Módulo 2 - Aulas 3 e 4

Módulo 2: Ameaças, malwares e controles

Aula 3: Categorias de controle de segurança

Objetivos

- [x] Compreender as categorias de controle de segurança.
- [x] Identificar os tipos funcionais de controle de segurança.
- [x] Reconhecer a importância de implementar os controles de segurança.

Conceitos

- [x] Controle de segurança técnico, operacional e gerencial.
- [x] Controle de segurança preventivo, detectivo, corretivo.
- [x] Controles de segurança físicos, dissuasor e de compensação.

Introdução

Bem-vindos à aula sobre categorias de controle de segurança. Nesta aula, vamos explorar os princípios fundamentais que sustentam a segurança da informação e como as organizações se esforçam para proteger seus ativos, dados e operações críticas. A segurança da informação é um dos pilares essenciais em um cenário onde ameaças cibernéticas evoluem constantemente. Entender e implementar estratégias de controle de segurança é crucial.

Hoje, nosso foco recai sobre as categorias de controle de segurança, que são técnico, operacional e gerencial, bem como os tipos funcionais de controle de

segurança: preventivo, detectivo, corretivo e outros tipos, como controles físicos, dissuasores e de compensação.

Ao término desta aula, vocês estarão munidos com o conhecimento necessário para compreender e selecionar os controles de segurança adequados para enfrentar os desafios da segurança da informação em qualquer organização.

Controle de segurança

A segurança da informação é uma disciplina complexa e multifacetada que envolve diversos aspectos para garantir a proteção dos ativos da organização. A garantia da segurança da informação e da cibersegurança é geralmente considerada como ocorrendo dentro de um processo global de gestão de riscos empresariais. A implementação de funções de segurança cibernética costuma ser responsabilidade do departamento de TI. Há muitas maneiras diferentes de pensar sobre como os serviços de TI devem ser governados para atender às necessidades gerais do negócio. Algumas organizações desenvolveram estruturas de serviços de TI para fornecer guias de melhores práticas para implementar TI e segurança cibernética. Essas estruturas podem moldar as políticas da empresa e fornecer listas de verificação de procedimentos, atividades e ferramentas que podem ser chamadas de controle de segurança.

Categorias de controle de segurança

Um controle de segurança é algo projetado para conferir as propriedades de confidencialidade, integridade, disponibilidade e não repúdio a um sistema ou ativo de dados. Os controles podem ser divididos em três grandes categorias que representam a forma como os controles são implementados: técnico, operacional e gerencial. Cada uma dessas categorias desempenha um papel fundamental na construção de um ambiente seguro e robusto. A seguir, abordaremos cada categoria com mais detalhes:

1. **Controles técnicos**: os controles técnicos são aqueles que se concentram na parte tecnológica da segurança da informação. Eles envolvem a implementação de sistemas, dispositivos e softwares projetados para proteger os ativos da organização. As principais características dos controles técnicos incluem a

automação, a capacidade de resposta rápida a ameaças e a eficiência na proteção de sistemas e dados. Os controles técnicos também podem ser descritos como controles lógicos. Eles são essenciais para fortalecer a segurança de ativos digitais.

Funcionamento:

- Os controles técnicos funcionam monitorando, bloqueando ou restringindo o acesso a sistemas e dados com base em regras, configurações e políticas predefinidas.
- Eles operam em tempo real, permitindo respostas rápidas a ameaças e ataques em potencial. Por exemplo, um firewall pode bloquear automaticamente o tráfego de uma fonte suspeita com base em regras de filtragem de pacotes.

Exemplos de controles técnicos:

- **Firewalls**: são dispositivos que monitoram o tráfego de rede, permitindo ou bloqueando o acesso a sistemas com base em regras predefinidas. Eles servem para proteger a rede contra ameaças externas. São dispositivos ou software que atuam como barreiras entre uma rede interna e a internet ou outras redes externas. Eles monitoram o tráfego de rede e aplicam regras predefinidas para permitir ou bloquear o acesso. Atua para impedir que ameaças externas, como hackers, acessem sistemas internos.
- **Antivírus e antimalware**: os programas antivírus são controles técnicos que identificam e removem malware e vírus de sistemas e dispositivos. Esses programas são projetados para detectar e remover software malicioso, como vírus, trojans e spyware, dos sistemas. Eles fazem varreduras periódicas em arquivos e tráfego de rede em busca de ameaças em potencial.
- **Criptografia de dados**: a criptografia é uma técnica que protege os dados sensíveis, tornando-os ilegíveis para qualquer pessoa que não tenha a chave de descriptografia correta. Protege informações sensíveis, como senhas, informações financeiras e dados confidenciais de clientes.
- **Sistemas de Detecção de Intrusão (IDS) e Sistemas de Prevenção de Intrusão (IPS)**: IDS monitoram a rede em busca de atividades suspeitas, enquanto IPS podem bloquear ou restringir automaticamente o tráfego que é identificado como malicioso.

2. **Controles operacionais**: concentram-se nas práticas, procedimentos e ações diárias que as organizações adotam para garantir a segurança da informação.

Os controles operacionais são fundamentais para a implementação consistente das políticas de segurança e para garantir que os funcionários estejam cientes das melhores práticas de segurança. Eles contribuem para uma cultura de segurança sólida dentro da organização.

Exemplos de controles operacionais:

- **Políticas de senhas**: estabelecer regras para criação e gerenciamento de senhas, como a exigência de senhas fortes e a troca regular de senhas.
- **Treinamento de conscientização em segurança**: oferecer treinamento aos funcionários para que estejam cientes das ameaças cibernéticas e saibam como se proteger.
- **Gerenciamento de acesso de usuário**: controle de quem tem acesso a determinados sistemas e dados, garantindo que apenas as pessoas autorizadas possam acessá-los.

3. **Controles gerenciais**: fornecem a estrutura necessária para a segurança da informação, permitindo que a organização desenvolva estratégias de longo prazo para lidar com ameaças e riscos. Esses controles têm como foco a alta administração, e envolvem a definição de políticas, estratégias e diretrizes gerais de segurança. Eles não lidam diretamente com aspectos técnicos, mas estabelecem a estrutura e a governança da segurança da informação.

Exemplos de controles gerenciais:

- **Políticas de segurança da informação**: definir as diretrizes gerais de segurança da organização, incluindo a classificação de informações e a resposta a incidentes de segurança.
- **Avaliação de riscos**: realizar avaliações regulares de riscos para identificar ameaças e vulnerabilidades e tomar decisões baseadas nessa análise.
- **Planejamento de continuidade de negócios**: estabelecer planos para garantir a continuidade das operações em caso de desastres ou incidentes graves.

Categorias de controle de segurança.

Exemplos práticos

Esses exemplos demonstram como as categorias de controle de segurança podem ser aplicadas em um cenário do mundo real, mostrando como cada categoria desempenha um papel crítico na proteção dos ativos da organização. Para tornar isso mais claro, vamos considerar um exemplo prático. Suponhamos que uma empresa deseja proteger seu sistema de gerenciamento de estoque.

1. **Controles técnicos**: a empresa pode implementar firewalls para proteger o sistema contra ataques externos, bem como criptografar os dados de estoque para impedir o acesso não autorizado.
2. **Controles operacionais**: a empresa pode estabelecer políticas que exigem que os funcionários usem senhas fortes e façam login apenas em computadores seguros. Além disso, podem fornecer treinamento de conscientização em segurança para que os funcionários saibam como identificar e relatar possíveis ameaças.
3. **Controles gerenciais**: a empresa pode definir políticas de segurança da informação que orientem a proteção de dados do estoque e garantam a conformidade com regulamentações. Além disso, podem realizar avaliações regulares de risco para identificar possíveis vulnerabilidades no sistema de gerenciamento de estoque.

Tipos funcionais de controle de segurança

Além das categorias de controle de segurança (técnico, operacional e gerencial), é essencial compreender os tipos funcionais de controle de segurança. Esses tipos representam abordagens específicas para a proteção de ativos e a gestão de riscos. Vamos explorar os seguintes tipos funcionais de controle de segurança: preventivo, detectivo, corretivo e outros tipos que não se encaixam nessa classificação, discutindo como funcionam e em que contexto cada um pode ser mais adequado.

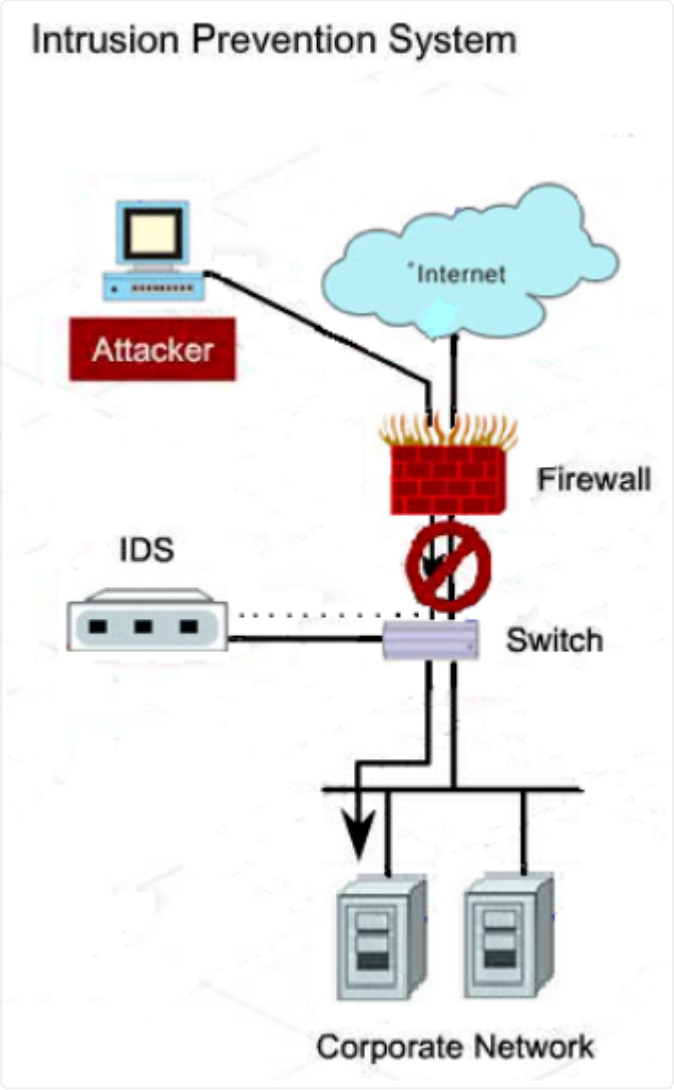
Controles de segurança funcionais

Os controles de segurança podem ser classificados também de acordo com seu objetivo ou com a função que ele executa. A seguir, veremos cada tipo:

1. **Controles preventivos**: são projetados para evitar que incidentes de segurança ocorram. Eles visam à minimização de riscos, uma vez que evitam a ocorrência de ameaças antes que elas possam causar danos significativos. São amplamente aplicados na proteção proativa dos ativos.

Exemplos de controles preventivos:

- **Firewalls**: como mencionado anteriormente, firewalls são um exemplo de controle técnico preventivo. Eles bloqueiam o acesso não autorizado à rede e, assim, previnem potenciais ameaças.
- **Políticas de segurança de senhas**: exigir senhas fortes e políticas de rotação regular de senhas impede o acesso não autorizado a contas e sistemas.

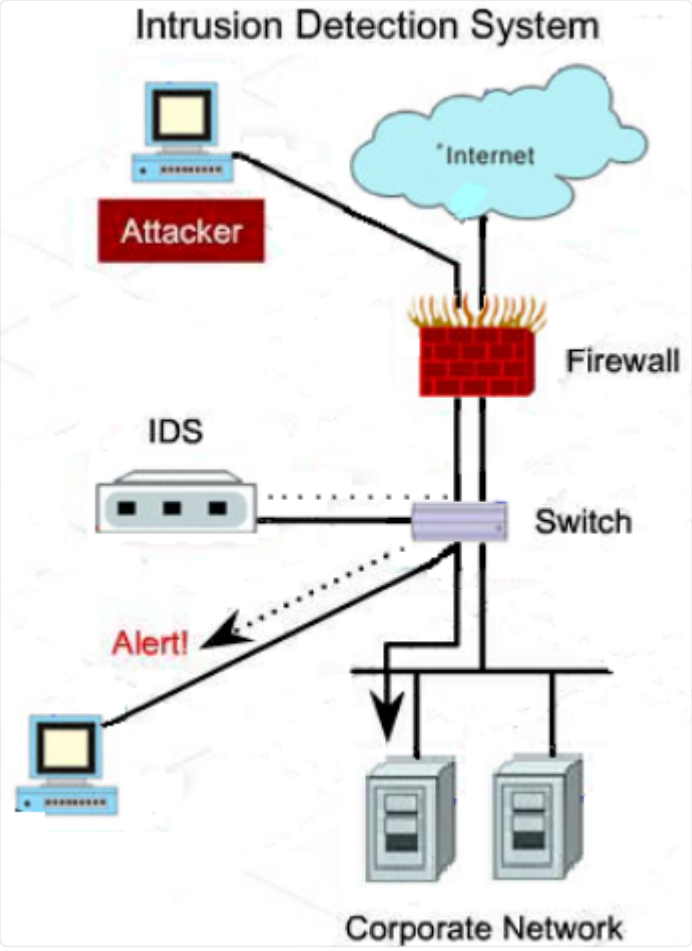


Intrusion Prevention System.

2. **Controles detectivos**: como o nome sugere, são voltados para a identificação precoce de incidentes de segurança. Funcionam monitorando sistemas e redes em busca de atividades anormais. São valiosos para identificar ameaças à medida que ocorrem, permitindo uma resposta rápida e eficaz. Eles são essenciais para a detecção precoce de incidentes de segurança.

Exemplos de controles detectivos:

- **Sistemas de Detecção de Intrusão (IDS)**: monitoram o tráfego de rede em busca de padrões suspeitos ou atividades maliciosas, e emitem alertas quando identificam tais atividades.
- **Registros de eventos (logs)**: a análise de logs de sistemas e aplicativos pode ajudar a identificar eventos não autorizados ou atividades incomuns.



Intrusion Detection System.

3. **Controles corretivos**: visam restaurar a normalidade após um incidente de segurança ter ocorrido. Eles têm o objetivo de mitigar os danos e recuperar sistemas e dados. São vitais para a continuidade dos negócios, garantindo que a organização possa se recuperar de incidentes de segurança e minimizar interrupções.

Exemplos de controles corretivos:

- **Backups**: manter cópias de segurança dos dados permite a restauração dos sistemas após a perda de dados devido a incidentes como falhas de hardware, ataques de ransomware ou desastres naturais.
- **Planos de Recuperação de Desastres (DRP)**: detalham como a organização deve responder a desastres e incidentes críticos, incluindo a restauração de sistemas e processos.

4. **Outros tipos de controles**: a categoria "Outros" engloba controles que não se encaixam claramente nos três tipos mencionados acima, mas desempenham

papéis importantes na segurança da informação. Os controles físicos, dissuasores e de compensação podem ser utilizados para reforçar outros tipos de controles.

Exemplos de outros tipos de controles:

- **Controles físicos**: envolvem restrições de acesso físico a instalações, salas de servidores e dispositivos críticos, como câmeras de segurança e sistemas de controle de acesso. Controles como alarmes, portais, fechaduras, iluminação, câmeras de segurança e guardas que impedem e detectam o acesso às instalações e ao hardware são frequentemente classificados nessa categoria.
- **Controles dissuasores**: esses controles podem não impedir fisicamente ou logicamente o acesso, mas desencoraja psicologicamente um invasor de tentar uma intrusão. Isso pode incluir placas e avisos de sanções legais contra transgressões ou intrusões, cercas e sinalizações de segurança.
- **Controles de compensação**: podem ser usados para compensar a falta de um controle mais forte. Por exemplo, o uso de autenticação de dois fatores pode compensar senhas menos fortes.

Controle físico.

Seleção de controles de segurança

A escolha e implementação de controles de segurança adequados é uma das etapas na construção de uma estratégia de segurança da informação eficaz. Entender como selecionar e aplicar os controles certos é crucial para proteger os ativos da organização. Neste tópico, abordaremos o processo de seleção e implementação de controles de segurança, considerando as necessidades específicas da organização, os critérios de seleção, o custo-benefício e a importância da revisão contínua.

Processo de seleção e implementação

1. **Avaliação de riscos**: o primeiro passo no processo de seleção de controles de segurança é a avaliação de riscos. Isso envolve identificar ameaças, vulnerabilidades e ativos críticos, bem como avaliar o impacto potencial de incidentes de segurança. A avaliação de riscos é fundamental para entender as necessidades de segurança da organização.
2. **Definição de requisitos de segurança**: com base na avaliação de riscos, a organização deve definir os requisitos de segurança. Isso inclui determinar quais controles são necessários para mitigar os riscos identificados. Os requisitos podem variar de acordo com o setor, regulamentações específicas e características da organização.
3. **Seleção de controles adequados**: após a definição dos requisitos de segurança, o próximo passo é a seleção de controles adequados. Isso implica escolher os controles técnicos, operacionais, gerenciais e funcionais que melhor se alinham com as necessidades da organização. É importante considerar a abordagem em camadas, implementando controles de diversos tipos para uma proteção mais abrangente.
4. **Implementação e testes**: depois de selecionar os controles, é hora de implementá-los. Isso envolve configurar sistemas, treinar funcionários, desenvolver políticas e procedimentos e garantir que os controles estejam funcionando conforme o planejado. Testes regulares são essenciais para verificar a eficácia dos controles em um ambiente real.

Seleção de controles.

Critérios de seleção

Para escolher os controles de segurança apropriados, é importante levar em consideração os seguintes critérios:

1. **Relevância para riscos**: os controles selecionados devem ser diretamente relevantes para os riscos identificados durante a avaliação. Eles devem abordar as ameaças e vulnerabilidades específicas que podem afetar a organização.
2. **Custo-benefício**: avaliar o custo-benefício é fundamental. Os controles devem fornecer uma proteção proporcional ao investimento. Isso significa que o custo de implementação e manutenção dos controles deve ser justificado pelo valor da proteção que eles oferecem.
3. **Conformidade regulatória**: em muitos setores, existem regulamentações específicas que ditam os controles de segurança necessários. A organização deve garantir a conformidade com essas regulamentações.
4. **Viabilidade técnica e operacional**: os controles escolhidos devem ser tecnicamente viáveis e operacionalmente sustentáveis. Eles devem poder ser implementados e mantidos pela equipe da organização.

Revisão contínua

A seleção e implementação de controles de segurança não são processos estáticos. É essencial revisar periodicamente os controles e ajustá-los conforme as circunstâncias mudam. Alguns motivos para revisar controles incluem:

1. **Mudanças no ambiente de ameaças**: as ameaças cibernéticas evoluem constantemente, e os controles precisam se adaptar para enfrentar novos desafios.
2. **Mudanças na organização**: à medida que a organização cresce ou muda, os requisitos de segurança podem se alterar. É importante que os controles acompanhem essas mudanças.
3. **Resultados de testes e incidentes**: os resultados de testes de segurança e incidentes de segurança anteriores podem indicar a necessidade de ajustar ou reforçar os controles.
4. **Alterações em regulamentações**: mudanças nas regulamentações e requisitos legais também podem afetar a seleção de controles de segurança.

Conclusão

Agora, você está equipado com um conjunto sólido de ferramentas e conhecimentos para enfrentar os desafios em constante evolução no cenário da segurança cibernética. Você explorou o Processo de Resposta a Incidentes, compreendendo cada etapa, desde a preparação até a aprendizagem de lições, e a importância vital de um Plano de Resposta a Incidentes (IRP) para orientar ações coordenadas e eficazes.

Lembre-se: a segurança cibernética é uma jornada contínua. À medida que você avança em sua carreira, a aplicação desses conceitos e práticas fortalecerá a resiliência de sua organização e contribuirá para um ambiente digital mais seguro.

Aula 4: Fontes de ameaça

Objetivos

- [ ] Conhecer as fontes de ameaças à segurança da informação.
- [ ] Compreender as ameaças internas e externas.
- [ ] Entender o conceito das camadas da internet e seu potencial.

Conceitos

- [ ] Fontes de ameaça.
- [ ] Ameaças internas e externas.
- [ ] Deep web, dark web e dark net.

Introdução

Bem-vindos a mais uma aula do nosso curso de segurança da informação. Nesta aula, exploraremos um tema fundamental: as fontes de ameaça. Vamos nos aprofundar em dois aspectos críticos da segurança cibernética: ameaças internas e externas, bem como o intrigante mundo da darknet e darkweb.

Na primeira parte, estudaremos o conceito de ameaças internas e externas. Vamos analisar quem são esses atores, o que os motiva e quais são suas capacidades. A compreensão das motivações por trás de suas ações é fundamental para adotar medidas de proteção eficazes.

Na segunda parte da aula, entraremos no obscuro mundo da darkweb e darknet. Vamos explorar o funcionamento dessas redes e entender como elas são organizadas. Também discutiremos o potencial de utilização dessas redes como contra-ameaça e como isso se relaciona com a segurança da informação.

Vamos dar início ao nosso estudo lembrando que a segurança cibernética é uma responsabilidade compartilhada, e juntos podemos fortalecer nossas defesas contra ameaças em constante evolução.

Fontes de ameaça

As fontes de ameaça são as origens ou os pontos de onde as ameaças à segurança da informação podem surgir. Elas representam os locais, atores ou entidades que têm o potencial de causar danos, roubar informações, realizar atividades maliciosas ou comprometer a segurança de sistemas, redes e dados. Essas fontes incluem fontes internas e externas. Identificar e avaliar as ameaças internas e externas permite às organizações desenvolver estratégias de proteção mais eficazes e se preparar para possíveis incidentes de segurança.

Ameaças internas

As ameaças internas são um dos principais desafios de segurança da informação que as organizações enfrentam. Elas se originam dentro da própria organização, e são representadas por atores internos, ou seja, pessoas que têm acesso legítimo aos recursos e sistemas da empresa. A linha que separa atores internos de atores externos pode ser tênue em alguns casos. Os contratados, parceiros de negócios e ex-funcionários que ainda mantêm vínculo com a organização podem ter algum acesso aos recursos.

As ameaças internas são representadas por qualquer pessoa que tenha acesso privilegiado aos sistemas e dados da empresa. Elas podem ser acidentais (erros não intencionais) ou propositadas, onde os indivíduos agem deliberadamente para prejudicar a organização. As ameaças internas frequentemente envolvem uma quebra de confiança, uma vez que os perpetradores têm conhecimento interno e acesso. Compreender essa dinâmica de fatos é fundamental para adotar medidas de proteção eficazes contra ameaças internas.

A prevenção, detecção e resposta a ameaças internas requerem uma abordagem holística que inclui educação em segurança, monitoramento contínuo e acesso controlado a sistemas e informações críticas. A conscientização e a vigilância são elementos-chave na mitigação desse tipo de ameaça. Os atores internos que representam ameaças podem ser divididos em duas categorias principais:

1. **Atores internos acidentais**: essas ameaças não têm a intenção de prejudicar a organização, mas podem inadvertidamente colocar em risco a segurança da informação. Isso inclui funcionários que cometem erros não intencionais, como clicar em links de phishing, compartilhar informações sensíveis acidentalmente ou perder dispositivos que contenham dados confidenciais.

2. **Atores internos maliciosos**: nessa categoria, incluímos pessoas que têm a intenção de causar danos ou agir contra os interesses da organização. Isso pode envolver funcionários descontentes, ex-funcionários com ressentimento, colaboradores coagidos ou qualquer pessoa que abuse de seu acesso privilegiado para cometer ações maliciosas.

Atributos dos atores internos:

Para entender as ameaças internas com mais profundidade, é crucial analisar os atributos dos atores envolvidos:

- **Motivação**: a motivação dos atores internos pode variar consideravelmente. Alguns podem ser motivados por razões financeiras, buscando ganho pessoal, enquanto outros podem ser motivados por vingança, descontentamento no trabalho ou coerção por terceiros. Compreender as motivações é essencial para prever e prevenir possíveis ameaças.
- **Nível de sofisticação/capacidade**: o nível de sofisticação e capacidade dos atores internos é um fator a ser considerado na avaliação de riscos de ameaça. Funcionários que têm conhecimento profundo dos sistemas e processos da organização podem ser capazes de realizar ações mais elaboradas, como a criação de malware personalizado ou a exploração de vulnerabilidades complexas.
- **Recursos**: os recursos disponíveis para os atores internos vão determinar suas capacidades. Alguns podem depender de recursos internos da organização, como acesso a sistemas ou informações, enquanto outros podem obter apoio de fontes externas, o que pode aumentar sua capacidade de causar danos.

Estratégias comuns usadas nas ameaças internas

As estratégias adotadas por ameaças internas podem ser diversas e evoluir com o tempo. Algumas das estratégias comuns incluem:

- **Abuso de Privilégios de Acesso**: Ameaças internas muitas vezes exploram seu acesso privilegiado para realizar atividades não autorizadas, como a exfiltração de dados confidenciais, a modificação de registros ou a criação de contas falsas.
- **Roubo de Informações Confidenciais**: Funcionários podem roubar informações sensíveis, como propriedade intelectual, listas de clientes, planos estratégicos

ou informações financeiras para uso pessoal ou para benefício de concorrentes.

- **Destruição de Dados ou Ativos**: Alguns atores internos podem buscar causar danos deliberados, destruindo dados ou ativos críticos para a operação da organização.
- **Divulgação de Informações Confidenciais**: Ameaças internas podem deliberadamente divulgar informações confidenciais para prejudicar a reputação da organização ou causar outros tipos de danos.
- **Vazamento de Dados**: Isso pode envolver a divulgação de informações confidenciais ou a venda dessas informações a terceiros, frequentemente para ganho pessoal.

Ameaças Internas.

Ameaças Externas

As ameaças externas constituem um grande desafio para a segurança da informação. Essas ameaças se originam de fora da organização e são

representadas por atores externos incluindo hackers, grupos criminosos, concorrentes, governos ou qualquer outra entidade que não têm uma afiliação direta com a organização e busque explorar vulnerabilidades em sistemas e redes. Tais ameaças geralmente não têm conhecimento interno e, frequentemente, buscam ganhos financeiros, acesso a informações confidenciais ou causar danos à reputação da organização. Atores externos podem ser divididos em várias categorias:

1. **Hackers Individuais**: São indivíduos que, por várias motivações, se envolvem em atividades de hacking para explorar vulnerabilidades em sistemas e redes.
2. **Grupos Criminosos**: Organizações criminosas ou grupos de cibercriminosos que buscam ganhos financeiros por meio de atividades como extorsão, fraude, roubo de dados e distribuição de malware.
3. **Concorrentes**: Empresas concorrentes que podem tentar obter vantagem competitiva por meio de atividades ilícitas, como espionagem industrial ou roubo de propriedade intelectual.
4. **Hacktivistas**: Grupos ou indivíduos com motivações políticas ou sociais que conduzem ataques cibernéticos para promover uma causa ou divulgar informações.
5. **Governos Estrangeiros**: Estados-nação que buscam obter informações sensíveis, realizar espionagem cibernética, ou até mesmo realizar ataques cibernéticos para fins políticos, militares ou de inteligência.

Atributos dos Atores Externos:

Para entender as ameaças externas em maior profundidade, é fundamental analisar os atributos dos atores envolvidos:

- **Motivação**: A motivação dos atores externos varia amplamente. Alguns são movidos por ganhos financeiros, enquanto outros buscam causas políticas, sociais ou até mesmo pessoais. Compreender as motivações auxilia a prever ações desses atores por meio de análise comportamental.
- **Nível de Sofisticação/Capacidade**: O nível de sofisticação e capacidade dos atores externos pode variar significativamente. Alguns atores, como grupos criminosos altamente organizados, possuem considerável expertise técnica, enquanto outros podem ser menos sofisticados, realizando ataques mais simples.
-

- **Recursos/Financiamento**: A disponibilidade de recursos e financiamento é um fator crítico na determinação das capacidades dos atores externos. Grupos criminosos, por exemplo, podem ter acesso a financiamentos substanciais para conduzir suas operações, enquanto hackers individuais podem ter recursos limitados.

Estratégias Comuns Usadas em Ameaças Externas:

As estratégias adotadas por ameaças externas são diversas e continuam a evoluir com o tempo. Algumas das estratégias comuns incluem:

- **Ataques de Engenharia Social**: Isso envolve a manipulação psicológica das vítimas para obter informações confidenciais, como senhas ou acesso a sistemas.
- **Malware e Exploits (Explorações)**: Ameaças externas frequentemente usam malware (software malicioso) e exploits para explorar vulnerabilidades em sistemas e redes.
- **Roubo de Identidade**: Atores externos podem assumir a identidade de outras pessoas, frequentemente para obter acesso não autorizado a sistemas ou realizar atividades ilegais.
- **Ataques de Negação de Serviço (DDoS)**: Os ataques DDoS visam sobrecarregar sistemas, tornando-os inacessíveis.
- **Ataques de Injeção (SQL, XSS)**: Esses ataques exploram vulnerabilidades de aplicativos da web para acessar ou modificar dados.
- **Exploração de Vulnerabilidades**: Ameaças externas podem explorar vulnerabilidades conhecidas em sistemas e aplicativos.
- **Ataques de Ransomware**: Grupos criminosos frequentemente usam ransomware para criptografar dados e exigir resgates em troca da chave de descriptografia.

Ameaças Externas.

Deep web, dark web e dark net

Nosso estudo no sentido de obter a compreensão das fontes de ameaça continua, e agora entraremos um universo misterioso que muitos ouviram falar, mas poucos compreendem completamente — a deep web, a dark web e a dark net. Esses termos evocam imagens de anonimato, segredo e atividades clandestinas, mas é essencial entender o que realmente representam e como se relacionam com a segurança da informação. A base do aprendizado começa pela definição de cada um desses ambientes. Primeiro, precisamos definir as camadas da internet, pois esses termos são frequentemente usados de forma intercambiável, mas têm significados distintos:

Definição das Camadas da Internet

1. **Surface Web (Web de Superfície)**: É a parte visível da internet que é indexada por mecanismos de busca comuns, como o Google, Bing ou Yahoo. Representa

a rede como a maioria das pessoas usa e conhece. Corresponde a todo conteúdo disponível pelos mecanismos de busca e que pode ser facilmente acessado por meio de navegadores convencionais, como o Google Chrome, Mozilla Firefox ou Safari. Aqui, encontramos sites públicos, páginas da web e conteúdo acessível a qualquer pessoa. A maioria das atividades online ocorre na Web Superficial.

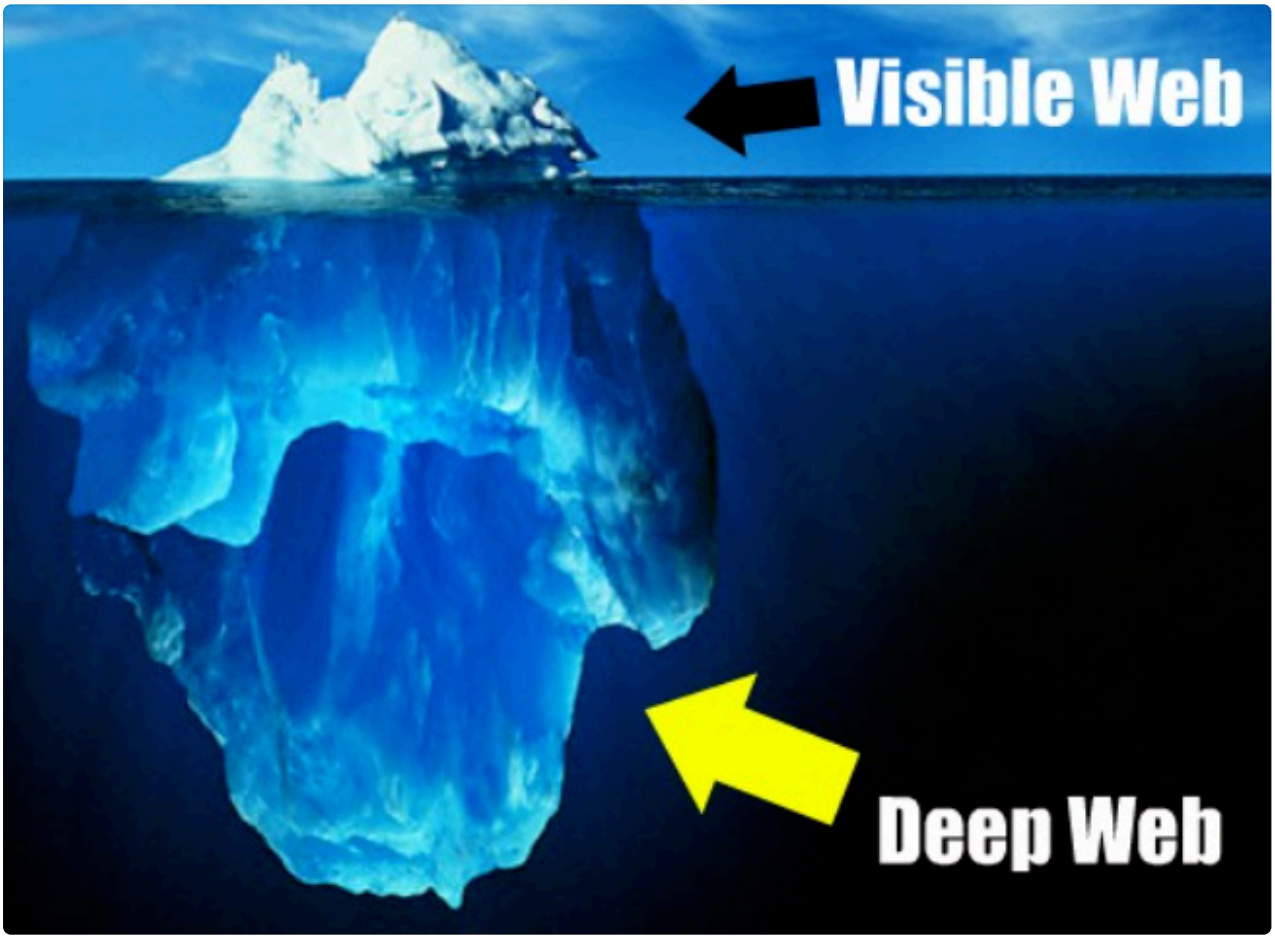
2. **Deep Web (Web Profunda)**: A Deep Web, frequentemente mal compreendida e confundida com a Dark Web, representa uma parte substancial, porém menos visível, da internet. Ela engloba todas as partes da rede que não são indexadas pelos mecanismos de busca tradicionais, tornando-as inacessíveis por meio de pesquisas no Google, Bing ou outros mecanismos de busca comuns. Embora a Deep Web não seja acessível diretamente por mecanismos de busca, não é necessariamente obscura ou maliciosa; muitas atividades legítimas ocorrem aqui.

Características da deep web:

- **Conteúdo não indexado**: a principal característica da deep web é que seu conteúdo não é acessível por meio de mecanismos de busca convencionais. Isso inclui sistemas de gerenciamento de banco de dados, intranets corporativas, sistemas de e-mail privado, informações governamentais confidenciais e qualquer outro tipo de conteúdo que não seja destinado ao acesso público.
- **Acesso controlado**: muitos recursos da deep web são protegidos por senhas, autenticação ou outras medidas de controle de acesso. Isso significa que apenas pessoas autorizadas têm permissão para acessar essas informações, serviços ou sistemas.
- **Atividades legítimas**: é importante destacar que a maior parte da deep web é composta por atividades legítimas e inofensivas. Empresas utilizam intranets para gerenciar informações internas, e sistemas de gerenciamento de banco de dados são usados para armazenar registros confidenciais. As atividades na deep web são essenciais para o funcionamento de muitas organizações.
- **Privacidade e segurança**: a natureza não indexada da deep web fornece um nível de privacidade e segurança, tornando-a um local preferido para atividades que requerem discrição, como troca segura de mensagens, comunicações empresariais confidenciais e acesso seguro a informações de pacientes em hospitais.
- **Papel na cibersegurança**: a deep web desempenha um papel importante na cibersegurança, pois as empresas muitas vezes usam sistemas internos e

sistemas de autenticação para proteger informações sensíveis. Também é um espaço onde as organizações podem compartilhar informações confidenciais com terceiros de maneira segura, como relatórios de auditoria, documentos legais e contratos.

- **Desafios de segurança**: embora a deep web seja predominantemente utilizada para fins legítimos, também pode ser alvo de ataques. A segurança dos sistemas e a autenticação desempenham um papel crucial na proteção desses recursos contra o acesso não autorizado.
- **Conhecimento técnico**: navegar e acessar a deep web exige conhecimento técnico e, muitas vezes, credenciais de acesso. Além disso, a segurança da informação é fundamental, uma vez que a exposição de informações confidenciais na deep web pode ter graves consequências.



Deep web.

3. **Dark web (web escura)**: a dark web é uma parte específica da Deep Web que é deliberadamente oculta e inacessível através de navegadores padrão. Ela utiliza redes criptografadas e sistemas de anonimato, como o Tor (The Onion Router), para ocultar a identidade dos usuários e servidores. A dark web é conhecida por

hospedar mercados clandestinos, fóruns de hacking, conteúdo ilegal e atividades ilícitas. No entanto, é importante observar que a dark web não é inerentemente má; ela pode ser usada para a privacidade e comunicação segura em regiões com censura ou para proteger ativistas de direitos humanos.

Funcionamento da dark web

A dark web opera em grande parte sob o princípio do anonimato. Os usuários acessam sites e recursos usando redes como o Tor, que roteiam o tráfego através de uma série de servidores criptografados, tornando difícil a rastreabilidade. Isso permite que indivíduos naveguem e participem de atividades sem revelar sua localização ou identidade.

Acesso à dark web

Para acessar a dark web, é necessário utilizar um navegador especializado, como o Tor Browser. Esse navegador roteia o tráfego através da rede Tor, permitindo o acesso a sites .onion, que são exclusivos da dark web. Esses sites muitas vezes contêm fóruns, mercados clandestinos, serviços de hospedagem e outros recursos.

Organização da dark web

A organização da dark web é descentralizada e baseada em comunidades. É composta por várias redes independentes denominadas dark nets, compartilhando o espaço da dark web. A rede Onion é uma delas. É acessada por meio do navegador TOR, cujas URLs terminam com a extensão “.onion”. Dentro dessas dark nets, grupos e indivíduos operam sites, fóruns e serviços independents. A organização muitas vezes é obscura e de difícil rastreamento. Além disso, a dark web está em constante evolução, com sites aparecendo e desaparecendo rapidamente.

Potencial de utilização como contra-ameaça

Embora a dark web seja frequentemente associada a atividades ilegais e maliciosas, também tem potencial para uso legítimo. Pode ser usada como uma ferramenta para ativistas, jornalistas e pessoas em países com censura para se comunicarem de forma segura. Além disso, as organizações de segurança

cibernética e de aplicação da lei monitoram a Dark Web para identificar ameaças e investigar atividades criminosas.

Dark web.

4. **Dark net**: A dark net é uma parte da internet que não é acessível por meio dos navegadores padrão e não é indexada pelos mecanismos de busca convencionais. Ela é uma rede obscura, muitas vezes associada a atividades clandestinas e anônimas. A dark net opera por meio de redes privadas e sistemas criptografados, garantindo um alto grau de anonimato para seus usuários. Os principais aspectos da dark net são:

- **Definição e acesso**: a dark net consiste de um conjunto de redes privadas como a rede Onion, I2P ou Freenet compostas de sites, fóruns, comunidades e serviços que não estão disponíveis na internet convencional. Para acessá-la, os usuários precisam usar software especializado, como o Tor (The Onion Route da

rede Onion), que encaminha as conexões por meio de uma série de servidores, mascarando o endereço IP do usuário. Esse anonimato dificulta o rastreamento das atividades dos usuários, o que a torna um ambiente atraente para quem busca privacidade ou anonimato na web.

- **Organização da Dark Net**: A organização da Dark Net é descentralizada. Os sites e serviços são frequentemente hospedados em servidores que operam sob domínios exclusivos chamados de "sites .onion.". Os proprietários desses sites variam desde defensores da privacidade e jornalistas até cibercriminosos e grupos de hackers. A natureza obscura e descentralizada da Dark Net a torna um espaço onde comunidades se reúnem com base em interesses comuns, criando uma ampla gama de recursos e serviços.
- **Potencial de utilização como contra-ameaça**: a dark net tem potencial tanto para atividades maliciosas quanto para ações legítimas, e seu papel na segurança cibernética é complexo:
- Cibersegurança: as organizações de segurança cibernética e de aplicação da lei monitoram a dark net para identificar ameaças em desenvolvimento, como a venda de informações roubadas, vulnerabilidades de software e malware. A obtenção de inteligência da dark net é uma ferramenta valiosa para proteger sistemas e redes.
- Privacidade e liberdade de expressão: a dark net também é usada por ativistas, jornalistas e cidadãos em países com censura rigorosa para se comunicar de forma segura e compartilhar informações que, de outra forma, seriam restringidas. Ela desempenha um papel importante na promoção da liberdade de expressão.
- Atividades maliciosas: a dark net é frequentemente associada a mercados clandestinos que vendem drogas, armas, informações roubadas, serviços de hacking e outros bens ilegais. Além disso, ela é um espaço onde indivíduos mal-intencionados podem planejar e coordenar ataques cibernéticos.
- Contramedidas: as organizações usam informações obtidas na dark net para fortalecer suas defesas cibernéticas e adotar contramedidas eficazes contra ameaças emergentes. Isso inclui a identificação de novas ameaças, a análise de vulnerabilidades e a preparação contra ataques.

Dark net.

Conclusão

Parabenizamos a todos pela conclusão de mais uma aula onde abordamos ameaças internas e externas, bem como a tríade da deep web, dark web e dark net.

A compreensão das ameaças internas, que podem surgir de dentro de uma organização e das ameaças externas, originárias de atores fora da organização, é fundamental para a construção de uma estratégia de segurança eficaz. Avaliamos os atributos desses atores, como motivação, nível de sofisticação e recursos, e discutimos estratégias comuns usadas por eles. Essa compreensão sólida é um primeiro passo essencial para proteger sistemas, dados e informações críticas.

Aprofundando ainda mais, exploramos a deep web, uma vasta área da internet que não é indexada por mecanismos de busca tradicionais, onde informações confidenciais e atividades legítimas residem. Além disso, adentramos na dark web e darknet, que são frequentemente associadas a atividades clandestinas e anônimas. No entanto, também reconhecemos o potencial dessas redes para a privacidade, a segurança e a promoção da liberdade de expressão.

Como estudantes dedicados da segurança da informação, vocês agora estão equipados com um conhecimento mais profundo sobre as fontes de ameaça que podem afetar as organizações e indivíduos. À medida que continuam sua jornada, lembrem-se de que o cenário de cibersegurança está em constante evolução, e a vigilância e a adaptação contínuas são essenciais. Parabéns pela conclusão desta aula e pelo compromisso com a cibersegurança.