. « Adaptability Is Key To Survival In The Age Of Digital Darwinism. » Forbes. 24 mai.

3 https://www.verizon.com/business/reports/payment-security-report/

4 Holmes, David. Juin 2022. « Best Practices For Zero Trust Microsegmentation. » Forrester. Avril.

5 Holmes, David et Jess Burn. Janvier 2022. « The Definition Of Modern Zero Trust. » Forrester. Avril.

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous concevez, quel que soit l'endroit où vous le développez et où vous le diffusez. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre posture de sécurité, pour activer le Zero Trust, arrêter les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS, en vous donnant la confiance nécessaire pour innover, vous développer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de sécurité, de traitement et de diffusion d'Akamai, consultez akamai.com et akamai.com/blog, ou suivez Akamai Technologies sur Twitter et LinkedIn. Publication : 05/23.