**Introdução**

18.0.1

**Por que devo fazer este módulo?**

Proteger as nossas redes continuará a ser um desafio. Milhões de novos dispositivos estão se juntando às nossas redes todos os anos à medida que a Internet das Coisas (IoT) continua se expandindo e os indivíduos precisam conectar seus próprios dispositivos à rede. Além disso, com recursos sem fio, esses dispositivos podem estar em praticamente qualquer lugar. Muitas organizações precisam proteger usuários e recursos internos, trabalhadores móveis e serviços virtuais e baseados em nuvem, enquanto os atores de ameaças continuam procurando vulnerabilidades que podem ser exploradas.

Usamos uma variedade de métodos para proteger nossas redes, dispositivos e dados. Este capítulo aborda abordagens para a defesa de segurança de rede e as políticas de segurança necessárias para garantir que as práticas de segurança sejam seguidas.

18.0.2

**O que vou aprender neste módulo?**

**Título do módulo:** Compreendendo a defesa

**Objetivo do módulo**: Explicar abordagens para a defesa da segurança da rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Defesa em profundidade | Explicar como a estratégia de defense-in-depth é usada para proteger as redes. |
| Políticas, regulamentos e padrões de segurança | Explicar as políticas, os regulamentos e os padrões de segurança. |

# Defesa em profundidade

18.1.1

## Ativos, vulnerabilidades, ameaças

Analistas de segurança cibernética devem se preparar para qualquer tipo de ataque. É seu trabalho proteger os ativos da rede da organização. Para fazer isso, os analistas de segurança cibernética devem primeiro identificar:

* **Ativos** - qualquer coisa de valor para uma organização que deve ser protegida, incluindo servidores, dispositivos de infraestrutura, dispositivos finais e o maior ativo, dados.
* **Vulnerabilidades** - Uma fraqueza em um sistema ou em seu design que pode ser explorada por um agente de ameaça.
* **Ameaças** - Qualquer perigo potencial para um ativo.

18.1.2

## Identificar ativos

À medida que uma organização cresce, seus ativos também crescem. Considere o número de ativos que uma grande organização teria de proteger. Pode igualmente adquirir outros ativos através de fusões com outras empresas. O resultado é que muitas organizações só têm uma ideia geral dos ativos que precisam ser protegidos.

A coleta de todos os dispositivos e informações de propriedade ou gerenciadas pela organização são ativos. Os ativos constituem a superfície de ataque que os atores da ameaça podem atingir. Estes ativos devem ser inventariados e avaliados quanto ao nível de proteção necessário para impedir potenciais ataques.

O gerenciamento de ativos consiste em inventários de todos os ativos e, em seguida, desenvolver e implementar políticas e procedimentos para protegê-los. Essa tarefa pode ser assustadora, considerando que muitas organizações precisam proteger usuários e recursos internos, trabalhadores móveis e serviços virtuais e baseados em nuvem.

Além disso, as organizações precisam identificar onde os ativos de informações essenciais estão armazenados e como o acesso é obtido a essas informações. Os ativos de informação variam, assim como as ameaças contra eles. Por exemplo, uma empresa de varejo pode armazenar informações de cartão de crédito do cliente. Uma empresa de engenharia armazenará projetos e softwares sensíveis à concorrência. Um banco armazenará dados de clientes, informações de conta e outras informações financeiras confidenciais. Cada um desses ativos pode atrair diferentes atores de ameaças que têm diferentes níveis de habilidade e motivações.

18.1.3

## Identificar vulnerabilidades

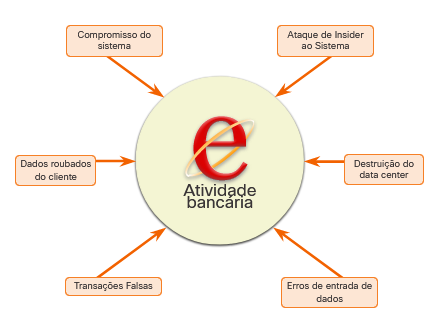
A identificação de ameaças fornece a uma organização uma lista de prováveis ameaças para um ambiente específico. Ao identificar ameaças, é importante fazer várias perguntas:

* Quais são as possíveis vulnerabilidades de um sistema?
* Quem pode querer explorar essas vulnerabilidades para acessar ativos de informações específicos?
* Quais são as consequências se as vulnerabilidades do sistema forem exploradas e os ativos forem perdidos?

Por exemplo, consulte a figura.

A figura mostra vários tipos de ameaças eBanking.

### Ameaças de e-banking



A identificação da ameaça para um sistema de banca electrónica incluiria:

* **Compromisso interno do sistema** - O atacante usa os servidores de e-banking expostos para invadir um sistema bancário interno.
* **Dados roubados do cliente** - Um atacante rouba os dados pessoais e financeiros dos clientes bancários do banco de dados do cliente.
* **Transações falsas de um servidor externo** - Um invasor altera o código do aplicativo de e-banking e faz transações personificando um usuário legítimo.
* **Transações falsas usando um PIN de cliente roubado ou cartão inteligente** - Um invasor rouba a identidade de um cliente e conclui transações mal-intencionadas da conta comprometida.
* **Ataque insider no sistema** - Um funcionário do banco encontra uma falha no sistema a partir do qual montar um ataque.
* **Erros de entrada de dados** - Um usuário insere dados incorretos ou faz solicitações de transação incorretas.
* **Destruição do data center** - Um evento cataclísmico danifica gravemente ou destrói o data center.

Identificar vulnerabilidades em uma rede requer uma compreensão dos aplicativos importantes que são usados, bem como das diferentes vulnerabilidades desse aplicativo e hardware. Isso pode exigir uma quantidade significativa de pesquisa por parte do administrador de rede.

18.1.4

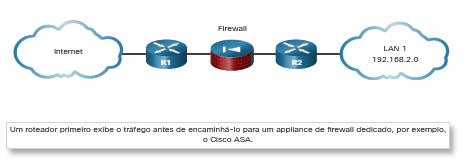
## Identificar ameaças

As organizações devem usar uma abordagem de defesa profunda para identificar ameaças e proteger ativos vulneráveis. Essa abordagem usa várias camadas de segurança na borda da rede, na rede e nos pontos de extremidade da rede.

Para obter um exemplo, consulte a figura.

A figura mostra uma nuvem de internet conectada ao roteador R1 que se conecta a um firewall. Do outro lado do firewall está o roteador R2 que também se conecta a uma nuvem rotulada lan 1 192 dot 168 ponto 2 ponto 0. Palavras na parte inferior: Um roteador primeiro exibe o tráfego antes de encaminhá-lo para um appliance de firewall dedicado, por exemplo, o Cisco ASA.

### Abordagem de defesa em profundidade



A figura exibe uma topologia simples de uma abordagem de defesa em profundidade:

* **Roteador de borda** - A primeira linha de defesa é conhecida como um roteador de borda (R1 na figura). O roteador de borda tem um conjunto de regras especificando qual tráfego ele permite ou nega. Ele passa todas as conexões que se destinam à LAN interna para o firewall.
* **Firewall** - A segunda linha de defesa é o firewall. O firewall é um dispositivo de ponto de verificação que executa filtragem adicional e rastreia o estado das conexões. Ele nega o início de conexões de redes externas (não confiáveis) para a rede interna (confiável), enquanto permite que usuários internos estabeleçam conexões bidirecionais com as redes não confiáveis. Ele também pode executar autenticação de usuário (proxy de autenticação) para conceder aos usuários remotos externos acesso a recursos de rede interna.
* **Roteador interno** - Outra linha de defesa é o roteador interno (R2 na figura). Ele pode aplicar regras de filtragem finais no tráfego antes de ser encaminhado para seu destino.

Os roteadores e firewalls não são os únicos dispositivos que são usados em uma abordagem de defesa profunda. Outros dispositivos de segurança incluem IPS (Intrusion Prevention Systems), Proteção Avançada contra Malware (AMP), sistemas de segurança de conteúdo da Web e de e-mail, serviços de identidade, controles de acesso à rede e muito mais.

Na abordagem de segurança em camadas de defesa profunda, as diferentes camadas trabalham juntas para criar uma arquitetura de segurança na qual a falha de uma salvaguarda não afeta a eficácia das outras salvaguardas.

18.1.5

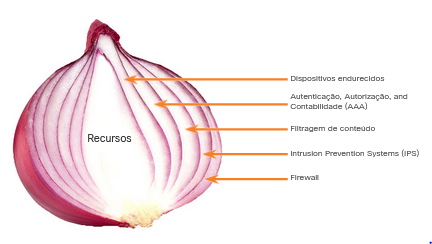
## A cebola de segurança e a alcachofra de segurança

Existem duas analogias comuns que são usadas para descrever uma abordagem de defesa em profundidade.

Cebola de segurança

Uma analogia comum usada para descrever uma abordagem de defesa em profundidade é chamada de “cebola de segurança”. Como ilustrado na figura, um ator de ameaça teria que descascar as defesas de uma rede camada por camada de uma maneira semelhante a descascar uma cebola. Somente depois de penetrar cada camada, o ator da ameaça alcançaria os dados ou o sistema de destino.

**Observação**: A cebola de segurança descrita nesta página é uma forma de visualizar a defesa em profundidade. Isso não deve ser confundido com o conjunto Security Onion de ferramentas de segurança de rede.



Alcachofra de segurança

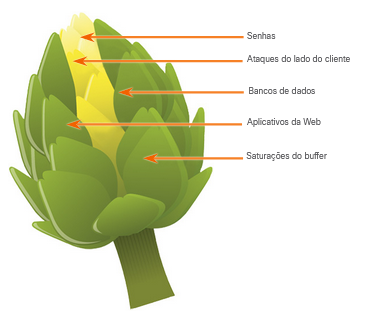
O cenário em mudança da rede, como a evolução das redes sem fronteiras, mudou essa analogia para a “alcachofra de segurança”, que beneficia o ator de ameaça.

Conforme ilustrado na figura, os atores da ameaça não precisam mais descascar cada camada. Eles só precisam remover certas “folhas de alcachofra”. O bônus é que cada “folha” da rede pode revelar dados confidenciais que não estão bem protegidos.

Por exemplo, é mais fácil para um agente de ameaça comprometer um dispositivo móvel do que comprometer um computador ou servidor interno protegido por camadas de defesa. Cada dispositivo móvel é uma folha. E folha após folha, tudo leva o hacker a mais dados. O coração da alcachofra é onde os dados mais confidenciais são encontrados. Cada folha fornece uma camada de proteção enquanto fornece simultaneamente um caminho para o ataque.

Nem todas as folhas precisam ser removidas para chegar ao coração da alcachofra. O hacker arranca a armadura de segurança ao longo do perímetro para chegar ao “coração” da empresa.

Enquanto os sistemas voltados para a Internet são geralmente muito bem protegidos e as proteções de limites são tipicamente sólidos, hackers persistentes, auxiliados por uma mistura de habilidade e sorte, eventualmente encontram uma lacuna nesse exterior hard-core através do qual eles podem entrar e ir onde quiserem.



# Políticas, regulamentos e padrões de segurança

18.2.1

## Políticas de Negócios

Políticas de negócios são as diretrizes que são desenvolvidas por uma organização para governar suas ações. As políticas definem padrões de comportamento correto para a empresa e seus funcionários. Na rede, as políticas definem as atividades permitidas na rede. Isso define uma linha de base de uso aceitável. Se um comportamento que viola a política de negócios for detectado na rede, é possível que tenha ocorrido uma violação de segurança.

Uma organização pode ter várias diretivas orientadoras, conforme listado na tabela.

| **Política** | **Descrição** |
| --- | --- |
| **Políticas da empresa** | * Estas políticas estabelecem as regras de conduta e as responsabilidades dos trabalhadores e dos empregadores. * As políticas protegem os direitos dos trabalhadores, bem como os interesses comerciais dos empregadores. * Dependendo das necessidades da organização, várias políticas e procedimentos estabelecem regras relativas à conduta dos funcionários, assiduidade, código de vestimenta, privacidade e outras áreas relacionadas com os termos e condições de emprego. |
| **Políticas de funcionários** | * Essas políticas são criadas e mantidas pela equipe de recursos humanos para identificar o salário dos funcionários, o cronograma de pagamento, os benefícios dos funcionários, o horário de trabalho, as férias e muito mais. * Muitas vezes, eles são fornecidos a novos funcionários para revisar e assinar. |
| **Políticas de segurança** | * Essas políticas identificam um conjunto de objetivos de segurança para uma empresa, definem as regras de comportamento para usuários e administradores e especificam os requisitos do sistema. * Esses objetivos, regras e requisitos garantem coletivamente a segurança de uma rede e dos sistemas de computador em uma organização. * Assim como um plano de continuidade, uma política de segurança é um documento em constante evolução com base em mudanças no cenário de ameaças, vulnerabilidades e requisitos de negócios e funcionários. |

18.2.2

**Política de Segurança**

Uma política de segurança abrangente tem uma série de benefícios, incluindo os seguintes:

* Demonstra o compromisso de uma organização com a segurança
* Define as regras para o comportamento esperado
* Garante a consistência nas operações do sistema, aquisição e uso de software e hardware e manutenção
* Define as consequências legais das violações
* Dá ao pessoal de segurança o apoio da gestão

As políticas de segurança são usadas para informar os usuários, funcionários e gerentes sobre os requisitos de uma organização para proteger os ativos de tecnologia e informação. Uma política de segurança também especifica os mecanismos necessários para atender aos requisitos de segurança e fornece uma linha de base a partir da qual adquirir, configurar e auditar sistemas e redes de computadores para conformidade.

A tabela lista as diretivas que podem ser incluídas em uma diretiva de segurança.

| **Política** | **Descrição** |
| --- | --- |
| **Política de identificação e autenticação** | Especifica pessoas autorizadas que podem ter acesso a recursos de rede e procedimentos de verificação de identidade. |
| **Políticas de senha** | Garante que as senhas atendam aos requisitos mínimos e sejam alteradas regularmente. |
| **Acceptable Use Policy (AUP)** | Identifica os aplicativos e usos de rede que são aceitáveis para a organização. Também podem identificar as ramificações, se esta política for violada. |
| **Política de acesso remoto** | Identifica como os usuários remotos podem acessar uma rede e o que é acessível por meio de conectividade remota. |
| **Políticas de Manutenção de Rede** | Especifica procedimentos de atualização de sistemas operacionais dos dispositivos de rede e de aplicativos de usuário final. |
| **Procedimentos de tratamento de incidentes** | Descreve como os incidentes de segurança são tratados. |

Um dos componentes de política de segurança mais comuns é um AUP. Isso também pode ser referido como uma política de uso apropriada. Este componente define o que os usuários têm ou não permissão para fazer nos vários componentes do sistema. Isso inclui o tipo de tráfego permitido na rede. A AUP deve ser o mais explícita possível, para evitar mal-entendidos.

Por exemplo, um AUP pode listar sites específicos, grupos de notícias ou aplicativos de uso intensivo de largura de banda que são proibidos de serem acessados por computadores da empresa ou da rede da empresa. Cada funcionário deve ser obrigado a assinar uma AUP, e as AUPs assinadas devem ser mantidas durante a duração do emprego.

18.2.3

**Políticas BYOD**

Muitas organizações agora também devem oferecer suporte ao BYOD (Traga seu próprio dispositivo). Isso permite que os funcionários usem seus próprios dispositivos móveis para acessar sistemas, software, redes ou informações da empresa. O BYOD oferece vários benefícios importantes para as empresas, incluindo aumento da produtividade, redução dos custos operacionais e de TI, melhor mobilidade para os funcionários e maior atração quando se trata de contratar e reter funcionários.

No entanto, esses benefícios também trazem um maior risco de segurança das informações, pois o BYOD pode levar a violações de dados e maior responsabilidade para a organização.

Uma política de segurança BYOD deve ser desenvolvida para realizar o seguinte:

* Especifique os objetivos do programa BYOD.
* Identifique quais funcionários podem trazer seus próprios dispositivos.
* Identifique quais dispositivos serão suportados.
* Identificar o nível de acesso que os funcionários são concedidos ao usar dispositivos pessoais.
* Descrever os direitos de acesso e as atividades permitidas ao pessoal de segurança no dispositivo.
* Identifique quais regulamentos devem ser cumpridos ao usar dispositivos de funcionários.
* Identifique as salvaguardas a serem implementadas se um dispositivo for comprometido.

A tabela lista as práticas recomendadas de segurança BYOD para ajudar a mitigar vulnerabilidades BYOD.

| **Práticas recomendadas** | **Descrição** |
| --- | --- |
| Acesso protegido por senha | Use senhas exclusivas para cada dispositivo e conta. |
| Controle manualmente a conectividade sem fio | Desative a conectividade Wi-Fi e Bluetooth quando não estiver em uso. Conecte-se apenas a redes confiáveis. |
| Mantenha-se atualizado | Mantenha sempre o sistema operacional do dispositivo e outros softwares atualizados. O software atualizado geralmente contém patches de segurança para mitigar contra as ameaças ou explorações mais recentes. |
| Dados de backup | Ative o backup do dispositivo caso ele seja perdido ou roubado. |
| Ativar “Localizar meu dispositivo” | Assine um serviço de localizador de dispositivos com o recurso de apagamento remoto. |
| Fornece software antivírus | Fornecer software antivírus para dispositivos BYOD aprovados. |
| Use um software gerenciamento de dispositivos móveis (MDM) | O software MDM permite que as equipes de TI implementem configurações de segurança e configurações de software em todos os dispositivos que se conectam às redes da empresa. |

18.2.4

## Conformidade com regulamentações e padrões

Há também regulamentos externos em relação à segurança da rede. Os profissionais de segurança de rede devem estar familiarizados com as leis e códigos de ética que são vinculativos para os profissionais de Segurança de Sistemas de Informação (INFOSEC).

Muitas organizações são obrigadas a desenvolver e implementar políticas de segurança. Os regulamentos de conformidade definem o que as organizações são responsáveis pelo fornecimento e a responsabilidade caso não cumpram. Os regulamentos de conformidade que uma organização é obrigada a seguir dependem do tipo de organização e dos dados que a organização manipula. Regulamentos específicos de conformidade serão discutidos mais tarde no curso.

18.3.1

## O que aprendi neste módulo?

**Defesa em profundidade**

Neste capítulo, você aprendeu a importância de proteger nossas redes, dispositivos e dados de atores de ameaças. O ponto de partida para a defesa de rede é a identificação de ativos, vulnerabilidades e ameaças. Os ativos são tudo de valor para uma organização que deve ser protegida, incluindo servidores, dispositivos de infraestrutura, dispositivos finais e o maior ativo, os dados. O gerenciamento de ativos consiste em inventários de todos os ativos e, em seguida, desenvolver e implementar políticas e procedimentos para protegê-los. Vulnerabilidades são pontos fracos em um sistema ou em seu design que podem ser explorados por um ator de ameaça. Ameaças são qualquer perigo potencial para um ativo. As organizações devem usar uma abordagem de defesa profunda para identificar ameaças e proteger ativos vulneráveis. Essa abordagem usa várias camadas de segurança na borda da rede, na rede e nos pontos de extremidade da rede.

**Políticas, regulamentos e padrões de segurança**

As organizações devem ter um conjunto de políticas que definem as atividades permitidas na rede. Elas incluem políticas de negócios, políticas de segurança, políticas BYOD e políticas que garantem que a organização esteja em conformidade com as regulamentações governamentais. As políticas de negócios definem padrões de comportamento correto para a empresa e seus funcionários. As políticas de segurança são usadas para informar os usuários, funcionários e gerentes sobre os requisitos de uma organização para proteger os ativos de tecnologia e informação. Algumas políticas de segurança comuns incluem política de utilização aceitável, política de acesso remoto, política de manutenção de rede e procedimentos de tratamento de incidentes. O objetivo de uma política BYOD (Traga seu próprio dispositivo) é permitir que os funcionários usem seus próprios dispositivos móveis para acessar sistemas, software, redes ou informações da empresa. O BYOD oferece vários benefícios importantes para as empresas, incluindo aumento da produtividade, redução dos custos operacionais e de TI, melhor mobilidade para os funcionários e maior atração quando se trata de contratar e reter funcionários.

**Conformidade com regulamentações e padrões**

Os regulamentos de conformidade definem o que as organizações são responsáveis pelo fornecimento e a responsabilidade caso não cumpram. Os regulamentos de conformidade que uma organização é obrigada a seguir dependem do tipo de organização e dos dados que a organização manipula.

# Introdução

19.0.1

## Por que devo fazer este módulo?

Como você pode restringir o acesso dentro da sua rede? Você permitirá que todos os funcionários tenham acesso a tudo? Ou será projetado para permitir que os usuários acessem com base em seu papel na empresa? Como você pode rastrear o que o usuário acessou e o que ele fez quando estava conectado? Responda a essas perguntas e muito mais aprendendo sobre conceitos de controle de acesso e uso e operação do AAA.

19.0.2

## O que vou aprender neste módulo?

**Título do módulo**: Controle de acesso

**Objetivo do Módulo:** Explique o controle de acesso como um método de proteção de uma rede.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Conceitos de controle de acesso | Explicar como o controle de acesso protege os dados da rede. |
| Uso e operação AAA | Explicar como o AAA é usado para controlar o acesso à rede. |

# Conceitos de controle de acesso

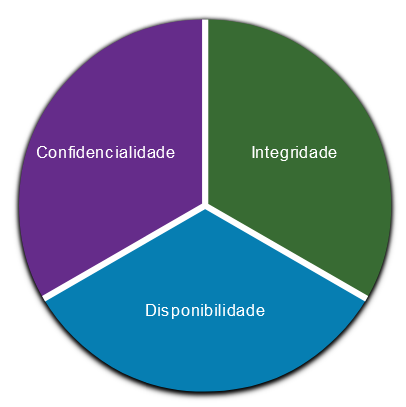
19.1.1

## Segurança das comunicações: CIA

A segurança da informação trata da proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição.

A figura mostra a tríade C I A que consiste em Confidencialidade, Integridade e Disponibilidade.

### Tríade CIA



Como mostrado na figura, a tríade da CIA consiste em três componentes da segurança da informação:

* **Confidencialidade** -Somente indivíduos, entidades ou processos autorizados podem acessar informações confidenciais.
* **Integridade** - refere-se à proteção de dados contra alterações não autorizadas.
* **Disponibilidade** - os usuários autorizados devem ter acesso ininterrupto aos recursos e dados da rede de que necessitam.

Os dados de rede podem ser criptografados (tornados ilegíveis para usuários não autorizados) usando vários aplicativos de criptografia. A conversa entre dois usuários de telefone IP pode ser criptografada. Os arquivos em um computador também podem ser criptografados. Estes são apenas alguns exemplos. A criptografia pode ser usada em praticamente qualquer lugar em que haja comunicação de dados. De fato, a tendência é que toda comunicação seja criptografada.

Como mostrado na figura, a tríade da CIA consiste em três componentes da segurança da informação:

* **Confidencialidade** -Somente indivíduos, entidades ou processos autorizados podem acessar informações confidenciais.
* **Integridade** - refere-se à proteção de dados contra alterações não autorizadas.
* **Disponibilidade** - os usuários autorizados devem ter acesso ininterrupto aos recursos e dados da rede de que necessitam.

Os dados de rede podem ser criptografados (tornados ilegíveis para usuários não autorizados) usando vários aplicativos de criptografia. A conversa entre dois usuários de telefone IP pode ser criptografada. Os arquivos em um computador também podem ser criptografados. Estes são apenas alguns exemplos. A criptografia pode ser usada em praticamente qualquer lugar em que haja comunicação de dados. De fato, a tendência é que toda comunicação seja criptografada.

**Confiança zero para a força de trabalho**

Este pilar consiste em pessoas (por exemplo, funcionários, prestadores de serviços, parceiros e fornecedores) que acessam aplicativos de trabalho usando seus dispositivos pessoais ou gerenciados por empresas. Esse pilar garante que apenas os usuários certos e dispositivos seguros possam acessar aplicativos, independentemente da localização.

**Confiança zero para cargos de trabalho**

Esse pilar está preocupado com aplicativos que estão sendo executados na nuvem, em data centers e outros ambientes virtualizados que interagem uns com os outros. Ele se concentra no acesso seguro quando uma API, um microsserviço ou um contêiner está acessando um banco de dados dentro de um aplicativo.

**Confiança zero para o local de trabalho**

Este pilar se concentra no acesso seguro para qualquer e todos os dispositivos, inclusive na Internet das Coisas (IoT), que se conectam a redes empresariais, como terminais de usuário, servidores físicos e virtuais, impressoras, câmeras, sistemas de AVAC, quiosques, bombas de infusão, sistemas de controle industrial e muito mais.

19.1.3

## Modelos de controle de acesso

Uma organização deve implementar controles de acesso adequados para proteger seus recursos de rede, recursos do sistema de informações e informações.

Um analista de segurança deve entender os diferentes modelos básicos de controle de acesso para ter uma melhor compreensão de como os invasores podem quebrar os controles de acesso.

A tabela lista vários tipos de métodos de controle de acesso.

| **Modelos de controle de acesso** | **Descrição** |
| --- | --- |
| **Controle de acesso discricionário (DAC)** | * Este é o modelo menos restritivo e permite que os usuários controlem o acesso aos seus dados como proprietários desses dados. * O DAC pode usar ACLs ou outros métodos para especificar quais usuários ou grupos de usuários têm acesso às informações. |
| **Controle de acesso obrigatório (MAC)** | * Isso aplica o controle de acesso mais rigoroso e é normalmente usado em aplicações militares ou de missão crítica. * Ele atribui rótulos de nível de segurança às informações e permite que os usuários tenham acesso com base em sua autorização de nível de segurança. |
| **Controle de acesso baseado em funções** | * As decisões de acesso são baseadas nas funções e responsabilidades de um indivíduo dentro da organização. * Diferentes funções recebem privilégios de segurança e indivíduos são atribuídos ao perfil RBAC para a função. * As funções podem incluir diferentes posições, classificações de cargo ou grupos de classificações de emprego. * Também conhecido como um tipo de controle de acesso **não discricionário**. |
| **Controle de acesso baseado em atributos (ABAC)** | O ABAC permite o acesso com base em atributos do objeto (recurso) a ser acessado, o sujeito (usuário) acessando o recurso e fatores ambientais sobre como o objeto deve ser acessado, como a hora do dia. |
| **Controle de acesso baseado em regras (RBAC)** | * A equipe de segurança de rede especifica conjuntos de regras ou condições associadas ao acesso a dados ou sistemas. * Essas regras podem especificar endereços IP permitidos ou negados, ou determinados protocolos e outras condições. * Também conhecido como **RBAC Baseado em Regras.** |
| **Controle de acesso baseado em tempo (TAC)** | TAC Permite o acesso a recursos de rede com base na hora e no dia. |

Outro modelo de controle de acesso é o princípio do privilégio mínimo, que especifica uma abordagem limitada, conforme necessário, para conceder direitos de acesso ao usuário e ao processo a informações e ferramentas específicas. O princípio do privilégio mínimo afirma que os usuários devem receber a quantidade mínima de acesso necessária para desempenhar sua função de trabalho.

Uma exploração comum é conhecida como escalação de privilégios. Nesta exploração, vulnerabilidades em servidores ou sistemas de controle de acesso são exploradas para conceder a um usuário não autorizado, ou processo de software, níveis de privilégio mais altos do que deveriam ter. Depois que o privilégio é concedido, o agente de ameaça pode acessar informações confidenciais ou assumir o controle de um sistema.

Qual modelo de controle de acesso é baseado nas funções e responsabilidades de um indivíduo dentro da organização? Controle de acesso não discricionário

# Uso e operação AAA

19.2.1

## Operação AAA

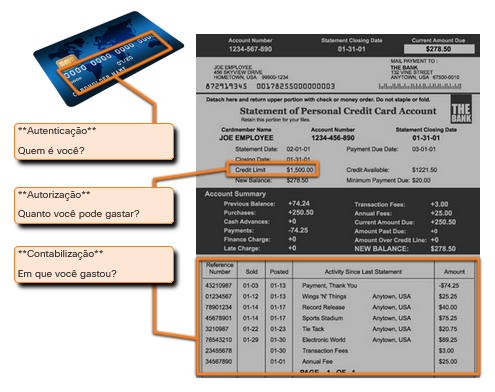
Uma rede deve ser projetada para controlar quem tem permissão para se conectar a ela e o que eles têm permissão para fazer quando estão conectados. Estes requisitos de design são identificados na política de segurança de rede. A política especifica como administradores de rede, usuários corporativos, usuários remotos, parceiros de negócios e clientes acessam recursos de rede. A política de segurança de rede também pode exigir a implementação de um sistema de contabilidade que rastreia quem iniciou sessão e quando e o que fizeram durante a sessão iniciada. Alguns regulamentos de conformidade podem especificar que o acesso deve ser registrado e os logs mantidos por um determinado período de tempo.

O protocolo AAA (Authentication, Authorization and Accounting) fornece a estrutura necessária para habilitar a segurança de acesso escalável.

A tabela lista as três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA.

| **Componente AAA** | **Descrição** |
| --- | --- |
| **Autenticação** | * Os usuários e administradores devem provar quem são. * A autenticação pode ser estabelecida usando combinações de nome de usuário e senha, perguntas e respostas de desafio, tokens e outros métodos. * A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede. |
| **Autorização** | * Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar. * Um exemplo é “O usuário 'aluno' pode acessar o servidor host XYZ usando apenas SSH.” |
| **Accounting** | * O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas. * O accounting rastreia como os recursos de rede são usados. * Um exemplo é “O usuário 'aluno' acessou o servidor host XYZ usando SSH por 15 minutos.“ |

Esse conceito é semelhante ao uso de um cartão de crédito, conforme indicado na figura. O cartão de crédito identifica quem pode utilizá-lo, estipula um limite de uso e mantém o controle dos itens comprados pelo usuário, como mostrado na figura.



19.2.2

## autenticação AAA

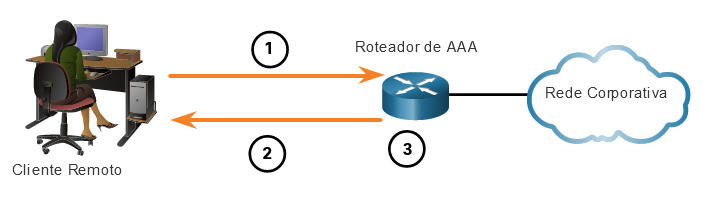
A autenticação AAA pode ser usada para autenticar usuários para o acesso administrativo ou pode ser usada para autenticar usuários para o acesso à rede remota.

A Cisco fornece dois métodos comuns de implementação de serviços AAA.

Autenticação de AAA local

Esse método às vezes é conhecido como autenticação autônoma porque autentica usuários contra nomes de usuário e senhas armazenados localmente, como mostrado na figura. A AAA local é ideal para redes pequenas.

um cliente remoto se conecta a um roteador AAA, é solicitado um nome de usuário e senha, o roteador verifica seu banco de dados local antes de permitir o acesso à rede corporativa

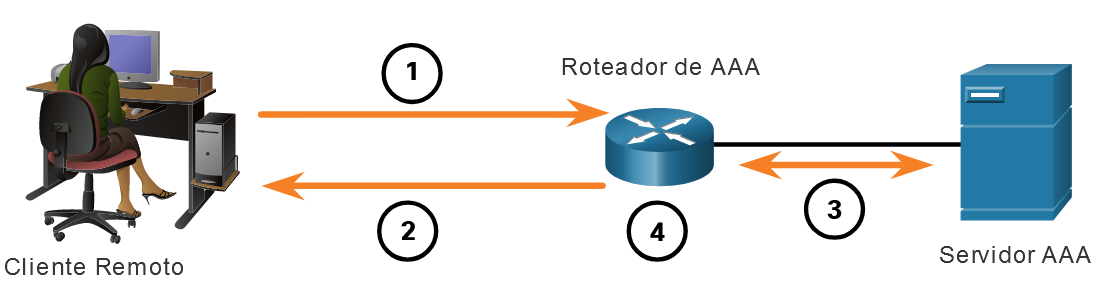


1. O cliente estabelece uma conexão com o roteador.
2. O roteador AAA solicita que o usuário forneça o nome de usuário e a senha.
3. O roteador autentica o nome do usuário e a senha usando o banco de dados local e o usuário obtém o acesso à rede com base nas informações do banco de dados local.

Autenticação de AAA com base em servidor

Esse método se autentica em um servidor AAA central que contém os nomes de usuário e senhas para todos os usuários, conforme mostrado na figura. A autenticação AAA baseada em servidor é apropriada para redes de médio a grande porte.

um cliente remoto se conecta a um roteador AAA, é solicitado a prover um nome de usuário e senha, o roteador autentica as credenciais usando um servidor AAA e o usuário recebe acesso à rede



1. O cliente estabelece uma conexão com o roteador.
2. O roteador AAA solicita que o usuário forneça o nome de usuário e a senha.
3. O roteador autentica o nome do usuário e a senha usando um servidor AAA.
4. O usuário recebe acesso à rede com base nas informações no servidor AAA remoto.

O AAA centralizado é mais escalável e gerenciável do que a autenticação AAA local e, portanto, é a implementação AAA preferida.

Um sistema AAA centralizado pode manter bancos de dados independentemente para autenticação, autorização e contabilidade. Ele pode aproveitar o Active Directory ou o Lightweight Directory Access Protocol (LDAP) para autenticação de usuário e associação de grupo, mantendo seus próprios bancos de dados de autorização e contabilidade.

Os dispositivos se comunicam com o servidor AAA centralizado usando os protocolos RADIUS (Remote Authentication Dial-In User Service) ou Terminal Access Controller Access Control System (TACACS +).

A tabela lista as diferenças entre os dois protocolos.

|  | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| **Funcionalidade** | Ele separa as funções de autenticação, autorização e contabilidade de acordo com a arquitetura AAA. Isso permite a modularidade da implementação do servidor de segurança. | Ele combina autenticação e autorização, mas separa a contabilidade, o que permite menos flexibilidade na implementação do TACACS+ |
| **Padrão** | Principalmente com suporte Cisco | Padrão aberto/RFC |
| **Transporte** | Porta TCP 49 | Portas UDP 1812 e 1813, ou 1645 e 1646 |
| **Protocolo CHAP** | Desafio bidirecional e resposta conforme usado no Challenge Handshake Authentication Protocol (CHAP) | Desafio unidirecional e resposta do servidor de segurança RADIUS para o cliente RADIUS |
| **Confidencialidade** | Criptografa todo o corpo do pacote, mas deixa um cabeçalho TACACS+ padrão. | Criptografa somente a senha no pacote de solicitação de acesso do cliente para o servidor. O restante do pacote é descriptografado, deixando o nome de usuário, os serviços autorizados e a contabilidade desprotegidos. |
| **Personalização** | Fornece autorização de comandos do roteador por usuário ou por grupo | Não tem opção para autorizar comandos de roteador por usuário ou por grupo |
| **Contabilidade** | Limitado | Abrangente |

**Accouting**

* Registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo que o recurso é acessado e quaisquer alterações que foram feitas
* Coleta e relata dados de uso para que possam ser utilizados para fins como auditoria ou faturamento
* Fornece alavancagem contra indivíduos que executam ações mal-intencionados

**Autorização**

* Usa um conjunto criado de atributos que descreve o acesso do usuário à rede
* O que um usuário pode e não pode fazer na rede
* Quais recursos o usuário pode acessar e quais operações o usuário tem permissão para realizar

**Autenticação**

* Estabelecido usando combinações de nome de usuário e senha, perguntas de desafio e resposta, cartões de token e outros métodos
* Os usuários e administradores devem provar que são quem dizem ser
* Uma forma de controlar quem tem permissão para acessar uma rede

# Uso e operação AAA

19.2.1

## Operação AAA

Uma rede deve ser projetada para controlar quem tem permissão para se conectar a ela e o que eles têm permissão para fazer quando estão conectados. Estes requisitos de design são identificados na política de segurança de rede. A política especifica como administradores de rede, usuários corporativos, usuários remotos, parceiros de negócios e clientes acessam recursos de rede. A política de segurança de rede também pode exigir a implementação de um sistema de contabilidade que rastreia quem iniciou sessão e quando e o que fizeram durante a sessão iniciada. Alguns regulamentos de conformidade podem especificar que o acesso deve ser registrado e os logs mantidos por um determinado período de tempo.

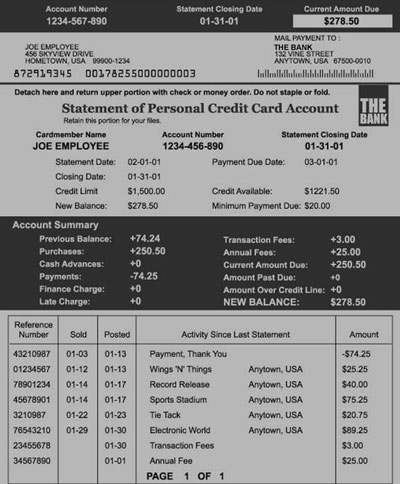
O protocolo AAA (Authentication, Authorization and Accounting) fornece a estrutura necessária para habilitar a segurança de acesso escalável.

A tabela lista as três funções de segurança independentes fornecidas pela estrutura arquitetônica AAA.

| **Componente AAA** | **Descrição** |
| --- | --- |
| **Autenticação** | * Os usuários e administradores devem provar quem são. * A autenticação pode ser estabelecida usando combinações de nome de usuário e senha, perguntas e respostas de desafio, tokens e outros métodos. * A autenticação AAA fornece uma maneira centralizada de controlar o acesso à rede. |
| **Autorização** | * Após a autenticação do usuário, os serviços de autorização determinam quais recursos o usuário pode acessar e quais operações ele tem permissão para executar. * Um exemplo é “O usuário 'aluno' pode acessar o servidor host XYZ usando apenas SSH.” |
| **Accounting** | * O accounting registra o que o usuário faz, incluindo o que é acessado, a quantidade de tempo em que o recurso é acessado e todas as alterações efetuadas. * O accounting rastreia como os recursos de rede são usados. * Um exemplo é “O usuário 'aluno' acessou o servidor host XYZ usando SSH por 15 minutos.“ |

Esse conceito é semelhante ao uso de um cartão de crédito, conforme indicado na figura. O cartão de crédito identifica quem pode utilizá-lo, estipula um limite de uso e mantém o controle dos itens comprados pelo usuário, como mostrado na figura.

A figura mostra um cartão de crédito ao lado de um extrato do cartão de crédito. Há um retângulo ao redor dos números no cartão de crédito com o texto Autenticação Quem é você? Um segundo retângulo gira em torno do limite de crédito no extrato do cartão de crédito com o texto Autorização. Quanto você pode gastar? Um terceiro retângulo está ao redor da parte da transação do resumo do cartão de crédito com o texto Contabilidade. O que você gastou nele?



\*\*Autenticação\*\*  
  
Quem é você?\*\*Autorização\*\*  
  
Quanto você pode gastar?\*\*Contabilização\*\*  
  
Em que você gastou?

19.2.2

## autenticação AAA

A autenticação AAA pode ser usada para autenticar usuários para o acesso administrativo ou pode ser usada para autenticar usuários para o acesso à rede remota.

A Cisco fornece dois métodos comuns de implementação de serviços AAA.

Esse método se autentica em um servidor AAA central que contém os nomes de usuário e senhas para todos os usuários, conforme mostrado na figura. A autenticação AAA baseada em servidor é apropriada para redes de médio a grande porte.

um cliente remoto se conecta a um roteador AAA, é solicitado a prover um nome de usuário e senha, o roteador autentica as credenciais usando um servidor AAA e o usuário recebe acesso à rede

1 2 3

4

Cliente RemotoRoteador de AAAServidor AAA

1. O cliente estabelece uma conexão com o roteador.
2. O roteador AAA solicita que o usuário forneça o nome de usuário e a senha.
3. O roteador autentica o nome do usuário e a senha usando um servidor AAA.
4. O usuário recebe acesso à rede com base nas informações no servidor AAA remoto.

O AAA centralizado é mais escalável e gerenciável do que a autenticação AAA local e, portanto, é a implementação AAA preferida.

Um sistema AAA centralizado pode manter bancos de dados independentemente para autenticação, autorização e contabilidade. Ele pode aproveitar o Active Directory ou o Lightweight Directory Access Protocol (LDAP) para autenticação de usuário e associação de grupo, mantendo seus próprios bancos de dados de autorização e contabilidade.

Os dispositivos se comunicam com o servidor AAA centralizado usando os protocolos RADIUS (Remote Authentication Dial-In User Service) ou Terminal Access Controller Access Control System (TACACS +).

A tabela lista as diferenças entre os dois protocolos.

|  | **TACACS+** | **RADIUS** |
| --- | --- | --- |
| **Funcionalidade** | Ele separa as funções de autenticação, autorização e contabilidade de acordo com a arquitetura AAA. Isso permite a modularidade da implementação do servidor de segurança. | Ele combina autenticação e autorização, mas separa a contabilidade, o que permite menos flexibilidade na implementação do TACACS+ |
| **Padrão** | Principalmente com suporte Cisco | Padrão aberto/RFC |
| **Transporte** | Porta TCP 49 | Portas UDP 1812 e 1813, ou 1645 e 1646 |
| **Protocolo CHAP** | Desafio bidirecional e resposta conforme usado no Challenge Handshake Authentication Protocol (CHAP) | Desafio unidirecional e resposta do servidor de segurança RADIUS para o cliente RADIUS |
| **Confidencialidade** | Criptografa todo o corpo do pacote, mas deixa um cabeçalho TACACS+ padrão. | Criptografa somente a senha no pacote de solicitação de acesso do cliente para o servidor. O restante do pacote é descriptografado, deixando o nome de usuário, os serviços autorizados e a contabilidade desprotegidos. |
| **Personalização** | Fornece autorização de comandos do roteador por usuário ou por grupo | Não tem opção para autorizar comandos de roteador por usuário ou por grupo |
| **Contabilidade** | Limitado | Abrangente |

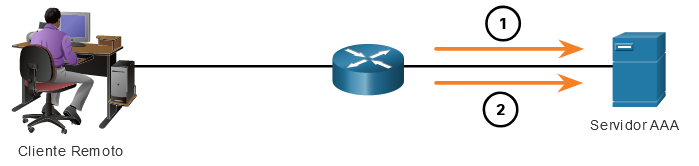
19.2.3

## Registros de Contabilidade AAA

O AAA centralizado também permite o uso do método de contabilidade. Os registros contábeis de todos os dispositivos são enviados para repositórios centralizados, o que simplifica a auditoria das ações do usuário.

AAA Accounting coleta e relata dados de uso em registros AAA. Esses logs são úteis para auditoria de segurança. Os dados coletados podem incluir os horários de conexão inicial e final, comandos executados, número de pacotes e número de bytes.

Um uso amplamente difundido da contabilidade é combiná-lo com a autenticação AAA. Isso ajuda a gerenciar o acesso a dispositivos de interrede pela equipe administrativa da rede. Contabilidade fornece mais segurança do que apenas autenticação. Os servidores AAA mantêm um registro detalhado de exatamente o que o usuário autenticado faz no dispositivo, conforme mostrado na figura. Isso inclui todos os comandos EXEC e de configuração emitidos pelo usuário. O log contém vários campos de dados, incluindo o nome de usuário, a data e a hora, e o comando real que foi inserido pelo usuário. Esta informação é útil na solução de problemas de dispositivos. Ele também fornece evidências contra indivíduos que realizam ações maliciosas.



1. Quando um usuário realiza autenticação, o processo de contabilização AAA gera uma mensagem inicial para iniciar a contabilização.
2. Quando o usuário termina, uma mensagem de parada é inserida e o processo contábil finaliza.

A tabela exibe os vários tipos de informações contábeis que podem ser coletadas.

| **Tipo de informação contábil** | **Descrição** |
| --- | --- |
| **Contabilidade de Rede** | A contabilidade de rede captura informações para todas as sessões PPP (Point-to-Point Protocol), incluindo contagens de pacotes e bytes. |
| **Contabilidade de Conexão** | Contabilidade de conexão captura informações sobre todas as conexões de saída feitas a partir do cliente AAA, como por SSH. |
| **Contabilidade EXEC** | A contabilidade EXEC captura informações sobre sessões de terminal EXEC do usuário (shells do usuário) no servidor de acesso à rede, incluindo nome de usuário, data, horas de início e parada e o endereço IP do servidor de acesso. |
| **Contabilidade do Sistema** | A contabilidade do sistema captura informações sobre todos os eventos no nível do sistema (por exemplo, quando o sistema é reinicializado ou quando a contabilidade é ativada ou desativada). |
| **Contabilidade de Comando** | A contabilidade de comandos captura informações sobre os comandos do shell EXEC para um nível de privilégio especificado, bem como a data e hora em que cada comando foi executado e o usuário que o executou. |
| **Contabilidade de Recursos** | A implementação Cisco da contabilidade AAA captura o suporte a registros “start” e “stop” para conexões que passaram pela autenticação do usuário. O recurso adicional de gerar registros “stop” para conexões que não conseguem se autenticar como parte da autenticação do usuário também é suportado. Esses registros são necessários para que os usuários que empregam registros contábeis gerenciem e monitorem suas redes. |

# Resumo de controle de acesso

19.3.1

## O que aprendi neste módulo?

**Controle de acesso**

A tríade da CIA consiste nos três componentes principais da segurança da informação: confidencialidade, integridade e disponibilidade (avaiability). Os dados de rede podem ser criptografados (tornados ilegíveis para usuários não autorizados) usando uma variedade de aplicativos de criptografia. A tendência é que todos os dados sejam criptografados. Zero Trust é uma abordagem abrangente para proteger todo o acesso em redes, aplicações e ambientes. O princípio da confiança zero é “nunca confiar, sempre verificar”. Tradicionalmente, o perímetro da rede, ou borda, era o limite entre dentro e fora, ou confiável e não confiável. Numa abordagem de confiança zero, qualquer local em que seja necessária uma decisão de controle de acesso deve ser considerado um perímetro. Isso significa que, embora um usuário ou outra entidade possa ter passado com êxito o controle de acesso anteriormente, eles não são confiáveis para acessar outra área ou recurso até que sejam autenticados. Os pilares da confiança são a confiança zero para a força de trabalho, a confiança zero para cargas de trabalho e a confiança zero para o local de trabalho. Os métodos de controle de acesso incluem controle de acesso discricionário (DAC), controle de acesso obrigatório (MAC), controle de acesso baseado em função (RBAC), controle baseado em atributos (ABAC), acesso baseado em regras (RBAC) e controle de acesso baseado em tempo (TAC). Uma exploração comum é conhecida como escalação de privilégios. Nesta exploração, vulnerabilidades em servidores ou sistemas de controle de acesso são exploradas para conceder acesso a um usuário não autorizado ou processo de software.

**Uso e operação AAA**

Uma rede deve ser projetada para controlar quem tem permissão para se conectar a ela e o que eles têm permissão para fazer quando estão conectados. Estes requisitos de design são identificados na política de segurança de rede. A política também pode exigir a implementação de um sistema de contabilidade que rastreia quem logou e quando e o que fizeram quando estavam logados. Os sistemas AAA (Authentication, Authorization and Accounting) fornecem a estrutura necessária para permitir uma segurança escalável. A autenticação AAA pode ser usada para autenticar usuários para acesso local ou pode ser usada para autenticar usuários para acesso remoto à rede. A Cisco fornece dois métodos comuns de implementação de serviços AAA: Autenticação AAA local e Autenticação AAA baseada em servidor. O AAA centralizado é mais escalável e gerenciável do que o AAA local e é a implementação AAA preferida. Um sistema AAA centralizado pode aproveitar o Active Directory ou o Lightweight Directory Access Protocol (LDAP) para autenticação de usuário e associação de grupo, mantendo seus próprios bancos de dados de autorização e contabilidade. Os dispositivos se comunicam com o servidor AAA centralizado usando os protocolos RADIUS (Remote Authentication Dial-In User Service) ou Terminal Access Controller Access Control System (TACACS +). O AAA centralizado também permite o uso do método de contabilidade. AAA Accounting coleta e relata dados de uso em registros AAA. Vários tipos de informações contábeis que podem ser coletadas são contabilidade de rede, contabilidade de conexão, contabilidade EXEC, contabilidade de sistema, contabilidade de comando e contabilidade de recursos.

# Introdução

20.0.1

## Por que devo fazer este módulo?

É importante que você fique por dentro das informações mais recentes quando se trata de segurança cibernética. Como você faz isso? Leia este módulo para saber mais sobre fontes de informações e serviços de inteligência contra ameaças.

20.0.2

## O que vou aprender neste módulo?

**Título do módulo**: Inteligência de Ameaças

**Objetivos do Módulo:.** Usar várias fontes de inteligência para localizar as ameaças à segurança atuais.

| **Título do Tópico** | **Objetivo do Tópico** |
| --- | --- |
| Fontes de informação | Descrever as fontes de informações usadas para comunicar ameaças emergentes à segurança de rede. |
| Serviços de inteligência de ameaças | Descrever vários serviços de inteligência de ameaças. |

# Fontes de informação

20.1.1

## Comunidades de Inteligência de Rede

Para proteger uma rede com eficácia, os profissionais de segurança devem se manter informados sobre as ameaças e vulnerabilidades conforme elas evoluem. Existem muitas organizações de segurança que fornecem inteligência de rede. Eles fornecem recursos, workshops e conferências para ajudar os profissionais de segurança. Essas organizações geralmente possuem as informações mais recentes sobre ameaças e vulnerabilidades.

A tabela lista algumas organizações importantes de segurança de rede.

| **Empresa** | **Descrição** |
| --- | --- |
| SANS | Os recursos do SysAdmin, Audit, Network, Security (SANS) Institute são amplamente gratuitos mediante solicitação e incluem:   * O Internet Storm Center - o popular sistema de alerta antecipado da internet * NewsBites, o resumo semanal de artigos de notícias sobre segurança de computadores. * @RISK, o resumo semanal de vetores de ataque recém-descobertos, vulnerabilidades com exploits ativos e explicações de como os ataques recentes funcionaram * Alertas de segurança rápidos * Sala de Leitura - mais de 1.200 trabalhos de pesquisa originais premiados. * O SANS também desenvolve cursos de segurança. |
| Mitre | A Mitre Corporation mantém uma lista de vulnerabilidades e exposições comuns (CVE) usadas por empresas de segurança famosas. |
| FIRST | O Forum of Incident Response and Security Teams (FIRST) é uma empresa de segurança que une uma variedade de equipes de resposta a incidentes de segurança do computador provenientes de organizações governamentais, comerciais e educacionais, com o objetivo de promover a cooperação e a coordenação de compartilhamento de informações, prevenção de incidente e reação rápida. |
| SecurityNewsWire | Um portal de notícias de segurança que agrega as últimas notícias relacionadas a alertas, explorações e vulnerabilidades. |
| (ISC)2 | O Consórcio Internacional de Certificação de Segurança de Sistemas de Informação (ISC2) fornece produtos educacionais neutros de fornecedores e serviços de carreira para mais de 75.000 profissionais da indústria em mais de 135 países. |
| CIS | O Center for Internet Security (CIS) é um ponto focal para prevenção, proteção, resposta e recuperação de ameaças cibernéticas para governos estaduais, locais, tribais e territoriais (SLTT) por meio do Centro de Análise e Compartilhamento de Informações Multiestaduais (MS-ISAC ) O MS-ISAC oferece alertas e alertas de ameaças cibernéticas 24 horas por dia, 7 dias por semana, identificação de vulnerabilidades e mitigação e resposta a incidentes. |

To remain effective, a network security professional must:

* **Fique por dentro das ameaças mais recentes** – Isso inclui a assinatura de feeds em tempo real sobre ameaças, leitura rotineira de sites relacionados à segurança, acompanhamento de blogs e podcasts de segurança e muito mais.
* **Continue a atualizar as habilidades** – Isso inclui participar de treinamentos, workshops e conferências relacionados à segurança.

**Nota**: A segurança de rede tem uma curva de aprendizado muito acentuada e exige um compromisso com o desenvolvimento profissional contínuo.

20.1.2

**Relatórios de Segurança Cibernética da Cisco**

Os recursos para ajudar os profissionais de segurança a se manterem atualizados sobre as ameaças mais recentes são o Cisco Annual Cybersecurity Report e o Mid-Year Cybersecurity Report. Esses relatórios fornecem uma atualização sobre o estado de preparação da segurança, análise especializada das principais vulnerabilidades, fatores por trás da explosão de ataques usando adware, spam e muito mais.

Os analistas de segurança cibernética devem assinar e ler esses relatórios para saber como os agentes de ameaças estão direcionando suas redes e o que pode ser feito para mitigar esses ataques.

Pesquise na Internet para localizar e fazer download dos Cisco Cybersecurity Reports do site da Cisco.

20.1.3

**Blogs e podcasts de segurança**

Outro método para se manter atualizado sobre as ameaças mais recentes é ler blogs e ouvir podcasts. Blogs e podcasts também fornecem conselhos, pesquisas e técnicas de mitigação recomendadas.

Existem vários blogs e podcasts de segurança disponíveis que um analista de segurança cibernética deve seguir para aprender sobre as ameaças, vulnerabilidades e explorações mais recentes.

A Cisco fornece blogs sobre tópicos relacionados à segurança de vários especialistas do setor e do Cisco Talos Group. Pesquise blogs de segurança da Cisco para localizá-los. Você também pode se inscrever para receber notificações de novos blogs por e-mail. O Cisco Talos também oferece uma série de mais de 80 podcasts que podem ser reproduzidos da Internet ou baixados para o dispositivo de sua escolha.

# Serviços de inteligência de ameaças

20.2.1

## Cisco Talos

Os serviços de inteligência contra ameaças permitem a troca de informações sobre ameaças, como vulnerabilidades, indicadores de comprometimento (IOC) e técnicas de mitigação. Essas informações não são compartilhadas apenas com o pessoal, mas também com sistemas de segurança. À medida que as ameaças surgem, os serviços de inteligência de ameaças criam e distribuem regras de firewall e IOCs para os dispositivos que assinaram o serviço.

Um desses serviços é o Cisco Talos Threat Intelligence Group, mostrado na figura. Talos é uma das maiores equipes de inteligência de ameaças comerciais do mundo e é composta por pesquisadores, analistas e engenheiros de classe mundial. O objetivo do Talos é ajudar a proteger os usuários, dados e infraestrutura da empresa de adversários ativos. A equipe do Talos coleta informações sobre ameaças ativas, existentes e emergentes. O Talos então fornece proteção abrangente contra esses ataques e malware aos seus assinantes.

﻿Os produtos da Cisco Security podem usar a inteligência de ameaças Talos em tempo real para fornecer soluções de segurança rápidas e eficazes. O Cisco Talos também fornece software, serviços, recursos e dados gratuitos. Talos mantém os conjuntos de regras de detecção de incidentes de segurança para as ferramentas de segurança de rede Snort.org, ClamAV e SpamCop.

20.2.2

**FireEye**

FireEye é outra empresa de segurança que oferece serviços para ajudar as empresas a proteger suas redes. A FireEye usa uma abordagem de três frentes combinando inteligência de segurança, experiência em segurança e tecnologia.

A FireEye oferece SIEM e SOAR com a Helix Security Platform, que usa análise comportamental e detecção avançada de ameaças e é suportada pela rede mundial de inteligência contra ameaças da FireEye Mandiant. Helix é uma plataforma de operações de segurança hospedada em nuvem que combina diversas ferramentas de segurança e inteligência de ameaças em uma única plataforma.

O FireEye Security System bloqueia ataques em vetores de ameaças da Web e de e-mail e malware latente que reside em compartilhamentos de arquivos. Ele pode bloquear malware avançado que facilmente ignora as defesas tradicionais baseadas em assinaturas e compromete a maioria das redes empresariais. Ele aborda todos os estágios de um ciclo de vida de ataque com um mecanismo sem assinatura que utiliza análise de ataque stateful para detectar ameaças de dia zero.

Pesquise FireEye na Internet e veja os recursos de inteligência de segurança que ela oferece.

20.2.3

**Compartilhamento automatizado de indicadores**

O Departamento de Segurança Interna dos EUA (DHS) oferece um serviço gratuito chamado Compartilhamento Automatizado de Indicador (AIS). O AIS permite a troca em tempo real de indicadores de ameaças cibernéticas (por exemplo, endereços IP maliciosos, o endereço do remetente de um e-mail de phishing, etc.) entre o Governo Federal dos EUA e o setor privado.

O AIS cria um ecossistema onde, assim que uma ameaça é reconhecida, ela é imediatamente compartilhada com a comunidade para ajudá-la a proteger suas redes dessa ameaça específica.

Pesquise na Internet pelo serviço “DHS AIS” para saber mais.

20.2.4

**Banco de Dados de Vulnerabilidades e Exposições Comuns (CVE)**

O governo dos Estados Unidos patrocinou uma MITER Corporation para criar e manter um catálogo de segurança de segurança chamadas Vulnerabilidades e Exposições Comuns (CVE). O CVE serve como um dicionário de nomes comuns (ou seja, identificadores CVE) para vulnerabilidades de segurança cibernética publicamente conhecidas.

A MITRE Corporation define identificadores CVE exclusivos para vulnerabilidades de segurança da informação publicamente conhecidas para facilitar o compartilhamento de dados.

Pesquise na internet por “Mitre Corporation” e veja informações sobre CVE

20.2.5

**Padrões de comunicação de inteligência de ameaças**

Organizações e profissionais de rede devem compartilhar informações para aumentar o conhecimento sobre os atores da ameaça e os ativos que desejam acessar. Vários padrões abertos de compartilhamento de inteligência evoluíram para permitir a comunicação em várias plataformas de rede. Esses padrões permitem a troca de inteligência contra ameaças cibernéticas (CTI) em um formato automatizado, consistente e legível por máquina.

Três padrões comuns de compartilhamento de informações sobre ameaças incluem o seguinte:

* **Expressão de Informações Estruturadas de Ameaças (STIX)** - Este é um conjunto de especificações para a troca de informações sobre ameaças cibernéticas entre organizações. O padrão Cyber Observable Expression (CybOX) foi incorporado ao STIX.
* **Troca Confiável e Automatizada de Informações de Indicadores (TAXII)** – Esta é a especificação de um protocolo da camada de aplicativo que permite a comunicação de CTI sobre HTTPS. TAXII foi projetado para suportar STIX.
* **CybOX** - Este é um conjunto de esquemas padronizados para especificar, capturar, caracterizar e comunicar eventos e propriedades de operações de rede que oferecem suporte a muitas funções de segurança cibernética.

Esses padrões abertos fornecem as especificações que auxiliam na troca automatizada de informações de inteligência de ameaças cibernéticas em um formato padronizado. Pesquise na Internet para saber mais sobre STIX, TAXII e CybOX.

A Malware Information Sharing Platform (MISP) é uma plataforma de código aberto para compartilhar indicadores de comprometimento para ameaças recém-descobertas. O MISP é apoiado pela União Europeia e usado por mais de 6.000 organizações em todo o mundo. O MISP permite o compartilhamento automatizado de IOCs entre pessoas e máquinas usando STIX e outros formatos de exportação.

20.2.6

**Plataformas de inteligência de ameaças**

Como vimos, existem muitas fontes de informações de inteligência de ameaças, cada uma das quais pode ter seu próprio formato de dados. Acessar e usar várias fontes de inteligência de ameaças pode consumir muito tempo. Para ajudar o pessoal de segurança cibernética a fazer o melhor uso da inteligência de ameaças, as plataformas de inteligência de ameaças (TIP) foram desenvolvidas.

Uma plataforma de inteligência de ameaças centraliza a coleta de dados de ameaças de várias fontes e formatos de dados. Existem três tipos principais de dados de inteligência de ameaças. O primeiro são indicadores de compromisso (IOC). O segundo são ferramentas, técnicas e procedimentos (TTP). A terceira são as informações de reputação sobre destinos ou domínios da Internet. O volume de dados de inteligência de ameaças pode ser esmagador, portanto, a plataforma de inteligência de ameaças foi projetada para agregar os dados em um só lugar e - o mais importante - apresentar os dados em um formato compreensível e utilizável.

As organizações podem contribuir com informações sobre ameaças compartilhando seus dados de intrusão pela Internet, geralmente por meio de automação. Muitos serviços de inteligência de ameaças usam dados de assinantes para aprimorar seus produtos e se manter atualizados com o cenário de ameaças em constante mudança.

Honeypots são redes simuladas ou servidores projetados para atrair atacantes. As informações relacionadas ao ataque coletadas de honeypots podem então ser compartilhadas com os assinantes da plataforma de inteligência de ameaças. No entanto, hospedar honeypots pode ser um risco. Basear um honeypot na nuvem isola o honeypot das redes de produção. Essa abordagem é uma alternativa atraente para coletar informações sobre ameaças.

# Resumo de Inteligência de Ameaças

20.3.1

## O que aprendi neste módulo?

**Comunidades de Inteligência de Rede**

Existem muitas organizações que fornecem inteligência de rede. As organizações de segurança de rede incluem SANS, Mitre, FIRST, SecurityNewsWire, (ISC) 2 e CIS. Você deve se manter atualizado sobre as ameaças mais recentes e continuar a atualizar suas habilidades. O Cisco Annual Cybersecurity Report e o Mid-Year Cybersecurity Report são ótimos recursos para usar. Também é útil ler blogs e ouvir podcasts.

**Serviços de inteligência de ameaças**

Os serviços de inteligência contra ameaças permitem a troca de informações sobre ameaças, como vulnerabilidades, indicadores de comprometimento (IOC) e técnicas de mitigação. Essas informações não são compartilhadas apenas com o pessoal, mas também com sistemas de segurança. À medida que as ameaças surgem, os serviços de inteligência de ameaças criam e distribuem regras de firewall e IOCs para os dispositivos que assinaram o serviço. Um desses serviços é o Cisco Talos Threat Intelligence Group. FireEye é outra empresa de segurança que oferece serviços para ajudar as empresas a proteger suas redes. A FireEye usa uma abordagem de três frentes combinando inteligência de segurança, experiência em segurança e tecnologia. A FireEye oferece SIEM e SOAR com a Helix Security Platform, que usa análise comportamental e detecção avançada de ameaças, com suporte da rede mundial de inteligência contra ameaças da FireEye Mandiant. O Departamento de Segurança Interna dos EUA (DHS) oferece um serviço gratuito chamado Automated Indicator Sharing (AIS). O AIS permite a troca em tempo real de indicadores de ameaças cibernéticas entre o Governo Federal dos EUA e o setor privado. O governo dos Estados Unidos patrocinou a MITRE Corporation para criar e manter um catálogo de ameaças de segurança conhecidas chamadas Common Vulnerabilities and Exposure (CVE). Três padrões comuns de compartilhamento de informações sobre ameaças incluem STIX (Structured Threat Information Expression), Trusted Automated Exchange of Indicator Information (TAXII) e CyBox. Esses padrões abertos fornecem as especificações que auxiliam na troca automatizada de informações de inteligência de ameaças cibernéticas em um formato padrão.

Qual é o serviço gratuito oferecido pelo Departamento de Segurança Interna dos EUA?

AIS

O que é uma equipe de inteligência de ameaças líder mundial com o objetivo de ajudar a proteger os usuários, dados e infraestrutura corporativos de adversários ativos?

Talos

Qual plataforma de operações de segurança integra e aprimora uma variedade de ferramentas de segurança e inteligência contra ameaças?

FireEye Helix

Quais são as três especificações de compartilhamento de informações de inteligência de ameaças?

STIX

TAXII

CyberOX