



Módulo 18: Compreendendo a defesa



CyberOps Associate v1.0

Prof. Clemilson Oliveira

clemilson.oliveira@edu.sc.senai.br



Objetivos do 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 Defesa em profundidade é usada para proteger as redes.
Políticas, regulamentos e padrões de segurança	Explicar as políticas, os regulamentos e os padrões de segurança.

18.1 Defesa em profundidade

ativos de defesa, vulnerabilidades e 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 ator de ameaça.
 - **Ameaças**- Qualquer perigo potencial para um ativo.

Noções básicas sobre OS ativos

- A coleta de todos os dispositivos e informações de propriedade ou gerenciadas pela organização são os ativos.
- Estes activos devem ser inventariados e avaliados quanto ao nível de protecção 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. Cada um desses ativos pode atrair diferentes atores de ameaças que têm diferentes níveis de habilidade e motivações.

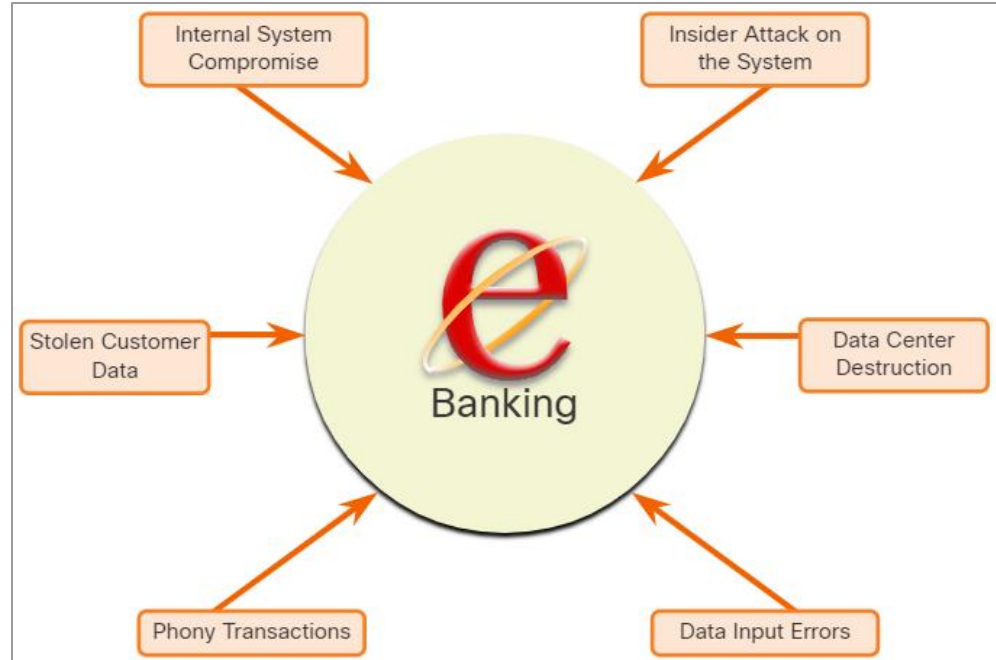
Identificar Vulnerabilidades

- 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?

Identificar Vulnerabilidades

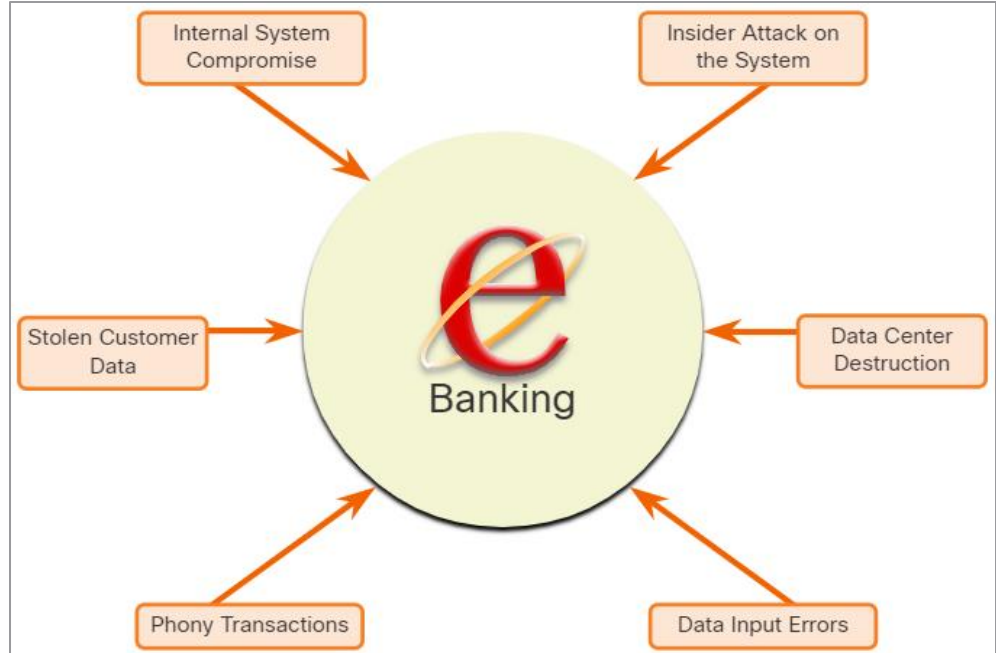
A identificação de ameaças para um sistema de e-banking incluiria:

- **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.



Identificar Vulnerabilidades (Cont.)

- **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.
- **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 usados, bem como das diferentes vulnerabilidades desse aplicativo e hardware. Isso requer uma quantidade significativa de pesquisa por parte do administrador de rede.

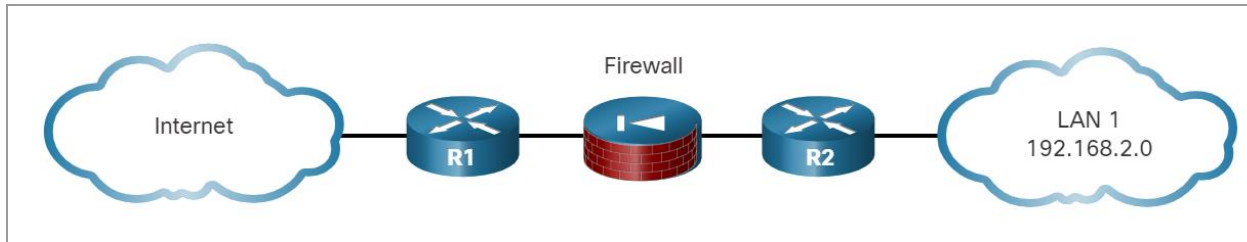


identificar ameaças

- 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.
- Nessa abordagem, um roteador primeiro faz a triagem do tráfego antes de encaminhá-lo para um appliance de firewall dedicado, por exemplo, o Cisco ASA.
- Os roteadores e firewalls não são os únicos dispositivos que são usados em uma abordagem de defesa em profundidade.
- 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 em profundidade, 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.

Identificar Ameaças (Cont.)

- 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** - Uma 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 das redes não confiáveis para a rede confiável, ao mesmo tempo em que permite que os usuários internos estabeleçam conexões bidirecionais com as redes não confiáveis.
 - **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.

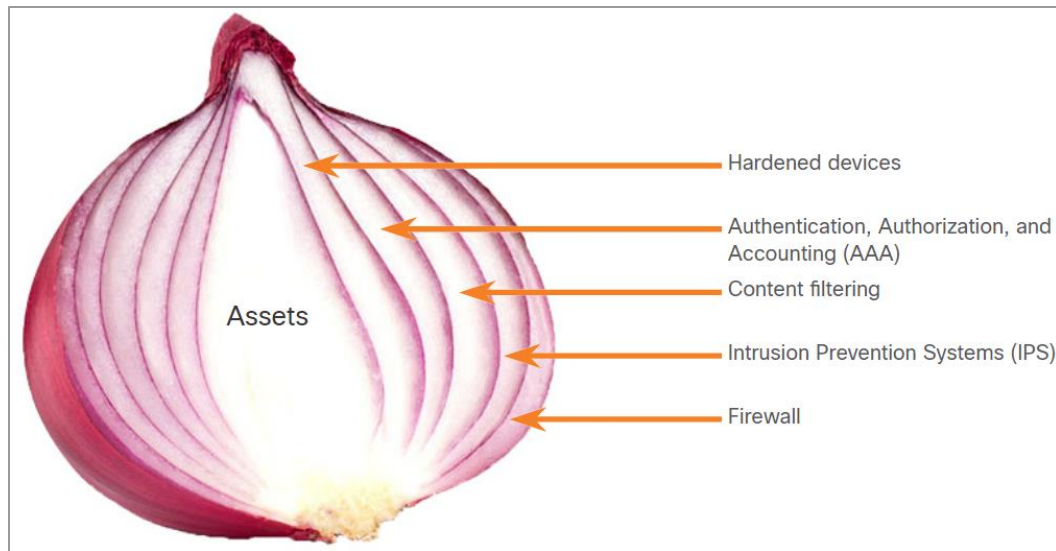


a Defesa, a Security Onion e Security Artichoke

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

Security Onion

- Uma analogia comum usada para descrever uma abordagem de defesa em profundidade é chamada de “The Security Onion”
- 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.

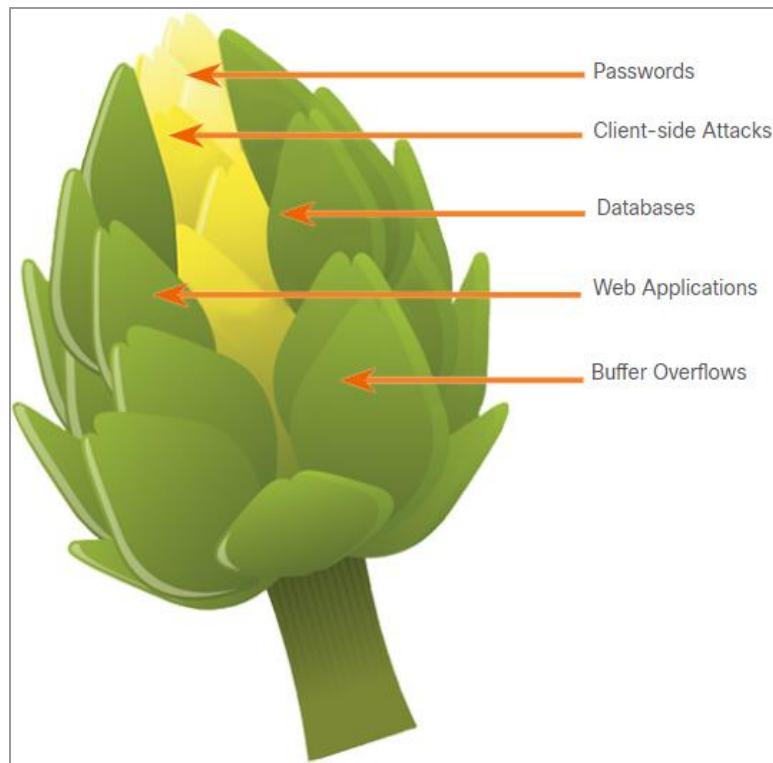


Observação: A Security Onion descrita nesta página é uma forma de visualizar a defesa em profundidade. Isso não deve ser confundido com o conjunto Security Onion de ferramentas de segurança de rede.

a defesa A Security Onion e Security Artichoke (Cont.)

Security Artichoke

- A evolução das redes sem fronteiras mudou a analogia com a “Security Artichoke”, 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 “artichoke leaves.” (folhas de alcachofra)
- O bônus é que cada “folha” da rede pode revelar dados confidenciais que não estão bem protegidos.
- Para chegar ao coração da alcachofra, o hacker arranca a armadura de segurança ao longo do perímetro.
- Embora os sistemas voltados para a Internet estejam muito bem protegidos, os hackers persistentes encontram uma lacuna nesse exterior hard-core através do qual eles podem entrar.



18.2 Políticas de segurança, regulamentos e padrões

Business Policies

- 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.

Políticas de Segurança, Regulamentos e Políticas de Negócios de Padrões (Cont.)

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

Política	Descrição
Políticas da empresa	<ul style="list-style-type: none">• Estabelece as regras de conduta e as responsabilidades dos trabalhadores e dos empregadores.• Protege 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.• É um documento em constante evolução com base nas mudanças no cenário de ameaças, vulnerabilidades e requisitos de negócios e funcionários.

Política de Segurança

- 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 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
- 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.

Política de segurança (Cont.)

A tabela a seguir lista as diretivas que podem ser incluídas em uma diretiva de segurança:

Política	Descrição
Política de identificação e autenticação	Ele especifica pessoas autorizadas que podem ter acesso a recursos de rede e procedimentos de verificação de identidade.
Políticas de senha	Isso garante que as senhas atendam aos requisitos mínimos e sejam alteradas regularmente.
Política de uso aceitável (AUP)	Ele identifica os aplicativos de rede e os usos aceitáveis para a organização. Também podem identificar as ramificações, se esta política for violada.
Política de acesso remoto	Ele identifica como os usuários remotos podem acessar uma rede e o que é acessível por meio de conectividade remota.
Políticas de Manutenção de Rede	Ele especifica os sistemas operacionais do dispositivo de rede e os procedimentos de atualização do aplicativo do usuário final.
Procedimentos de tratamento de incidentes	Descrevem como os incidentes de segurança são tratados.

Políticas de BYOD

- O BYOD (Traga seu próprio dispositivo) permite que os funcionários usem seus próprios dispositivos móveis para acessar sistemas, software, redes ou informações da empresa.
- Fornece benefícios importantes para as empresas, incluindo aumento da produtividade, custos reduzidos, melhor mobilidade para os funcionários, etc. Esses benefícios também trazem um risco de segurança maior, pois o BYOD pode levar a violações de dados e maior responsabilidade para a organização.
- Portanto, uma política de segurança BYOD deve ser desenvolvida para realizar o seguinte:
 - Especificar os objetivos do programa BYOD
 - Identificar quais funcionários podem trazer seus próprios dispositivos
 - Identificar 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
 - Identificar quais regulamentos devem ser cumpridos ao usar dispositivos de funcionários
 - Identificar proteções a serem implementadas se um dispositivo for comprometido

Políticas, regulamentos e padrões de segurança e Políticas de BYOD (Cont.)

A tabela a seguir 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.

Regulamentação e conformidade com 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.

18.3 Resumo das noções básicas de defesa

o resumo da defesa O que aprendi neste módulo?

- 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.
- 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 em profundidade para identificar ameaças e proteger ativos vulneráveis.
- As organizações devem ter um conjunto de políticas que definem as atividades permitidas na rede.
- As políticas de negócios definem padrões de comportamento correto para a empresa e seus funcionários.

o resumo da defesa O que aprendi neste módulo? (Continuação)

- 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.
- 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.
- Os regulamentos de conformidade que uma organização é obrigada a seguir dependem do tipo de organização e dos dados que a organização trata.

