TRÊS ETAPAS IMPORTANTES PARA TRANSFORMAR A SEGURANÇA DE TI

Segurança é a principal preocupação de todas as empresas

À medida que pessoas, dispositivos e objetos se tornam mais conectados, proteger todas essas conexões e ambientes se tornou mais importante do que nunca. Em uma pesquisa recente sobre prioridades de TI, 69% dos entrevistados disseram à Tech Pro Research que melhorar a segurança representou a principal iniciativa de TI para 2017.[1]

Na mesma pesquisa, os entrevistados também disseram que a segurança seria o maior desafio de TI no próximo ano. Isso ocorre porque as organizações de TI precisam proteger cada interação entre usuários, aplicativos e dados, independentemente de como e onde eles estejam se conectando. Além disso, elas precisam fazer isso em um ambiente cada vez mais dinâmico e que está em constante mudança.

Os riscos à segurança são elevados para empresas de todos os setores e continuam aumentando. De acordo com um estudo recente, o custo total médio de uma violação de dados aumentou de US$ 3,52 milhões para US$ 3,79 milhões em apenas um ano.[2] Para organizações que estão adotando ambientes em nuvem e virtualizados, visibilidade e controle máximos são fundamentais para atenuar esse risco.

Riscos evoluídos em um cenário dinâmico de ameaças

Todos os negócios se tornaram um negócio digital; uma transformação que deu origem a mudanças significativas no cenário de TI e, consequentemente, novos desafios para a segurança de TI.

Comece com a evolução das infraestruturas de aplicativos, que passaram de data centers locais que executam infraestrutura física a ambientes altamente dinâmicos que residem em nuvens públicas e privadas. Além disso, considere como os próprios aplicativos estão mudando. As organizações estão migrando das pilhas de aplicativos monolíticos para os aplicativos distribuídos e de multicamadas baseados em microsserviços. À medida que a força de trabalho se torna mais móvel e distribuída, os ambientes de usuários finais também estão evoluindo. Eles não estão mais limitados aos desktops administrados corporativamente, mas estão centrados em dispositivos móveis, estratégia BYOD e a Internet das Coisas (IoT, Internet of Things).

Como resultado, os modelos de segurança de perímetro de rede tradicionais já não são suficientes para proteger a expansão de aplicativos e usuários ou atender aos requisitos crescentes de conformidade. Ambientes e usuários não estão perfeitamente protegidos por firewalls de perímetro, mas exigem uma proteção mais flexível e ágil contra invasores que se tornaram cada vez mais sofisticados. O ciberespaço está cada vez mais armado. Mesmo um hacker inexperiente que usa kits de ferramentas, como Zeus e BlackPoS, pode segmentar um negócio com ataques avançados e causar danos reais à produtividade, aos recursos e à reputação.

À medida que nos ajustamos para responder a esses novos desafios de desenvolvimento, os padrões de conformidade estão se tornando cada vez mais complexos e forçando a equipe de TI média a gastar 20% de seu tempo em esforços para manter a conformidade.

OS RISCOS DE SEGURANÇA SÃO ALTOS

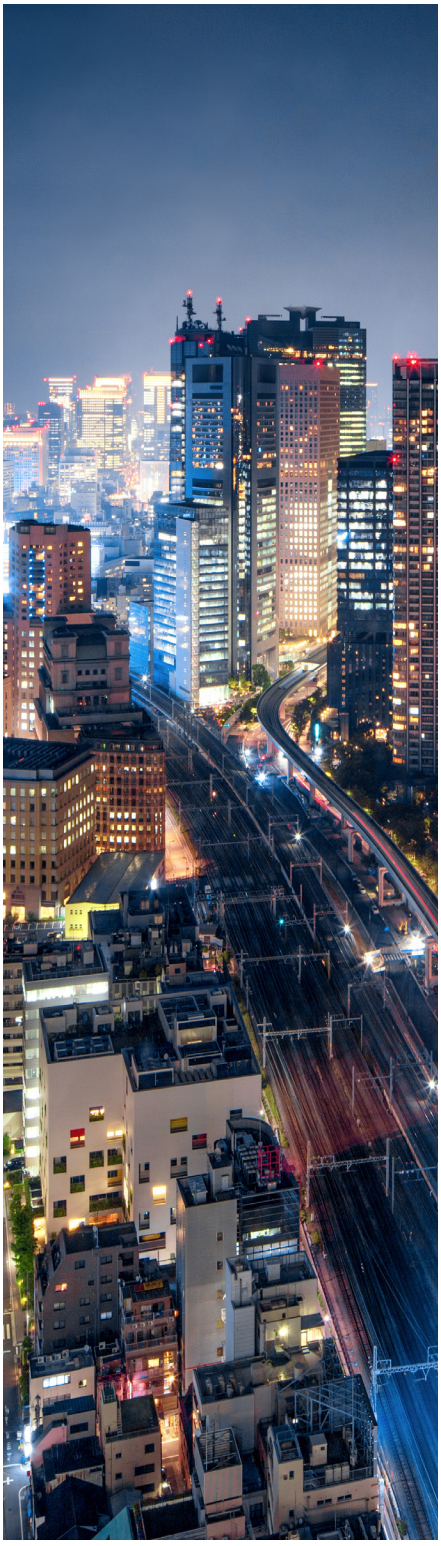
- O crime cibernético representa a causa mais rápida de interrupções de data centers, aumentando de 2% em 2010 para 22% em 2016.[3]
- O custo médio de uma interrupção de data center aumentou para US$ 740.357 em 2016.[4]

[1] "IT Budget Research: Where CXOs are placing their bets for 2017", Tech Pro Research, julho de 2016.

[2] https://www.sdxcentral.com/articles/analysis/securing-cloud-sdn/2016/05/.

[3] Cost of Data Center Outages, Ponemon Institute, janeiro de 2016.

[4] Ibid.



Três áreas de foco para segurança de TI efetiva

Proteger uma organização com uma solução de segurança robusta e compatível não é fácil quando a infraestrutura e seus usuários estão mudando rapidamente. As antigas regras básicas de segurança da rede simplesmente não se aplicam mais, e as equipes de TI precisam acompanhar o ritmo de:

- Alteração de infraestruturas: a infraestrutura utilizada para executar aplicativos como servidores Web e de banco de dados está evoluindo a partir de ambientes locais para oferecer suporte a aplicativos distribuídos e em nuvem.
- Aumento da mobilidade: a TI precisa expandir suas políticas de segurança para oferecer suporte a uma grande quantidade de novos dispositivos e modelos.
- Maior conformidade: o ambiente de conformidade normativa se torna cada vez mais complexo à medida que as organizações enfrentam novos requisitos.

Fornecer visibilidade e contexto para transformação da segurança

Para ficar um passo à frente de suas necessidades de segurança em constante mudança, você precisa de visibilidade aprofundada em todas as interações entre usuários e aplicativos. Você também precisa de uma solução que forneça contexto para entender o que essas interações significam. Em combinação, maior visibilidade e contexto podem ajudar a alinhar os controles e as políticas de segurança aos aplicativos que você deve proteger.

Qual é a base para essa solução? Uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints que seja independente da infraestrutura física subjacente ou da localização.

FIGURA 1. Uma camada de software onipresente significa que a segurança está em todos os lugares

Na verdade, a segurança efetiva exige várias camadas de proteção. E a solução de software certa na infraestrutura fornece o melhor ponto de controle possível para aumentar a visibilidade, reforçar a política e permitir a inserção de serviços de terceiros para proteção inteligente adicional.

Vamos dar uma olhada nas três etapas principais para transformar sua segurança de TI:

- Infraestrutura de aplicativos segura: abstraia a infraestrutura de aplicativos, melhorando a visibilidade e o alinhamento da segurança aos aplicativos.
- Identidade e endpoints protegidos: use uma camada de software onipresente em todos os usuários e endpoints para obter melhor visibilidade e controle, sem afetar a experiência do usuário.
- Conformidade simplificada: aplique software em toda a infraestrutura de aplicativos, identidades e endpoints para simplificar a conformidade.

1. Infraestrutura de aplicativos segura

À medida que os modelos de infraestrutura de aplicativos evoluem, a abordagem de segurança de rede centrada no perímetro tradicional não pode fornecer visibilidade e controle suficientes no data center. Ao mesmo tempo, os dados estáticos armazenados se tornaram um alvo muito mais valioso para os invasores. Para resolver esses problemas, é necessário mudar a sua maneira de proteger a infraestrutura de aplicativos.

A solução começa com a virtualização e a capacidade de abstrair a infraestrutura subjacente dos aplicativos que estão sendo executados nela, independentemente dessa infraestrutura estar no local ou na nuvem pública. Essa camada de abstração fornece visibilidade total no caminho de dados e um ponto de aplicação ideal para compartimentar aplicativos por meio da microssegmentação da rede. O uso de microssegmentação em softwares permite que as organizações simplifiquem a política de segurança e alinhem-na mais de perto às necessidades dos aplicativos. Também permite que a política siga o aplicativo à medida que ele se move em nuvens privadas e públicas. Uma camada de abstração também fornece uma plataforma para serviços de terceiros adicionais a serem inseridos, a fim de garantir uma proteção de segurança mais avançada.

A microssegmentação também ajuda a TI a evitar ameaças de segurança contra as defesas de violação, permitindo o princípio do menor privilégio centrado em aplicativos, o que reduz a superfície de ataque da infraestrutura.

Uma camada de abstração entre os aplicativos e a infraestrutura subjacente não só ajuda a TI a evitar ataques, mas também fornece um ponto ideal para criptografar dados armazenados. Ao criptografar dados estáticos, no nível da carga de trabalho, as organizações podem garantir a segurança dos dados da infraestrutura de aplicativos, mesmo que caiam em mãos erradas.

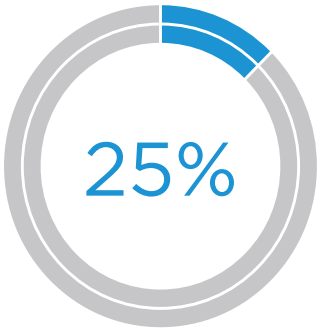
2. Identidade e endpoints protegidos

À medida que os seus negócios se tornam digitais, os dispositivos móveis crescem rapidamente. Organizações como a sua estão usando tudo, desde Android, iOS, Windows, MacOS e outros dispositivos para capacitar a força de trabalho e repensar os processos de negócios tradicionais. O suporte a todos esses dispositivos e plataformas é um desafio, especialmente porque as empresas adotam iniciativas de mobilidade corporativa, estratégia BYOD e IOT.

"Quanto mais empresas competirem por talento em um mercado limitado, a falta de habilidades se tornará um problema ainda maior. As empresas serão forçadas a repensar estratégias e procurar soluções (de segurança) mais proativas e exigir menos gerenciamento para permitir o melhor uso dos recursos."[5]

JAMES MAUDE
ENGENHEIRO DE SEGURANÇA
AVECTO

[5] http://www.information-management.com/gallery/6-top-it-security-trends-for-2017-10030567-1.html.



Até 2020, mais de 25% de todos os ataques identificados na empresa envolverão a Internet das Coisas (IoT).[6]

Ao aplicar uma camada de software onipresente em todos os usuários e endpoints para verificar a identidade do usuário e a postura do dispositivo, você estará equipado para enfrentar esse desafio. Essa abordagem fornece visibilidade e controle de ponta a ponta do usuário e do endpoint, estendendo-se até o data center ou a nuvem, onde está a infraestrutura de aplicativos. Com uma camada de software, a TI pode adicionar uma camada adaptável e condicional de segurança em cada nível transacional, desde os usuários até os recursos acessados. Ela ajuda a proteger os dados corporativos e reduzir a superfície do ataque cibernético, sem afetar a experiência do usuário.

Procure uma solução simples que possa proteger todos os endpoints, incluindo smartphones, tablets, laptops, acessórios e dispositivos de IoT. Como resultado, a TI pode implantar facilmente qualquer aplicativo, incluindo aplicativos nativos, Web, remotos, virtuais e desktops Windows, por meio de um único catálogo de aplicativos com logon único integrado, segurança de dados e conformidade de endpoint. Para os espaços de trabalho dinâmicos atuais, você deseja uma solução que estenda a segurança além da interface de desktop virtual (VDI, Virtual Desktop Interface) e dos endpoints móveis no data center com microssegmentação.

Como cada empresa possui necessidades de segurança específicas, sua solução também deve ajudar a personalizar o ambiente para se alinhar às suas prioridades. Você terá uma base para trabalhar com parceiros de segurança, que podem aproveitar os pontos de visibilidade e controle fornecidos para complementar a solução com suas próprias ofertas de serviços.

"Os clientes estão se afastando dos negócios que sofrem violações, e o ambiente regulatório é tal que as empresas precisam de proteção substancial, independentemente de criá-la em suas organizações ou de terceirizar a responsabilidade."[7]

FADI ALBATAL
VICE-PRESIDENTE SÊNIOR
ABOVE SECURITY

3. Conformidade simplificada

O gerenciamento de riscos e a manutenção de conformidade contínua são sempre grandes preocupações. É especialmente importante para os setores, como serviços financeiros, governo e organizações de saúde, que enfrentam requisitos rigorosos, como PCI, HIPAA, ECPA, a Diretiva relacionada à proteção de dados para a Europa e muito mais. Os regulamentos e requisitos estão crescendo, enquanto o cenário digital e as ameaças avançadas persistentes continuam a evoluir, tornando-se mais desafiador do que nunca garantir e demonstrar a conformidade.

Para complicar ainda mais, as organizações estão em rápida transição de data centers locais e adotando a nuvem, o que dificulta ainda mais atender às demandas de regulamentos, negócios e políticas.

Com uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints, você adotará uma abordagem holística sobre a conformidade. Essa abordagem única oferece uma localização ideal para implementar controles de conformidade e obter a visibilidade necessária para demonstrar conformidade. A solução certa fornece uma plataforma tecnológica na qual as ferramentas e serviços validados de parceiros do ecossistema podem ser inseridos dinamicamente para agilizar ainda mais o processo de conformidade.

Com uma estrutura de arquitetura de referência para conformidade, é possível vincular recursos integrados de software e hardware e controles regulatórios específicos com validação de auditoria independente. Além disso, você pode aproveitar um programa validado de forma independente para executar cargas de trabalho altamente regulamentadas com segurança. Seja usando um ambiente de nuvem privada ou pública, você deseja garantir que sua organização mantenha a conformidade sempre. Isso requer uma solução com a velocidade, eficiência e agilidade necessárias, ao mesmo tempo que simplifica o seu processo de conformidade.

[6] "Gartner Says Worldwide IoT Security Spending to Reach $348 Million in 2016", Gartner Inc., abril de 2016.
[7] http://www.datacenterjournal.com/cybersecurity-trends-2017-companies-fight-back/.

TRANSFORMAÇÃO DA SEGURANÇA

A VMware e a Intel transformam a segurança ao fornecer medidas abrangentes de segurança com base tanto em software quanto em hardware na infraestrutura e nos endpoints de aplicativos que maximizam a visibilidade, o contexto e o controle, a fim de proteger as interações entre usuários, aplicativos e dados.

Segurança para cenário e necessidades em constante mudança

Uma segurança robusta sempre foi essencial para as redes de negócios e, à medida que o ritmo das mudanças acelera, ela é mais necessária do que nunca. Enquanto a infraestrutura, os aplicativos e os modelos de força de trabalho tradicionais evoluem, sua equipe de TI sofre cada vez mais pressão para proteger a empresa de novas ameaças.

Uma camada de software onipresente em toda a infraestrutura de aplicativos e endpoints pode ajudar a transformar sua segurança. Ela permite maximizar a visibilidade e o contexto da interação entre seus usuários e aplicativos, para que você possa alinhar os controles e as políticas de segurança aos aplicativos protegidos. Além disso, facilita a complementação da solução com serviços de segurança de terceiros para oferecer mais proteção inteligente.

COMECE HOJE

Transforme a segurança de TI para o cenário atual

SAIBA MAIS >

Junte-se a nós on-line:

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