WHITE PAPER – **FEVEREIRO DE 2018**

DICAS E SUGESTÕES PARA IMPLANTAÇÃO DA SEGURANÇA CIBERNÉTICA DE PRÓXIMA GERAÇÃO USANDO A MICROSSEGMENTAÇÃO

Reformulação da estratégia de segurança para atender aos desafios de segurança de próxima geração

vmware®

Índice

O "mercado" de invasões tornou-se multibilionário e tem como objetivo roubar dados importantes e obter acesso aos sistemas mais confidenciais das organizações. Essa prática recebe o apoio de talentosos hackers e engenheiros que possuem recursos financeiros substanciais. Além disso, as empresas estão descobrindo que as estratégias tradicionais de segurança focadas no perímetro não são mais eficazes.

As vulnerabilidades não vão desaparecer. Os profissionais de segurança das empresas precisam acertar sempre, o hacker precisa acertar uma só vez. Os dados da Ponemon deixam isso bem claro: De acordo com a pesquisa, 89% das organizações já sofreram uma violação de dados.[1] Os hackers também buscam roubar credenciais de administradores privilegiados para atravessar o firewall e ter acesso a toda a infraestrutura de TI. Isso exige que novas estratégias de segurança cibernética sejam implantadas dentro do perímetro.

No entanto, adicionar uma infinidade de produtos de segurança novos e exclusivos também não é a melhor abordagem. Isso aumenta a complexidade da pilha de segurança e exige recursos humanos adicionais, que são escassos. A estratégia correta deve simplificar as operações diárias, oferecer uma abordagem fundamental de proteção e comportar a agilidade da TI, que é o objetivo de toda organização. O foco deve estar na proteção aprimorada de dados e cargas de trabalho/aplicativos críticos e não na criação de uma cerca maior. Assim, se uma organização sofrer violações, a segurança poderá impedir a disseminação lateral de ameaças. As empresas precisam de uma plataforma projetada para atender a essas necessidades e para facilitar a interação e a implantação eficientes de políticas e processos em operações de sistema, operações de rede e operações de segurança (SysOps, NetOps, SecOps respectivamente, pelas siglas em inglês).

Para alcançar esse novo nível de proteção dentro da infraestrutura de TI, as organizações precisam ter visibilidade completa da rede e do tráfego. Uma rede virtual é a melhor maneira de conseguir isso. Uma rede virtual também oferece microssegmentação que protege, com eficiência, as cargas de trabalho críticas dentro do firewall. Ela oferece suporte a comunicação e coordenação aprimoradas entre SysOps, NetOps e SecOps, permitindo a criação e a implantação de políticas de segurança refinadas para proteger os ativos mais valiosos da organização. Com a virtualização de redes e a microssegmentação, a mesma linguagem e os mesmos termos são usados em todos os três grupos, permitindo a implantação de políticas consistentes de modo muito mais simples. A visibilidade consistente também é fornecida aos grupos para permitir tarefas e atividades específicas.

A virtualização da rede oferece mais do que apenas benefícios de segurança

Este white paper se concentra nos benefícios da implantação da microssegmentação por meio de uma infraestrutura de rede virtual. No entanto, há outros benefícios importantes provenientes da rede virtual que resolvem problemas comuns em empresas de pequeno e médio porte. Esse "aproveitamento da solução" é importante, pois oferece melhor retorno sobre o investimento em uma implantação de rede virtual. Além disso, usar uma plataforma comum para múltiplas funções simplifica as operações e melhora a eficiência.

Talvez o benefício adicional mais notável de uma rede virtual seja o fornecimento de recursos importantes de recuperação de desastre (DR, pela sigla em inglês). Usando uma plataforma de rede virtual, como o VMware NSX®, as organizações podem transferir a configuração de rede e segurança para um site diferente ou para um site de recuperação se houver alguma falha. O NSX reconfigura automaticamente endereços IP, implementa políticas de segurança e elimina a necessidade de tarefas manuais para sincronizar a configuração em muitos sites físicos.

1 "The Evolving Role of CISOs and Their Importance to the Business", Ponemon Institute, 2 de novembro de 2017

Outro benefício é a utilização do recurso de balanceamento de carga da rede virtual. Ele atenua a necessidade de soluções pontuais que adicionam custo e complexidade ao ambiente. Além disso, ao usar o balanceamento de carga na plataforma de rede virtual, é possível ter uma visão mais completa para garantir os níveis de serviço, principalmente quando a plataforma está vinculada às informações sobre cargas de servidor.

As redes virtuais também melhoram a produtividade das equipes de rede e segurança. O uso de uma plataforma comum na qual as equipes de SecOps, NetOps e SysOps possam interagir reduz as frustrações diárias e elimina as exigências de uma das equipes que geram dificuldades para as outras duas. Todos trabalham em condições de igualdade. Embora o benefício mais importante da implantação da microssegmentação em uma rede virtual seja evitar ou reduzir drasticamente o impacto das violações, ela também protege as carreiras dos membros de equipe. Fazer parte de uma equipe que sofreu uma violação substancial de dados é algo ruim para o currículo dos profissionais.

Como começar a usar a microssegmentação

A microssegmentação é uma nova solução de segurança cibernética para muitas empresas de pequeno e médio porte. No entanto, para que a solução tenha êxito, as equipes precisam desenvolver um processo de implantação eficaz. Existem três etapas importantes que fornecem um ponto de partida para o processo:

1. **Determinar os fluxos de rede na sua organização.** O foco deve estar nos dados que entram, saem e permanecem no data center. Essa atividade também pode revelar ineficiências que afetam a latência do aplicativo e criam cargas na rede. Para iniciar a análise, revise as regras de firewall do perímetro e identifique o tráfego norte-sul e leste-oeste. É possível usar diferentes ferramentas para coletar e analisar fluxos de tráfego. Para começar, você pode usar o IPFIX (um protocolo de monitoramento de fluxos) para coletar e analisar o tráfego. Em seguida, você pode usar ferramentas comerciais de monitoramento para desenvolver um nível mais profundo de análise e correlacionar fluxos de tráfego com as políticas do firewall.

2. **Identificar padrões e relações no tráfego.** O conjunto inicial de políticas de segurança para o modelo de microssegmentação pode ser criado correlacionando os padrões de fluxo coletados na etapa anterior e as políticas atuais do firewall do perímetro. Os padrões de fluxo fornecem as principais informações sobre as relações entre as cargas de trabalho no data center. É importante entender como as cargas de trabalho interagem umas com as outras. Isso inclui a forma como uma carga de trabalho específica interage com os serviços de TI compartilhados, com outros aplicativos e com outras cargas de trabalho. Também é importante entender as interações em ambientes diferentes, como produção e desenvolvimento/teste. Depois que essas relações forem identificadas e documentadas, você terá os principais dados de entrada para definir os microssegmentos e as políticas de interação.

3. **Criar e aplicar o modelo de política.** Uma abordagem comprovada é a aplicação da microssegmentação a um aplicativo por vez. Essa abordagem tem muitos méritos, pois não sobrecarrega a equipe e permite que a organização implante a microssegmentação de acordo com seu próprio ritmo. Muitas empresas de pequeno e médio porte começam com uma abordagem de "bloco padrão" que proíbe toda a comunicação entre as cargas de trabalho no aplicativo em que elas estão concentradas. Em seguida, elas podem começar a abrir a comunicação com base na análise dos seus respectivos padrões de tráfego. Se comunicação adicional for necessária, será possível abri-la com base na demanda. No entanto, se você estiver preocupado com a interrupção de um serviço, ao implantar uma abordagem de bloco padrão, será possível começar com uma "permissão padrão", que permite comunicações abertas. Use essa abordagem com o máximo de cuidado. É possível adicionar restrições, pois elas não têm impacto sobre o aplicativo.

Além disso, conforme os novos requisitos de aplicativos, usuários e dados tornam-se conhecidos, o modelo de microssegmentação pode ser atualizado para refleti-los. Para tornar esse processo ainda mais simples, o VMware NSX também fornece o Application Rule Manager, uma ferramenta automatizada que recomenda políticas de microssegmentação com base nesses dados.

Dicas e sugestões para implantação bem-sucedida da microssegmentação

Assim como em qualquer solução de tecnologia, há dicas e sugestões específicas que podem ajudar a tornar a implantação mais eficiente. Algumas das mais importantes incluem:

- Utilizar o VMware Application Rule Manager (ARM): o ARM é um recurso que reúne todas as informações de fluxo de que você precisa ou que convém avaliar para um subconjunto de máquinas virtuais no ambiente. O ARM recomenda automaticamente políticas de microssegmentação com base na própria inteligência analítica da ferramenta para logo inseri-las na tabela de regras com apenas alguns cliques.
- Mapear primeiro seus grupos de segurança: começando com um senso de estrutura e definição de seus grupos de segurança, você iniciará a partir de um ponto adequado para a sua organização.
- Desenvolver convenções de nomenclatura consistentes para os grupos de segurança: as convenções de nomenclatura e os nomes reais são facilitadores importantes para obter uma implantação coesa da microssegmentação. Antes de ser usada, a convenção de nomenclatura deve ser consistente e estar de acordo com SysOps, SecOps e NetOps.
- Criar uma equipe multifuncional para oferecer suporte à implantação da microssegmentação: o êxito de uma implantação de microssegmentação é diretamente afetado pelo suporte dos três principais grupos que a usarão. Por esse motivo, é essencial que a equipe que projeta e implanta a solução tenha funcionários de SysOps, SecOps e NetOps.

Suporte executivo para uma iniciativa de microssegmentação

Para garantir suporte ao investimento e recursos necessários para o êxito do projeto, é importante contar com a gerência executiva e a gerência de TI. Falar a língua deles é essencial.

Gerência executiva/superior

Os principais executivos estarão focados nos benefícios dos negócios. A discussão com eles deve se concentrar na capacidade de reduzir o impacto de qualquer violação de dados, impedindo que os invasores tenham acesso a aplicativos e dados confidenciais. A microssegmentação também ajuda a atender às diretivas de conformidade, reduzindo ou eliminando a perda de dados.

Informe também aos executivos que os novos aplicativos, as mudanças nos processos de negócios e as novas demandas de segurança são facilmente gerenciados e contabilizados por meio da microssegmentação. Do ponto de vista dos custos, implantar a microssegmentação em uma rede virtual, como o NSX, trará economia, ao reduzir a necessidade de ferramentas separadas de DR e balanceamento de carga. A conversa com esses executivos deve tratar de uma plataforma única, muito mais econômica, que oferece segurança aprimorada e outros benefícios.

Diretor-executivo de informação e vice-presidente de TI

É provável que esses executivos já conheçam os benefícios básicos da microssegmentação. Portanto, o foco da discussão deve se centrar nas vantagens que a microssegmentação oferece com respeito às suas principais preocupações: segurança de dados, agilidade e economia.

Do ponto de vista da segurança de dados, a microssegmentação é a melhor ferramenta. Ela oferece proteção eficaz para os dados e aplicativos confidenciais. Além disso, ela oferece suporte à proteção ágil de aplicativos e dados, permitindo a modificação das políticas de segurança em tempo real. Isso leva à agilidade. À medida que novos aplicativos são lançados ou novas fontes de dados são definidas, as políticas de microssegmentação podem ser usadas para proteger esses recursos de maneira imediata, eliminando os "atrasos" de segurança.

A microssegmentação também permite comunicação e coordenação claras entre as equipes de SecOps, NetOps e SysOps para garantir que a colaboração entre elas seja coerente. A plataforma de rede virtual que oferece a microssegmentação disponibiliza recursos de DR e balanceamento de carga, eliminando a necessidade de adquirir outras soluções caras.

Resumo e principais conclusões

As empresas de pequeno e médio porte deparam-se com as mesmas exigências de segurança cibernética que as empresas de grande porte, mas possuem muito menos recursos para se proteger. Por esse motivo, elas precisam trabalhar de maneira mais inteligente e eficiente para implantar a proteção cibernética. A microssegmentação é excelente para essas demandas. Ela aumenta o firewall de perímetro, fornecendo proteção contra ameaças que conseguem violar a segurança de perímetro e impedindo-as de obter acesso adicional a sistemas confidenciais. Ela também é uma solução mais simples de operar.

A microssegmentação de uma rede virtual melhora a segurança cibernética, mas a rede virtual oferece outros benefícios operacionais importantes, como recuperação de desastres e balanceamento de cargas, sem a necessidade de adquirir soluções adicionais e caras. Para obter mais informações, veja estes recursos adicionais:

- Cinco etapas para microssegmentação
- Forrester: The Total Economic Impact™ of VMware NSX
- Micro-segmentation for Dummies, 2nd Edition
- Avaliação da rede virtual da VMware

Esses recursos, juntamente com as dicas e sugestões deste documento, ajudarão você a implantar com êxito essa importante tecnologia.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel.: +1-877-486-9273 Fax: +1-650-427-5001 www.vmware.com
Rua Surubim, 504 4º andar CEP: 04571-050 Cidade Monções – São Paulo - SP Tel.: (11) 5509-7200 www.vmware.com/br

2/18