



SecurityTM
Standards Council

Padrão: Padrão de Segurança de Dados do PCI (PCI DSS)
Versão: 2.0
Data: Junho de 2011
Autor: Grupo de interesse especial de virtualização
PCI Security Standards Council

Suplemento de Informações: Diretrizes de virtualização do PCI DSS

Índice

1	Introdução.....	3
1.1	Público	3
1.2	Uso pretendido.....	4
2	Visão geral da virtualização.....	5
2.1	Conceitos e classes de virtualização	5
2.2	Componentes do sistema virtual e orientação de escopo.....	7
3	Riscos para ambientes virtualizados.....	11
3.1	Vulnerabilidades no ambiente físico se aplicam em um ambiente virtual	11
3.2	Hipervisor cria nova superfície de ataque	11
3.3	Maior complexidade de sistemas e redes virtualizados	12
3.4	Mais de uma função por sistema físico	12
3.5	Mistura de VMs de diferentes níveis de confiança	13
3.6	Falta de separação de tarefas	13
3.7	Máquinas virtuais inativas	13
3.8	Imagens e instantâneos de VM	14
3.9	Imaturidade das soluções de monitoramento	14
3.10	Vazamento de informações entre segmentos de rede virtual	15
3.11	Vazamento de informações entre componentes virtuais.....	15
4	Recomendações.....	16
4.1	Recomendações gerais	16
4.2	Recomendações para ambientes de modo misto	22
4.3	Recomendações para ambientes de computação em nuvem	24
4.4	Orientação para avaliar riscos em ambientes virtuais	27
5	Conclusão.....	30
6	Agradecimentos	31
	Sobre o PCI Security Standards Council	31
7	Anexo – Considerações de virtualização para PCI DSS	29

1 Introdução

Virtualização separa aplicativos, desktops, máquinas, redes, dados e serviços de suas restrições físicas. A virtualização é um conceito em evolução, abrangendo uma ampla gama de tecnologias, ferramentas e métodos, e pode trazer benefícios operacionais significativos para organizações que escolhem alavancá-las. No entanto, como ocorre com qualquer tecnologia em evolução, os riscos também continuam a evoluir e são frequentemente menos compreendidos do que os riscos associados a tecnologias mais tradicionais.

O objetivo deste Suplemento de informações é fornecer orientação sobre o uso da virtualização de acordo com o Padrão de segurança de dados do setor de cartões de pagamento (Payment Card Industry Data Security Standard, PCI DSS). Para os fins deste artigo, todas as referências são feitas à versão 2.0 do PCI DSS.

Há quatro princípios simples associados ao uso de virtualização nos ambientes de dados do portador do cartão:

- a. Se as tecnologias de virtualização forem usadas em um ambiente de dados do portador do cartão, os requisitos do PCI DSS se aplicam a essas tecnologias de virtualização.
- b. A tecnologia de virtualização introduz novos riscos que podem não ser relevantes para outras tecnologias e que devem ser avaliados ao adotar a virtualização em ambientes de dados do portador do cartão.
- c. Implementações de tecnologias virtuais podem variar muito, e as entidades precisarão realizar uma descoberta completa para identificar e documentar as características exclusivas de sua implementação virtualizada específica, incluindo todas as interações com processos de transação de pagamento e dados de cartão de pagamento.
- d. Não há nenhum método ou solução genérico para configurar ambientes virtualizados para atender aos requisitos do PCI DSS. Controles e procedimentos específicos variam para cada ambiente, de acordo com a forma como a virtualização é usada e implementada.

1.1 Público

Este Suplemento de informações destina-se a comerciantes e prestadores de serviços que usam ou estão considerando o uso de tecnologias de virtualização no ambiente de dados do portador do cartão (CDE). Isso também pode ser de valor para avaliadores que analisam ambientes com virtualização como parte de uma avaliação PCI DSS.

Observação: *Este documento pressupõe um nível básico de compreensão das tecnologias e princípios de virtualização. No entanto, um entendimento de nível arquitetônico das tecnologias de virtualização é necessário para avaliar controles técnicos em ambientes virtualizados, já que a natureza desses ambientes, particularmente nas áreas de isolamento de processo e rede virtualizada, pode ser substancialmente diferente dos ambientes físicos tradicionais.*

1.2 Uso pretendido

Este documento fornece orientação complementar sobre o uso de tecnologias de virtualização nos ambientes de dados do portador do cartão e não substitui os requisitos do PCI DSS. Para critérios de conformidade específicos e requisitos de auditoria, os ambientes virtualizados devem ser avaliados em relação aos critérios estabelecidos no PCI DSS.

Este documento não se destina como um endosso para quaisquer tecnologias, produtos ou serviços específicos, mas como reconhecimento de que essas tecnologias existem e podem influenciar a segurança dos dados do cartão de pagamento.

2 Visão geral da virtualização

2.1 Conceitos e classes de virtualização

A virtualização refere-se à abstração lógica dos recursos de computação de limitações físicas. As abstrações comuns são referidas como máquinas virtuais ou VMs, compondo o conteúdo de uma máquina física e permitindo que ela opere em um hardware físico diferente e/ou juntamente com outras máquinas virtuais no mesmo hardware físico. Além das VMs, a virtualização pode ser realizada em muitos outros recursos de computação, incluindo sistemas operacionais, redes, memória e armazenamento.

O termo "carga de trabalho" é cada vez mais usado para descrever a vasta gama de recursos virtualizados. Por exemplo, uma máquina virtual é um tipo de carga de trabalho. Embora as VMs sejam a tecnologia de virtualização predominante implementada hoje, há várias outras cargas de trabalho a serem consideradas, incluindo modelos de aplicativos, desktops, rede e virtualização de armazenamento. Os seguintes tipos de virtualização estão incluídos no foco deste documento.

2.1.1 Sistema operacional

A virtualização do sistema operacional (OS) é comumente usada para levar os recursos executados em um sistema operacional em um único servidor físico e separá-los em partições múltiplas e menores, como ambientes virtuais, servidores privados virtuais, hóspedes, zonas, etc. Neste cenário, todas as partições usariam o mesmo kernel de sistema operacional básico (ou seja, executariam o mesmo sistema operacional que o sistema base), mas podem executar bibliotecas, distribuições, etc.

Da mesma forma, a virtualização de aplicativos separa instâncias individuais de uma aplicação do sistema operacional fundamental, fornecendo um espaço de trabalho de aplicativo discreto para cada usuário.

2.1.2 Hardware/plataforma

A virtualização de hardware é realizada através de particionamento de hardware ou tecnologia de hipervisor. O hipervisor medeia todo o acesso de hardware para as VMs executadas na plataforma física. Há dois tipos de virtualização de hardware:

Hipervisor Tipo 1 – Um hipervisor Tipo 1 (também conhecido como nativo ou bare metal) é um software ou firmware que é executado diretamente no hardware e é responsável por coordenar o acesso a recursos de hardware, bem como hospedar e gerenciar VMs.

Hipervisor Tipo 2 – Um hipervisor Tipo 2 (também conhecido como hospedeiro [hosted]) funciona como um aplicativo em um sistema operacional existente. Esse tipo de hipervisor imita os recursos físicos exigidos para cada VM e é considerado apenas outro aplicativo no que diz respeito ao OS fundamental.

2.1.3 Rede

A virtualização de rede distingue a rede lógica da física. Para quase todos os tipos de componentes de rede física (por exemplo, switches, roteadores, firewalls, sistemas de prevenção de invasão, balanceadores de carga, etc.), há uma contraparte lógica disponível como um dispositivo virtual.

Ao contrário de outros hosts autônomos (como servidor, estação de trabalho ou outro tipo de sistema), os dispositivos de rede operam nos seguintes planos lógicos:

- Plano de dados: Encaminha comunicações de dados entre hosts na rede.
- Plano de controle: Gerencia informações de tráfego, rede e roteamento, incluindo comunicações entre dispositivos de rede relacionados a caminhos de topologia, estado e roteamento de rede.
- Plano de gerenciamento: Lida com comunicações diretas no próprio dispositivo para fins de gerenciamento de dispositivos (por exemplo, configuração, monitoramento e atividades de manutenção).

2.1.4 Armazenamento de dados

O armazenamento de dados virtualizado ocorre quando vários dispositivos de armazenamento físico em uma rede são combinados e apresentados como um único dispositivo de armazenamento. Essa consolidação de dados é comumente usada em redes de área de armazenamento (SANs).

Um dos benefícios do armazenamento virtualizado é que a complexidade da infraestrutura de armazenamento fica oculta, fora da visão do usuário. No entanto, isso também representa um desafio significativo para as entidades que desejam documentar e gerenciar seus armazenamentos de dados, pois um determinado conjunto de dados pode ser armazenado em vários locais distribuídos a qualquer momento.

2.1.5 Memória

A virtualização de memória é a consolidação da memória física disponível de vários sistemas individuais para criar um pool de memória virtualizada, que é compartilhada entre os componentes do sistema.

Semelhante ao armazenamento de dados virtualizado, a consolidação de vários recursos de memória física em um único recurso virtual pode adicionar níveis de complexidade quando se trata de mapear e documentar locais de dados.

2.2 Componentes do sistema virtual e orientação de escopo

Esta seção identifica algumas das abstrações virtuais mais comuns ou de componentes de sistema virtual, que podem estar presentes em muitos ambientes virtuais e fornecem orientação de escopo de alto nível para cada um.

Observe que a orientação de escopo fornecida nesta seção deve ser considerada adicionalmente ao princípio básico que o PCI DSS aplica a todos os componentes do sistema, incluindo componentes virtualizados, incluídos ou conectados ao ambiente de dados do portador do cartão. Determinar se um componente de sistema virtual específico deve ser considerado no escopo dependerá da tecnologia específica e como ele é implementado no ambiente.

2.2.1 Hipervisor

O hipervisor é o software ou firmware responsável pela hospedagem e gerenciamento de máquinas virtuais. O componente do sistema hipervisor também pode incluir o monitor da máquina virtual (VMM). O VMM é um componente de software que implementa e gerencia a abstração de hardware de máquina virtual e pode ser considerado a função de gerenciamento de uma plataforma de hipervisor. O VMM gerencia o processador, a memória e outros recursos do sistema para alocar o que cada sistema operacional (também conhecido como convidado [guest]) da máquina virtual requer. Em algumas circunstâncias, ele fornece essa funcionalidade em conjunto com a tecnologia de virtualização de hardware.

Orientação do escopo: Se algum componente virtual conectado (ou hospedado) ao hipervisor estiver no escopo para o PCI DSS, o hipervisor estará sempre no escopo. Para obter orientação adicional sobre a presença de VMs no escopo e fora do escopo no mesmo hipervisor, consulte a Seção 4.2 Recomendações para ambientes de modo misto.

Observação: o termo “modo misto” refere-se a uma configuração de virtualização onde componentes virtuais dentro e fora do escopo estão sendo executados no mesmo hipervisor ou host.

2.2.2 Máquina virtual

Uma máquina virtual (VM) é um ambiente operacional independente que se comporta como um computador separado. Também é conhecido como “convidado” e é executado sobre o hipervisor.

Orientação do escopo: Uma VM inteira estará no escopo se armazenar, processar ou transmitir dados do portador do cartão ou se ele se conectar ou fornecer um ponto de entrada no CDE. Se uma VM estiver no escopo, tanto o sistema hospedeiro básico quanto o hipervisor também seriam considerados no escopo, visto que estão diretamente conectados e têm um impacto fundamental sobre a funcionalidade e a segurança da VM.

2.2.3 Dispositivo virtual (VA)

Um dispositivo virtual pode ser descrito como uma imagem de software pré-embalada projetada para ser executada dentro de uma máquina virtual. Os dispositivos virtuais são todos destinados a fornecer uma função específica e, tipicamente, consistem em componentes básicos do sistema operacional e um único aplicativo. Dispositivos de rede física como roteadores, comutadores ou firewalls podem ser virtualizados e executados como dispositivos virtuais.

Um Virtual Security Appliance (VSA) — também conhecido como Security Virtual Appliance (SVA) — é um dispositivo virtual que consiste em um sistema operacional reforçado e um único aplicativo de segurança. Os VSAs são normalmente atribuídos a um nível mais elevado de confiança do que um VA regular, incluindo acesso privilegiado ao hipervisor e outros recursos. Para que o VSA execute funções de gerenciamento de sistema e rede, ele geralmente tem maior visibilidade do hipervisor e de qualquer rede virtual que funcione dentro do hipervisor. Algumas soluções VSA podem conectar-se diretamente ao hipervisor, fornecendo segurança adicional à plataforma. Exemplos de dispositivos que têm implementações virtuais incluem firewalls, IPS/IDS e antivírus.

Orientação do escopo: Os dispositivos virtuais usados para conectar ou fornecer serviços para componentes ou redes do sistema no escopo seriam considerados no escopo. Qualquer VSA/SVA que poderia afetar a segurança do CDE também seria considerado no escopo.

2.2.4 Comutador ou roteador virtual

Um comutador virtual ou roteador é um componente de software que fornece roteamento de dados de nível de rede e funcionalidade de comutação. Um comutador virtual é geralmente uma parte da plataforma do servidor virtualizado, por exemplo, driver do hipervisor, módulo ou plug-in. Um roteador virtual pode ser implementado como um dispositivo virtual distinto ou como um componente de um dispositivo físico. Além disso, comutadores e roteadores virtuais podem ser usados para gerar vários dispositivos de rede lógica a partir de uma única plataforma física.

Orientação do escopo: As redes provisionadas em um comutador virtual baseado em hipervisor estarão no escopo se fornecidas com um componente no escopo ou se fornecerem serviços ou se conectarem a um componente no escopo. Dispositivos físicos que hospedam comutadores virtuais ou roteadores seriam considerados no escopo se algum dos componentes hospedados se conectar a uma rede no escopo.

2.2.5 Desktops e aplicativos virtuais

Ambientes de desktop e aplicativos individuais também podem ser virtualizados para fornecer funcionalidade para usuários finais. Aplicativos e desktops virtuais são normalmente instalados em um local central e acessados remotamente através de uma interface de desktop remota. Os desktops virtuais podem ser configurados para permitir acesso através de vários tipos de dispositivos, incluindo thin clients e dispositivos móveis, e podem ser executados usando recursos de computação locais ou remotos. Aplicativos e desktops virtuais podem estar presentes no ponto de venda, atendimento ao cliente e outras interações com a cadeia de pagamento.

Orientação do escopo: Aplicativos e desktops virtuais estarão no escopo se estiverem envolvidos no processamento, armazenamento ou transmissão dos dados do portador do cartão, ou fornecerem acesso ao CDE. Se um aplicativo virtual ou desktop for provisionado no mesmo host físico ou hipervisor como componente no escopo, o aplicativo virtual/desktop também estará no escopo, a menos que haja uma segmentação adequada que isole todos os componentes no escopo dos componentes fora do escopo. Para obter orientação adicional sobre a presença de componentes dentro e fora do escopo no mesmo host ou hipervisor, consulte a Seção 4.2 Recomendações para ambientes de modo misto.

2.2.6 Computação em nuvem

A computação em nuvem é um uso de virtualização em rápida evolução que fornece recursos de computação como serviço ou utilitário em infraestruturas públicas, semipúblicas ou privadas. Ofertas de serviços baseadas em nuvem são geralmente entregues de um pool ou cluster de sistemas conectados e fornecem acesso baseado em serviços a recursos de computação compartilhados para vários usuários, entidades ou locatários.

Orientação do escopo: O uso de computação em nuvem apresenta vários desafios e considerações de escopo. As entidades que planejam usar a computação em nuvem para seus ambientes PCI DSS devem primeiro garantir que entendem bem os detalhes dos serviços oferecidos e realizar uma avaliação detalhada dos riscos exclusivos associados a cada serviço. Além disso, como ocorre com qualquer serviço gerenciado, é crucial que a entidade e o provedor hospedados definam e documentem claramente as responsabilidades atribuídas a cada parte para manter os requisitos do PCI DSS e quaisquer outros controles que possam afetar a segurança dos dados do portador do cartão.

O provedor de nuvem deve identificar claramente quais requisitos, componentes do sistema e serviços do PCI DSS são cobertos pelo programa de conformidade PCI DSS do provedor de nuvem. Quaisquer aspectos do serviço que não estejam cobertos pelo provedor de nuvem, devem ser identificados e claramente documentados no contrato de serviço de que a responsabilidade de gerenciamento e avaliação desses aspectos, componentes do sistema e requisitos do PCI DSS são da entidade hospedada. O provedor de nuvem deve fornecer evidências suficientes e garantir que todos os processos e componentes sob seu controle estejam em conformidade com o PCI DSS.

Para obter orientação adicional sobre o uso de ambientes de nuvem, consulte a Seção 4.3 Recomendações para ambientes de computação em nuvem.

3 Riscos para ambientes virtualizados

Embora a virtualização possa fornecer vários benefícios funcionais e operacionais, migrar para um ambiente virtual não reduz os riscos que existiam nos sistemas físicos e também pode introduzir riscos novos e exclusivos. Consequentemente, há vários fatores a serem considerados ao implementar tecnologias virtuais, incluindo, entre outros, aqueles definidos abaixo.

3.1 Vulnerabilidades no ambiente físico se aplicam em um ambiente virtual

Os sistemas e redes virtuais estão sujeitos aos mesmos ataques e vulnerabilidades que existem em uma infraestrutura física. Um aplicativo que tem falhas de configuração ou é vulnerável a explorações ainda terá essas mesmas falhas e vulnerabilidades quando instalado em uma implementação virtual.

Da mesma forma, um firewall virtual mal configurado poderia expor, inesperadamente, sistemas internos a ataques baseados na internet da mesma forma que a configuração incorreta em um firewall físico faria.

As ameaças físicas também se aplicam a implementações virtuais; as partições lógicas mais bem definidas e bem contidas ainda precisarão de controles físicos adequados para proteção do hardware. Por esse motivo, o sistema hospedeiro físico permanecerá sempre no escopo, mesmo onde houver redução lógica.

3.2 Hipervisor cria nova superfície de ataque

Um fator de risco principal, exclusivo dos ambientes virtuais, é o hipervisor — se ele estiver comprometido ou não configurado adequadamente, todas as VMs hospedadas nesse hipervisor estão potencialmente em risco. O hipervisor fornece um único ponto de acesso ao ambiente virtual e também é potencialmente um ponto único de falha. Hipervisores mal configurados podem resultar em um único ponto de comprometimento para a segurança de todos os componentes hospedados. Por mais segura que seja a configuração das máquinas virtuais individuais ou componentes, um hipervisor comprometido pode substituir esses controles e obter acesso direto aos sistemas virtuais.

Além de fornecer um possível ponto de entrada para as VMs hospedadas nele, o hipervisor cria uma nova superfície de ataque que não existe no mundo físico e pode ser vulnerável a ataques diretos. Pontos fracos em tecnologia de isolamento de hipervisor, controles de acesso, reforço de segurança e patching podem ser identificados e explorados, permitindo que os invasores obtenham acesso a VMs individuais.

Além disso, a configuração padrão do hipervisor geralmente não é a mais segura; e a menos que seja configurado adequadamente, até mesmo um hipervisor seguro pode ser explorado.

É fundamental que o acesso ao hipervisor seja restrito de acordo com o privilégio mínimo e a necessidade de saber, e que o monitoramento independente de todas as atividades seja aplicado. Os hipervisores não são criados iguais, e é particularmente importante escolher uma solução que ofereça suporte às funções de segurança necessárias para cada ambiente.

3.3 Maior complexidade de sistemas e redes virtualizados

Configurações virtualizadas podem abranger sistemas e redes; por exemplo, VMs podem transmitir dados entre si através do hipervisor, bem como por conexões de rede virtual e através de dispositivos de segurança de rede virtual, como firewalls virtuais. Embora essas configurações possam oferecer benefícios operacionais significativos, essas camadas adicionais de tecnologia também introduzem um nível considerável de complexidade que deve ser cuidadosamente gerenciada e pode exigir controles de segurança adicionais e gerenciamento de políticas complexo para garantir que a segurança apropriada seja aplicada em cada camada. Combinada a possíveis vulnerabilidades em sistemas operacionais virtuais e aplicativos, essa maior complexidade também pode levar ao erro acidental na configuração ou até mesmo ameaças totalmente novas que não foram previstas pelos designers do sistema. Como as instâncias de componentes virtuais são frequentemente replicadas em vários sistemas, a presença dessas vulnerabilidades pode resultar em comprometimento significativo em todo um ambiente.

3.4 Mais de uma função por sistema físico

Uma preocupação específica em ambientes virtuais é a possibilidade de que o comprometimento de uma função de sistema virtual possa levar a um comprometimento de outras funções no mesmo sistema físico. Uma VM comprometida poderia usar mecanismos de comunicação de camada de virtualização para iniciar ataques em outras VMs no mesmo host ou até mesmo no hipervisor. As tecnologias de virtualização podem ser capazes de atenuar parte desse risco, aplicando a separação do processo entre diferentes funções. Mesmo assim, o risco associado à localização de múltiplas funções ou componentes em um único sistema físico ainda deve ser considerado. Por exemplo, ter várias funções hospedadas em um sistema físico aumenta o possível escopo de comprometimento caso um invasor obtenha acesso físico ao sistema host.

Consulte também Mistura de VMs de diferentes níveis de confiança abaixo para considerações de risco relacionadas.

3.5 Mistura de VMs de diferentes níveis de confiança

Um dos desafios ao planejar uma implantação de virtualização é identificar as configurações apropriadas para a variedade de cargas de trabalho a serem alojadas dentro da tecnologia de virtualização específica. O risco de hospedar VMs de diferentes níveis de confiança no mesmo host precisa ser cuidadosamente avaliado. No contexto virtual, uma VM de menor confiança normalmente terá controles de segurança menores do que VMs de níveis de confiança mais altos. A VM de menor confiança poderia, portanto, ser mais fácil de comprometer, potencialmente transformando-se em um trampolim para as VMs mais sensíveis e de alto risco no mesmo sistema. Teoricamente, a hospedagem de VMs de diferentes níveis de confiança no mesmo hipervisor ou host poderia reduzir a segurança geral para todos os componentes ao nível de segurança do componente menos protegido (também conhecido como o princípio do elo fraco, ou seja, a segurança é tão forte quanto o elo mais fraco da corrente).

Devido ao aumento de riscos e desafios de configuração, a confiança e o nível de risco associados a cada função de VM devem ser levados em conta ao considerar um projeto virtualizado. Da mesma forma, bancos de dados e outros sistemas que armazenam dados do portador do cartão exigem um nível de segurança maior do que os armazenamentos de dados não confidenciais. O risco de misturar dados sensíveis com dados de menor confiança deve ser cuidadosamente avaliado.

3.6 Falta de separação de tarefas

Pode ser particularmente desafiador definir funções de usuário granulares (por exemplo, separação do administrador de rede do administrador do servidor) e políticas de acesso em um ambiente distribuído e virtualizado. Os riscos de não definir adequadamente funções e políticas de acesso são significativos, porque o acesso ao hipervisor pode potencialmente fornecer amplo acesso a componentes-chave de infraestrutura (incluindo comutadores, firewalls, aplicativos de pagamento, servidores de agregação de registros, bancos de dados, etc.). Devido ao aumento da acessibilidade a vários dispositivos virtuais e funções de um único local lógico ou usuário, o monitoramento e a aplicação da separação adequada de tarefas é crucial em um ambiente virtual.

3.7 Máquinas virtuais inativas

Em muitas plataformas de virtualização, as VMs podem existir em estados ativos ou inativos. VMs que não estão ativas (inativas ou não mais usadas) podem ainda armazenar dados confidenciais como credenciais de autenticação, chaves de criptografia ou informações críticas de configuração. VMs inativas contendo dados de cartão de pagamento podem se tornar armazenamentos de dados desconhecidos, não seguros, que são frequentemente redescobertos apenas no caso de uma violação de dados.

Como as VMs inativas não são usadas ativamente, elas podem ser facilmente ignoradas e inadvertidamente deixadas de fora dos procedimentos de segurança. Uma VM inativa provavelmente não será atualizada com os patches de segurança mais recentes, resultando na exposição do sistema a vulnerabilidades conhecidas que a organização acha que foram abordadas. Também é improvável que VMs inativas tenham políticas de acesso atualizadas e podem ser excluídas das funções de segurança e monitoramento, possivelmente criando uma porta de entrada não verificada para o ambiente virtual.

Além disso, os dados na memória de uma VM (que podem incluir, por exemplo, PAN não criptografado) geralmente são capturados em seu estado inativo, resultando em armazenamento não intencional dos dados. Como esses dados estavam na memória quando foram capturados, eles poderiam ser facilmente negligenciados e deixados desprotegidos, mesmo que agora estejam armazenados na VM inativa. Porém, VMs inativas representam uma ameaça de segurança viável e, portanto, devem ser identificadas e monitoradas para que os controles de segurança apropriados possam ser aplicados.

3.8 Imagens e instantâneos de VM

Imagens e instantâneos de máquina virtual fornecem um meio de implantar ou restaurar rapidamente sistemas virtuais em vários hosts dentro de um curto período de tempo. Deve-se prestar atenção especial à preparação de imagens e instantâneos de VM, pois eles podem capturar dados sensíveis presentes no sistema no momento em que a imagem foi tirada, incluindo conteúdo de memória ativa. Isso pode resultar na captura, armazenamento ou até mesmo na implantação não intencional de informações sensíveis em todo o ambiente.

Além disso, se as imagens não estiverem seguras e protegidas contra modificação, um invasor pode obter acesso e inserir vulnerabilidades ou código malicioso na imagem. A imagem comprometida pode então ser implantada em todo o ambiente, resultando em um rápido comprometimento de vários hosts.

3.9 Imaturidade das soluções de monitoramento

Ao mesmo tempo em que a virtualização aumenta a necessidade de registro e monitoramento, atualmente é reconhecido que as ferramentas para monitorar as redes virtuais, firewalls virtuais, sistemas de conformidade virtual, etc., não são tão maduras quanto suas contrapartes físicas.

Em comparação com as ferramentas de monitoramento tradicionais para uma rede física, as para sistemas virtuais podem não fornecer o mesmo nível de informação ou monitoramento nas comunicações entre hosts ou tráfego que flui entre VMs em uma rede virtual. Da mesma forma, ferramentas especializadas para monitoramento e registro de ambientes virtuais podem ser necessárias para capturar o nível de detalhe obrigatório dos vários componentes, incluindo hipervisores, interfaces de gerenciamento, máquinas virtuais, sistemas host e dispositivos virtuais.

3.10 Vazamento de informações entre segmentos de rede virtual

Os possíveis riscos de vazamento de informações entre segmentos de rede lógica devem ser entendidos ao considerar a virtualização de rede. O vazamento de informações no plano de dados resulta em dados confidenciais existentes fora dos locais conhecidos, burlando os controles de proteção de dados que, de outra forma, seriam aplicáveis. O vazamento de informações no plano de controle ou plano de gerenciamento pode ser explorado para permitir vazamento de informações no plano de dados, ou para influenciar rotas de rede e o comportamento de encaminhamento para burlar controles de segurança baseados em rede. Idealmente, as capacidades de virtualização em todos os três planos de operação na infraestrutura de rede devem fornecer controles e recursos para proteger a infraestrutura virtualizada em um nível equivalente aos dispositivos físicos individuais.

3.11 Vazamento de informações entre componentes virtuais

O vazamento de informações entre componentes virtuais pode ocorrer quando o acesso a recursos compartilhados permite que um componente colete informações sobre outro componente no mesmo host. Por exemplo, um invasor pode usar um componente comprometido para coletar informações sobre outros componentes que funcionam no mesmo host e potencialmente obter conhecimento suficiente para criar um comprometimento adicional. Em outro exemplo, o invasor poderia obter acesso à memória básica do sistema operacional, resultando na possível captura de informações sensíveis de vários componentes. Um hipervisor mal configurado também pode se tornar um canal para vazamento de informações entre componentes e redes virtuais hospedados. O isolamento de todos os recursos físicos (incluindo memória, CPU, rede, etc.) é essencial para evitar vazamento de informações entre VMs e outros componentes ou redes no mesmo host.

4 Recomendações

Os controles identificados nesta seção são recomendações e as melhores práticas que podem ajudar a atender aos requisitos do PCI DSS em ambientes virtuais.

4.1 Recomendações gerais

4.1.1 Avaliar os riscos associados às tecnologias virtuais

As entidades devem avaliar cuidadosamente os riscos associados com a virtualização dos componentes do sistema antes de selecionar ou implementar uma solução de virtualização. O fluxo e o armazenamento dos dados do titular do cartão devem ser documentados de forma precisa como parte desse processo de avaliação de risco, para garantir que todas as áreas de risco sejam identificadas e atenuadas adequadamente. A virtualização deve ser implantada com uma visão completa dos seus benefícios e riscos e um conjunto abrangente e definido de controles de sistema, aplicativos, dados e ambientais eficazes.

Ambientes virtualizados e componentes do sistema devem continuar a ser incluídos em um processo anual de avaliação de risco. As decisões de avaliação e gerenciamento de risco devem ser totalmente documentadas e apoiadas por avaliações técnicas e empresariais detalhadas.

4.1.2 Compreender o impacto da virtualização junto ao escopo do CDE

Entidades que usam a virtualização para consolidar seu ambiente em uma ou mais plataformas físicas de hardware podem achar que, como resultado, agora têm um conjunto complexo de configurações de sistema virtual, dificultando a identificação dos limites ou escopo de seu CDE.

A exemplo dos sistemas físicos, o escopo do PCI DSS em todos os componentes virtuais deve ser cuidadosamente verificado e documentado. O ambiente virtual deve ser avaliado usando a orientação fornecida na seção do PCI DSS, Escopo da avaliação para conformidade com os requisitos do PCI DSS. Se algum componente executado em um único hipervisor estiver no escopo, recomenda-se que todos os componentes nesse hipervisor também sejam considerados no escopo, incluindo, entre outros, máquinas virtuais, dispositivos virtuais e plug-ins do hipervisor. Projetar todos os componentes de virtualização, mesmo aqueles considerados fora do escopo, para atender aos requisitos de segurança do PCI DSS não apenas fornecerá uma base segura para o ambiente virtual como um todo, mas também reduzirá a complexidade e o risco associados ao gerenciamento de vários perfis de segurança e a sobrecarga e o esforço necessários para manter e validar a conformidade dos componentes no escopo.

4.1.3 Restringir o acesso físico

Conforme identificado anteriormente neste documento, a hospedagem de vários componentes em um sistema físico pode aumentar enormemente o impacto potencial se um invasor obter acesso físico a esse sistema host. Portanto, os controles de acesso físico são particularmente importantes em ambientes virtualizados e devem ser reforçados conforme necessário para atenuar os riscos associados. Ao avaliar controles físicos, considere o dano potencial de um indivíduo não autorizado ou mal-intencionado obter acesso simultâneo a todas as VMs, redes, dispositivos de segurança, aplicativos e hipervisores que um host físico poderia fornecer. Certifique-se de que todas as interfaces físicas não utilizadas estejam desativadas e que o acesso físico ou do console seja restrito e monitorado.

4.1.4 Implementar a defesa em profundidade

Em um ambiente físico, uma abordagem de defesa profunda, que engloba controles preventivos, de detecção e responsivos, é uma prática comum para proteger dados e outros ativos. Controles lógicos de segurança são normalmente aplicados na rede, host, aplicativo e camada de dados, e controles de segurança física são implementados para proteger mídia, sistemas e instalações contra acesso físico não autorizado. Monitorar a eficácia dos controles e a capacidade de responder rápida e eficazmente a uma possível violação também é de primordial importância. Uma abordagem de defesa profunda também inclui treinar e instruir o pessoal sobre o uso adequado de ativos sensíveis, a identificação de possíveis ameaças à segurança e a ação apropriada a ser tomada no caso de uma violação. Além disso, um ambiente de defesa profunda tem políticas, processos e procedimentos bem definidos e documentados que são compreendidos e seguidos por todos os funcionários.

Controles de segurança apropriados devem ser identificados e implementados em um ambiente virtualizado que forneça o mesmo nível e profundidade de segurança que podem ser alcançados em um ambiente físico. Por exemplo, considere como a segurança pode ser aplicada para proteger cada camada técnica, incluindo, entre outros, o dispositivo físico, hipervisor, plataforma host, sistemas operacionais convidados, VMs, rede de perímetro, rede intra-host, aplicação e camadas de dados. Controles físicos, políticas e procedimentos documentados e treinamento de pessoal também devem ser parte de uma abordagem de defesa em profundidade para proteger ambientes virtuais.

4.1.5 Isolar funções de segurança

As funções de segurança fornecidas pelas VMs devem ser implementadas com a mesma separação de processo necessária no mundo físico. Recomenda-se que este requisito seja ainda mais rigorosamente aplicado em sistemas virtualizados porque ele complica significativamente os esforços exigidos por um invasor para comprometer vários componentes do sistema CDE. Por exemplo, controles preventivos, como um firewall de rede, nunca devem ser combinados em um único host lógico com os dados de cartão de pagamento que ele está configurado para proteger. Da mesma forma, os processos que controlam a segmentação da rede e a função de agregação de registros que detectariam adulteração dos controles de segmentação de rede não devem ser misturados. Se essas funções de segurança forem hospedadas no mesmo hipervisor ou host, o nível de isolamento entre as funções de segurança deve ser considerado como sendo instalado em máquinas separadas.

4.1.6 Impor menos privilégio e separação de tarefas

As contas e credenciais para acesso administrativo ao hipervisor devem ser cuidadosamente controladas e, dependendo do nível de risco, o uso de controles de acesso mais restritivos ao hipervisor é frequentemente justificado. As entidades devem considerar métodos adicionais para garantir acesso administrativo, como implementar autenticação de dois fatores ou estabelecer controle duplo ou dividido de senhas administrativas entre vários administradores. Os controles de acesso devem ser avaliados para acesso local e remoto ao hipervisor e ao sistema de gerenciamento. Atenção especial deve ser direcionada às funções dos componentes virtuais individuais, para garantir que controles de acesso adequados baseados em funções (RBAC) estejam em vigor para impedir o acesso desnecessário aos recursos e impor a separação de tarefas.

Os privilégios administrativos também precisam ser separados adequadamente. Por exemplo, um administrador de usuário único não deve receber acesso privilegiado a firewalls e servidores de monitoramento para esses firewalls. Esse amplo acesso poderia resultar em adulterações não detectadas e em perda de dados que poderiam ter sido evitadas com a devida aplicação da separação de funções. Como melhor prática, restrinja o acesso administrativo por função de VM específica, rede virtual, hipervisor, hardware, aplicativo e armazenamento de dados.

4.1.7 Avaliar tecnologias de hipervisor

Certifique-se de que a segurança do hipervisor tenha sido completamente testada antes da implantação e que haja gerenciamento apropriado de patches e outros controles para responder a ameaças e explorações. É essencial identificar e implementar tecnologias que facilitem práticas de segurança fortes, já que nem todos os hipervisores ou VMMs têm a funcionalidade de apoiar controles de segurança apropriados.

4.1.8 Fortalecer o hipervisor

As plataformas de hipervisor devem ser implantadas de forma segura, de acordo com as melhores práticas e diretrizes de segurança aceitas pelo setor. O gerenciamento cuidadoso de configurações de sistema virtual, patches e processos de controle de mudanças é essencial para garantir que todas as alterações de hipervisor sejam monitoradas, autorizadas, totalmente testadas e cuidadosamente controladas. Devido à gravidade potencial de um comprometimento de hipervisor, os patches e outros controles de mitigação devem ser implantados assim que possível, sempre que novas vulnerabilidades de segurança forem descobertas e incluir testes imediatos para a vulnerabilidade para confirmar que o risco foi abordado.

Como o hipervisor representa um único ponto de falha, uma modificação não autorizada ou maliciosa pode ameaçar a integridade de todos os sistemas hospedados no ambiente. Os seguintes controles adicionais são recomendados para o hipervisor e quaisquer ferramentas de gerenciamento significativas.

- Restringir o uso de funções administrativas para redes e dispositivos de endpoint definidos, como laptops ou desktops específicos que tenham sido aprovados para esse acesso.
- Exigir autenticação de múltiplos fatores para todas as funções administrativas.
- Garantir que todas as alterações sejam implementadas e testadas adequadamente. Considere exigir supervisão adicional da gerência, acima e além daquela exigida através do processo normal de gestão de mudanças.
- Separar funções administrativas, de modo que os administradores do hipervisor não tenham a capacidade de modificar, excluir ou desativar registros de auditoria de hipervisor.
- Enviar registros de hipervisor para armazenamento fisicamente separado e seguro o mais próximo possível do tempo real.
- Monitorar registros de auditoria para identificar atividades que poderiam indicar uma violação na integridade da segmentação, controles de segurança ou canais de comunicação entre cargas de trabalho.
- Separar as obrigações para as funções administrativas, de modo que as credenciais de autenticação para o hipervisor não tenham acesso a aplicativos, dados ou componentes virtuais individuais.
- Antes de implementar uma solução de virtualização, verifique quais controles de segurança a solução suporta e como eles minimizam o risco de comprometimento para o hipervisor.

Observe que, como o hipervisor e as ferramentas de gerenciamento podem afetar diretamente a segurança dos componentes virtuais, eles sempre devem ser considerados no escopo para o PCI DSS.

4.1.9 Fortalecer máquinas virtuais e outros componentes

Também é fundamental que todas as máquinas virtuais individuais sejam instaladas e configuradas com segurança e de acordo com as melhores práticas e diretrizes de segurança do setor. As recomendações fornecidas acima para fortalecer o hipervisor também são aplicáveis a VMs e componentes virtuais.

Observe que talvez essas recomendações não sejam aplicáveis a todo tipo de máquina virtual ou componente. As implementações devem ser avaliadas individualmente para confirmar se o seguinte está sendo considerado:

- Desativar ou remover todas as interfaces, portas, dispositivos e serviços desnecessários;
- Configurar com segurança todas as interfaces de rede virtual e áreas de armazenamento;
- Estabelecer limites sobre uso de recursos de VM;
- Garantir que todos os sistemas operacionais e aplicativos executados dentro da máquina virtual também sejam fortalecidos;
- Enviar registros para armazenamento separado e seguro o mais próximo possível do tempo real;
- Validar a integridade das operações de gerenciamento de chaves criptográficas;
- Fortalecer o hardware e compartimentos virtuais de VMs;
- Outros controles de segurança, conforme aplicável.

Os requisitos de segurança e fortalecimento podem diferir dependendo dos serviços ou aplicativos específicos executados em cada componente virtual. Consequentemente, as configurações de segurança apropriadas precisarão ser determinadas individualmente.

4.1.10 Definir o uso adequado das ferramentas de gerenciamento

As ferramentas de gerenciamento permitem que os administradores executem essas funções, como backup, restauração, conectividade remota, migração e alterações de configuração para sistemas virtuais. Ferramentas de gerenciamento para os componentes dentro do escopo também seriam consideradas neste, pois elas afetam diretamente a segurança e o funcionamento desses componentes. O acesso às ferramentas de gerenciamento deve ser limitado àquelas que tenham uma necessidade relacionada ao trabalho de ter esse acesso. A segregação de funções e responsabilidades é recomendada para as funções da ferramenta de gerenciamento, e o uso dessas ferramentas deve ser monitorado e registrado.

4.1.11 Reconhecer a natureza dinâmica das VMs

VMs são efetivamente apenas dados que podem residir em estados ativos (em um hipervisor) ou inativos (em qualquer lugar). VMs inativas são conjuntos de dados armazenados efetivamente que podem conter informações sensíveis e detalhes de configuração de dispositivo virtual. Um indivíduo com acesso a uma VM inativa poderia copiá-la e ativá-la em outro local, ou poderia ler os arquivos inativos para dados de cartão de pagamento e outras informações confidenciais. Portanto, o acesso a VMs inativas deve ser restrito, monitorado e controlado cuidadosamente.

VMs inativas que contêm dados de cartão de pagamento precisam ser tratadas com o mesmo nível de sensibilidade e ter as mesmas proteções que qualquer outro armazenamento de dados do titular do cartão. Os caminhos de migração de VMs inativas devem ser cuidadosamente avaliados, pois podem trazer sistemas adicionais ao escopo. Backups de VMs, VMs ativas e VMs inativas devem sempre ser protegidos e excluídos com segurança ou apagados, quando os dados não forem mais necessários. Processos completos de gerenciamento, monitoramento e alerta de mudanças são essenciais para garantir que apenas VMs autorizadas sejam adicionadas e removidas do ambiente e que todos os acessos e ações sejam registrados.

4.1.12 Avaliar recursos de segurança de redes virtualizadas

Idealmente, qualquer implantação de infraestrutura de rede virtualizada deve incluir medidas de segurança efetivas no plano de dados, plano de controle e plano de gerenciamento. Isso ajudará a minimizar a possibilidade de vulnerabilidades diretas e indiretas em cascata de um plano para outro e o comprometimento dos dispositivos da rede virtual. Embora ideais, nem sempre as medidas de segurança eficazes são possíveis em todos os três planos operacionais. Nesses casos, torna-se cada vez mais importante garantir que os componentes físicos fundamentais sejam adequadamente isolados e protegidos e que não forneçam um caminho entre os dispositivos de rede virtual. O isolamento entre dispositivos de rede virtualizados deve ser tal que os sistemas virtuais possam ser considerados de forma eficaz como hardware separado.

Cada dispositivo virtualizado deve manter configurações individuais e independentes controladas por acesso. As trilhas de auditoria para infraestruturas virtuais devem ser granulares e detalhadas o suficiente para identificar o acesso individual e atividades realizadas em cada componente virtual específico. Os controles de acesso devem aplicar menos privilégios, tanto individualmente para cada dispositivo quanto em toda a plataforma.

4.1.13 Definir claramente todos os serviços virtuais hospedados

Às vezes, os provedores de hospedagem compartilhada virtualizam suas ofertas, provisionando cargas de trabalho separadas para os clientes em vez de provisionar sistemas físicos separados. Entidades que consideram um serviço virtual hospedado devem garantir que a oferta de serviço imponha a segmentação administrativa, do processo e técnica para isolar o ambiente de cada entidade hospedada de outras entidades. Esse isolamento deve, no mínimo, abranger todos os controles PCI DSS, incluindo, entre outros, autenticação segmentada, controles de rede e de acesso, criptografia e registro.

Além disso, é fundamental garantir que todos os detalhes do serviço, incluindo responsabilidades para manter controles que possam afetar a segurança ou a integridade de dados sensíveis ou que possam afetar a conformidade com o PCI DSS da entidade, sejam claramente definidos e documentados em um acordo formal.

4.1.14 Entender a tecnologia

Ambientes virtualizados são substancialmente diferentes dos ambientes físicos tradicionais, e é necessário o entendimento completo das tecnologias de virtualização para avaliar e proteger qualquer ambiente com eficácia. Na ausência de padrões formais de segurança de virtualização, as entidades devem se familiarizar com as melhores práticas e diretrizes aceitas pelo setor para proteger ambientes virtualizados. Exemplos de recursos que podem fornecer orientação incluem publicações de:

- The Center for Internet Security (CIS)
- International Organization for Standardization (ISO)
- ISACA (antiga Information Systems Audit and Control Association) (Associação de Auditoria e Controle de Sistemas de Informação)
- National Institute of Standards and Technology (NIST)
- Instituto SysAdmin Audit Network Security (SANS)

4.2 Recomendações para ambientes de modo misto

É altamente recomendável, e um princípio básico de segurança, que VMs de diferentes níveis de segurança não sejam hospedadas no mesmo hipervisor ou host físico; a principal preocupação é que uma VM com requisitos de segurança mais baixos terá menos controles de segurança, e poderia ser usada para lançar um ataque ou fornecer acesso a VMs mais sensíveis no mesmo sistema.

Esse princípio também deve ser aplicado se sistemas virtuais, dentro e fora do escopo, estiverem localizados no mesmo host ou hipervisor. Como regra geral, qualquer VM ou outro componente virtual que esteja hospedado no mesmo hardware ou hipervisor que um componente no escopo, também estaria no escopo do PCI DSS, já que tanto o hipervisor quanto o host básico fornecem uma conexão (física, lógica ou ambas) entre os componentes virtuais, e talvez não seja possível alcançar um nível apropriado de isolamento ou segmentação entre componentes dentro e fora do escopo localizados no mesmo host ou hipervisor.

Conforme afirmado anteriormente neste documento, qualquer hipervisor ou sistema host que aloje um componente virtual no escopo também estará no escopo para o PCI DSS. Para que VMs dentro do escopo e fora do escopo coexistam no mesmo host ou hipervisor, elas devem ser isoladas umas das outras, de modo que possam ser consideradas de forma eficaz como hardware separado em diferentes segmentos de rede sem conectividade entre si. Quaisquer componentes do sistema compartilhados pelas VMs, incluindo o hipervisor e o sistema host básico, não devem, portanto, fornecer um caminho de acesso entre as VMs.

Mesmo que a segmentação adequada entre componentes virtuais possa ser alcançada, o esforço de recursos e a sobrecarga administrativa necessários para impor a segmentação e para manter diferentes níveis de segurança em cada componente provavelmente seriam mais complicados do que aplicar controles PCI DSS ao sistema como um todo.

4.2.1 Segmentação em ambientes de modo misto

O nível de segmentação necessário para sistemas dentro e fora do escopo no mesmo host deve ser equivalente a um nível de isolamento alcançável no mundo físico; ou seja, a segmentação deve garantir que cargas de trabalho fora do escopo ou componentes não possam ser usados para acessar um componente que esteja dentro do escopo. Diferentemente dos sistemas físicos separados, a segmentação baseada em rede sozinha não pode isolar componentes no escopo daqueles fora do escopo em um ambiente virtual.

A segmentação de componentes virtuais também deve ser aplicada a todos os mecanismos de comunicação virtual, incluindo o hipervisor e o host básico, bem como qualquer outro componente comum ou compartilhado. Em ambientes virtuais, podem ocorrer comunicações fora de banda, frequentemente através de um mecanismo de comunicação específico da solução, ou através do uso de recursos compartilhados como sistemas de arquivos, processadores, memória volátil e não volátil, drivers de dispositivo, dispositivos de hardware, APIs e assim por diante. Canais de comunicação fora de banda são geralmente específicos para a tecnologia de virtualização em uso. Portanto, um entendimento detalhado de todos os mecanismos fundamentais é crítico ao planejar os componentes virtuais do segmento. Todos os canais existentes fora de banda devem ser identificados e documentados, sejam eles ativamente usados ou não, e os controles apropriados para isolar cargas de trabalho e componentes virtuais devem ser implementados. Em alguns casos, a separação física dos recursos de hardware pode ser necessária para evitar que o hardware seja usado como um caminho de acesso entre os componentes virtuais.

É importante observar que os canais fora de banda são frequentemente necessários para funções específicas do sistema virtual, e muitas vezes não é possível isolar componentes desses canais sem afetar as operações do sistema. Se não for viável para uma implementação específica aplicar o isolamento dos componentes dentro do escopo daqueles fora do escopo através de recursos compartilhados ou outros canais fora de banda, todos os componentes que acessam o recurso compartilhado ou o canal fora de banda devem ser considerados como dentro do escopo, uma vez que estão efetivamente conectados ao componente no escopo.

O isolamento do processo também é um componente inerente da segmentação entre os sistemas virtuais. Em uma configuração de modo misto, o hipervisor desempenha um papel fundamental na aplicação de isolamento de processo entre os sistemas dentro e fora do escopo. Portanto, é fundamental que esses controles estejam funcionando adequadamente e que o acesso às funções de hipervisor que possam afetar esses controles seja rigorosamente controlado e monitorado.

Assim como o isolamento de processos e recursos compartilhados, o armazenamento virtual dos dados do titular do cartão é uma consideração fundamental e, muitas vezes, é ignorado quando se trata de segmentação de componentes virtuais. Dependendo da configuração e dos controles específicos implementados, um SAN inteiro pode estar potencialmente no escopo, a menos que seja verificado que todos os sistemas e armazenamentos de dados dentro do escopo estejam isolados de todos os aqueles fora do escopo.

4.3 Recomendações para ambientes de computação em nuvem

A computação em nuvem oferece uma ampla gama de ofertas de serviços e modelos de implantação que englobam muitas tecnologias, produtos e serviços diferentes. Os ambientes de nuvem podem ser implantados em uma infraestrutura privada, pública ou em um híbrido de ambas, conforme descrito abaixo.

Nuvem privada

Uma nuvem privada consiste apenas de componentes do sistema que são confiáveis e controlados pela entidade. Os sistemas confiáveis podem estar localizados em várias instalações que são de propriedade da entidade ou de terceiros. Da mesma forma, os sistemas e componentes podem ser propriedade da entidade, ou podem ser de propriedade de um provedor de serviços e provisionados para uso dedicado por um único cliente.

Independentemente da propriedade, os sistemas em nuvem privada são dedicados a uma única entidade e os recursos de computação não são compartilhados com nenhum outro cliente ou locatário.

Nuvem pública

Uma nuvem pública consiste de componentes do sistema que não são de propriedade da organização ou sobre os quais ela não tem qualquer controle. Em uma nuvem pública, parte dos sistemas e infraestrutura básicos é sempre controlada pelo prestador de serviços em nuvem. Os componentes específicos que permanecem sob o controle do provedor de nuvem variam de acordo com o tipo de serviço — por exemplo, Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Software como Serviço (SaaS). Os serviços de nuvem pública são normalmente entregues por um conjunto ou cluster de sistemas para fornecer acesso baseado em serviços a vários clientes, ou locatários, aos recursos de computação compartilhados. A separação física entre os locatários não é prática em um ambiente de nuvem pública porque, por sua própria natureza, todos os recursos são compartilhados por todos.

Nuvem híbrida

Como sugerido pelo nome, uma nuvem híbrida é uma combinação de infraestruturas de nuvem privada e pública. Uma nuvem híbrida é tipicamente criada quando uma entidade interconecta sua nuvem privada a uma nuvem pública ou à nuvem privada de outra entidade. Em uma nuvem híbrida, a propriedade e o controle de dados e componentes do sistema podem ser divididos entre três ou mais entidades separadas, adicionando complexidade à tarefa de identificar limites de escopo e definir responsabilidades.

A computação em nuvem também engloba vários tipos de serviços, entre eles IaaS, PaaS e SaaS. Cada tipo de serviço representa uma atribuição diferente de gerenciamento de recursos e propriedade, que variará dependendo da oferta de serviço específica.

Por exemplo, uma entidade que se inscreve para um serviço IaaS pode reter o controle completo e, portanto, ser responsável pela segurança contínua e pela manutenção de todos os sistemas operacionais, aplicativos, configurações virtuais, incluindo o hipervisor e dispositivos de segurança virtual, e dados. Nesse cenário, o provedor de nuvem só seria responsável por manter a rede física básica e o hardware de computação. Em um cenário alternativo, uma oferta de serviço SaaS pode abranger o gerenciamento de todo hardware e software, incluindo componentes virtuais e configurações de hipervisor. Nesse cenário, a entidade só pode ser responsável por proteger seus dados, e todos os outros requisitos de segurança seriam implementados e gerenciados pelo prestador de serviços.

O diagrama a seguir fornece um exemplo de como o escopo e a responsabilidade de uma entidade podem variar em diferentes tipos de ofertas de serviços em nuvem.

Exemplo de como o escopo e a responsabilidade podem diferir* por tipo de serviço em nuvem:

Responsabilidade do cliente em nuvem			
Responsabilidade do prestador de serviços em nuvem			
<u>Área de responsabilidade</u>	<u>Tipo de serviço em nuvem</u>		
	IAAS	PAAS	SAAS
Dados			
Software, aplicativos de usuário			
Sistemas operacionais, bancos de dados			
Infraestrutura virtual (hipervisor, dispositivos virtuais, VMs, redes virtuais, etc.)			
Hardware de computador e rede (processador, memória, armazenamento, cabeamento, etc.)			
Datacenter (instalação física)			

* **Observação:** Esse é apenas um exemplo. As ofertas de serviços em nuvem devem ser analisadas individualmente para determinar como as responsabilidades entre o provedor de nuvem e o cliente em nuvem são atribuídas.

Em um ambiente de nuvem pública, os serviços e recursos de computação fornecidos pelo provedor de nuvem são normalmente compartilhados entre várias entidades ou locatários. Isso se contrasta aos ambientes de hospedagem tradicionais, onde recursos dedicados são geralmente provisionados para cada entidade ou locatário hospedado. Diferentemente dos ambientes de hospedagem tradicionais, onde o isolamento físico entre os locatários é geralmente aplicado, a separação física entre os locatários em um ambiente de nuvem não é prática porque, como mencionado anteriormente, todos os recursos são compartilhados por todos.

Além dos desafios de definição de escopo e atribuição de responsabilidades em uma infraestrutura compartilhada, as características inerentes de muitos ambientes de nuvem apresentam barreiras adicionais para alcançar a conformidade com o PCI DSS. Algumas dessas características incluem:

- As arquiteturas distribuídas de ambientes em nuvem adicionam camadas de tecnologia e complexidade ao ambiente.
- Os ambientes de nuvem pública são projetados para serem voltados para o público, para permitir acesso ao ambiente em qualquer lugar da Internet.
- A infraestrutura é por natureza dinâmica, e os limites entre ambientes de locatários podem ser fluidos.
- A entidade hospedada tem uma visibilidade limitada ou nenhuma visibilidade da infraestrutura básica e dos controles de segurança relacionados.
- A entidade hospedada tem pouca ou nenhuma supervisão ou controle sobre o armazenamento de dados do titular do cartão.
- A entidade hospedada não conhece com quem está compartilhando recursos, nem sabe dos possíveis riscos que seus vizinhos hospedados podem estar introduzindo no sistema host, armazenamentos de dados ou outros recursos compartilhados em um ambiente de vários clientes.

Em um ambiente de nuvem pública, controles adicionais devem ser implementados para compensar os riscos inerentes e a falta de visibilidade na arquitetura de nuvem pública. Um ambiente de nuvem pública poderia, por exemplo, hospedar cargas de trabalho fora do escopo hostis na mesma infraestrutura de virtualização que um ambiente de dados do titular do cartão. Controles preventivos, investigativos e corretivos mais rigorosos são necessários para compensar o risco adicional que uma nuvem pública, ou ambiente semelhante, poderia representar para o CDE de uma entidade.

Esses desafios podem tornar impossível para alguns serviços baseados em nuvem operar em conformidade com o PCI DSS. Consequentemente, o ônus para comprovar a conformidade do PCI DSS para um serviço baseado em nuvem recai fortemente sobre o provedor de nuvem, e tal prova deve ser aceita apenas com base em evidências rigorosas de controles adequados.

Assim como com todos os serviços hospedados no escopo do PCI DSS, a entidade hospedada deve solicitar garantia suficiente de seu provedor de nuvem de que o escopo da revisão do PCI DSS do provedor é suficiente e que todos os controles relevantes para o ambiente da entidade hospedada foram avaliados e determinados como compatíveis com o PCI DSS. O provedor de nuvem deve estar preparado para fornecer aos seus clientes hospedados evidências que indiquem claramente o que foi incluído no escopo de sua avaliação PCI DSS, bem como o que não estava no escopo; detalhes dos controles que não foram cobertos e que são, portanto, de responsabilidade de o cliente cobrir em sua própria avaliação PCI DSS; detalhes de quais requisitos do PCI DSS foram revisados e considerados como "em vigor" e "não em vigor" e confirmação de quando a avaliação foi realizada.

Quaisquer aspectos do serviço baseado em nuvem, não cobertos pela revisão do PCI DSS do provedor de nuvem, devem ser identificados e documentados em um acordo por escrito. A entidade hospedada deve estar totalmente ciente de todos e quaisquer aspectos do serviço em nuvem, incluindo componentes específicos do sistema e controles de segurança que não são cobertos pelo provedor, sendo, portanto, de responsabilidade da entidade gerenciá-los e avaliá-los.

4.4 Orientação para avaliar riscos em ambientes virtuais

Devido à falta de padronização entre as tecnologias de virtualização e a ampla variedade de possíveis implementações, as organizações que usam a virtualização precisam avaliar seu ambiente específico, os riscos associados e identificar controles adequados para abordar esse risco.

Há várias metodologias e ferramentas de avaliação de risco aceitas pelo setor disponíveis para ajudar a orientar o processo de avaliação de risco. Qualquer que seja o processo utilizado, ele deve incluir a identificação de ameaças e vulnerabilidades e resultar em um entendimento claro do risco avaliado para o ambiente.

Alguns dos elementos-chave a serem considerados ao realizar uma avaliação de risco de ambientes virtuais são fornecidos abaixo.

4.4.1 Definir o ambiente

Antes que ameaças e vulnerabilidades possam ser identificadas e avaliadas, primeiramente uma entidade deve entender seu ambiente, bem como as pessoas, processos e tecnologias que compreendem ou interagem com ele. Ao definir o ambiente a ser avaliado, as entidades devem considerar todos os aspectos que tenham um possível impacto de risco, independentemente de serem considerados no escopo ou fora do escopo para o PCI DSS.

Definir o ambiente virtual deve incluir, no mínimo, as seguintes atividades:

- Identificação de todos os componentes, incluindo hipervisores, cargas de trabalho, hosts, redes, consoles de gerenciamento e outros componentes;
- Detalhes físicos do local para cada componente;
- Descrição das funções primárias e dos responsáveis designados para cada componente;
- Detalhes da visibilidade dentro e entre os componentes;
- Identificação de fluxos de tráfego entre componentes diferentes, entre componentes e hipervisores, e entre componentes e sistemas host básicos ou recursos de hardware;
- Identificação de todas as comunicações e fluxos de dados trocados entre os hosts, bem como aqueles trocados entre os componentes virtuais e outros componentes do sistema.
- Identificação de todos os canais de comunicação fora da banda, configurados para operar ou não, que poderiam permitir comunicações entre componentes;
- Detalhes de todas as interfaces de gerenciamento e mecanismos de acesso de hipervisor, incluindo funções e permissões definidas;
- Todos os componentes de hardware virtual e físico, como unidades de disco removíveis e portas USB, paralelas e seriais.
- Detalhes do número e tipos de componentes virtuais em cada host, tipos de segmentação entre componentes e hosts, funções e níveis de segurança de todos os componentes virtualizados, etc.

4.4.2 Identificar ameaças

Este processo inclui a identificação de ameaças atuais e potenciais que, se bem-sucedidas ou permitidas, podem resultar em perda de confidencialidade, integridade ou disponibilidade do ambiente. As considerações sobre ameaças devem incluir todos os cenários, ações ou eventos que possam resultar em evasão deliberada ou não intencional dos controles de segurança.

Ambientes virtualizados normalmente estão sujeitos aos mesmos tipos de ameaças que os ambientes tradicionais. No entanto, a virtualização em si pode fornecer uma camada adicional para possíveis ameaças ao alvo. Um exemplo de possíveis ameaças específicas às tecnologias de virtualização pode incluir novos tipos de código malicioso ou ataques lógicos especificamente direcionados a componentes virtuais exclusivos, como o hipervisor, ou canais de comunicação fora de banda desprotegidos entre componentes de hardware compartilhados.

Ter um entendimento detalhado da função principal e do proprietário de cada componente no ambiente ajudará a identificar o impacto potencial de um ataque bem-sucedido ou outro evento de ameaça.

4.4.3 Identificar vulnerabilidades

Assim como as vulnerabilidades técnicas tradicionais a serem identificadas (por exemplo, dentro de sistemas operacionais, aplicativos, etc.), as entidades também precisam identificar vulnerabilidades específicas para as tecnologias e configurações de virtualização implementadas em seu ambiente. Vulnerabilidades adicionais podem resultar da maior complexidade introduzida por camadas de virtualização, a natureza dinâmica e compartilhada dos ambientes virtuais e a potencial falta de visibilidade da arquitetura básica.

Vulnerabilidades não estão limitadas a problemas técnicos. Falhas em processos operacionais, treinamento inadequado de pessoal, falta de monitoramento de controle e lacunas na segurança física são exemplos de áreas adicionais onde possíveis vulnerabilidades podem existir e ser exploradas.

4.4.4 Avaliar e abordar o risco

A avaliação de risco deve identificar se quaisquer controles adicionais são necessários para proteger dados do portador do cartão e outras informações confidenciais em um ambiente virtualizado. Deve-se observar que a implementação de controles especializados pode ser necessária *além dos* requisitos do PCI DSS para atenuar possíveis problemas de segurança associados ao uso de tecnologias de virtualização.

5 Conclusão

Não há um método único para proteger sistemas virtualizados. As tecnologias virtuais têm muitas aplicações e usos, e os controles de segurança apropriados para uma implementação podem não ser adequados para outra. Assim como as funções visíveis de uma implementação virtual, há serviços funcionais e de comunicação básicos inseridos na arquitetura da virtualização, que podem fornecer vetores de ataque desconhecidos se não forem compreendidos e gerenciados adequadamente.

Como ocorre com muitas tecnologias em evolução, a falta de padrões do setor de virtualização resultou em uma série de melhores práticas específicas do fornecedor e recomendações que podem ou não ser aplicáveis a um ambiente específico. As entidades precisam entender e avaliar seus próprios ambientes para identificar os riscos exclusivos que a virtualização traz, bem como as implicações potenciais para a segurança do ambiente de dados do portador do cartão.

Em um ambiente virtual, cada componente individual precisa ser protegido, pois a insegurança de uma VM ou componente em um sistema host pode levar ao comprometimento de outras VMs no mesmo host. Projetar todos os componentes de virtualização, mesmo aqueles considerados fora do escopo, para atender aos requisitos de segurança do PCI DSS não apenas fornecerá uma base segura para o ambiente virtual como um todo, mas também reduzirá a complexidade e o risco associados ao gerenciamento de vários perfis de segurança e a sobrecarga e o esforço necessários para manter e validar a conformidade dos componentes no escopo. Por esse motivo, se qualquer componente executado em um hipervisor ou host específico estiver no escopo do PCI DSS, recomenda-se que todos os componentes nesse hipervisor ou host também sejam considerados no escopo.

6 Agradecimentos

O PCI SSC gostaria de agradecer a contribuição do Grupo de Interesse Especial de Virtualização (SIG) na preparação deste documento. O SIG de virtualização consiste em representantes das seguintes organizações:

Alliance Data	LL Bean
Altor Networks	Microsoft
Assurant	Net SPI
AT&T	Protiviti
Bank of America	Quicktrip
Capita Group PLC	Red Island
Cisco	Reliant Security
Citrix	Savvis
Coalfire Systems	SecureState
ConfigureSoft	Southwest Airlines
DRG	Speedway
Dufry/Hudson News	Stanford University
Firehost	SystemExperts
HP	The Members Group
HyTrust	Trend Micro
IGX Global	Verizon Business
VMware	

Sobre o PCI Security Standards Council

A missão do PCI Security Standards Council é aprimorar a segurança das contas de pagamento estimulando a educação e a conscientização do Padrão de Segurança de Dados PCI e de outros padrões que aumentem a segurança dos dados de pagamento.

O PCI Security Standards Council foi formado pelas principais empresas de cartão de crédito, American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc. para proporcionar um fórum transparente no qual todos os interessados possam participar do contínuo desenvolvimento, aprimoramento e disseminação do Padrão de Segurança de Dados PCI (DSS), Requisitos de segurança de transação PIN (PTS) e o Padrão de Segurança de Dados de Aplicativos de Pagamento (PA-DSS). O comércio, bancos, financeiras e pontos de venda de varejo são estimulados a associar-se como Organizações Participantes.

7 Anexo – Considerações de virtualização para PCI DSS

Quando uma virtualização for implantada, todos os componentes que estiverem no ambiente virtual deverão ser identificados e considerados dentro do escopo para a revisão de PCI DSS, incluindo os hosts individuais virtuais ou dispositivos, máquinas visitantes, aplicativos, interfaces de gerenciamento, consoles de gerenciamento centrais, hipervisores, etc. Todas as comunicações entre hosts e fluxos de dados precisam ser identificadas e documentadas, bem como aquelas entre o componente virtual e outros componentes do sistema.

A implantação de um ambiente virtualizado deverá atender às intenções de todos os requerimentos de PCI DSS de forma que os sistemas virtualizados possam de fato ser considerados hardwares separados. Por exemplo: deverá haver uma segmentação clara das funções e segregação de redes com níveis de segurança diferentes. A segmentação deverá evitar o compartilhamento dos ambientes de produção e de teste e desenvolvimento. A configuração virtual deverá ser protegida de forma que as vulnerabilidades em uma função não interfiram na segurança de outras. E dispositivos como USB ou em série não possam ser acessados por todas as instâncias virtuais.

Além disso, todos os protocolos de interface de gerenciamento virtuais deverão ser incluídos na documentação do sistema, e deverão ser definidas funções e permissões para gerenciamento das redes virtuais e dos componentes virtuais do sistema. As plataformas de virtualização deverão ter a capacidade de aplicar a separação de tarefas e de privilégios menores, de forma a separar o gerenciamento de rede virtual do gerenciamento de servidor virtual. Deve-se ter atenção especial ao implantar os controles de autenticação, de forma a garantir que a autenticação dos usuários seja realizada nos componentes de sistema virtual adequados e que haja distinção entre as máquinas virtuais (VMs - virtual machines) do visitante e o hipervisor.

A seção a seguir identifica algumas das características de virtualização descritas anteriormente neste documento e apresenta orientação sobre como essas características podem ser particularmente relevantes para algumas áreas de controle do PCI DSS. Recomendações adicionais e melhores práticas também estão incluídas para consideração.

Observação: Este anexo destina-se apenas à orientação. Implementações e configurações virtuais precisarão ser avaliadas individualmente para cada ambiente específico para determinar o impacto dessas considerações para os requisitos do PCI DSS.

Também é importante lembrar que **TODOS os requisitos aplicáveis do PCI DSS devem ser avaliados**. A orientação a seguir identifica apenas algumas das áreas potenciais para consideração quando a virtualização é usada.

As Considerações de virtualização neste anexo não substituem, sobrepõem nem ampliam os requisitos do PCI DSS. Todas as melhores práticas e recomendações aqui contidas são fornecidas apenas como orientação.

A tabela a seguir é dividida em duas colunas primárias:

- **Requisitos do PCI DSS (resumidos e abreviados):** Essas colunas contêm extratos resumidos de requisitos do PCI DSS. Observe que o conteúdo completo dos requisitos não é fornecido aqui — consulte *Requisitos do PCI DSS e Procedimentos de Avaliação de Segurança* para todos os requisitos do PCI DSS e procedimentos de teste.
- **Considerações sobre virtualização:** esta coluna identifica as características das tecnologias de virtualização que podem exigir consideração adicional para os requisitos do PCI DSS.

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 1: Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão	1.1 Defina os padrões de configuração do firewall e do roteador.	<ul style="list-style-type: none"> • Devido à complexidade dos ambientes virtuais, pode ser necessário examinar várias camadas virtuais para garantir que todos os componentes e fluxos de dados sejam identificados. Por exemplo: <ul style="list-style-type: none"> ○ Firewalls e roteadores virtuais podem ser incorporados dentro do hipervisor ou podem ser implementados como dispositivos de rede virtual ou dispositivos virtuais. ○ Da mesma forma, as conexões de rede virtual podem existir dentro de um host, entre hosts e entre um host e a rede física. ○ O tráfego de entrada e saída de/para o CDE pode incluir interações VM-para-VM que nunca atravessam a rede física. ○ Os caminhos de acesso entre sistemas virtuais e redes podem existir em vários níveis da infraestrutura virtual — por exemplo, entre hosts, dispositivos ou hipervisores. • Soluções especializadas podem ser necessárias para monitorar e restringir o tráfego de rede entre sistemas virtuais e redes, incluindo redes virtuais sem fio. <ul style="list-style-type: none"> ○ Alterações na configuração de rede virtual podem ter impacto significativo — por exemplo, um componente virtual localizado em uma rede de escopo ou zona de alta segurança poderia ser inadvertidamente reconfigurado ou movido para uma rede fora do escopo ou zona de baixa segurança. • A atribuição de funções e responsabilidades pode ser mais complexa em ambientes virtuais. Por exemplo, uma conta de administrador de hipervisor poderia, inadvertidamente, incluir privilégios para administrar redes virtuais. • Os limites entre redes confiáveis e não confiáveis podem ser dinâmicos e difíceis de definir em uma infraestrutura baseada em nuvem ou infraestrutura de host compartilhada virtual.
	1.2 Elabore configurações de firewall e roteador que restrinjam as conexões entre redes não confiáveis e componentes do sistema no CDE. Observação: Uma “rede não confiável” é qualquer rede que seja externa às redes pertencentes à entidade e/ou que a entidade seja incapaz de controlar ou gerenciar.	
	1.3 Proíba o acesso público direto entre a Internet e qualquer componente do sistema no CDE.	

(continua na próxima página)

Requisitos do PCI DSS (resumidos e abreviados)	Considerações sobre virtualização
<p>1.4 Instale o software de firewall pessoal em quaisquer computadores móveis e/ou de propriedade do funcionário com conectividade direta à Internet, que são usados para acessar a rede da empresa.</p>	<ul style="list-style-type: none"> O uso de desktops virtuais remotos pode ampliar inadvertidamente os limites do CDE. <p>Melhores práticas/recomendações adicionais:</p> <ul style="list-style-type: none"> Não coloque sistemas ou redes não confiáveis no mesmo host ou hipervisor que os sistemas no CDE. Implemente a segmentação de rede física para isolar qualquer sistema que hospede sistemas e redes de contato público ou não confiáveis de sistemas que hospedem componentes virtuais inseridos ou conectados ao CDE.
<p>Requisito 2: Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança.</p> <p>2.1 Sempre altere os valores padrão entregues pelo fornecedor antes de instalar um sistema na rede.</p> <p>2.2 Desenvolva padrões de configuração para todos os componentes do sistema. Certifique-se de que esses padrões abrangem todas as vulnerabilidades de segurança conhecidas e estão em conformidade com os padrões de fortalecimento do sistema aceitos pelo setor.</p> <p>2.3 Criptografe todo o acesso administrativo que não utiliza console durante a criptografia forte.</p> <p>2.4 Os provedores de hospedagem compartilhada devem proteger cada ambiente hospedado da entidade e os dados do titular do cartão. Esses provedores devem atender a requisitos específicos, conforme detalhado no <i>Apêndice A: Requisitos adicionais do PCI DSS para provedores de hospedagem compartilhada</i>.</p>	<ul style="list-style-type: none"> Padrões de fortalecimento do sistema aceitos pelo setor talvez não existam para todas as tecnologias virtuais implementadas. Um componente virtual que exige maior segurança poderia ser exposto involuntariamente a risco adicional se hospedado no mesmo sistema ou hipervisor que um componente virtual de menor segurança. Métodos para proteger serviços, protocolos ou daemons não seguros podem ser necessários em várias camadas virtuais. Parâmetros e configurações de segurança podem ser exclusivos de uma determinada tecnologia virtual ou implementação. Pode ser necessário um treinamento especializado para garantir que os administradores do sistema e pessoal de segurança tenham conhecimento de segurança para tecnologias virtuais. O acesso administrativo sem console pode existir em vários níveis da arquitetura virtual, por exemplo: acesso a hipervisores, interfaces de gerenciamento e consoles de host, bem como para VMs individuais, dispositivos e outros componentes hospedados. A separação adequada entre os locatários talvez não seja possível em um ambiente virtual de hospedagem compartilhada ou em um ambiente de nuvem pública. <p>Melhores práticas/recomendações adicionais:</p> <ul style="list-style-type: none"> Não coloque componentes virtuais de alta segurança e componentes virtuais de baixa segurança no mesmo host ou hipervisor.

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 3: Proteger os dados armazenados do portador do cartão	3.1 Mantenha a armazenagem dos dados do titular do cartão no mínimo possível, implemente políticas, processos e procedimentos de retenção e descarte de dados.	<ul style="list-style-type: none"> Além de estar presente em locais conhecidos, os dados do titular do cartão podem existir em imagens de VM arquivadas, offline ou inativas, ou não devem ser migradas de forma inconsciente entre sistemas virtuais por meio de mecanismos dinâmicos, como migração ao vivo ou ferramentas de migração de armazenamento. Dados sensíveis, como PAN não criptografado, dados de autenticação confidenciais e chaves criptográficas, podem ser capturados inadvertidamente em memória ativa e replicados por meio de funções de imagem e instantâneo de VM. A criptografia em disco pode ser implementada em várias camadas virtuais, por exemplo, no host básico, na imagem de VM ou em uma unidade de rede separada acessível pelo host básico, hipervisor ou imagem de VM. O uso da criptografia de disco pode estar sujeito a problemas de implementação específicos relacionados à virtualização, o que poderia tornar a criptografia ineficaz. Por exemplo, mover ou migrar imagens de VM criptografadas contendo dados do portador do cartão para outro host, imagem de VM ou mídia removível pode anular a eficácia do mecanismo de criptografia. Separar o acesso lógico a sistemas de arquivos criptografados de contas em todas as camadas virtuais (incluindo o sistema host, VMs individuais, contas de hipervisor, etc.) cria níveis adicionais de complexidade. Contas ou processos privilegiados executados no host ou hipervisor podem inadvertidamente receber acesso a chaves criptográficas de dentro de um componente hospedado. Se as chaves criptográficas forem armazenadas ou hospedadas no mesmo hipervisor ou host que os dados criptografados com essas chaves, qualquer pessoa com acesso ao hipervisor ou host poderia potencialmente descriptografar os dados, tornando-os desprotegidos. Ferramentas e processos especializados podem ser necessários para localizar e gerenciar chaves criptográficas armazenadas em imagens arquivadas, offline ou reposicionadas. <p>Melhores práticas/recomendações adicionais:</p> <ul style="list-style-type: none"> Não virtualize os recursos críticos usados na geração de chaves criptográficas (por exemplo, módulos FIPS físicos). Se as funções de gerenciamento de chaves forem virtualizadas, não abrigue componentes virtuais que executam funções de gerenciamento de chaves nem armazene chaves criptográficas no mesmo hipervisor ou host que os componentes virtuais que armazenam ou acessam dados protegidos por essas chaves.
	3.2 Não armazene dados de autenticação confidenciais após a autorização (mesmo se estiverem criptografados).	
	3.3 Mascare o PAN quando exibido	
	3.4 Torne o PAN ilegível em qualquer local onde ele esteja armazenado (inclusive em mídia digital portátil, mídia de backup e em registros) utilizando qualquer uma das seguintes abordagens: <ul style="list-style-type: none"> Hashes unidirecionais com base em criptografia forte (um hash deve ser do PAN inteiro) Truncamento (a codificação hash não pode ser usada para substituir o segmento truncado do PAN) Tokens e blocos de índice (os blocos devem ser armazenados de forma segura) Criptografia robusta com processos e procedimentos de gerenciamento de chaves associados 	
	3.5 Proteção das chaves de criptografia utilizadas para criptografia de dados do titular do cartão em relação a divulgações ou mau uso.	
	3.6 Documente e implemente totalmente todos os processos e procedimentos de gerenciamento das chaves criptográficas.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 4: Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas	4.1 Use protocolos de segurança e criptografia robusta para proteger dados sensíveis do titular do cartão em redes abertas e públicas.	<ul style="list-style-type: none"> Ferramentas especializadas podem ser necessárias para proteger dados confidenciais que viajam por redes virtuais da exposição não intencional.
	4.2 Nunca envie PANs desprotegidos por tecnologias de mensagens do usuário final.	
Requisito 5: Usar e atualizar regularmente o software ou programas antivírus	5.1 Implemente os softwares antivírus em todos os sistemas normalmente afetados por softwares mal-intencionados.	<ul style="list-style-type: none"> Vários produtos antivírus podem ser necessários para proteger os sistemas operacionais convidados bem como o sistema operacional host básico (por exemplo, Windows e Linux rodando no mesmo host). Mecanismos antivírus tradicionais podem interferir em certas funções de virtualização. Mecanismos antivírus tradicionais talvez não forneçam proteção adequada para todas as camadas de virtualização.
	5.2 Certifique-se de que todos os mecanismos antivírus estejam atualizados, funcionem ativamente e possam gerar registros de auditoria.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 6: Desenvolver e manter sistemas e aplicativos seguros	6.1 Certifique-se de que todos os componentes do sistema e softwares estão protegidos de vulnerabilidades conhecidas pois têm os patches de segurança mais recentes disponibilizados pelos fornecedores instalados.	<ul style="list-style-type: none"> Ferramentas especializadas podem ser necessárias para implantar e verificar patches para componentes virtualizados. A correção de um único host pode exigir a coordenação de várias programações de patch para abordar vulnerabilidades em todas as camadas, incluindo o sistema host, todos os sistemas operacionais hospedados e aplicativos, e todas as tecnologias específicas de virtualização, por exemplo, o hipervisor e o console de gerenciamento. Programações adicionais de gerenciamento de patches podem ser necessárias para imagens de máquina virtual inativa ou offline para garantir que também estejam protegidas contra vulnerabilidades conhecidas. A separação de funções e controles de acesso podem precisar ser aplicados em vários níveis, por exemplo, no hipervisor, componente individual e nível de host. Os sistemas de desenvolvimento/teste e os dados podem ser inadvertidamente movidos para ambientes de produção, ou vice-versa, através de mecanismos de replicação virtual, imagem ou instantâneo. O teste de alterações em componentes virtualizados talvez precise considerar vários níveis de impacto potencial. <p>Melhores práticas/recomendações adicionais:</p> <ul style="list-style-type: none"> Não coloque sistemas de desenvolvimento/teste ou redes no mesmo host ou hipervisor que sistemas de produção ou redes.
	6.2 Estabeleça um processo para identificar e designar um ranking de risco para as vulnerabilidades de segurança recém-descobertas.	
	6.3 Desenvolva aplicativos de software de acordo com o PCI DSS e com base nas melhores práticas do setor.	
	6.4 Siga os procedimentos de controle de alterações para todas as alterações nos componentes do sistema.	
	6.5 Desenvolva aplicativos baseados nas diretrizes de código seguro. Previna vulnerabilidades de codificação comuns nos processos de desenvolvimento.	
	6.6 Para aplicativos web voltados para o público, aborde novas ameaças e vulnerabilidades continuamente.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 7: Restringir o acesso aos dados do titular do cartão de acordo com a necessidade de conhecimento para o negócio	7.1 Limite o acesso aos componentes do sistema e aos dados do titular do cartão àquelas pessoas cuja função requer tal acesso.	<ul style="list-style-type: none"> Controles de acesso baseados na necessidade de saber e menos privilégios podem precisar ser implementados em várias camadas para serem eficazes (por exemplo, no hipervisor, host, interface de gerenciamento e camada de console, bem como para componentes virtuais individuais, dispositivos e armazenamento de dados). Nem todas as tecnologias de virtualização são capazes de separar o acesso administrativo ao host ou hipervisor do acesso administrativo em componentes virtuais individuais hospedados. Isso pode resultar na atribuição não autorizada ou desnecessária de acesso privilegiado dentro dos componentes hospedados. O uso de ferramentas ou soluções especializadas pode, portanto, ser necessário para garantir a atribuição efetiva e granular de privilégios em todas as camadas virtualizadas.
	7.2 Estabeleça um sistema de controle de acesso que restrinja o acesso com base na necessidade de conhecimento do usuário e que esteja configurado para "recusar todos", a menos que permitido de forma específica.	
Requisito 8: Atribuir uma identidade exclusiva para cada pessoa que tenha acesso ao computador	8.1 Atribua a todos os usuários um ID exclusivo antes de permitir que eles acessem os componentes do sistema ou os dados do titular do cartão.	<ul style="list-style-type: none"> Identificações exclusivas e autenticação segura podem ser necessárias em várias camadas virtuais, bem como para quaisquer tecnologias intermediárias usadas para acessar componentes virtualizados. Devido ao possível impacto do acesso não autorizado ao hipervisor, podem ser necessários controles de autenticação adicionais — por exemplo, restringindo todo o acesso remoto ao hipervisor para sistemas de fonte definidos, interfaces de gerenciamento e consoles. Componentes virtuais inativos ou offline também podem conter dados do titular do cartão e também podem exigir controles de acesso fortes. Imagens virtuais e instantâneos podem inadvertidamente capturar senhas na memória ativa, resultando em armazenamento não intencional e não protegido dos dados. Soluções especializadas podem ser necessárias para garantir que a autenticação do usuário seja aplicada no nível apropriado, distinguindo entre autenticação para componentes virtuais individuais, armazenamento de dados, hipervisores e sistemas de gerenciamento.
	8.2 Além de atribuir um ID exclusivo, empregue no mínimo um dos seguintes: <ul style="list-style-type: none"> - Algo que você conhece - Algo que você possui - Algo que você é 	
	8.3 Incorpore a autenticação de dois fatores para acesso remoto à rede.	
	8.4 Converta todas as senhas em ilegíveis durante a transmissão e armazenamento em todos os componentes do sistema usando criptografia robusta.	
	8.5 Garanta um controle adequado da autenticação e da senha do usuário em todos os componentes do sistema.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 9: Restringir o acesso físico aos dados do portador do cartão	9.1 Use controles de entrada de instalações para limitar e monitorar o acesso físico aos sistemas no CDE.	<ul style="list-style-type: none"> Fornecer acesso físico a um único host ou hipervisor concede, explicitamente, o equivalente ao acesso físico a todas as máquinas virtuais e componentes executados nesse host/hipervisor e o possível acesso a outros sistemas físicos conectados. Devido ao possível impacto do acesso físico não autorizado, a autenticação adicional e o monitoramento do acesso físico podem ser necessários, por exemplo, exigindo autenticação de fator duplo e uma escolta supervisionada para todo o acesso físico ao datacenter. Além de serem armazenados em locais conhecidos, os dados do titular do cartão também podem existir em mídia contendo backups de componentes virtuais, ou em mídia contendo instantâneos, imagens de VM arquivadas, offline ou inativas.
	9.2 Desenvolva procedimentos para diferenciar facilmente a equipe interna dos visitantes.	
	9.3 Certifique-se de que todos os visitantes estejam autorizados.	
	9.4 Mantenha um registro de visitantes.	
	9.5 Armazene backups de mídia em um local seguro.	
	9.6 Proteja toda a mídia fisicamente.	
	9.7 Mantenha um controle rigoroso quanto à distribuição interna ou externa de mídia.	
	9.8 Certifique-se de que o gerenciamento aprova quaisquer e todas as mídias que são movidas de uma área segura.	
	9.9 Mantenha um controle rigoroso sobre o armazenamento e a acessibilidade das mídias que contêm dados do titular do cartão.	
	9.10 Destrua as mídias que contêm dados do titular do cartão quando eles não forem mais necessários por motivos comerciais ou legais.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 10: Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão	10.1 Estabeleça um processo para vincular todo o acesso aos componentes do sistema.	<ul style="list-style-type: none"> O registro de atividades exclusivas de ambientes virtualizados pode ser necessário para reconstruir os eventos exigidos pelo Requisito 10.2 do PCI DSS. Por exemplo, registros de APIs especializadas que são usados para visualizar o processo virtual, memória ou armazenamento offline podem ser necessários para identificar o acesso individual aos dados do titular do cartão. As funções e objetos específicos do sistema a serem registrados podem diferir de acordo com a tecnologia de virtualização específica em uso. As trilhas de auditoria contidas em máquinas virtuais geralmente são acessíveis para qualquer pessoa com acesso à imagem da máquina virtual. Ferramentas especializadas podem ser necessárias para correlacionar e revisar dados de registro de auditoria de dentro de componentes e redes virtualizados. Pode ser difícil capturar, correlacionar ou revisar registros de um ambiente virtual compartilhado ou ambiente baseado em nuvem. <p>Melhores práticas/recomendações adicionais:</p> <ul style="list-style-type: none"> Não coloque registros de auditoria no mesmo host ou hipervisor que os componentes que geram esses registros.
	10.2 Implemente trilhas de auditoria automatizadas para todos os componentes do sistema.	
	10.3 Registre entradas de trilhas de auditoria para todos os componentes do sistema para cada evento.	
	10.4 Sincronize todos os relógios e horários do sistema crítico.	
	10.5 Proteja as trilhas de auditoria para que não possam ser alteradas.	
	10.6 Analise os registros de todos os componentes do sistema pelo menos diariamente.	
	10.7 Mantenha um histórico de trilha de auditoria por pelo menos um ano, com disponibilidade imediata por um mínimo de três meses.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 11: Testar regularmente os sistemas e processos de segurança	11.1 Teste a presença de pontos de acesso sem fio e detecte pontos de acesso sem fio não autorizados no mínimo trimestralmente.	<ul style="list-style-type: none"> As varreduras de rede e as atividades de teste podem ser necessárias em várias camadas virtuais para garantir a cobertura de todos os componentes no escopo, incluindo todos os endpoints virtuais, hosts, interfaces de hipervisor e consoles de gerenciamento. Varreduras de vulnerabilidade adicionais podem ser necessárias para imagens de máquina virtual inativa ou offline para garantir que também estejam protegidas contra vulnerabilidades conhecidas. Vulnerabilidades específicas de virtualização podem não ser detectadas pelas ferramentas tradicionais de varredura de vulnerabilidades. Ferramentas especializadas podem ser necessárias para fazer a varredura e testar componentes virtuais e dispositivos de rede de dentro de sistemas e redes virtuais. O impacto das mudanças feitas dentro de uma infraestrutura virtualizada pode ser complexo e os cronogramas de varredura talvez precisem ser expandidos de forma correspondente. O treinamento especializado sobre as tecnologias de virtualização específicas em uso pode ser necessário para os recursos que realizam testes de penetração de ambientes virtualizados. Soluções IDS/IPS especializadas podem ser necessárias para monitorar o fluxo do tráfego em redes virtuais e/ou entre sistemas virtuais. Ferramentas especializadas podem ser necessárias para monitorar arquivos críticos em ambientes virtualizados. Controles para monitoramento de tráfego e arquivos críticos no CDE talvez tenham que abranger imagens de máquinas virtuais inativas e offline.
	11.2 Execute varreduras de vulnerabilidades de redes internas e externas pelo menos trimestralmente e após qualquer mudança significativa na rede.	
	11.3 Realize testes de penetração internos e externos pelo menos uma vez por ano e depois de qualquer modificação ou upgrade no aplicativo ou na infraestrutura.	
	11.4 Use sistemas de detecção de invasão e/ou sistemas de prevenção contra invasão para monitorar todo o tráfego no perímetro do CDE e nos pontos críticos dentro dele.	
	11.5 Implante ferramentas de monitoramento de integridade do arquivo para alertar os funcionários quanto à modificação não autorizada de arquivos críticos do sistema, arquivos de configuração ou arquivos de conteúdo.	

Requisitos do PCI DSS (resumidos e abreviados)		Considerações sobre virtualização
Requisito 12: Manter uma política que aborde a segurança das informações para todas as equipes	12.1 Defina, publique, mantenha e dissemine uma política de segurança.	<ul style="list-style-type: none"> Políticas de segurança específicas, políticas de uso e procedimentos de segurança operacional podem precisar ser expandidos para abordar aspectos únicos de ambientes virtuais (por exemplo, tecnologias implementadas, tipo de infraestrutura, modelos de implantação, etc.). O perfil de risco de um ambiente virtualizado será diferente daquele para um ambiente físico tradicional. Compreender e avaliar o risco pode exigir consideração de fatores adicionais exclusivos para um ambiente específico. Políticas de uso adicionais podem ser necessárias para identificar o uso adequado de tecnologias baseadas em virtualização. Pode ser necessário treinamento adicional do usuário para garantir a compreensão das implicações de segurança e o uso adequado das tecnologias virtualizadas. Detalhes que descrevem controles específicos e responsabilidades atribuídas talvez precisem ser incluídos em contratos por escrito com prestadores de serviços onde os dados do titular do cartão ou controles de segurança estão sob o controle do prestador de serviços terceirizado em um ambiente virtual. Pode ser necessário um treinamento especializado para o pessoal responsável pelo monitoramento e resposta a incidentes de segurança em ambientes virtualizados.
	12.2 Desenvolva os procedimentos de segurança operacional diariamente.	
	12.3 Desenvolva o uso de políticas de tecnologias críticas e defina o uso apropriado destas tecnologias.	
	12.4 Certifique-se de que a política e os procedimentos de segurança definem claramente as responsabilidades quanto à segurança da informação para todos os funcionários.	
	12.5 Atribua responsabilidades de gerenciamento de segurança da informação.	
	12.6 Implemente um programa formal de conscientização de segurança.	
	12.7 Verifique o pessoal em potencial.	
	12.8 Mantenha e implemente políticas e procedimentos para gerenciar prestadores de serviços.	
	12.9 Implemente um plano de resposta a incidentes.	
Requisito A.1: Provedores de hospedagem compartilhada devem proteger o CDE.	A.1 Proteja o ambiente hospedado e os dados de cada entidade.	<ul style="list-style-type: none"> A separação adequada entre os locatários talvez não seja possível em um ambiente virtual de hospedagem compartilhada ou em um ambiente de nuvem pública.