

# Protegendo a Infraestrutura de Armazenamento

## Apresentação

Com a grande diversidade e particularidade das informações, pessoais e/ou empresariais, o cuidado deve ser cada vez mais maior, principalmente com os problemas de falhas de mídia, hardware e/ou vírus e suas variantes. Portanto, proteger as redes de armazenamento tornou-se uma atividade complexa e imprescindível no processo de gerenciamento de armazenamento. Nesta Unidade de Aprendizagem você vai conhecer como a infraestrutura de armazenamento pode ser protegida.

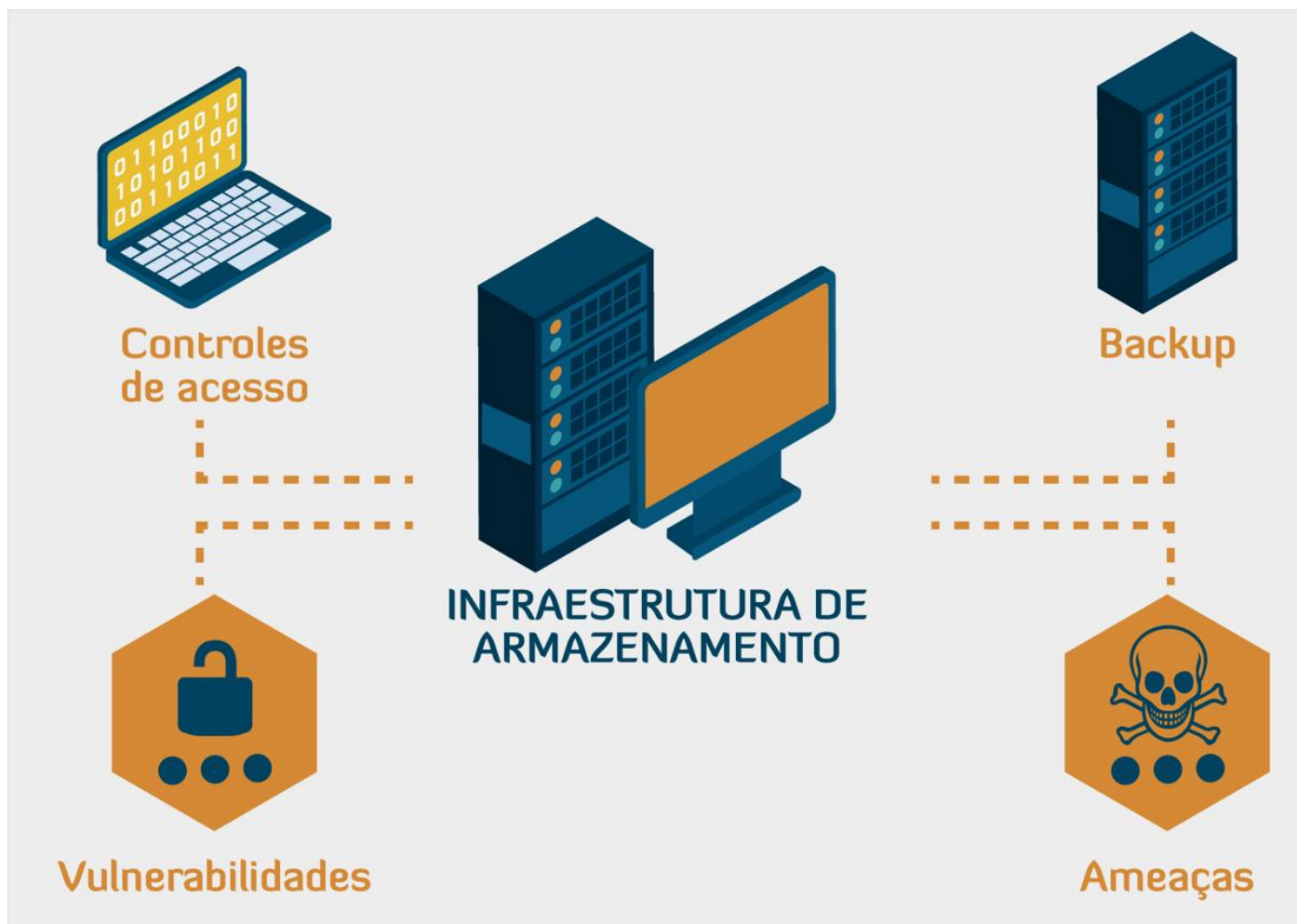
Bons estudos.

**Ao final desta Unidade de Aprendizagem, você deve apresentar os seguintes aprendizados:**

- Selecionar a estrutura de segurança.
- Identificar a tríade de riscos.
- Reconhecer as ameaças à infraestrutura organizacional.

# Infográfico

No infográfico desta unidade você vai conhecer as ameaças à infraestrutura de armazenamento e as formas de protegê-la desses intrusos.



# Conteúdo do Livro

---

A infraestrutura operacional da empresa é vital. Assim, é necessário analisar como um todo a montagem da rede, dos aplicativos utilizados e as tecnologias de armazenamento. Portanto, deve-se ter uma abordagem bem coesa e alinhada para montar a proteção da infraestrutura de armazenamento. Acompanhe um trecho da obra Armazenamento e gerenciamento de informações: como armazenar, gerenciar e proteger informações digitais, que aborda o estudo da proteção da infraestrutura de armazenamento.

Boa leitura.

EMC Education Services

# Armazenamento e Gerenciamento de Informações

Como armazenar, gerenciar e proteger informações digitais



**EMC<sup>2</sup>**  
where information lives®



S693a Somasundaram, G.

Armazenamento e gerenciamento de informações : como armazenar, gerenciar e proteger informações digitais / G.

Somasundaram, Alok Shrivastava, EMC Education Services ; tradução: Acauan Pereira Fernandes ; revisão técnica: EMC Brasil. – Porto Alegre : Bookman, 2011.

480 p. ; 25 cm.

ISBN 978-85-7780-750-5

1. Computação. 2. Armazenamento e gerenciamento de informação digital. I. Shrivastava, Alok. II. EMC Education Services. III. Título.

CDU 004.658

## Protegendo a Infraestrutura de Armazenamento

A Internet é uma mídia disponível globalmente para conexão de computadores pessoais, servidores, redes e armazenamento, o que a torna muito vulnerável a ataques. Informações valiosas, inclusive propriedade intelectual, identidades pessoais e transações financeiras são processadas rotineiramente, armazenadas em storage arrays e acessadas pela rede. Como consequência, o armazenamento agora está mais exposto a diversas ameaças à segurança que podem potencialmente danificar dados cruciais para o negócio e interromper serviços críticos. Proteger as redes de armazenamento tornou-se uma atividade imprescindível no processo de gerenciamento de armazenamento. É uma tarefa intensa e necessária, essencial para o gerenciamento e a proteção de informações importantes.

Este capítulo descreve uma estrutura de proteção do armazenamento projetada para atenuar ameaças à segurança que podem surgir e combater ataques mal-intencionados à infraestrutura de segurança. Além disso, são descritas implementações básicas de segurança de armazenamento, como a arquitetura de segurança e mecanismos de proteção em SAN, NAS e IP-SAN.

### CONCEITOS-CHAVE

Estrutura de segurança do armazenamento

A tríade de riscos

Negação de serviço

Domínio de armazenamento de seguranças

Gerenciamento correto da infraestrutura

Controle de acesso

### 15.1 A estrutura de segurança do armazenamento

A estrutura de segurança básica é construída em torno dos quatro serviços principais de segurança: controle, confidencialidade, integridade e disponibilidade. Ela incorpora todas as medidas de segurança requeridas para atenuar as ameaças a estes quatro atributos primários de segurança:

- **Serviço de responsabilidade:** Refere-se a todos os eventos e operações que ocorram na infraestrutura do data center. O serviço de responsabili-

dade mantém um registro de eventos que podem ser auditados ou rastreados posteriormente por motivo de segurança.

- **Serviço de confidencialidade:** Fornece o sigilo de informação necessário e assegura que apenas usuários autorizados tenham acesso aos dados. Este serviço autentica usuários que precisam acessar informações e geralmente cobre tanto dados em trânsito (transmitidos por cabos) quanto armazenados (em uma mídia de backup ou em arquivos).

Dados em trânsito e armazenados podem ser criptografados para manter sua confidencialidade. Além de impedir usuários não autorizados de acessar informações, os serviços de confidencialidade também implementam medidas de proteção ao fluxo do tráfego como parte do protocolo de segurança. Essas medidas geralmente incluem o ocultamento de endereços de origem e destino, a frequência e o volume de dados enviados.

- **Serviço de integridade:** Assegura que as informações não sejam alteradas. O objetivo do serviço é detectar e proteger contra a alteração ou exclusão não autorizada de informações. Semelhantes aos serviços de confidencialidade, os de integridade trabalham em colaboração com o serviço de responsabilidade para identificar e autenticar os usuários. Os serviços de integridade estipulam medidas para dados em trânsito e armazenados.
- **Serviço de disponibilidade:** Garante que usuários autorizados tenham acesso confiável e apropriado aos dados. Estes serviços permitem aos usuários acessar os sistemas computacionais, além dos dados e aplicativos necessários presentes nestes sistemas. Serviços de disponibilidade também são implementados em sistemas de comunicação usados para transmitir informações entre computadores que podem estar em diferentes locais. Isso assegura a disponibilidade da informação caso ocorra uma falha em determinado local. Estes serviços devem ser implementados para dados eletrônicos e físicos.

---

## 15.2 A tríade de riscos

---

A tríade de riscos define a probabilidade de perigo em termos de ameaças, bens e vulnerabilidades. Riscos surgem quando um agente ameaçador (invasor) tenta acessar bens explorando uma vulnerabilidade existente.

Para gerenciar riscos, as organizações enfocam principalmente as vulnerabilidades, pois elas não possuem a capacidade de eliminar os agentes de ameaças aos seus bens que possam aparecer em diversas formas e origens. As organizações podem instalar contramedidas para diminuir o impacto de um ataque por parte de um agente ameaçador, reduzindo assim a vulnerabilidade.

A avaliação de riscos é o primeiro passo na determinação da extensão de potenciais ameaças em uma infraestrutura de TI. O processo considera riscos e ajuda a identificar controles apropriados para atenuá-los ou eliminá-los. Para

determinar a probabilidade de um evento adverso ocorrer, ameaças a um sistema de TI devem ser analisadas junto com as potenciais vulnerabilidades e os controles de segurança existentes.

A gravidade de um evento adverso é avaliada pelo impacto que ele pode ter sobre atividades críticas do negócio. Com base nessa análise, um valor relativo de criticalidade e sensibilidade pode ser atribuído a bens e recursos de TI. Por exemplo, determinado componente do sistema de TI pode receber um valor de alta criticalidade se um ataque sobre este componente específico puder causar um término completo de serviços de missão crítica.

As seções a seguir examinam os três elementos-chave da tríade de riscos. Bens, ameaças e vulnerabilidade são considerados a partir da perspectiva de identificação de riscos e análise de controle.

### 15.2.1 Bens


A informação é um dos *bens* mais importantes de qualquer organização. Outros bens incluem hardware, software e a infraestrutura de rede necessária para acessar estas informações. Para protegê-los, as organizações devem desenvolver um conjunto de parâmetros para assegurar a disponibilidade dos recursos a usuários autorizados e redes confiáveis. Estes parâmetros se aplicam aos recursos de armazenamento, à infraestrutura de rede e às políticas organizacionais.

Diversos fatores precisam ser considerados ao planejar a segurança dos bens. Métodos de segurança têm dois objetivos. O primeiro é garantir que a rede fique facilmente acessível a usuários autorizados. Também deve ser confiável e estável sob condições ambientais e volumes de uso muito diferentes. O segundo objetivo é dificultar ao máximo o acesso de potenciais invasores que possam comprometer o sistema. Estes métodos devem fornecer proteção adequada contra acesso não autorizado a recursos, vírus, worms, cavalos de Troia e outros tipos de software mal-intencionados. Medidas de segurança também devem criptografar dados críticos e desabilitar serviços não utilizados para minimizar o número de potenciais falhas de segurança. O método de segurança deve garantir que atualizações no sistema operacional e em outros tipos de software sejam instaladas regularmente. Ao mesmo tempo, precisa fornecer redundância adequada na forma de replicação e espelhamento dos dados de produção para evitar perdas catastróficas de dados se houver uma falha inesperada. Para que o sistema de segurança funcione sem sobressaltos, é importante garantir que todos os usuários estejam informados sobre as políticas que controlam o uso da rede.

A eficácia de uma metodologia de segurança de armazenamento pode ser medida por dois critérios. O primeiro garante que o custo da implementação do sistema deva ser somente uma fração do valor dos dados protegidos. O outro assegura que comprometer o sistema custe a um potencial invasor, em termos de dinheiro e tempo, mais do que o valor dos dados protegidos.



**TIPOS DE ATAQUES PASSIVOS**



- **Eavesdropping:** Acesso não autorizado à escuta de uma conversa.
- **Snooping:** Acesso não autorizado aos dados de outro usuário. De modo geral, snooping e eavesdropping são sinônimos.

Hackers mal-intencionados frequentemente usam equipamento e técnicas de snooping, como key loggers, para monitorar o teclado, capturar senhas e informações de log-in, ou interceptar e-mails e outras comunicações e transmissões de dados privadas. As organizações às vezes executam snooping legítimo em funcionários com a intenção de monitorar o uso de computadores da empresa e registrar a utilização da Internet.

15.2.2 Ameaças

Ameaças são os potenciais ataques que podem ser executados em uma infraestrutura de TI. Estes ataques podem ser classificados como ativos ou passivos. Ataques *passivos* são tentativas de obter acesso não autorizado ao sistema. Eles colocam ameaças à confidencialidade das informações. Ataques *ativos* incluem a modificação de dados, DoS (Denial of Service, negação de serviço) e ataques de recusa. Eles colocam ameaças à integridade e à disponibilidade dos dados.

Em um ataque de *modificação*, o usuário não autorizado tenta alterar as informações para propósitos mal-intencionados. Um ataque de modificação pode alvejar os dados armazenados ou em trânsito. Estes ataques ameaçam a integridade dos dados.

Ataques de *DoS* negam o uso de recursos por usuários legítimos. Estes ataques geralmente não envolvem acesso nem modificação de informações no sistema computacional. Em vez disso, ameaçam a disponibilidade dos dados. A inundação intencional de uma rede ou site para impedir acesso legítimo por parte de usuários autorizados é um exemplo de ataque DoS.

A recusa é um ataque contra o controle das informações. Ele tenta fornecer informações falsas fingindo ser alguém ou impedindo que um evento ou transação ocorra.

A Tabela 15-1 descreve diferentes formas de ataque e os serviços de segurança usados para gerenciá-los.

Tabela 15-1    Serviços de segurança para diversos tipos de ataque

Ataque	Confidencialidade	Integridade	Disponibilidade	Controle
Acesso	X			X
Modificação	X	X		X
Negação de Serviço			X	
Recusa		X		X

### 15.2.3 Vulnerabilidade

Os caminhos que dão acesso às informações são mais vulneráveis a potenciais ataques. Cada um desses caminhos pode conter vários pontos de acesso e cada um deles fornece diferentes níveis de acesso aos recursos de armazenamento. É muito importante implementar controles de segurança adequados em *todos* os pontos de um caminho de acesso. A implementação de controles de segurança em cada ponto de acesso de cada caminho é chamado de *defesa integral*.

A defesa integral recomenda a proteção de todos os pontos de acesso dentro de um ambiente. Isso reduz a vulnerabilidade a um invasor que consiga ter acesso a recursos de armazenamento contornando controles de segurança inadequados implementados no único ponto de acesso vulnerável. Tal ataque pode colocar em risco a segurança dos bens de informação. Por exemplo, uma falha na autenticação apropriada de um usuário pode colocar em risco a confidencialidade da informação. De forma semelhante, um ataque de DoS contra um dispositivo de armazenamento pode ameaçar a disponibilidade das informações.

*Superfície de ataque*, *vetor de ataque* e *fator de trabalho* são os três fatores a se considerar durante a avaliação da extensão de vulnerabilidade de um ambiente. A *superfície de ataque* se refere aos diversos pontos de entrada que um invasor pode usar para lançar um ataque. Cada componente de uma rede de armazenamento é uma fonte de potencial vulnerabilidade. Todas as interfaces externas suportadas por esse componente, como as interfaces de hardware, os protocolos suportados e as interfaces de gerenciamento e administrativas, podem ser exploradas por um invasor para a execução de diversos ataques. Essas interfaces formam a superfície de ataque para o invasor. Até mesmo serviços de rede não usados, se estiverem habilitados, poderão se tornar parte da superfície de ataque.

Um *vetor de ataque* é um dos passos necessários para se completar um ataque. Por exemplo, um invasor poderia explorar uma falha na interface de gerenciamento para executar um ataque snoop, em que o invasor modifica a configuração do dispositivo de armazenamento para permitir que o tráfego seja acessado a partir de mais um host. Esse tráfego redirecionado pode ser utilizado para vasculhar os dados em trânsito.

O *fator de trabalho* se refere ao montante de tempo e esforço necessário para explorar um vetor de ataque. Por exemplo, se os invasores tentam recuperar informações sensíveis, analisam o tempo e o esforço que seriam necessários para a execução de um ataque em um banco de dados. Isso pode incluir a determinação de contas com privilégios, a avaliação do esquema do banco de dados e a escrita de consulta SQL. Em vez disso, baseados no fator de trabalho, eles consideram uma forma menos trabalhosa de explorar o storage array atacando-o diretamente e lendo dos blocos de disco brutos.

Tendo avaliado a vulnerabilidade do ambiente de rede quanto a ameaças de segurança, as organizações podem planejar e implantar medidas específicas de controle direcionadas a reduzir a vulnerabilidade minimizando as superfícies de ataque e maximizando o fator de trabalho. Esses controles podem ser técnicos ou não técnicos. Controles técnicos são implementados geralmente a partir de

sistemas computacionais, enquanto os não técnicos são implantados por meio de controles administrativos e físicos. Estes últimos incluem políticas de segurança e de pessoal ou procedimentos padrão para direcionar a execução segura de diversas operações. Controles físicos incluem o estabelecimento de barreiras físicas, como guardas de segurança, cercas ou trancas.

Com base nos papéis que executam, os controles podem ser classificados como de prevenção, de detecção, de correção, de recuperação ou de compensação. A discussão aqui enfoca apenas os controles de prevenção, de correção e detecção. O controle de prevenção tenta evitar um ataque; o de detecção revela se um ataque está acontecendo; e, depois de um ataque ter sido detectado, os controles de correção são implementados. Controles de *prevenção* evitam que as vulnerabilidades sejam exploradas e previnem contra um ataque ou reduzem seu impacto. Controles de *correção* reduzem o efeito de um ataque, enquanto os controles de *detecção* descobrem ataques e disparam controles de prevenção ou de correção. Por exemplo, um Intrusion Detection/Intrusion Prevention System (IDS/IPS) é um controle de detecção que determina se um ataque está ocorrendo e tenta pará-lo terminando uma conexão de rede ou chamando uma regra de firewall para bloquear o tráfego.

### 15.3 Domínios de segurança de armazenamento

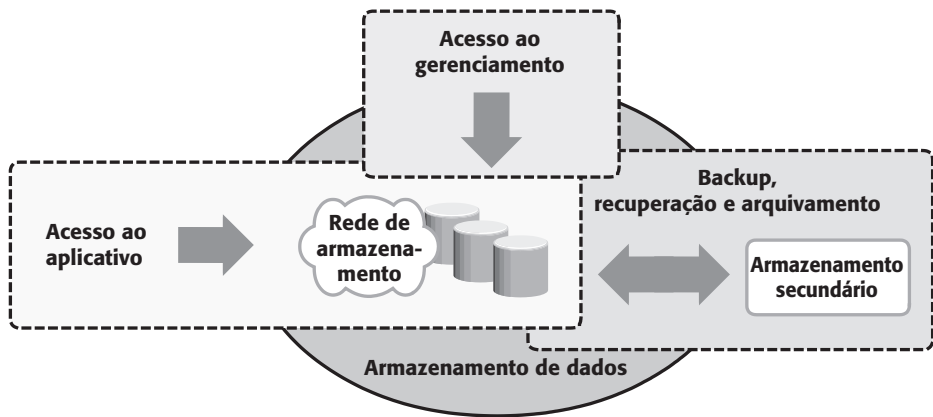
Dispositivos de segurança que não estejam conectados a uma rede de armazenamento são menos vulneráveis porque não estão expostos a ameaças à segurança via redes. Todavia, com o uso cada vez maior de redes em ambientes de armazenamento, os dispositivos de armazenamento estão se tornando altamente vulneráveis a ameaças a partir de uma diversidade de origens. Controles específicos devem ser implementados para garantir um ambiente seguro de rede de armazenamento. Isto requer um exame mais próximo na segurança da rede de armazenamento e uma compreensão clara dos caminhos de acesso que levam aos recursos de armazenamento. Se determinado caminho não estiver autorizado e precisar ser proibido por controles técnicos, será necessário assegurar que esses controles não estejam comprometidos. Se cada componente dentro da rede de armazenamento for considerado um potencial ponto de acesso, será preciso analisar a superfície de ataque que cada um desses pontos de acesso fornece e identificar a vulnerabilidade associada.

Para identificar as ameaças que se aplicam à rede de armazenamento, os caminhos de acesso ao armazenamento de dados podem ser classificados em três domínios de segurança: *acesso ao aplicativo*, *acesso ao gerenciamento* e *BURA* (*backup, recuperação e arquivamento*). A Figura 15-1 mostra os três domínios de segurança de um ambiente de sistema de armazenamento.

O primeiro domínio de segurança envolve o acesso dos aplicativos aos dados armazenados através da rede de armazenamento. O segundo domínio de segurança inclui o acesso de gerenciamento ao armazenamento e dispositivos de interconexão e aos dados que se encontram nesses dispositivos. Este domínio é acessado primariamente por administradores de armazenamento que configu-

ram e gerenciam o ambiente. O terceiro domínio consiste em acesso BURA. Junto com os pontos de acesso nos outros dois domínios, a mídia de backup também precisa ser protegida.

Para assegurar a proteção do ambiente de rede do armazenamento, identifique as ameaças existentes em cada domínio de segurança e classifique-as com base no tipo de serviços de segurança – disponibilidade, confidencialidade, integridade e controle. O próximo passo é selecionar e implementar diversos controles como contramedidas às ameaças.



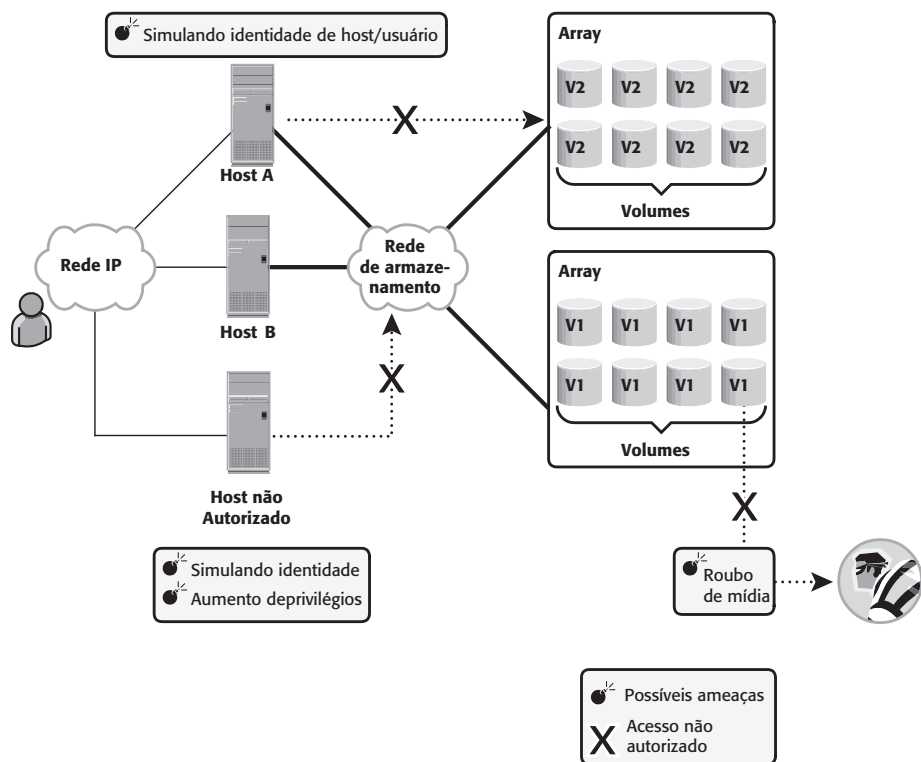
**Figura 15-1** Três domínios de segurança do armazenamento de dados.

### 15.3.1 Protegendo o domínio de acesso ao aplicativo

O domínio de acesso ao aplicativo pode incluir apenas aqueles aplicativos que acessam os dados através do sistema de arquivos ou de uma interface de banco de dados.

A Figura 15-2 apresenta o acesso ao aplicativo em um ambiente de rede de armazenamento. O host A pode acessar todos os volumes V1; o host B, todos os volumes V2. Estes volumes são classificados de acordo com o nível de acesso, como confidencial, restrito e público. Algumas das possíveis ameaças nesse cenário poderiam ser o host A falsificar a identidade ou aumentar os privilégios do host B para obter acesso aos recursos do host B. Outra ameaça poderia ser um host não autorizado obter acesso à rede; o invasor neste host pode tentar simular a identidade de outro e adulterar dados, vasculhar a rede ou executar um ataque de DoS. Além disso, qualquer forma de roubo de mídia também poderia comprometer a segurança da rede. Essas ameaças podem colocar diversos desafios à segurança da rede, de modo que precisam ser abordadas.

Um passo importante para proteger o domínio de acesso do aplicativo é identificar as funções básicas que podem evitar que as ameaças sejam exploradas e identificar os controles apropriados que devem ser aplicados. Implementar segurança física também é um fator importante para evitar o roubo de mídia.



**Figura 15-2** Ameaças à segurança no domínio de acesso do aplicativo.

### Controlando o acesso do usuário aos dados

Os serviços de controle de acesso regulam o acesso dos usuários aos dados. Estes serviços atenuam as ameaças de falsificação de identidade de host e de aumento de privilégios de host. Ambas as ameaças afetam a integridade e a confiabilidade dos dados.

O controle técnico na forma de autenticação de usuários e o controle administrativo por meio de autorização de usuários são os dois mecanismos usados no controle de acesso ao aplicativo. Eles podem ficar fora dos limites da rede de armazenamento e requerer que diversos sistemas se interconectem com outros sistemas de gerenciamento e autenticação de identidades da empresa – por exemplo, sistemas que fornecem um forte esquema de autenticação e autorização para proteger a identidade do usuário contra falsificações. Dispositivos NAS suportam a criação de *listas de controle de acesso* que são usadas para regular o acesso do usuário a determinados arquivos. O aplicativo Enterprise Content Management fiscaliza o acesso aos dados com o IRM (Information Rights Management), que especifica quais usuários têm quais direitos a um documento. Restringir o acesso no nível de host começa com a autenticação de um nó quando ele tenta se conectar a uma rede. Diferentes tecnologias de armazenamento de rede, como iSCSI, FC e armazenamento baseado em IP, usam vários mecanismos de autenticação, como Challenge-Handshake Authentication Protocol (CHAP), Fi-

bre Channel Security Protocol (FC-SP) e IPSec, respectivamente, para autenticar o acesso ao host.

Depois que um host é autenticado, o próximo passo é especificar controles de segurança para os recursos de armazenamento, como portas, volumes ou pools de armazenamento, que o host está autorizado a acessar. *Zoneamento* é um mecanismo de controle nos switches que segmenta a rede em caminhos específicos a serem usados pelo tráfego de dados; *máscaras LUN* determinam quais hosts podem acessar quais dispositivos de armazenamento. Alguns dispositivos aceitam a associação do WWN de um host a determinada porta FC e, a partir daí, a determinada LUN. Esta ligação do WWN a uma porta física é a mais segura.

Finalmente, é muito importante assegurar que controles administrativos, como padrões e políticas definidas, sejam implementados. Auditoria regular é necessária para assegurar o funcionamento apropriado dos controles administrativos. Isso é possível pelo registro de eventos significativos em todos os dispositivos participantes. O registro de eventos deve ser protegido contra acessos não autorizados porque ele pode não conseguir executar seus objetivos se o conteúdo registrado for exposto a modificações indesejadas por um invasor.

### ***Protegendo a infraestrutura de armazenamento***

Proteger a infraestrutura de armazenamento de acesso não autorizado envolve a atenção a todos os seus elementos. Os controles de segurança para proteção da infraestrutura de armazenamento abordam as ameaças de alteração não autorizada dos dados em trânsito, o que leva a uma perda na integridade deles, a uma negação de serviço que comprometa a disponibilidade e à falsificação de rede que pode resultar em uma perda de confidencialidade.

Os controles de segurança para proteção da rede se dividem em duas categorias gerais: *integridade da infraestrutura de conectividade* e *criptografia da rede de armazenamento*. Os controles para garantir a integridade da infraestrutura incluem uma função de fabric switch que assegura a integridade. Esse resultado é obtido evitando-se que um host seja adicionado a uma rede sem a autorização apropriada. Métodos de criptografia de rede de armazenamento incluem o uso de IPSec (para redes de armazenamento baseadas em IP) e FC-SP (para redes FC).

Em ambientes de armazenamento seguros, privilégios de root ou de administrador para um dispositivo específico não são concedidos a qualquer indivíduo. Em vez disso, é implantado o *controle de acesso baseado em papéis* (RBAC, *role-based access control*) para atribuir os privilégios necessários aos usuários, permitindo a estes executar seus papéis. Também é aconselhável considerar controles administrativos, como a “separação de funções”, ao definir procedimentos de data centers. A separação clara das funções assegura que nenhum indivíduo único possa especificar uma ação e executá-la. Por exemplo, a pessoa que autoriza a criação de contas administrativas não deve ser a mesma que usa essas contas. O acesso ao gerenciamento da segurança é examinado em detalhes na próxima seção.

As redes de gerenciamento para sistemas de armazenamento devem estar separadas logicamente de outras redes da empresa. Essa segmentação é crucial para facilitar o gerenciamento e aumentar a segurança permitindo o acesso ape-

nas aos componentes que existam dentro do mesmo segmento. Por exemplo, a segmentação de redes IP é imposta na camada 2 utilizando VLANs e segurança em nível de porta em switches Ethernet.

Finalmente, o acesso físico ao console do dispositivo e ao cabeamento de FC switches deve ser controlado para garantir proteção da infraestrutura de armazenamento. Todas as outras medidas de segurança estabelecidas falham se um dispositivo é acessado fisicamente por um usuário não autorizado; o simples fato do acesso pode mostrar que o dispositivo não é confiável.

### ***Criptografia de dados***

O aspecto mais importante da proteção de dados é resguardar os que estão guardados nos storage arrays. Ameaças neste nível incluem a alteração de dados, que viola sua integridade, e o roubo de mídia, que compromete sua disponibilidade e a confiabilidade. Para se proteger destas ameaças, criptografe os dados da mídia de armazenamento ou antes de eles serem transferidos para o disco. Também é crítico decidir sobre um método para garantir que os dados excluídos no final de seu ciclo de vida sejam completamente apagados dos discos e não possam ser reestruturados para propósitos mal-intencionados.

Os dados devem ser criptografados o mais próximo possível de sua origem. Se não for possível executar a criptografia no dispositivo do host, um dispositivo de criptografia pode ser usado para criptografar dados no ponto de entrada da rede de armazenamento. Dispositivos de criptografia podem ser implementados na rede que criptografa os dados entre o host e a mídia de armazenamento. Estes mecanismos têm a capacidade de proteger tanto os dados armazenados no dispositivo de destino quanto os dados em trânsito.

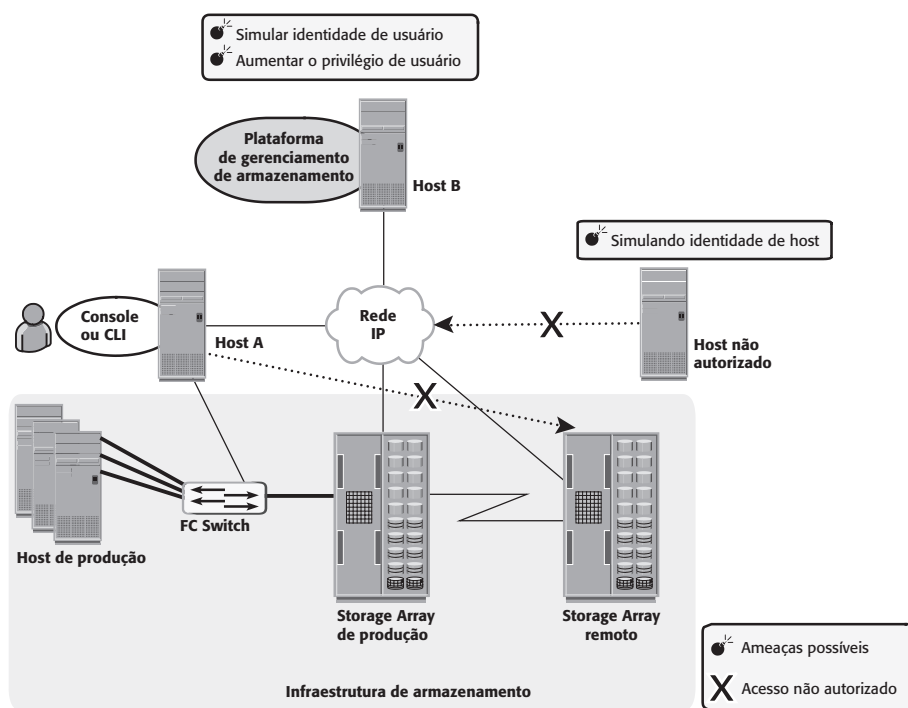
Em dispositivos NAS, adicionar verificações antivírus e controles de extensões de arquivos pode aumentar a integridade dos dados. No caso de CAS, o uso de algoritmos de criptografia MD5 ou SHA-256 garante a integridade dos dados detectando qualquer mudança nos padrões de conteúdo de bits. Além disso, o serviço de exclusão de dados do CAS assegura que os dados sejam completamente eliminados do disco antes de este ser descartado. A política de classificação de dados de uma organização determina se o disco precisa ser realmente limpo antes de ser descartado e qual o nível de exclusão necessário, com base em requisitos de regulamentação.

### **15.3.2 Protegendo o domínio de acesso ao gerenciamento**

O acesso ao gerenciamento, seja ao monitorar, provisionar ou gerenciar recursos de armazenamento, é associado a cada dispositivo dentro da rede de armazenamento. A maioria dos produtos de software de gerenciamento suporta alguma forma de CLI, console de gerenciamento de sistema ou uma interface baseada em Web. É muito importante implementar controles apropriados para proteger aplicativos de gerenciamento de armazenamento, uma vez que o dano causado ao sistema de armazenamento com o uso desses aplicativos pode ser muito maior do que o causado pela vulnerabilidade de um servidor.



A Figura 15-3 mostra um ambiente de rede de armazenamento no qual os hosts de produção estão conectados a uma rede SAN e estão acessando o storage array A, que está conectado a um storage array B por motivo de replicação. Além disso, esta configuração tem uma plataforma de gerenciamento de armazenamento no host B e um console de monitoração no host A. Todos esses hosts estão interconectados através de uma rede IP. Algumas das ameaças possíveis neste sistema são hosts não autorizados simularem a identidade do usuário ou do host para gerenciar os storage arrays ou a rede. Por exemplo, o host A pode obter acesso de gerenciamento ao array B. Usando suporte a console remoto, diversos outros sistemas na rede também podem ser explorados para executar um ataque.



**Figura 15-3** Ameaças à segurança no domínio de acesso ao gerenciamento.

Dar acesso ao gerenciamento através de uma rede externa aumenta o potencial de um host ou switch não autorizado se conectar a essa rede. Em tais circunstâncias, implementar medidas de segurança apropriadas evita que ocorram determinados tipos de comunicação. O uso de canais seguros de comunicação, como Secure Shell (SSH) ou Secure Sockets Layer (SSL)/Transport Layer Security (TLS), fornece proteção eficaz contra essas ameaças. A monitoração de registros de eventos ajuda a identificar acesso e alterações não autorizados na infraestrutura.





# Dica do Professor

---

Assista ao vídeo para saber mais sobre proteção da infraestrutura de armazenamento.



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

# Exercícios

---

**NÃO faz parte da estrutura de segurança do armazenamento:**

1)

- A) a) Serviço de responsabilidade.
- B) b) Serviço de confidencialidade.
- C) c) Serviço de integridade.
- D) d) Serviço de relacionamento.
- E) e) Serviço de disponibilidade.

**São elementos-chave da tríade de riscos:**

2)

- A) a) Bens, ameaças e vulnerabilidade.
- B) b) Bens, ameaças e replicação.
- C) c) Bens, vulnerabilidade e compilação.
- D) d) Vulnerabilidade, ameaças e hardware.
- E) e) Ameaças, software e bens.

**NÃO faz parte dos domínios de segurança e armazenamento:**

3)

- A) a) Backup.
- B) b) Recuperação.
- C) c) Arquivamento.
- D) d) Acesso ao aplicativo.
- E) e) Acesso ao LVM.

**Dentre as alternativas abaixo, qual NÃO é uma ameaça ao domínio de acesso do aplicativo?**

4)

- A) a) Simular identidade.

- B) b) Aumentar privilégios.
- C) c) Roubo de mídia.
- D) d) Forjar acesso host.
- E) e) Ataque criptográfico.

5) Analisando a estrutura em rede, qual padrão NÃO oferece proteção à estrutura de armazenamento?

- A) a) Utilizar SAN para armazenamento.
- B) b) Deixar domínios de broadcast entre as redes que compõem a estrutura.
- C) c) Efetuar controles de acesso com ACL.
- D) d) Efetuar a comunicação com SSH.
- E) e) Operar com VLANS.

# Na prática

Em uma empresa, a informação deve ser transportada e armazenada com segurança entre a matriz e as filiais, garantindo, assim, a integridade dos dados trafegados. Nesse caso, deve-se usar a criptografia para transportá-la, logo, o canal de comunicação utilizado como a VPN deverá ser criptografado. Ao armazenar a informação, ela deverá estar em local com segurança e controle de acessos, bem como onde se tenha a rotina de backup.

1



Com isso, não serão todos os usuários que terão acesso à informação, mas somente os autorizados.

2



Caso ocorra algum desastre, é possível ter a cópia de segurança da informação.

3



Somado a esses fatores, há também o uso de ferramentas de monitoramento de intrusos e anomalias (IDS), bem como softwares de antivírus.

4



Esse conjunto de softwares com monitoramento em tempo real e com um escaneamento mais detalhado ocorre em horários de menos acesso aos dados, logo, fora do horário de expediente.

# Saiba mais

---

Para ampliar o seu conhecimento a respeito desse assunto, veja abaixo as sugestões do professor:

## **Configurando IDS (snort) e Honeypot**



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

## **OpenVPN: Comunicação Segura em Canais Inseguros**



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

## **Aumentando a segurança em sua empresa. você sabe a diferença entre firewall, IPS e IDS?**



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

## **BURA – Backup, Recovery & Archiving**



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.

## **Instalação e configuração do IDS Snort**



Aponte a câmera para o código e acesse o link do conteúdo ou clique no código para acessar.