RESUMO EXECUTIVO

Os desafios do Gerenciamento de Segurança de Rede

Análise dos obstáculos para gerenciar risco, operações e recursos

Resumo

A rápida implantação de firewall e de outros serviços de segurança em redes hiperdistribuídas e a necessidade de mobilidade no "novo normal" ressaltam a necessidade de gerenciamento de segurança unificado em empresas de todos os tamanhos. Este resumo explora as tendências emergentes e examina os desafios de segurança da rede nas áreas de gerenciamento de risco, operações de segurança e alocação de recursos.

Introdução

O trabalho em casa, as redes distribuídas, a migração para a nuvem e a proliferação de aplicações e dispositivos resultaram em uma explosão de pontos de exposição. Em uma pequena empresa, uma empresa distribuída ou um fornecedor de serviços de segurança gerenciada, a necessidade de proteger os "negócios a qualquer hora e em qualquer lugar" é o novo normal.

Ao mesmo tempo, as ameaças são cada vez mais evasivas. Com o aumento do número de ameaças não detectadas de 145% ano a ano[1], as organizações talvez não tenham ideia das ameaças que estão passando despercebidas.

Além disso, as organizações de TI enfrentam aumento dos custos, redução de orçamentos e um conjunto mais restrito de funcionários qualificados.

Quando combinados, esses fatores criam desafios significativos de segurança de rede para a TI conter riscos, gerenciar operações e alocar recursos.

Necessidades diferentes

Todas as organizações precisam entender e identificar ameaças em evolução. Todas elas precisam ter conhecimento das atividades da rede, uso e risco. Também precisam monitorar, solucionar problemas e resolver desafios operacionais e de segurança. E todas elas devem cumprir diretrizes rigorosas de segurança interna.

As pequenas empresas, no entanto, podem ter recursos técnicos internos limitados. O gerenciamento da segurança e a otimização do desempenho podem ser tarefas demasiadamente exaustivas. Embora grandes empresas e fornecedores de serviços tenham funcionários internos de SecOps, podem enfrentar preocupações ainda maiores e mais desafiadoras. Talvez precisem escalar a implantação e o gerenciamento da segurança em redes distribuídas complexas. Têm preocupações sobre automação de segurança e gerenciamento de alterações, relatórios de auditoria e continuidade de políticas.

Gerenciamento de risco

As organizações hoje entendem que as coisas podem sair do normal em um dia para o completo caos em questão de segundos. O risco de ser vítima de ataques direcionados persiste para muitas organizações enquanto as violações de rede e a exposição maciça de dados continuam sendo noticiadas.

Como você sabe até que ponto sua organização está em risco? Suas operações internas contêm falhas de segurança? E quanto aos usuários da rede e aos ativos, sites e aplicações SaaS que utilizam? E como você decide priorizar e lidar com esses riscos?

O tráfego de aplicações e dados atravessa a Internet, unidades remotas, filiais e talvez até mesmo fornecedores de terceiros. As organizações podem ter visibilidade e controle insuficientes sobre atividades de rede inseguras, irregularidades de tráfego, acesso e movimentação incomuns de dados, firmware sem aplicação de patch, eventos de segurança e integridade do sistema.

Os riscos que não são gerenciados podem dar início a algo pior. Uma violação retarda o impulso e o crescimento de uma empresa. As operações são interrompidas quando a equipe principal desvia o foco das principais prioridades dos negócios. Os executivos são obrigados a dedicar

todo o seu tempo ao controle dos danos e às relações públicas. A incapacidade de reconhecer riscos de segurança impossibilita o planejamento de segurança, as decisões de política e as medidas decisivas.

Operações de segurança

Os próprios firewalls também são pontos de exposição. Uma pesquisa da Gartner[2] sugere que 99% das violações de firewall são causadas por configurações incorretas dos firewalls. Quando as regras do firewall são criadas, copiadas e alteradas, podem ter um conflito entre si, causando consequências indesejadas à segurança e ao desempenho. Configurações incorretas e regras conflitantes podem tornar a rede vulnerável a ameaças sofisticadas, acesso não autorizado ou invasão.

Em vez de rastrear brechas e vulnerabilidades de segurança, é possível utilizar melhor o tempo certificando-se de que as configurações do firewall não sejam excessivamente permissivas e não deixem backdoors abertas para as infraestruturas. As organizações precisam validar e auditar políticas e configurações antes de implementá-las e revertê-las rapidamente se necessário.

A migração para redes maiores e mais complexas com várias nuvens, comportando mais aplicações e usuários, forma um novo local de trabalho digital. Com o crescimento das redes, o gerenciamento das operações de segurança, a otimização do desempenho, a solução de problemas operacionais e a garantia de medidas de segurança e acesso ao controle para usuários, dispositivos e aplicações continuam sendo desafios complexos.

As organizações se esforçam para estabelecer operações adequadas de segurança interna para cumprir as políticas internas de nível de serviço. Essas políticas destinam-se a proteger as empresas e os funcionários, reduzir riscos de segurança e limitar as responsabilidades financeiras e jurídicas.

Com o gerenciamento de dispositivos de firewall diferentes, individual e manualmente, as organizações no geral experienciam políticas e procedimentos inconsistentes. Com frequência, há pouco ou nenhum processo de análise, teste, auditoria e aprovação, para garantir que a empresa esteja executando as regras corretas de firewall no momento certo e segundo os requisitos internos de conformidade.

Alocação de recursos

A falta de talento treinado no setor de segurança transformou a seleção de funcionários em uma preocupação importante. Muitas organizações, especificamente SMBs, não têm talentos e qualificações de segurança adequados para fazer a manutenção eficiente dos firewalls e solucionar problemas de segurança graves quando surgem.

Até mesmo um único firewall precisa de manutenção planejada regularmente, monitoramento diário, revisão e administração de políticas e atualizações de firmware. Com a expansão e o crescimento das redes em empresas distribuídas e redes de provedores com vários usuários, a responsabilidade da equipe de segurança se multiplica exponencialmente.

Para piorar a situação, a equipe de operações de segurança pode estar sobrecarregada com o gerenciamento e a operação de silos de firewall complexos e fragmentados. As administrações costumam ser complexas, complicadas e trabalhosas. As tarefas e os processos geralmente não são verificados, corroborados nem compatíveis. Isso gera uma situação em que redes pequenas possam acumular dezenas de regras de firewall por muitos anos, enquanto redes maiores podem ter milhares.

Conclusão

É necessário haver uma solução melhor. Ferramentas de gerenciamento mais inteligentes são necessárias para que as equipes de segurança façam seu trabalho com eficiência.

O SonicWall Network Security Manager (NSM) contém todo o necessário para um gerenciamento de firewall abrangente. Ele oferece ampla visibilidade, controle detalhado e capacidade para controlar todas as operações de segurança de rede da SonicWall com mais clareza, precisão e rapidez. E ele faz tudo isso por meio de uma única interface repleta de funções que pode ser acessada de qualquer local, em qualquer dispositivo com um navegador da Web.

Saiba mais. Entre em contato com seu representante da SonicWall hoje mesmo ou acesse www.sonicwall.com/nsm.

Sobre a SonicWall

A SonicWall oferece Boundless Cybersecurity ou Cibersegurança sem Limites para a era da hiperdistribuição e uma realidade de trabalho em que todos trabalham remotamente, têm mobilidade e estão protegidos. Com o conhecimento do desconhecido, a disponibilização de visibilidade em tempo real e a viabilização de uma economia revolucionária, a SonicWall fecha a lacuna no ramo de cibersegurança para corporações, governos e pequenas e médias empresas no mundo inteiro. Para obter mais informações, visite www.sonicwall.com.

[1] Relatório de Ameaças Cibernéticas da SonicWall 2020
[2] Segurança de Informações

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consulte nosso website para obter informações adicionais.
www.sonicwall.com/pt-br/

ExecutiveBrief-TheChallengeOfNSM-US-VG-1965