NOTE DE SYNTHÈSE

Les défis de la gestion de la sécurité réseau

Examiner les obstacles à la gestion des risques, des opérations et des ressources

Résumé

Le déploiement rapide de pare-feux et d'autres services de sécurité sur les réseaux hyper-distribués et le besoin de mobilité dans la « nouvelle normalité » soulignent la nécessité d'une gestion unifiée de la sécurité dans les entreprises de toutes tailles. Cette note de synthèse explore les tendances émergentes et examine les défis de la sécurité réseau dans les domaines de la gestion des risques, des opérations de sécurité et de l'allocation des ressources.

Introduction

Le travail à domicile, les réseaux distribués, la migration vers le cloud et la prolifération des applications et des appareils ont entraîné une explosion des points d'exposition. Que ce soit pour une petite entreprise, une entreprise distribuée ou un fournisseur de services de sécurité gérés, la nécessité de protéger une entreprise « à tout moment et partout » est la nouvelle norme.

Dans le même temps, les menaces sont de plus en plus évasives. Avec une augmentation de 145 % des menaces non détectées d'une année à l'autre[1], les organisations ne peuvent tout simplement pas savoir quelles menaces ne sont pas détectées.

En outre, les départements informatiques sont confrontés à une augmentation des coûts, à une réduction des budgets et à un resserrement de la réserve de personnel qualifié.

Ensemble, ces forces créent des défis importants en matière de sécurité réseau, compliquant la tâche des départements informatiques pour contenir les risques, gérer les opérations et allouer les ressources.

Besoins différents

Toutes les organisations doivent comprendre et identifier les menaces en constante évolution. Elles ont toutes besoin d'informations sur les activités, l'utilisation et les risques du réseau. Elles doivent également toutes surveiller, dépanner et résoudre les problèmes opérationnels et de sécurité. Et elles doivent toutes respecter des règles de sécurité internes strictes.

Les petites entreprises peuvent cependant disposer de ressources techniques internes limitées. La gestion de la sécurité et l'optimisation des performances peuvent être accablantes. Et bien que les grandes entreprises et les grands fournisseurs de services puissent disposer d'équipes SecOps en interne, ils peuvent également être confrontés à des défis encore plus grands et plus complexes. Ils peuvent devoir étendre le déploiement et la gestion de la sécurité sur des réseaux distribués complexes. Ils s'inquiètent de l'automatisation de la sécurité et de la gestion des changements, des rapports d'audit et de la continuité des politiques.

Gestion des risques

Les organisations comprennent aujourd'hui qu'une journée normale peut virer au chaos complet en seulement quelques secondes. Le risque d'être victimes d'attaques ciblées persiste, alors que des informations sur le piratage de réseaux et l'exposition massive de données continuent de faire la une des journaux.

Comment savoir dans quelle mesure votre organisation est menacée ? Y a-t-il des failles de sécurité dans vos opérations internes ? Qu'en est-il des utilisateurs de votre réseau et des actifs, sites web et applications SaaS qu'ils utilisent ? Et comment décidez-vous de hiérarchiser et d'éliminer ces risques ?

Le trafic d'applications et de données passe par le réseau Internet, des campus distants, des succursales et peut-être même des fournisseurs tiers. Les organisations peuvent avoir une visibilité et un contrôle insuffisants sur les activités réseau dangereuses, les irrégularités du trafic, l'accès et le mouvement inhabituels des données, le firmware non corrigé, les événements de sécurité et la santé du système.

Les risques qui ne sont pas éliminés peuvent aggraver la situation. Une faille peut ralentir la dynamique et la croissance d'une entreprise. Les opérations sont perturbées car le personnel clé détourne son attention des priorités commerciales stratégiques. Les responsables sont obligés de tout mettre en œuvre pour limiter les dégâts et gérer les relations publiques. L'incapacité à reconnaître les risques de sécurité entrave la planification de la sécurité, les décisions en matière de politiques et les mesures décisives.

Opérations de sécurité

Les pare-feux eux-mêmes sont également des points d'exposition. Les recherches de Gartner[2] suggèrent que 99 % des brèches dans les pare-feux sont causées par une mauvaise configuration. Lorsque des règles de pare-feu sont créées, copiées et modifiées, elles peuvent être en contradiction les unes avec les autres, entraînant des conséquences indésirables sur la sécurité et les performances. Une mauvaise configuration et des règles contradictoires peuvent rendre le réseau vulnérable aux menaces sophistiquées, aux accès non autorisés ou aux intrusions.

Plutôt que de traquer les failles de sécurité et les vulnérabilités, il vaut mieux consacrer du temps à s'assurer que la configuration des pare-feux ne soit pas trop laxiste ni ouvre des portes dérobées à leurs infrastructures. Les organisations doivent valider et auditer les politiques et configurations avant de les déployer, et les inverser rapidement si nécessaire.

La transition vers des réseaux multi-cloud plus grands et plus complexes prenant en charge davantage d'applications et d'utilisateurs crée un nouvel espace de travail numérique. À mesure que les réseaux se développent, gérer les opérations de sécurité, optimiser les performances, résoudre les problèmes opérationnels, mettre en place des mesures de sécurité et contrôler l'accès pour les utilisateurs, les appareils et les applications restent des défis complexes.

Les organisations peinent à mettre en place des opérations de sécurité internes adéquates pour se conformer aux politiques internes de niveau de service. Ces politiques visent à protéger les entreprises et leurs employés, à réduire les risques de sécurité et à limiter les responsabilités financières et juridiques.

En gérant des pare-feux disparates individuellement et manuellement, les organisations sont souvent confrontées à des politiques et procédures incohérentes. Il existe souvent peu ou pas de processus d'analyse, de test, d'audit et d'approbation pour s'assurer que l'entreprise applique les bonnes règles de pare-feu, au bon moment et conformément aux exigences de conformité interne.

[1] Rapport 2020 sur les cybermenaces de SonicWall
[2] Sécurité des informations

Allocation des ressources

La pénurie de talents formés dans le secteur de la sécurité a fait du recrutement une préoccupation sérieuse. De nombreuses organisations, en particulier les PME, ne disposent pas des compétences et des talents adéquats en matière de sécurité pour maintenir efficacement les pare-feux et résoudre les graves problèmes de sécurité lorsqu'ils surviennent.

Même un seul pare-feu nécessite une maintenance planifiée régulière, une surveillance quotidienne, des tâches de révision et d'administration des politiques et des mises à niveau du firmware. À mesure que les réseaux s'étendent et se développent entre les entreprises distribuées et les réseaux de fournisseurs multi-locataires, la charge de travail du personnel de sécurité augmente de manière exponentielle.

Pire encore, le personnel des opérations de sécurité peut être accablé par la gestion et l'exploitation de silos de pare-feu complexes et fragmentés. Les tâches administratives sont souvent complexes, lourdes et laborieuses. Les tâches et processus sont généralement non contrôlés, non corroborés et non conformes. Cela mène à une situation où les petits réseaux peuvent accumuler des dizaines de règles de pare-feu sur de nombreuses années, tandis que les grands réseaux peuvent en accumuler des milliers.

Conclusion

Il faut trouver une meilleure solution pour l'avenir. Des outils de gestion plus intelligents sont nécessaires pour que les équipes de sécurité puissent faire leur travail efficacement.

La solution SonicWall Network Security Manager (NSM) vous offre tout ce dont vous avez besoin pour une gestion complète des pare-feux. Elle offre une visibilité complète, un contrôle granulaire et la capacité de gouverner l'ensemble des opérations de sécurité réseau de SonicWall avec plus de clarté, de précision et de rapidité. Et elle accomplit tout cela à partir d'une seule interface riche en fonctions, accessible de n'importe où en utilisant n'importe quel appareil disposant d'un navigateur Web.

Découvrez-en plus. Contactez votre représentant SonicWall ou rendez-vous sur www.sonicwall.com/nsm.

À propos de SonicWall

SonicWall offre une Boundless Cybersecurity pour l'ère de l'hyper-distribution dans une réalité professionnelle où tout le monde est mobile, travaille à distance et sans sécurité. En connaissant l'inconnu, en offrant une visibilité en temps réel et en permettant de véritables économies, SonicWall comble le fossé commercial en matière de cybersécurité pour les entreprises, les gouvernements et les PME du monde entier. Pour en savoir plus, rendez-vous sur www.sonicwall.com.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

SONICWALL®

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965