DOCUMENTAÇÃO TÉCNICA | DEZEMBRO DE 2015

Abordando a conformidade com PCI

por meio do gerenciamento de acesso com privilégios

ca technologies

Resumo executivo

Desafio

As organizações que lidam com transações envolvendo cartões de crédito ou débito estão enfrentando uma pressão cada vez maior para atender a requisitos de conformidade regulamentar. Especificamente, elas devem estar em conformidade com o PCI DSS (Payment Card Industry Data Security Standard - Padrão de segurança de dados do setor de cartões de pagamento) versão 3, que entrou em vigor em janeiro de 2015.[1] O PCI DSS v3 estabeleceu diversos requisitos para proteger os sistemas e redes relevantes de uma organização, que compõem o CDE (Cardholder Data Environment - Ambiente de dados de titulares de cartão). Com requisitos de autenticação forte e controle de acesso ao CDE, as organizações estão sendo desafiadas com as difíceis tarefas de implementar ferramentas ou práticas de autenticação multifatorial, controle de acesso e geração de relatórios de atividades, especificamente para acesso com privilégios ou administrativo a esses sistemas.

Oportunidade

Os requisitos do PCI DSS referentes ao gerenciamento de acesso com privilégios indicam os riscos associados ao uso indevido de contas com privilégios e o acesso que elas permitem a ativos de negócios importantes. Quase todos os incidentes de segurança recentes apontam os usuários ou credenciais com privilégios como o principal vetor de ataque quando ocorre uma violação bem-sucedida. Uma abordagem eficaz de gerenciamento de acesso com privilégios permite que as organizações restrinjam, criem um log e monitorem todas as atividades realizadas por contas com privilégios, como as de administradores de redes, sistemas e bancos de dados. Consequentemente, elas conseguem ter melhor controle e visibilidade sobre os usuários com privilégios e seu acesso de "superusuário" aos ativos valiosos da empresa. Sem isso, muitas organizações precisam se empenhar para atender aos requisitos de identificação, autenticação e controle de acesso do PCI DSS v3 e não conseguem minimizar a exposição aos riscos de violações e ataques.

Benefícios

Uma abordagem de defesa abrangente tendo em vista o gerenciamento de acesso com privilégios em uma solução fácil de implantar, como o CA Privileged Access Manager, pode ajudar as organizações a atender aos requisitos do PCI DSS v3 e a proteger melhor não somente os CDEs, mas também a TI híbrida da empresa, abrangendo redes, servidores e os ambientes virtuais e na nuvem. Desse modo, as organizações conseguem ter uma defesa melhor contra violações e diminuem os riscos de omissão ou não conformidade com o PCI DSS.

Seção 1:

A necessidade do gerenciamento de acesso com privilégios

A necessidade do gerenciamento de acesso com privilégios nunca foi tão grande. Estudos em série mostram falhas nos sistemas de proteção tradicionais. Alguns até mesmo sugerem que quase toda organização tem pelo menos uma concessão ativa em um determinado período.[2] A imprensa sempre divulga casos de violações de dados graves, como as que ocorreram na Target no final de 2013, na Home Depot em 2014 e no OPM (Office of Personnel Management) dos EUA em 2015, todos envolvendo o roubo de credenciais usadas por terceiros. De fato, o relatório de 2014 da Verizon sobre investigações de violações de dados citou o uso de credenciais roubadas como a principal ameaça contra as organizações.[3]

Muitas vezes, as organizações ignoram os perigos que as contas com privilégios oferecem e o número absoluto dessas contas que podem existir. As contas com privilégios não são usadas somente por funcionários de uma organização, mas também por terceiros, como fornecedores, prestadores de serviços e outros que dão suporte técnico para sistemas, dispositivos em rede e aplicativos. Uma única empresa pode ter milhares ou até mesmo milhões de contas com privilégios, e cada uma traz riscos de segurança para a organização.

A ideia por trás do gerenciamento de acesso com privilégios é conferir maior responsabilidade e visibilidade no que diz respeito às ações dos administradores. No modelo tradicional havia plena confiança em todos os administradores, mas esse ponto de vista ingênuo neglicencia dois grandes problemas: a possibilidade de um administrador descontente se tornar uma ameaça interna e as consequências do comprometimento de uma conta administrativa violada por um invasor externo, principalmente quando o administrador em questão é um fornecedor ou outro terceiro.

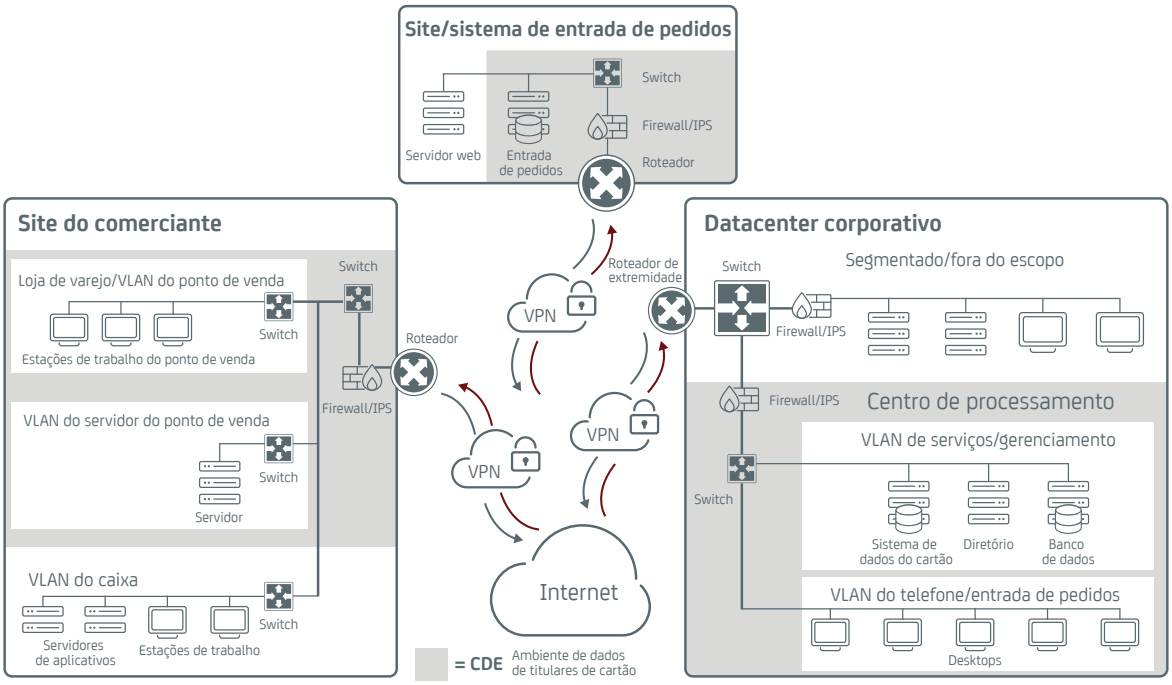
Uma forma de superar isso é adotar um modelo de "confiança zero", uma abordagem do CA Privileged Access Manager (anteriormente, Xceedium Xsuite), um componente-chave das soluções de gerenciamento de acesso com privilégios da CA Technologies, para os casos em que os administradores não são considerados totalmente confiáveis. Nesse modelo, há uma redução do número de violações, e a gravidade das que ainda ocorrem é menor. Em parte, os requisitos do PCI DSS refletem esse modelo de confiança zero, como podemos observar no requisito 7.1.2, "Restringir o acesso a IDs de usuários com privilégios para o mínimo de privilégios necessários para cumprir com responsabilidades do cargo".

No entanto, embora a conformidade com PCI ofereça uma base sólida para proteger os CDEs, não basta "marcar o quadradinho" e atender somente aos requisitos mínimos para ter uma defesa suficiente contra as ameaças de hoje. O gerenciamento de acesso com privilégios vai muito além dos requisitos do PCI para proteger melhor o CDE de uma organização.

Além de conquistar a conformidade com PCI, outros motivos importantes para implementar o gerenciamento de acesso com privilégios são: interromper a cadeia de destruição (kill chain), atenuar as ameaças internas, criar logs e monitorar comandos e eliminar senhas embutidas em código.

Figura A: O escopo dos requisitos do PCI DSS

O PCI DSS v3 exige medidas para proteger o CDE (Cardholder Data Environment - Ambiente de dados de titulares de cartão)



Interrompendo a cadeia de destruição

O conceito básico de cadeia de destruição (kill chain) é que um invasor segue um padrão repetitivo de obter acesso a um sistema (ou expandir esse acesso) e, depois, aumentar os privilégios. Esses privilégios são, então, utilizados para conseguir acesso a outro sistema ou expandir o acesso já existente, depois aumentar os privilégios novamente e continuar nessa cadeia de exploração até atingir o objetivo final. Se essa cadeia de exploração for interrompida em algum ponto do ciclo, o ataque poderá ser paralisado antes de atingir o objetivo final.

O CA Privileged Access Manager oferece os recursos que ajudam a interromper a cadeia. Por exemplo, o CA Privileged Access Manager oferece suporte para autenticação multifatorial no caso de contas com privilégios, o que dificulta seu comprometimento, pois o invasor precisa comprometer várias credenciais para uma única conta. Além disso, quando o assunto é quais comandos podem ser emitidos por cada conta com privilégios em cada componente do CDE, o uso de privilégios mínimos reduz o acesso a informações confidenciais, dificultando o acesso não autorizado de um invasor a dados de interesse.

Uma outra maneira pela qual o CA Privileged Access Manager ajuda a interromper a cadeia de destruição é o suporte de segmentação de rede. Ele restringe quais sub-redes uma determinada conta com privilégios pode acessar e quais sistemas de cada sub-rede podem ser administrados. A segmentação de rede ajuda a limitar a propagação lateral de ataques de um sistema para outro e também restringe a visibilidade do invasor da rede de uma organização. Da mesma forma, o CA Privileged Access Manager oferece um SFA (Socket Filter Agent - Agente de filtro de soquete) que impede que um administrador abra uma conexão de rede não autorizada com outro sistema, como em uma tentativa de SSH ou telnet para um host não autorizado pela diretiva do CA Privileged Access Manager.

Todos esses recursos do CA Privileged Access Manager são recomendados especificamente por fontes como a Mandiant para reduzir fraudes com cartões de crédito.[4]

Atenuando as ameaças internas

Apesar do foco dos requisitos do PCI serem os invasores externos, eles também reconhecem a importância das ameaças internas, que hoje são uma preocupação cada vez maior das organizações. Um estudo indicou que mais de 10% dos funcionários roubaram informações de seus empregadores para obter algum tipo de vantagem ou conhecem alguém que já o fez.[5]

O CA Privileged Access Manager ajuda a atenuar as ameaças internas de diversas formas. A primeira delas é que a implementação dos princípios de privilégios mínimos restringe severamente quais comandos um invasor interno pode emitir e contra quais componentes do CDE é possível emiti-los. De fato, isso minimiza os danos que podem ser causados por um invasor interno. A segunda vantagem é que os logs e o monitoramento de todas as atividades das contas com privilégios criam um registro detalhado de todos os comandos emitidos, o que permite rastrear até uma pessoa específica, e não um ID genérico (compartilhado).

Criando logs e monitorando comandos

Independentemente da eficácia dos controles de segurança, ainda existirão pontos fracos, por isso as violações são inevitáveis em todos os ambientes. Como o CA Privileged Access Manager cria logs e monitora todas as atividades envolvendo contas com privilégios, ele simplifica muito os processos forenses que identificam o que um invasor conseguiu fazer usando credenciais administrativas não autorizadas.

Eliminando senhas embutidas em código

Muitos desenvolvedores de software, administradores e outros profissionais por muito tempo seguiram a prática de embutir senhas em scripts, código-fonte e outros. Esta é uma vulnerabilidade importante porque os desenvolvedores de software, testadores e outros podem acessar essas senhas, e os invasores também sabem procurá-las quando tomam um sistema. Assim poderão usá-las para ter acesso a outros sistemas, como bancos de dados com informações sobre titulares de cartões. O CA Privileged Access Manager oferece recursos de autenticação de aplicativo para aplicativo que tornam desnecessário embutir senhas em código.

Seção 2:

Como o gerenciamento de acesso com privilégios pode ajudar na conformidade com PCI

Como dito anteriormente, o gerenciamento de acesso com privilégios é uma parte fundamental do processo de conformidade com PCI. Simplesmente não é possível atender a uma infinidade de requisitos do PCI em ambientes corporativos comuns sem usar uma solução de gerenciamento de acesso com privilégios. Um grande varejista, por exemplo, estava pagando US$ 100.000 em multas por mês por não atender aos requisitos de PCI relacionados a identificação, autenticação e controle de acesso. Depois de acrescentar o CA Privileged Access Manager ao seu portfólio de soluções de segurança, o varejista conseguiu atender aos requisitos que faltavam e, desse modo, evitar outras multas.

O CA Privileged Access Manager atende a cada um dos seguintes requisitos de PCI.[6]

Requisito 2: Não usar padrões do fornecedor para senhas de sistema e outros parâmetros de segurança.

O CA Privileged Access Manager atende a esse requisito de duas maneiras. Primeiro, quando usado durante a implantação de um sistema, ele pode assumir o controle de contas com privilégios padrão e fazer com que todas as senhas padrão dessas contas sejam redefinidas. A segunda é que ele restringe quais protocolos podem ser utilizados para obter acesso administrativo remoto, como SSH ou SSL/TLS. Isso impede que o sistema seja administrado por redes usando protocolos que não são seguros.

Requisito 6: Desenvolver e manter sistemas e aplicativos seguros.

Uma parte importante deste requisito é o manuseio adequado de credenciais e a separação de tarefas em ambientes de desenvolvimento, teste e produção. O CA Privileged Access Manager aplica o controle de acesso com base na função para contas com privilégios em todos esses ambientes, ajudando na separação de tarefas e, ao mesmo tempo, facilitando a remoção de contas de desenvolvimento, teste e outras que deixam de ser necessárias após a implantação de um sistema ou aplicativo.

Requisito 7: Restringir o acesso a dados de titulares de cartões conforme a necessidade de conhecimento por parte da empresa.

O CA Privileged Access Manager permite que as organizações implementem o princípio de privilégios mínimos para acesso com privilégios, uma área que costuma ser negligenciada. Especificamente, o modelo de confiança zero do CA Privileged Access Manager aplica um controle de acesso refinado para usuários ou grupos de usuários com privilégios, como administradores de bancos de dados. Isso restringe os componentes do sistema aos quais cada usuário ou grupo com privilégios pode ter acesso (como servidores, dispositivos de rede e aplicativos) e quais comandos podem ser executados por cada usuário ou grupo com privilégios em cada um desses componentes. O CA Privileged Access Manager pode ser integrado ao Active Directory, LDAP e a outros diretórios corporativos para reutilizar suas definições de funções e grupos.

Requisito 8: Identificar e autenticar o acesso a componentes do sistema.

Quase todas as partes do Requisito 8 são explicitamente suportadas pelo CA Privileged Access Manager. O produto exige um ID exclusivo para cada usuário com privilégios, oferece todos os recursos de gerenciamento de senhas padrão e oferece suporte a diversas tecnologias de autenticação multifatorial e de fator único. Especificamente, o CA Privileged Access Manager oferece suporte para o Requisito 8 da seguinte maneira:

- **8.1:** O CA Privileged Access Management permite a identificação exclusiva de cada usuário com privilégios, mesmo quando as organizações usam "contas compartilhadas" para determinados componentes da infraestrutura, como os roteadores. Aplica a separação de tarefas entre usuários com privilégios. Oferece recursos padrão para imediatamente encerrar privilégios de acesso revogados, desativar contas com privilégios inativas e aplicar diretivas de bloqueio, quando ocorrem tentativas de autenticação malsucedidas, e diretivas de reautenticação, no caso de sessões ociosas.
- **8.2:** Integra-se a vários métodos de autenticação, exigindo a autenticação de todos os usuários com privilégios. Armazena senhas e outras credenciais (como chaves criptográficas privadas) em um armazenamento fortemente criptografado e as transmite somente por canais criptografados. Aplica diretivas padrão de tamanho, grau de segurança, duração e reutilização de senhas.
- **8.3:** Oferece suporte para inúmeros métodos de autenticação multifatorial e RADIUS, certificados X.509 e smart cards.
- **8.5, 8.6:** Permite que as organizações usem "contas compartilhadas" nos bastidores, ao mesmo tempo exigindo que cada usuário com privilégios, inclusive terceiros, seja identificado e autenticado com exclusividade. Essa identificação exclusiva abrange o uso de smart cards, certificados digitais, tokens criptográficos e outras formas de credenciais diferentes de senhas.
- **8.7:** Restringe o acesso direto a bancos de dados de titulares de cartões somente para administradores de bancos de dados autorizados. Oferece suporte de aplicativo para aplicativo, garantindo que pessoas não acessem ou reutilizem credenciais de aplicativos.

Requisito 10: Acompanhar e monitorar todo o acesso aos recursos da rede e aos dados de titulares de cartões.

Assim como o Requisito 8, o CA Privileged Access Manager oferece suporte a quase todas as partes do Requisito 10. O CA Privileged Access Manager cria logs e registra todas as atividades realizadas através de uma conta com privilégios.

Isso inclui registros de auditoria no formato syslog e gravações semelhantes a DVR de sessões de administrador, com tags indicando possíveis violações de diretivas para acelerar a verificação. O CA Privileged Access Manager oferece suporte para o Requisito 10 da seguinte maneira:

- **10.1:** O CA Privileged Access Manager vincula cada instância de acesso com privilégios a uma pessoa específica. Oferece faixas de auditoria para cada pessoa com acesso com privilégios a todos os componentes do sistema.
- **10.2:** Usa log nativo e syslog para gerar faixas de auditoria automatizadas que registram todas as ações realizadas por usuários com privilégios em servidores, dispositivos de rede, bancos de dados e outros aplicativos. Inclui todas as atividades de identificação e autenticação para contas com privilégios. Restringe o acesso a faixas de auditoria, de modo que somente os usuários autorizados podem examiná-las e criar logs de todas essas verificações.
- **10.3:** Ele registra todos os campos obrigatórios do PCI para cada evento contido no log, inclusive identificação do usuário, tipo de evento, data e hora, êxito ou falha, origem do evento e identidade do recurso afetado (nome do host etc.).
- **10.4:** Ele usa tecnologia de sincronização temporal (ou seja, o NTP [Network Time Protocol - Protocolo de horário da rede]) para realizar a sincronização do relógio.
- **10.5:** Usa técnicas de hashing para identificar qualquer violação em logs e registros de auditoria. Fornece encaminhamento de syslog para backup de registros de auditoria em um armazenamento de logs centralizado.
- **10.7:** Ele usa syslog e oferece suporte para encaminhamento de syslog, assim os registros de auditoria podem ser mantidos pelo tempo desejado.

Requisito 12: Manter uma diretiva voltada à segurança das informações para todos os funcionários.

O CA Privileged Access Manager permite capturar e aplicar diretivas relacionadas a usuários com privilégios. O CA Privileged Access Manager também gera logs de todas as tentativas de violação de diretivas, que são contribuições naturais para um processo de avaliação de riscos.

Protegendo o CDE do ponto de vista do controle do servidor

O Privileged Access Management da CA Technologies também atende a outros requisitos, para um controle de acesso localizado e muito refinado no host, protegendo ainda mais os recursos valiosos, inclusive o próprio CDE. O Controle de Servidor do CA Privileged Access Manager fornece uma camada extra fundamental de proteção de segurança em plataformas de servidor, permitindo controle de acesso refinado, gerenciamento com base em diretivas e os princípios básicos de auditoria de segurança para proteger ativos eletrônicos. É possível criar diretivas de acesso para regular o acesso a recursos do servidor, programas, arquivos e processos usando diversos critérios.

Seção 3:

Mudanças do PCI DSS versão 2 para a versão 3

Quando o PCI DSS foi atualizado da versão 2 para a 3, foram acrescentadas proteções importantes para o CDE, inclusive as seguintes:

- Implementar a segmentação de rede para o CDE para melhor isolar partes do CDE. Isso inclui assegurar que todos os fluxos de dados entre os componentes do sistema sejam documentados e auditar todas as atividades realizadas por usuários com privilégios.
- Realizar testes de penetração no perímetro do CDE.
- Gerenciar credenciais e implementar o controle de acesso com privilégios mínimos e auditoria para todos os acessos ao CDE.
- Reforçar os controles de segurança para provedores de serviço.[7]

Essas proteções ressaltam a necessidade de se ter uma solução de gerenciamento de acesso com privilégios como o CA Privileged Access Manager em vigor para proteger o CDE e atender aos requisitos de PCI. Na maioria dos ambientes, o gerenciamento de acesso com privilégios é a única maneira de efetivamente implementar o princípio de privilégios mínimos para o controle de acesso de administradores e gerar logs de todas as atividades dos administradores. Além disso, o gerenciamento de acesso com privilégios pode ser um recurso inestimável na implementação da segmentação de rede e do monitoramento de todas as atividades que envolvem fluxos de dados entre os segmentos de rede.

A atualização do PCI DSS continha outras mudanças relacionadas ao gerenciamento de acesso com privilégios. A principal delas é que o Requisito 8, sobre identificação e autenticação, foi severamente reestruturado, de forma que à primeira vista ele parece ter sido totalmente reformulado. No entanto, as mudanças envolveram principalmente uma reestruturação do requisito.

A mudança mais importante é a inclusão do requisito 8.6: "Quando se usam mecanismos de autenticação diferentes de senhas, como smart cards ou tokens criptográficos, o mecanismo de autenticação só deve ficar disponível para um usuário; não são permitidos mecanismos de autenticação compartilhados." O CA Privileged Access Manager atende a esse novo requisito, conforme visto na seção anterior.

Seção 4:

Benefícios

As organizações que estão implementando soluções de gerenciamento de acesso com privilégios obtêm mais proteção, menor risco de ameaças externas e internas e melhor conformidade com regulamentos, inclusive o PCI DSS.

Mais especificamente, o CA Privileged Access Manager pode ajudar as organizações das seguintes maneiras, não apenas para atender a conformidade com o PCI DSS, mas também para melhorar a postura de segurança como um todo da forma mais econômica e eficiente possível:

- **Redução de custos.** O CA Privileged Access Manager pode ajudar a reduzir consideravelmente o custo das auditorias do PCI DSS, principalmente porque oferece uma maneira simples e muito econômica de segmentar a rede de uma organização de forma lógica. Ele é um dispositivo semelhante a um proxy que trabalha na camada dos aplicativos da rede e controla quais usuários com privilégios podem acessar os sistemas. A segmentação lógica do plano de gerenciamento permite que as organizações mantenham topologias de rede física existentes e, ao mesmo tempo, segreguem em ilhas os sistemas com dados de titulares de cartões, aplicando um rigoroso controle de acesso. Com essa abordagem, o CA Privileged Access Manager permite que as organizações isolem de forma lógica os sistemas que contêm dados de titulares de cartões, limitando assim o escopo das auditorias de PCI sem ter os altos custos exigidos para segmentar redes fisicamente.
- **Mais segurança.** A abordagem de defesa abrangente do CA Privileged Access Manager à segurança ajuda as empresas a implementar um conjunto amplo de controles visando reduzir os riscos de usuários com privilégios e oferecer mais proteção contra ameaças externas, evitando violações ou minimizando o impacto delas.
- **Tempo para proteção mais rápido e gerenciamento.** A facilidade de implantação e gerenciamento a partir de uma única plataforma propicia um controle melhor e mais rápido do acesso com privilégios e a proteção de credenciais para sistemas no ambiente corporativo híbrido inteiro — desde os datacenters tradicionais aos ambientes virtualizados, nuvens públicas ou qualquer combinação destes — sem a sobrecarga desnecessária associada a abordagens alternativas.

Seção 5:

Conclusões

O gerenciamento de acesso com privilégios é fundamental para atender à conformidade com PCI. Sua importância vai além de apenas atender aos requisitos de conformidade com PCI, pois permite que uma organização melhore sua postura de segurança contra as ameaças internas e externas dos dias de hoje. O CA Privileged Access Manager oferece uma maneira eficaz de implementar o gerenciamento de acesso com privilégios para ajudar na conformidade com PCI e em outras necessidades de segurança.

Utilizando o CA Privileged Access Manager, as organizações podem:

- Reduzir os custos da conformidade com PCI atendendo a muitos requisitos do PCI com uma única solução que se integra perfeitamente às soluções já existentes da organização.
- Economizar nas despesas relacionadas a violações e preservar sua reputação evitando muitas violações de dados e minimizando o impacto das que ainda ocorrerão.

1 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

2 Relatório Anual de Segurança da Cisco de 2014, http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

3 Relatório sobre investigações de violações de dados da Verizon - 2014, http://www.verizonenterprise.com/DBIR/2014/?utm_source=earlyaccess&utm_medium=redirect&utm_campaign=DBIR

4 M-Trends 2014: Beyond the Breach, https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf

5 Data Leakage Worldwide: The High Cost of Insider Threats, http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-506224.pdf

6 PCI DSS v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

7 PCI DSS Summary of Changes v2.0 to v3.0, https://www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcids

CS200-163851_1215