WHITE PAPER

PRINCÍPIOS BÁSICOS DA HIGIENE CIBERNÉTICA EM UM MUNDO DE NUVEM E MOBILIDADE

vmware | intel

Índice

Introdução

A segurança cibernética é uma grande preocupação nos níveis mais altos do governo e da indústria no mundo todo. Mais do que nunca, líderes governamentais e corporativos, desde senadores e membros do parlamento até CEOs e membros do conselho de administração, estão profundamente comprometidos em garantir que estratégias eficazes de segurança cibernética estejam em vigor em empresas e agências governamentais.

No entanto, embora os investimentos em segurança cibernética estejam aumentando, as violações continuam acontecendo com frequência alarmante. Algo não está funcionando. O que é? E como corrigir isso? Há muitas teorias do que pode ser feito, desde seguir novas estruturas de governança até implantar novos produtos e serviços.

Na VMware, acreditamos que uma nova estrutura ou a compra de um produto específico não garante a segurança mais eficaz das informações. A resposta é voltar aos conceitos básicos da computação com menos privilégios e integrar a segurança à arquitetura em vez de adaptá-la posteriormente. Essa tem sido uma meta difícil para as organizações, mas os novos recursos oferecidos pela computação móvel e em nuvem já tornaram essa realidade viável (e essencial).

Migrar para uma abordagem mais eficaz à segurança exige dois passos fundamentais: implementar a higiene cibernética básica e concentrar-se na proteção dos ativos mais importantes: os aplicativos corporativos essenciais.

DEFINIÇÃO DE "HIGIENE CIBERNÉTICA"

Esse termo tem vários significados. Estamos utilizando-o para falar de itens básicos que uma organização deve ter em vigor para a defesa cibernética.

Nossa definição é diferente de outra visão comum de higiene cibernética, que se refere àquilo que os clientes fazem para proteger suas atividades pessoais on-line contra infecções.

Neste artigo, propomos **cinco princípios fundamentais de higiene cibernética** como linha de base universal: as medidas mais importantes e básicas que as organizações devem colocar em prática. Os conceitos não são novos, mas são fundamentais para adotar uma segurança mais eficaz. Eles estão fundamentados em estruturas bem-estabelecidas, como a estrutura de segurança cibernética (CSF, pela sigla em inglês) da NIST, e são tecnologicamente neutros. Nas violações de dados mais devastadoras dos últimos anos – da Target à Sony e ao Escritório de gestão de pessoal dos Estados Unidos (OPM, pela sigla em inglês), acreditamos que aderir a esses princípios de modo eficaz teria feito uma grande diferença.

Ainda assim, implementar princípios fundamentais de higiene cibernética com eficácia não é fácil, e as empresas enfrentam esse problema há anos. Embora seja difícil argumentar contra os benefícios de segurança de privilégio mínimo (ou "confiança zero"), muitos acreditam que isso é impossível do ponto de vista operacional. Por isso, também sugerimos que as organizações concentrem os esforços de segurança na proteção de aplicativos, principalmente dos aplicativos corporativos essenciais, que são ambientes nos quais é mais fácil controlar comportamentos. Além disso, recomendamos o uso de abordagens modernas de big data e aprendizado de máquina para validar bons comportamentos em vez de perseguir atividades maliciosas.

O objetivo deste artigo é ajudar líderes governamentais e corporativos a compreender os problemas específicos das estratégias atuais de segurança cibernética e como mudar para uma abordagem melhor. Ele foi escrito para líderes que tratam de problemas de segurança cibernética, não necessariamente para especialistas técnicos. Para profissionais de segurança e outros que possam ter interesse nos detalhes mais técnicos, oferecemos um conjunto de apêndices, incluindo sugestões práticas para implementação.

Melhorar a segurança cibernética é um item prioritário na pauta do governo e da indústria. Como especialistas em nuvem e mobilidade, temos orgulho em contribuir com nossa perspectiva única para melhorar a segurança cibernética. Acreditamos que este é um ponto de vista relevante para abordar os desafios de segurança da informação. Trazemos nossa capacidade de ver por um ângulo diferente.

O problema da segurança cibernética

O gasto global com segurança continua aumentando, com uma taxa de crescimento anual composta (CAGR, pela sigla em inglês) de 8,7% prevista até 2020.[1] No entanto, o número anual de violações de dados nos EUA atingiu um nível sem precedentes no ano passado.[2] Empresas e governos de todo o mundo estão perdendo quase US$ 500 bilhões por ano com as violações de dados.[3] Claramente, algo não está funcionando. O que é? O que podemos fazer a respeito?

Sem escassez de orientações

As falhas na segurança cibernética certamente não se devem à falta de orientação sobre o que as organizações devem fazer para proteger as informações. Há vários padrões aceitos pelo governo e pelo setor no que se refere à segurança das informações nos EUA e no mundo todo, incluindo NIST, ISO, SANS e muito mais. Todos indicam uma lista abrangente de práticas recomendadas aceitas de um modo geral.

A complexidade é incontrolável

Com as abordagens atuais, a complexidade inviabiliza a implementação de práticas recomendadas abrangentes no ambiente de TI. Há uma grande variedade de ferramentas de segurança para gerenciar: firewalls, antivírus, sistemas de prevenção contra intrusões e sistemas de detecção de ameaças, entre outros. Cada ferramenta tem uma grande quantidade de regras para gerenciar. Cada uma deve ser configurada para aplicar políticas de controle e/ou proteção de informações em escala empresarial para todos os usuários e sistemas na organização. Em alguns casos, isso pode representar milhões de regras, literalmente. Configurar tudo é maçante. Além disso, o cenário de ameaças muda periodicamente, trazendo complexidade.

A mudança é constante

E as ferramentas de segurança simplesmente não podem ser configuradas apenas uma vez e esquecidas logo em seguida. Os sistemas precisam ser atualizados constantemente para acompanhar as oscilações de atividade e proteger contra as vulnerabilidades recém-descobertas.

A automação está fora de alcance

O DevOps e as abordagens modernas de aplicativos continuam aumentando a velocidade na qual os aplicativos e a infraestrutura podem mudar. Embora seja um ótimo facilitador de negócios, isso dificulta ainda mais a segurança. Com muita frequência, a segurança é vista como um obstáculo para o fornecimento de aplicativos e infraestrutura modernos em grande escala. Embora as organizações tenham muitas ferramentas em vigor para automatizar tarefas de segurança, elas não são usadas em conjunto com a automação da infraestrutura.

Em vez de considerar a automação como um problema de segurança, as organizações devem adotar a automação como uma forma de configurar a política de segurança. A maioria das ferramentas de automação de infraestrutura tem manifestos altamente declarativos que descrevem o estado pretendido da infraestrutura ou do aplicativo e que podem ser usados como uma forma de impor menos privilégios e de acompanhar as mudanças sem necessidade de ajuste manual das regras.

[1] Worldwide Semiannual Security Spending Guide, IDC, março de 2017

[2] Identity Theft Resource Center (ITRC) Data Breach Report 2016

[3] Net Losses: Estimating the Global Cost of Cybercrime, Center for Strategic International Studies, junho de 2014

Responder a alertas é oneroso

Outra dificuldade é o volume de trabalho envolvido em acompanhar alertas de segurança. Cada uma das muitas ferramentas de segurança em uma organização envia milhares de alertas por dia. Em alguns casos, são milhares por hora. Clientes maiores confiam nos sistemas de Gerenciamento de eventos e incidentes de segurança (SIEM, pela sigla em inglês) para correlacionar esses alertas/eventos e priorizar o que deve ser investigado. No entanto, priorizar alertas sem o contexto adequado é difícil e, muitas vezes, trabalhoso. Por exemplo, uma ferramenta de detecção pode indicar que há atividade suspeita na rede, mas não dar detalhes sobre os sistemas afetados, o nível de risco ou as possíveis ações.

As organizações dependem muito de pessoas realizando funções de segurança, mas a escassez de talentos em segurança cibernética é grande.

Duas etapas para uma segurança mais eficaz

Avanços recentes em computação móvel e em nuvem agora permitem simplificar e automatizar a segurança de uma forma mais completa. Há duas etapas fundamentais: implementar a higiene cibernética básica e concentrar-se na proteção dos ativos mais importantes: os aplicativos corporativos essenciais.

Etapa 1: Implementar os princípios fundamentais da higiene cibernética

Estas são as medidas básicas mais importantes que as organizações devem colocar em prática.

A base: Educação

Um processo obrigatório de educação deve estar em vigor para todos, desde profissionais de TI e líderes da empresa até funcionários e prestadores de serviços terceirizados.

- Os profissionais de TI devem estar comprometidos com a integração da segurança aos sistemas.
- Os desenvolvedores devem ter conhecimentos mínimos de segurança por código.
- Os arquitetos de sistemas devem ser responsáveis pelos resultados de segurança. O conhecimento básico de segurança deve ser tão familiar quanto o conhecimento em processamento, sistemas de rede ou armazenamento.
- Os usuários finais devem estar cientes de suas responsabilidades na proteção das informações e conhecer os riscos. Os conceitos básicos de segurança também devem ser bem compreendidos ao acessar um site ou verificar e-mails.

MICROSSEGMENTAÇÃO

Proteger o ambiente de TI, dividindo-o em partes menores, é como usar os compartimentos de um navio. Isso facilita a proteção da embarcação. Se uma área do navio sofrer algum dano, o dano ficará contido nessa área específica.

Os princípios fundamentais

Com um processo de educação bem-estabelecido, estes cinco princípios são essenciais na migração para uma segurança mais eficaz:

1. Processamento com privilégio mínimo	Os aplicativos devem executar apenas os componentes mínimos necessários para o trabalho designado (controle de aplicativos/inclusão na lista branca). Os usuários ou as contas de sistema nas máquinas de data center devem ter permissão apenas para a função mínima necessária de modo que possam cumprir seus respectivos propósitos.
2. Microssegmentação	A rede deve ser dividida em pequenas partes para que seja mais fácil gerenciar, proteger e conter o dano, caso uma delas seja comprometida (consulte a barra lateral).
3. Criptografia	Em processos essenciais aos negócios, todos os dados devem ser criptografados ao serem armazenados ou transmitidos. No caso de uma violação de dados, o roubo de arquivos importantes deve resultar apenas na obtenção de dados que não podem ser lidos.
4. Autenticação de vários fatores	A identidade dos usuários e dos componentes do sistema deve ser verificada usando vários fatores (não apenas senhas simples), que podem ser proporcionais ao risco do acesso ou da função solicitados.
5. Aplicação de patches	Os sistemas devem ser mantidos atualizados de maneira consistente. Qualquer sistema essencial desatualizado representa um risco significativo à segurança.

Princípios bem-estabelecidos

Esses princípios fundamentais não são conceitos novos. Eles estão baseados em princípios bem-estabelecidos. Por exemplo, estão associados a várias funções na CSF da NIST (consulte o Apêndice 1).

Eles são apenas uma fração do que a CSF da NIST e outras estruturas abrangem. No entanto, são princípios capacitadores essenciais para migrar para uma abordagem mais simples e automatizada.

Pôr em prática essas cinco medidas de maneira eficaz e consistente dificultaria muito os ataques cibernéticos e os tornaria menos prejudiciais. Mesmo nas violações de dados mais devastadoras dos últimos anos, acreditamos que implementar esses princípios de modo eficaz teria feito uma grande diferença (veja abaixo).

Grandes violações em que os princípios fundamentais não foram implementados com eficácia

Princípio	**Exemplos de violações** Observação: Muitos fatores podem levar a violações de dados. Estes são exemplos de situações em que não implementar com eficácia um princípio fundamental contribuiu para uma violação (também pode haver outros fatores).
1. Processamento com privilégio mínimo	Se o controle de aplicativos não tiver sido implementado de maneira eficaz e os usuários ou sistemas tiverem liberdade para executar tarefas além das necessárias, os invasores aproveitarão esse amplo acesso aos sistemas para promover comportamentos mal-intencionados (geralmente sem usar malware conhecido). Por exemplo, nas violações da Target e da Sony, os invasores conseguiram obter privilégios de nível administrativo e promover comportamentos que não faziam parte da atividade normal do aplicativo.
2. Microssegmentação	Se a microssegmentação não for implementada com eficácia, os invasores poderão acessar uma parte da rede e, depois, moverem-se com facilidade para outras partes. Por exemplo, na violação da Target, depois de uma invasão inicial no sistema de HVAC, os invasores conseguiram acessar o sistema da rede de pagamento. Na violação da Sony, os invasores também conseguiram se mover de uma parte a outra da rede. No caso da violação do Escritório de gestão de pessoal dos Estados Unidos, os invasores obtiveram acesso à rede local da agência. Depois, acessaram o data center do Departamento do interior.
3. Criptografia	Se a criptografia não for implementada com eficácia, os invasores poderão extrair os dados em formato legível. Por exemplo, depois da violação de dados da Royal & Sun Alliance Insurance PLC, os investigadores do governo determinaram que a empresa não tinha criptografado adequadamente os dados.
4. Autenticação de vários fatores	Se a autenticação de vários fatores (MFA, pela sigla em inglês) não for implementada com eficácia, os invasores poderão obter senhas e usá-las para acessar sistemas. Por exemplo, no caso da violação do Escritório de gestão de pessoal dos Estados Unidos, se os logons dos prestadores de serviços tivessem recebido o nível adequado de risco na MFA, a capacidade dos invasores de usar as credenciais roubadas dos prestadores de serviços seria limitada. No caso da violação do LinkedIn, o hacker expôs senhas inadequadamente protegidas de 100 milhões de usuários. Como os clientes normalmente usam as mesmas senhas em mais de um site, a MFA teria reduzido esse risco.
5. Aplicação de patches	Se a aplicação de patches não for implementada adequadamente, os invasores poderão se aproveitar de falhas nos sistemas. Por exemplo, o ransomware WannaCry se aproveitou de uma vulnerabilidade de software conhecida para a qual havia um patch disponível. As organizações atingidas não conseguiram aplicar o patch com eficácia.

Não é fácil implementar os princípios fundamentais com eficácia

Em muitas organizações, os profissionais de segurança estão muito familiarizados com esses princípios, e a maioria não questionaria sua eficácia quando adequadamente implementados. Na verdade, mesmo em organizações que já passaram por uma violação, a equipe de segurança provavelmente já tentou implementá-los (e não conseguiu). O problema é que isso é muito difícil de conseguir, devido à abordagem atual de segurança que a maioria das organizações implementa, usando as ferramentas e técnicas disponíveis para eles.

"Ativos mais importantes = aplicativos essenciais"

Etapa 2: Concentrar-se na proteção de aplicativos *individuais* importantes

O próximo passo é se concentrar na proteção de aplicativos individuais importantes. Isso facilitará a implementação eficaz dos princípios fundamentais de higiene cibernética.

O foco deve estar nos ativos mais importantes: os aplicativos essenciais. Essencialmente, trata-se dos aplicativos corporativos essenciais e dos dados que eles contêm. Os exemplos incluem: um aplicativo financeiro empresarial que processa dados confidenciais na criação dos relatórios financeiros da empresa, um aplicativo de pedidos que preenche os pedidos dos clientes (incluindo o armazenamento de informações pessoais e dados do cartão de crédito), um aplicativo de RH que contém dados confidenciais dos funcionários e um aplicativo de pesquisa e desenvolvimento que contém segredos comerciais. O aplicativo é o mecanismo de acesso e interação com os dados.

Mesmo que a meta da segurança da informação seja proteger os ativos mais importantes, as abordagens atuais se concentram na proteção da infraestrutura de TI, como roteadores (hardwares que fazem o roteamento do tráfego em uma rede) ou servidores (computadores que oferecem capacidade de processamento). O pior é que a maioria das ferramentas considera esses componentes de infraestrutura como componentes genéricos e não aproveita o contexto do aplicativo que está tentando proteger. Proteger a infraestrutura de TI é necessário, mas não suficiente.

Adote uma abordagem baseada em riscos

Os dados e os aplicativos essenciais são importantes para a empresa. Abandonar esses ativos representa um grande risco para a organização. A infraestrutura oferece tudo o que um aplicativo precisa para funcionar, mas não é o ativo essencial.

Seja mais específico

Centrar a segurança na infraestrutura não oferece o grau de especificidade adequado. É como tentar proteger todas as casas em uma comunidade colocando uma só grade ao redor de todas elas com um portão trancado. Seria mais eficaz focar na proteção de cada casa (consulte o diagrama 1 a seguir).

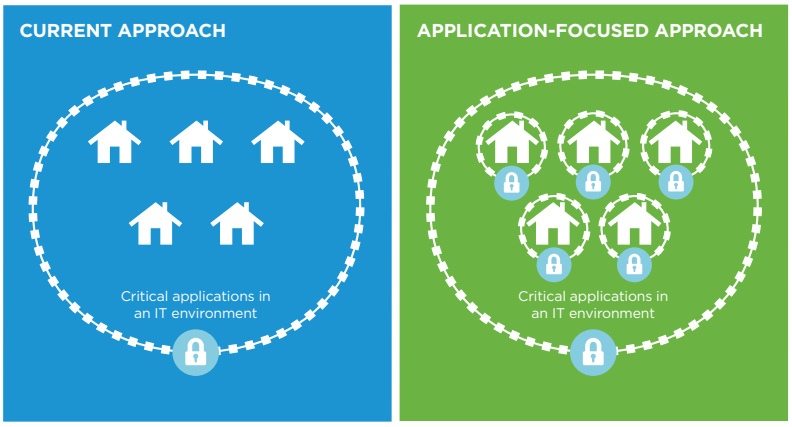

Diagrama 1: A atual abordagem para proteger um ambiente de TI é como tentar proteger as casas em uma comunidade colocando grades ao redor dela com um portão com tranca. Seria mais eficaz se concentrar nas casas (aplicativos críticos), adicionando cercas e fechaduras a cada uma delas.

Controle o acesso a cada aplicativo individual

Com as abordagens atuais, é difícil alcançar as metas de segurança com eficácia, como garantir apenas o acesso mínimo necessário. Por exemplo, um firewall normalmente é configurado no perímetro de toda a empresa (como a grade em torno de toda a comunidade) para controlar o acesso a um grupo com milhares de aplicativos. Nesse caso, a política de firewall para qualquer aplicativo é tão eficaz quanto o aplicativo menos seguro nesse grupo. Em vez disso, deve haver um firewall configurado para controlar o acesso a cada aplicativo essencial (como cada casa), permitindo que o acesso seja feito somente pelos usuários e componentes do sistema que realmente precisam acessá-lo (casa).

A segurança também precisa ser mais eficiente. Imagine que os guardas no portão recebem uma ligação alertando sobre uma atividade incomum em algum lugar da comunidade. Eles podem passar o dia inteiro procurando a atividade incomum na comunidade. Seria mais eficiente se soubessem exatamente em que casa ir, se a casa está vazia ou tem bens valiosos e se a atividade é normal para aquela casa. Consulte o diagrama 2 a seguir.

Monitore o mais próximo possível do aplicativo

Os sistemas de monitoramento de segurança normalmente enviam um alerta indicando uma intrusão na rede ou em parte da rede, sem especificar em qual aplicativo. A equipe de segurança cibernética precisa passar muito tempo investigando. Seria melhor se o evento fosse avaliado pela má intenção em potencial o mais próximo possível do aplicativo antes do encaminhamento para o sistema central de gerenciamento de eventos. Isso resultaria em mais alertas de alta fidelidade que indicariam qual aplicativo foi afetado, a gravidade do problema e se a atividade detectada era legítima para o aplicativo.

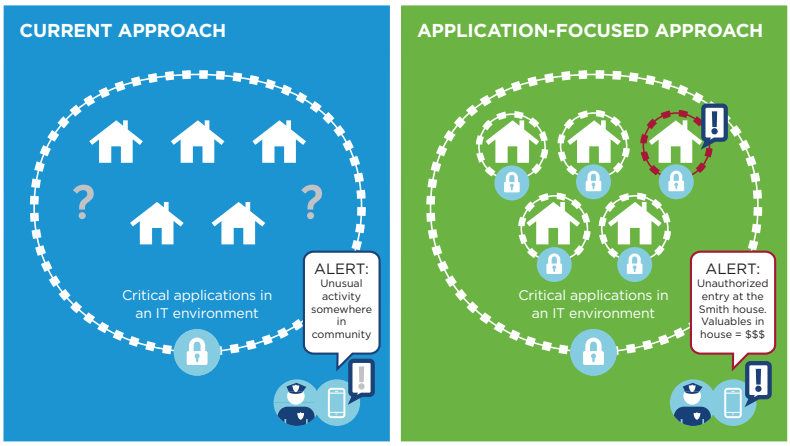

Diagrama 2: A abordagem atual ao monitoramento de um ambiente de TI é como alertar um guarda de que há atividade incomum em algum lugar da comunidade. Seria mais eficaz se o guarda soubesse exatamente qual é a casa que precisa de atenção (aplicativo essencial) e o que está acontecendo.

APLICATIVOS MODERNOS: SISTEMAS DISTRIBUÍDOS E DINÂMICOS

- Cada aplicativo é um "sistema" de componentes.
- As funções (ou os serviços) de software usam um pool de recursos: sistemas de rede, processamento, memória e armazenamento.
- Os recursos estão espalhados em um ambiente de TI (provavelmente no data center e nos provedores de nuvem da própria organização).
- O pool de recursos é compartilhado por muitos aplicativos.
- O uso dos recursos muda rapidamente ao longo do tempo.

Por que as organizações ainda não estão fazendo isso?

Se se concentrar nos aplicativos essenciais de forma individual com higiene cibernética melhora a segurança, então por que as organizações ainda não estão fazendo isso? Porque as tecnologias e técnicas que a maioria das organizações usa atualmente não torna isso viável.

As abordagens atuais não têm a capacidade de identificar os aplicativos individuais

Os aplicativos modernos são projetados como sistemas distribuídos e dinâmicos. Os serviços que fornecem o aplicativo estão difundidos em várias máquinas, com funções de software usando um pool de recursos compartilhados que mudam com o tempo (consulte a barra lateral). Com as abordagens atuais, as ferramentas de segurança não conseguem reconhecer ou compreender esses serviços e como eles compõem os aplicativos.

Com as abordagens atuais, as ferramentas de segurança:

- Não conseguem identificar que "esses serviços" formam o "Aplicativo A".
- Não sabem quais usuários devem acessar o "Aplicativo A".
- Não sabem exatamente qual infraestrutura é responsável por fornecer os serviços do "Aplicativo A".
- não sabem como os serviços devem ter permissão para se comunicarem entre si como parte do "Aplicativo A".
- Não conseguem acompanhar as mudanças do "Aplicativo A", por exemplo, quando o software usa diferentes recursos de hardware.

Os aplicativos continuam evoluindo

O ritmo dos aplicativos que mudam para essa abordagem orientada a serviços continua acelerado. Como resultado a abordagem atual, centrada na proteção da infraestrutura, terá ainda menos sucesso protegendo aplicativos individuais. Por isso, há uma certa urgência em mudar para uma abordagem focada em aplicativos, pois os problemas tendem a piorar.

Mesmo em ambientes tradicionais de aplicativos existentes, o uso dessa abordagem centrada em aplicativos pode resolver problemas significativos de segurança indiretos e ajudar a preparar melhor o futuro.

A computação móvel e em nuvem garante novas possibilidades

Com os avanços na computação móvel e em nuvem (privada e pública), as organizações têm os recursos necessários para se concentrar na proteção de aplicativos individuais, preparando o terreno para uma segurança mais eficaz.

Use recursos orientados aos aplicativos

Especificamente, a computação móvel e em nuvem permite:

Recurso I: Usar a automação de infraestrutura para reconhecer um aplicativo específico e estabelecer uma referência de linha de base para ele

- Identificar quais componentes formam o aplicativo
  - Obter visibilidade dos aplicativos
- Saber como um aplicativo deve funcionar e como ele realmente funciona no tempo de execução
  - Saber quem precisa acessar o que e como a interação acontece

- Usar essa informação de referência na proteção do aplicativo
  - Consultar essas informações para configurar as ferramentas de segurança

Recurso II: Compartimentalizar os componentes do sistema em aplicativos individuais

- Agrupar todos os componentes do sistema que formam um aplicativo específico
- Associar todos os componentes do sistema colocando um limite lógico em torno do agrupamento
- Usar o limite para rotular o aplicativo de forma exclusiva

Recurso III: Posicionar as defesas em torno de cada aplicativo

- Determinar o que pode transitar entre os limites do aplicativo
- Reforçar os comportamentos normais dentro desse limite
- Alinhar as ferramentas de segurança ao limite do aplicativo
- Configurar as ferramentas de segurança de acordo com as informações do valor de referência e ao usar os rótulos fornecidos pelo limite
- Monitorar o aplicativo e ajustar a proteção conforme ele muda

Consulte o diagrama 3 a seguir para ver como usar esses recursos para proteger com eficácia os aplicativos modernos. Para obter mais detalhes sobre os recursos e o que eles permitem que as organizações façam, consulte o Apêndice 2.

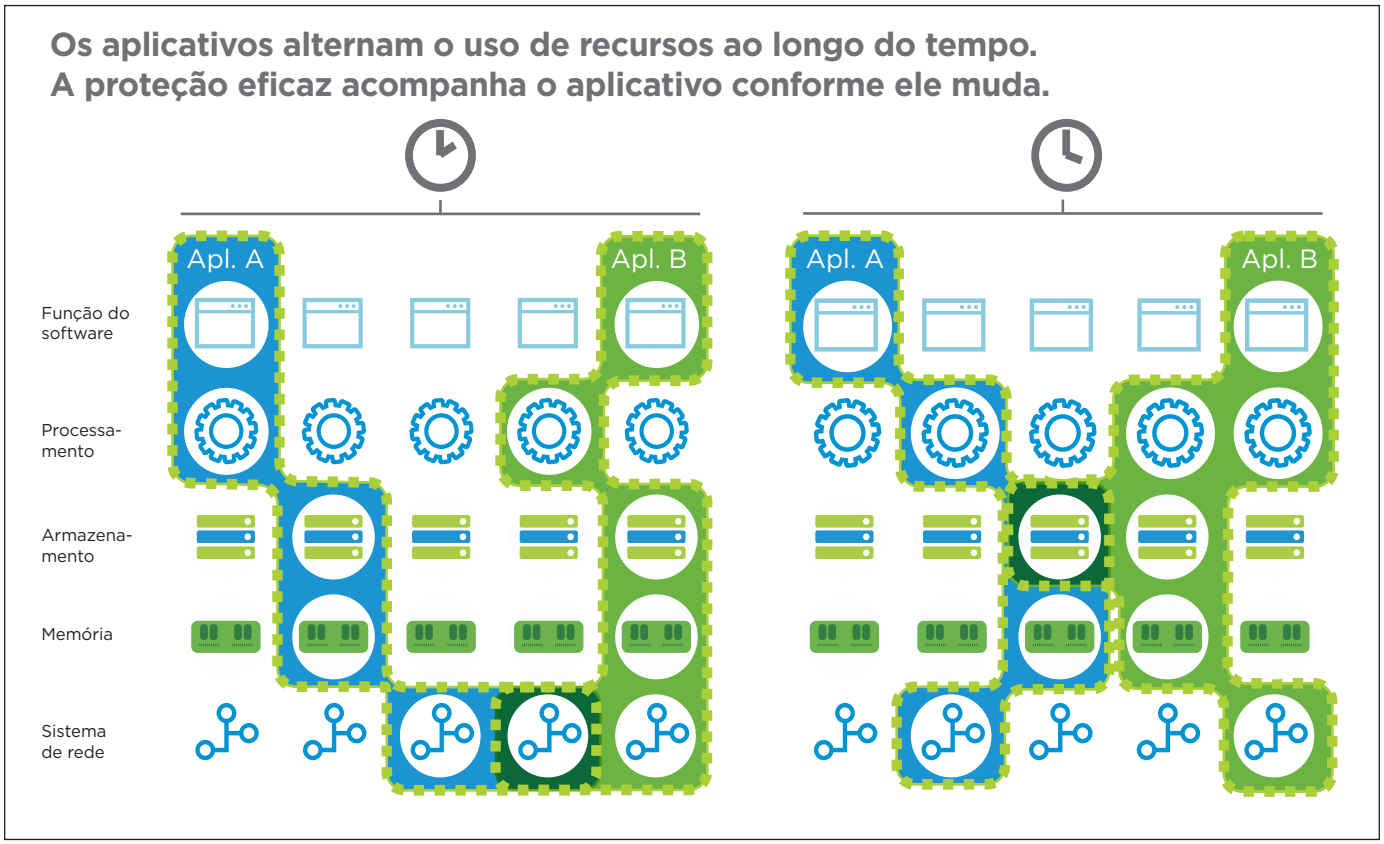

Diagrama 3: Um aplicativo moderno é um sistema distribuído e dinâmico. Ele usa um pool de recursos compartilhados, e o uso varia ao longo do tempo. Proteger um aplicativo com eficácia exige identificar todos os componentes de software e hardware que formam o aplicativo, agrupando-os, colocando um limite em torno deles, rotulando-os como "Aplicativo X" e posicionando defesas em torno do limite. Os limites e as defesas devem acompanhar as mudanças do aplicativo.

Implemente os princípios fundamentais com eficácia

Quando usamos uma abordagem orientada aos aplicativos, os princípios fundamentais podem ser implementados com eficácia. A segurança fica muito mais simples e fácil de automatizar:

Princípio	Abordagem orientada aos aplicativos	Implementação mais eficaz
A base: Educação	Um processo obrigatório de educação **com foco nos aplicativos** deve estar em vigor para todos, desde profissionais de TI e líderes da empresa até funcionários e prestadores de serviços terceirizados.	A educação será mais relevante, adaptada aos aplicativos com que os profissionais e/ou usuários de TI trabalham.
1. Processamento com privilégio mínimo	Os componentes e usuários do sistema também devem ter funções para acessar somente o mínimo necessário **por aplicativo específico** para cumprir seu propósito, nada mais (controle do aplicativo).	Será mais difícil para os invasores descobrirem maneiras de obter acesso, promover comportamentos mal-intencionados ou sequestrar interações (tanto "sistema a sistema" quanto "usuário a sistema").
2. Microssegmentação	Todo o ambiente de TI deve ser dividido em pequenas partes **ao configurar limites em torno de aplicativos individuais** para que seja mais fácil protegê-los e limitar o dano caso uma parte seja comprometida.	A movimentação no ambiente de TI será significativamente moderada. Se os invasores conseguirem acessar uma parte, estarão confinados a uma parte pequena (por exemplo: um único aplicativo), e será difícil alcançarem outras partes.
3. Criptografia	Em processos essenciais aos negócios, todos os dados devem ser criptografados ao serem armazenados ou transmitidos **pelos componentes de um aplicativo específico**. No caso de uma violação de dados, o roubo de arquivos importantes deve resultar apenas na obtenção de dados que não podem ser lidos.	Os dados críticos terão um "limite" lógico em torno do qual apenas os componentes de aplicativo apropriados poderão acessá-lo, independentemente de onde o aplicativo estiver sendo executado.
4. Autenticação de vários fatores	A identidade dos usuários e dos componentes do sistema deve ser verificada usando vários fatores (não apenas senhas simples), que podem ser proporcionais ao risco do acesso ou da função solicitados **para um aplicativo específico**.	Aplicar um nível adequado de autenticação de vários fatores (MFA, pela sigla em inglês) a cada solicitação será mais viável, já que o gerenciamento é feito por cada aplicativo. Será mais difícil para os invasores realizarem ataques se não conseguirem mais apenas roubar ou adivinhar senhas.
5. Aplicação de patches	Os sistemas são mantidos atualizados de maneira consistente, **com base no conhecimento sobre cada aplicativo**. Qualquer sistema essencial desatualizado representa um risco significativo à segurança.	Será muito mais fácil aplicar patches de modo consistente sabendo quais componentes de aplicativos serão afetados e os possíveis impactos nos sistemas. Será muito mais difícil para os invasores encontrarem sistemas vulneráveis para explorar.

Comece classificando aplicativos

Com uma abordagem focada em aplicativos, a equipe de segurança pode se concentrar nos ativos mais importantes, como aplicativos essenciais, em vez de distribuir investimentos superficialmente na infraestrutura. As organizações começam classificando aplicativos para determinar a gravidade e a priorização. Assim, podem concentrar seus esforços nos aplicativos mais essenciais. No entanto, lembre-se de que todos os aplicativos precisam de algum nível de proteção.

Melhorar a eficácia das ferramentas de segurança existentes

Uma abordagem orientada aos aplicativos permite que as empresas aproveitem as ferramentas de segurança ao máximo:

- Reduzir as configurações erradas de ferramentas de segurança
  - Os conjuntos de regras são simplificados: regras específicas de aplicativos são empregadas em cada aplicativo
- Configurar as ferramentas de segurança para trabalharem juntas
  - Todas as ferramentas de segurança (firewalls, antivírus, sistemas de prevenção contra intrusões e sistemas de detecção de ameaças) usam o mesmo rótulo (o limite do aplicativo) para identificar o recurso que protegem
- Interpretar e tomar medidas relacionadas a alertas com mais facilidade e rapidez
  - Os alertas das ferramentas de segurança identificam o aplicativo e apresentam informações sobre o nível de prioridade e possíveis cursos de ação
- Usar ferramentas de segurança de maneira mais automatizada
  - As funções das ferramentas de segurança podem ser coordenadas. A proteção, o monitoramento e as atividades de resposta podem ser organizados em torno de aplicativos individuais
- Reduzir o custo das operações de segurança
  - Haverá menos alertas gerados e menos tempo gasto em investigação

Inclua a segurança na arquitetura

Normalmente, a segurança é integrada posteriormente. As equipes de aplicativos criam um aplicativo, as equipes de infraestrutura criam uma infraestrutura relativamente genérica capaz de lidar com todos os aplicativos, e a equipe de segurança deve proteger tudo isso. As ferramentas de segurança são implantadas, mas não são integradas à malha dos aplicativos.

Uma abordagem orientada aos aplicativos exigirá uma mudança na arquitetura. Ela não será obtida apenas com a compra de um appliance específico de segurança ou com o upgrade de software.

Exige a adoção de propriedades exclusivas de aplicativos e infraestruturas modernos e o uso focado em beneficiar a segurança (consulte o Apêndice 3 para obter mais informações).

As tecnologias de nuvem e mobilidade oferecem uma arquitetura de sobreposição que pode ser usada para integrar a segurança não apenas a novos aplicativos, mas também a aplicativos existentes. Para ver sugestões práticas de implementação no data center e para computação para o usuário final, consulte os apêndices 4 e 5.

Conclusão

Ao pôr em prática duas etapas fundamentais (implementar os princípios fundamentais de higiene cibernética e concentrar-se na proteção dos aplicativos), as organizações podem migrar para uma segurança da informação mais eficaz. Agora, a computação móvel e em nuvem oferece uma maneira de incluir a segurança na arquitetura. Como os ambientes de TI continuam evoluindo, esse modelo atualizado pode ajudar a garantir que um programa de segurança da informação não só seja mais eficaz no presente, mas também esteja preparado para o futuro.

COMEÇAR

Saiba mais sobre como você pode ajudar sua organização a buscar uma infraestrutura de aplicativos segura >

Junte-se a nós on-line:

Apêndice 1: Correspondência dos princípios fundamentais com a estrutura de segurança cibernética da NIST

Os princípios fundamentais da higiene cibernética estão baseados em princípios bem-estabelecidos. Por exemplo, todos eles estão associados a várias funções na estrutura de segurança cibernética (CSF, pela sigla em inglês) da NIST (veja a seguir). Esses princípios são apenas uma parte do que a CSF da NIST e outras estruturas abrangem. No entanto, são princípios capacitadores essenciais para migrar para uma abordagem mais simples e automatizada à segurança.

Princípios fundamentais	Subcategorias da CSF da NIST
A base: Educação	PR.AT: a equipe e os parceiros da organização recebem instruções voltadas à conscientização de segurança cibernética e são adequadamente treinados para realizar suas tarefas e responsabilidades relacionadas à segurança da informação de acordo com as políticas, os procedimentos e os contratos adequados.
1. Processamento com privilégio mínimo	PR.AC-4: permissões e autorizações de acesso são gerenciados, incorporando os princípios do privilégio mínimo e da separação de tarefas PR.PT-3: o princípio da funcionalidade mínima é incorporado ao configurar os sistemas para fornecer somente os recursos essenciais PR.IP-1: uma configuração de linha de base dos sistemas de controle industriais/de tecnologia da informação é criada e mantida com a incorporação de princípios de segurança adequados (por exemplo: o conceito da funcionalidade mínima) DE.AE-1: uma linha de base de operações de rede e de fluxos de dados esperados para usuários e sistemas é estabelecida e gerenciada
2. Microssegmentação	PR.AC-5: a integridade da rede é protegida, incorporando a segregação de rede quando adequado
3. Criptografia	PR.DS-1: os dados em repouso são protegidos PR.DS-2: os dados em trânsito são protegidos
4. Autenticação de vários fatores	PR.AC: o acesso aos ativos físicos e lógicos e às instalações associadas é limitado a usuários, processos e dispositivos autorizados. É gerenciado de maneira consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas. PR.AC-1: identidades e credenciais são emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos autorizados PR.AC-6: as identidades são testadas e vinculadas a credenciais e recebem permissão para interações quando adequado
5. Aplicação de patches	PR.IP-3: os processos de controle de alteração de configurações estão em vigor PR.IP-7: os processos de proteção são constantemente melhorados PR.IP-12: um plano de gerenciamento de vulnerabilidades é desenvolvido e implementado ID.RA-1: as vulnerabilidades dos ativos são identificadas e documentadas DE.CM-8: as verificações de vulnerabilidade são realizadas

OBSERVAÇÃO: Os apêndices a seguir mostram informações interessantes para profissionais e outros responsáveis por implementar uma nova abordagem à segurança focada em aplicativos de uma organização.

Apêndice 2: Mais detalhes sobre recursos focados em aplicativos

As seções a seguir mostram uma explicação mais detalhada e técnica dos recursos orientados aos aplicativos apresentados anteriormente na página 10 do artigo.

O QUANTO ISSO É PRÁTICO DE REALIZAR?

Antes era difícil obter visibilidade do aplicativo e saber como ele operava; mas agora as novas tecnologias facilitam essa possibilidade.

Para aplicativos grandes atuais, já existem tecnologias que acompanham o tráfego da rede para ajudar a compreender os componentes do aplicativo e como eles interagem.

Para arquiteturas de aplicativos mais recentes, as técnicas de DevOps automatizam o processo de criação e o acompanhamento de todos os componentes usados para formar o aplicativo desde o começo.

Recurso I: Reconhecer um aplicativo e estabelecer uma referência de linha de base para ele

Esse recurso permite que as organizações entendam melhor seus aplicativos essenciais de uma perspectiva de segurança, determinem os componentes que formam o aplicativo, incluindo a identificação de quais serviços (por exemplo: funções de software) devem estar em execução em quais servidores e quais recursos estão sendo usados, como os componentes devem interagir etc.

Um aspecto importante é compreender o comportamento pretendido do aplicativo, como:

- O que deve estar sendo executado?
- Quais são as interações permitidas?
- Como os componentes devem se comunicar?

Como os aplicativos são dinâmicos, as organizações devem ser capazes de monitorar o aplicativo conforme ele muda e conforme os desenvolvedores o atualizam. Durante sua execução, precisam saber quantas instâncias estão sendo executadas, por exemplo.

O que as organizações podem fazer com esse recurso?

- Proteger os aplicativos com eficácia conhecendo os valores de referência
  - Entender o aplicativo e saber como protegê-lo
  - Usar uma fonte confiável de informações sobre o aplicativo para configurar todo o portfólio de controles de segurança do aplicativo
    - As equipes de garantia e auditoria de controles também pode usar esta referência para avaliar os controles
- Refinar os privilégios para que sejam rígidos, mas plausíveis operacionalmente (que não interrompam os processos)
  - Tenha as informações necessárias para determinar a função e as interações mínimas necessárias para os elementos que formam o aplicativo, criando um ambiente com menos privilégios para o próprio aplicativo.
  - Ter as informações essenciais para determinar a comunicação mínima necessária entre componentes do sistema que entram, saem e estão em cada aplicativo
    - Isso pode reduzir bastante a superfície de ataque.
- Tornar os alertas mais úteis
  - Os alertas das ferramentas de segurança identificarão o aplicativo e, com base nas informações de referência, a equipe de segurança saberá quanto esforço colocar na resposta, como priorizar e quais são as opções de correção
- Melhorar a relação sinal-ruído
  - Com sistemas altamente controlados, há muito menos potencial para acesso, funções ou interações não autorizados. A quantidade de alertas será menor.
  - Menos alertas significam um sinal muito mais claro: menos ruído e menos alarmes falsos.

POSSIBILITA O MODELO DEVOPS

Aplicativos mais recentes usam práticas e tecnologias de DevOps para criar, testar e implantar aplicativos com rapidez e frequência.

As organizações podem abrir mão da análise de segurança manual e dos processos de teste que têm tempos de implantação longos e não funcionam com aplicativos e processos de desenvolvimento ágeis.

SEGMENTAÇÃO EFICAZ

O modelo tradicional de segmentação de rede é baseado em atributos, como tipo de servidor (por exemplo: servidores da web ou servidores de bancos de dados). Ele não consegue inibir com eficácia a movimentação lateral de um aplicativo para outro, pois um aplicativo não funciona em um único segmento de servidores, mas cruza vários segmentos. Os invasores conseguem saltar entre segmentos. Proteger de modo eficaz um aplicativo exige colocar um limite em torno dele, além de ter um ponto de controle da rede do qual controlar e monitorar todo o tráfego entre qualquer parte do aplicativo.

- Parar de procurar ameaças continuamente
  - As ameaças estão em constante mudança. Este enfoque não consiste em ter que se adiantar sempre às novas ameaças.
- Criar uma aliança mais próxima entre as equipes de segurança e de aplicativos (consulte a barra lateral)
- Dimensionar a implementação de acordo com as necessidades: concentre-se em entender um conjunto pequeno de aplicativos essenciais primeiro
  - Comece com aplicativos essenciais que tenham um conjunto relativamente pequeno de componentes com tarefas muito específicas, por exemplo, "este servidor da web faz parte do aplicativo X, e esse processo deve ser o único item a se comunicar com Y".

Recurso II. Compartimentalizar os componentes do sistema em aplicativos individuais

As organizações podem usar as informações de referência descritas acima para determinar os componentes do sistema que formam um aplicativo específico. Depois, podem compartimentalizar os componentes do sistema e colocar um limite lógico em torno deles. O limite oferece uma maneira de definir e rotular um aplicativo de maneira única. Ele também confina um ataque a um único aplicativo, caso ele esteja comprometido.

O que as organizações podem fazer com esse recurso?

- Configurar um único gateway para aplicar as políticas no aplicativo com eficácia
- Melhorar a proteção dos aplicativos contra ameaças na rede
  - A segmentação baseada em infraestrutura, como tipo de servidor, não é eficaz (consulte a barra lateral)
- Identificar e rotular com exclusividade um aplicativo (consulte a barra lateral)
- Desenvolver uma política para aplicar em um aplicativo
  - Ao definir e rotular de modo exclusivo um aplicativo, a política pode ser aplicada a ele
- Impedir a movimentação lateral de um aplicativo para outro
  - Se um invasor acessar um aplicativo, terá dificuldades para acessar outro
- Aplicar controles específicos do aplicativo no limite dele
  - Aplicativos mais essenciais podem ter níveis mais altos de proteção e maior inspeção. Mesmo que um sistema mais fraco em algum ponto do ambiente fique comprometido, o invasor não poderá se mover lateralmente para um sistema mais essencial.

IDENTIFICADOR ÚNICO

Os controles tradicionais de segurança ainda dependem do mesmo rótulo estático para toda a pilha, desde o aplicativo até o sistema operacional e o hardware. No entanto, isso não funciona com aplicativos modernos, pois eles não estão armazenados em servidores estáticos. Os identificadores de VLAN também não resolvem nesse caso, pois isolam vários aplicativos e não fornecem um identificador único para cada um deles. Para que os controles de segurança sejam eficazes, precisam ter um identificador exclusivo para uso na aplicação de políticas em cada aplicativo.

Recurso III. Posicionar as defesas em torno de cada aplicativo

Usando o rótulo exclusivo fornecido pelo limite do aplicativo, as organizações podem configurar controles de segurança a serem aplicados a um aplicativo específico. Por exemplo, um firewall pode ser configurado para proteger um único aplicativo usando o rótulo do limite do aplicativo. As organizações também podem usar as informações de referência para configurar os controles de segurança. Por exemplo, usando as informações de referência, a organização pode configurar um sistema de prevenção contra invasões e desenvolver um conjunto de regras para o aplicativo específico que ele está protegendo.

O que as organizações podem fazer com esse recurso?

- Otimizar a localização dos pontos de aplicação de políticas
  - As políticas são aplicadas no limite do aplicativo
- Simplificar as políticas para proteger os aplicativos
  - As organizações não precisam mais lidar com as políticas muito complexas das abordagens atuais, que tentam, por exemplo, usar um firewall para proteger milhares de aplicativos (consulte o Diagrama 4 a seguir)
- Reduzir a complexidade de gerenciar chaves de criptografia
  - É muito mais fácil distribuir chaves de criptografia/descriptografia aos componentes do sistema de um aplicativo específico, em vez de muitos aplicativos
- Aplicar políticas de autenticação (de vários fatores) usando o mapeamento simplificado de quais usuários e componentes do sistema de aplicativos recebem acesso e quais fatores são obrigatórios
- Evitar as configurações erradas de controles de segurança
  - Os controles são configurados para proteger um aplicativo
- Aumentar a proteção de aplicativos individuais ao adicionar mais controles no limite
- Ter controles de segurança que funcionem juntos, como um sistema
  - Todos os controles podem ser sincronizados em um aplicativo, usando o limite do aplicativo para rotulá-lo
- Permitir que os controles sejam adaptados à dinâmica dos aplicativos
  - Os controles podem proteger nos limites conforme os aplicativos são migrados

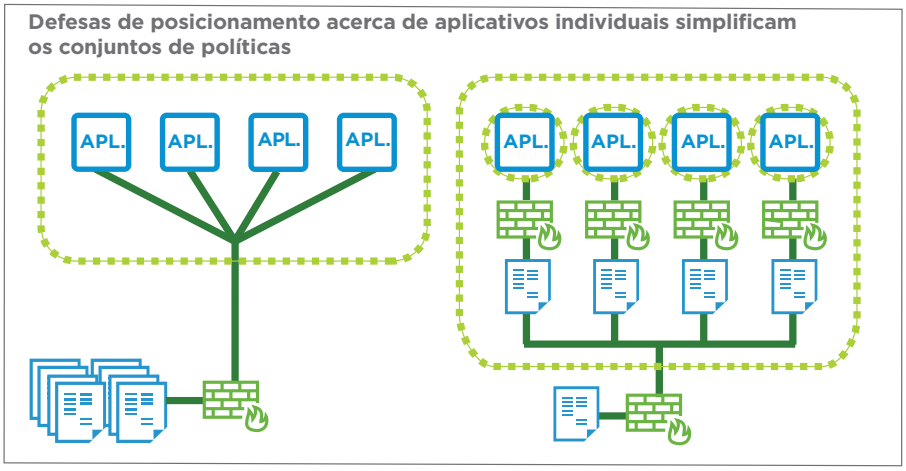

Diagrama 4: Com as abordagens atuais, normalmente um firewall é configurado no perímetro para aplicar políticas de tráfego de/para todos os componentes de todos os aplicativos em seus limites, o que pode envolver dezenas de milhares de regras de firewall. Os conjuntos de políticas são muito grandes e complexos. Quando um firewall é configurado para cada aplicativo, ele só precisa aplicar o tráfego de/para os componentes em apenas um aplicativo, reduzindo e simplificando muito o conjunto de políticas.

Apêndice 3: Propriedades exclusivas da computação móvel e em nuvem

Os recursos orientados aos aplicativos (descritos no Apêndice 2) que as organizações agora podem usar para implementar uma abordagem mais eficaz à segurança da informação foram possibilitados pelos avanços recentes na computação móvel e em nuvem.

PROPRIEDADES EXCLUSIVAS DA COMPUTAÇÃO EM NUVEM

A malha básica da nuvem é a virtualização, que fornece uma camada de abstração entre a infraestrutura física e os aplicativos.	
Contexto do aplicativo	• A camada de virtualização: • Coleta, protege e distribui informações contextuais sobre todos os aplicativos em execução em um ambiente virtualizado - Isso é inerente à função da virtualização, pois ela controla a dinâmica dos aplicativos, como mover cargas de trabalho para recursos disponíveis, realizar balanceamento de carga e dimensionar vertical e horizontalmente recursos conforme exigido pelo aplicativo - Também conta com um mapa de todas as cargas de trabalho e componentes do sistema no ambiente e atualiza esse mapa conforme as cargas de trabalho são constantemente movidas • Oferece uma única perspectiva da qual se pode ver: - A conexão entre o aplicativo em execução e o hardware em que é executado - A topologia do aplicativo • A disposição de vários componentes do sistema que formam o aplicativo na rede - Como o aplicativo foi aprovisionado e como ele funciona no tempo de execução
Isolamento	• A camada de virtualização: • Oferece um domínio de confiança separado - Oferece visibilidade ao guest, mas o isola • Oferece um ponto de inserção isolado para posicionar controles de segurança que protegem o limite de um aplicativo - Mantém o limite do aplicativo mesmo que as cargas de trabalho migrem para máquinas físicas ou links de rede diferentes
Inalterabilidade	• Com a camada de virtualização, componentes imutáveis podem ser substituídos para cada implantação, em vez de ser atualizados no local - Uma imagem comum pode ser criada uma vez por implantação e testada e validada
Definido por software	• Com a virtualização, o comportamento dos componentes do sistema é iniciado, controlado, alterado e gerenciado de maneira programática • É um ponto de controle flexível do qual colocar máquinas em quarentena, criar uma nova imagem das máquinas, bloquear tráfego, fazer snapshots de máquinas, inserir maior visibilidade etc.

PROPRIEDADES EXCLUSIVAS DA COMPUTAÇÃO MÓVEL

A computação móvel oferece recursos únicos pela funcionalidade nativa do dispositivo, pela funcionalidade de desktops virtuais e pelas tecnologias de gerenciamento de dispositivos móveis.	
Contexto do usuário e do dispositivo	• A computação móvel oferece um conjunto valioso de dados sobre o usuário e o dispositivo para ajudar a tomar decisões de autenticação e controle de acesso com base em riscos, por exemplo: - Dados de usuários e dispositivos • Biometria: impressão digital, voz, imagem • Localização geográfica • ID do dispositivo: número de série, certificado • Parâmetros de rede (Wi-Fi, Intranet etc.) e endereço IP • Configuração de dispositivo: hardware, sistema operacional, aplicativos instalados • Postura de segurança: gerenciada ou não gerenciada, software de segurança, comprometido ou invadido, status de atualização de software e aplicação de patches • Fora de banda: ligação telefônica, notificação push - Decisões de acesso condicional • Vários dispositivos: determine se a localização geográfica do smartphone ou laptop é diferente antes de conceder acesso • Combinação de dados do usuário e dispositivo: determine se o usuário é confiável e o dispositivo é gerenciado em uma rede segura antes de conceder acesso
Isolamento	• Os desktops virtuais oferecem uma conexão isolada para os aplicativos - Permite que as organizações restrinjam o acesso do usuário a um conjunto específico de aplicativos (em vez de todos os aplicativos na rede) • Desktops virtuais também isolam o uso dos aplicativos do uso do dispositivo - Impede que os aplicativos e os dados associados estejam presentes no próprio dispositivo móvel. Em vez disso, o dispositivo móvel apenas visualiza uma exibição remota dos aplicativos.
Inalterabilidade	• Os desktops virtuais não persistentes são imutáveis - Eles podem ser criados instantaneamente de uma imagem mestre controlada e, depois, destruídos e recriados a cada uso. Com a inalterabilidade, é muito difícil que os invasores sejam persistentes
Telemetria	• O monitoramento remoto, a aplicação de políticas e a correção permitem: - Atualizações e aplicações de patches contínuas - Eliminação do dispositivo em caso de perda/roubo, falha no acesso ou roaming fora do Wi-Fi seguro - Quarentena ou encerramento do dispositivo se ele não atender aos requisitos

Apêndice 4: Implementação no data center

Este apêndice apresenta sugestões específicas para implementar recursos orientados aos aplicativos no data center de uma organização.

Recurso	Sugestões para implementação
1. Reconhecer um aplicativo e estabelecer uma referência de linha de base para ele	• Crie sistemas de registros do nível da importância dos aplicativos na configuração e a interação pretendida entre os componentes do sistema - Isso pode ser feito ao trabalhar com equipes de aplicativos, observando sistemas de aprovisionamento, por meio do aprendizado/uso como linhas de base ou de sistemas de automação/esquemas - Serve como informação essencial de registro para identificar e diagnosticar problemas • Crie uma lista branca para um aplicativo (para um sistema de componentes, processos e a forma como interagem e se comunicam em uma rede)
2. Compartimentalizar os componentes do sistema em aplicativos individuais	• Aproveite a malha virtual para criar um limite lógico em torno do aplicativo ou serviço, como a microssegmentação - Aplique esse limite não apenas com um firewall distribuído, mas também com uma rede isolada de camadas 2/3, criando um espaço de endereço não contínuo - Todos os componentes do aplicativo estão contidos em um só segmento isolado com um único limite de controle • Configure um único ponto de saída - Os componentes de um aplicativo dentro do segmento são livres para se comunicarem entre si - Um conjunto limitado de serviços se comunica entre esse limite (DHCP, DNS, AD etc.) - O limite do aplicativo é um ponto definido no qual você pode alinhar seus controles para inspecionar o tráfego desses provedores de serviços
3. Posicionar as defesas em torno de cada aplicativo	• Use a camada de virtualização para alinhar controles para o aplicativo - O sistema de rede definido por software e os controles e segurança baseados em software agora viabilizam operacionalmente o posicionamento de defesas em torno de cada aplicativo.

Apêndice 5: Implementação para a computação para o usuário final.

Este apêndice apresenta sugestões específicas para implementar recursos orientados aos aplicativos no data center para computação para o usuário final.

Recurso	Sugestões para implementação
1. Reconhecer um aplicativo e estabelecer uma referência de linha de base para ele	• Use desktops virtuais não persistentes em vez de aplicativos persistentes em dispositivos de endpoint como parte dos processos para garantir que os aplicativos mantenham os níveis de operação esperados - Com uma imagem de desktop não persistente, o sistema operacional e os aplicativos são mantidos no estado esperado ao ter a imagem de desktop destruída no logoff e recriada no logon seguinte. - Caso uma imagem de desktop não persistente esteja comprometida, o ataque será encerrado posteriormente quando o usuário fizer logoff. Os invasores normalmente precisam de tempo (dias ou mais) para propagar o ataque da máquina inicial para a rede. Por isso, os desktops não persistentes podem impedir que esses invasores se expandam além da sua posição inicial. - Eles impedem que o invasor mantenha uma posição no ambiente. Também impedem que ameaças persistentes avançadas (APT, pela sigla em inglês) façam jus a seu nome. • Use verificações de conformidade de segurança em tempo real em dispositivos para determinar rapidamente se o dispositivo não está em conformidade com as políticas de segurança. Corrija-o na hora ou desative seu acesso aos recursos corporativos.
2. Compartimentalizar os componentes do sistema em aplicativos individuais	• Confine o processo todo, como a conexão do usuário a um aplicativo - Conecte o aplicativo compartimentalizado à infraestrutura do usuário final. • Use a tecnologia de infraestrutura de desktop virtual (VDI, pela sigla em inglês) para garantir que os usuários possam acessar apenas os sistemas necessários. - Com o uso de controles de acesso na camada do aplicativo - Por exemplo, permita que prestadores de serviços acessem apenas os aplicativos de que precisam • Quando os prestadores de serviços se conectam ao desktop virtual, acessam apenas um microssegmento (aplicativo) • Use a tecnologia de VDI em conjunto com a microssegmentação para evitar que um invasor espalhe o ataque pela rede - A plataforma de desktop virtual pode usar microssegmentação para garantir que, caso a máquina de um usuário esteja comprometida (por exemplo, por spear phishing), o invasor só possa acessar um número limitado de hosts, em vez de milhares. • O invasor só poderia obter acesso a um conjunto limitado de aplicativos que o usuário pode acessar por VDI. - O uso de microssegmentação por VDI simplifica a segregação. • É baseado na identidade do usuário: depois que o usuário faz logon, recebe dinamicamente sua própria visualização da rede • Não é necessário realizar um mapeamento muito complexo da rede antes da hora ou configurar previamente diferentes conjuntos de pools de desktops, cada um com diferentes VLANs associadas a eles.

	• Use a tecnologia de mobilidade em conjunto com a microssegmentação para restringir os recursos do data center aos que um aplicativo ou dispositivo móvel pode acessar. - Quando o dispositivo acessa recursos no data center com base na sua identidade, só pode acessar uma parte muito limitada da rede, como um IP ou uma porta específicos • Encerre a VPN no limite da microssegmentação fornecendo ao usuário uma conexão autenticada segura diretamente a um aplicativo - Tradicionalmente, a VPN é encerrada no perímetro; por isso, depois de entrar, o usuário tem acesso a muitas partes da rede
3. Posicionar as defesas em torno de cada aplicativo	• Use a tecnologia de VDI para aplicar controles de segurança diretamente nos aplicativos - É mais eficaz aplicar controles de segurança em aplicativos centralizados no data center do que em milhares de dispositivos • Aproveite as tecnologias de conteinerização de sistema operacional e aplicativos para separar de maneira segura aplicativos e dados da empresa de aplicativos e dados pessoais em um caso de uso de BYOD. Assim, os controles de segurança corporativos podem ser aplicados diretamente nos aplicativos da empresa - Os aplicativos são fornecidos em sandbox e criptografados. • Aproveite os dados de dispositivos de endpoint para garantir que o nível de evidência relativo a identidade e confiança seja proporcional ao nível de risco da solicitação de acesso a um único aplicativo essencial. - Por exemplo, com um dispositivo desconhecido, o usuário precisa passar pela autenticação de dois fatores para acessar um aplicativo. Com um dispositivo confiável e cadastrado, o usuário prossegue com uma autenticação de um fator. O dispositivo age como um segundo fator. Ou, com uma rede Wi-Fi confiável (em um escritório corporativo), o usuário prossegue com uma autenticação de um fator. A verificação da rede age como um segundo fator. • Use a informação de geolocalização para tomar decisões de risco em tempo real sobre o acesso a um único aplicativo essencial. - Veja a geolocalização do laptop e do smartphone do usuário. Se estiverem em locais geograficamente diferentes, o nível de risco exigirá etapas adicionais no processo de autenticação. Por exemplo, uma notificação push pode ser enviada para o smartphone solicitando verificação. • Use a identidade federada para tornar a autenticação mais segura e simplificar o logon para o usuário. - As autenticações federadas para diretórios de terceiros evitam práticas inseguras, como: • Sincronização dos seus diretórios • Ter várias senhas, o que inevitavelmente faz com que os usuários as escrevam ou as reutilizem em vários aplicativos • Use a tecnologia móvel para garantir automaticamente a disponibilidade da segurança em dispositivos, qualquer que seja o sistema operacional (Windows, OSX, iOS, Android, QNX etc.) - Por exemplo, faça uma sondagem nos dispositivos para identificar problemas de segurança, como patches ausentes, e os corrija imediatamente enviando os patches.

A VMware e a Intel transformaram o sistema de rede e a segurança com o Virtual Cloud Network, uma visão de sistema de rede voltada à era digital. A Virtual Cloud Network, criada com base na tecnologia do NSX e executada na arquitetura Intel, fornece uma camada de software onipresente em todo o data center, na nuvem, no perímetro e em outras infraestruturas de hardware, além de conectividade e segurança abrangentes para aplicativos e dados, independentemente de onde eles residam.

COMEÇAR

Saiba mais sobre como você pode ajudar sua organização a buscar uma infraestrutura de aplicativos segura >

Junte-se a nós on-line:

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

Nº do item: TS-0500_VM_Intel_Core-Principles-Of-Cyber-Hygiene-In-A-World-Of-Cloud-And-Mobility_WP_BR
09/18