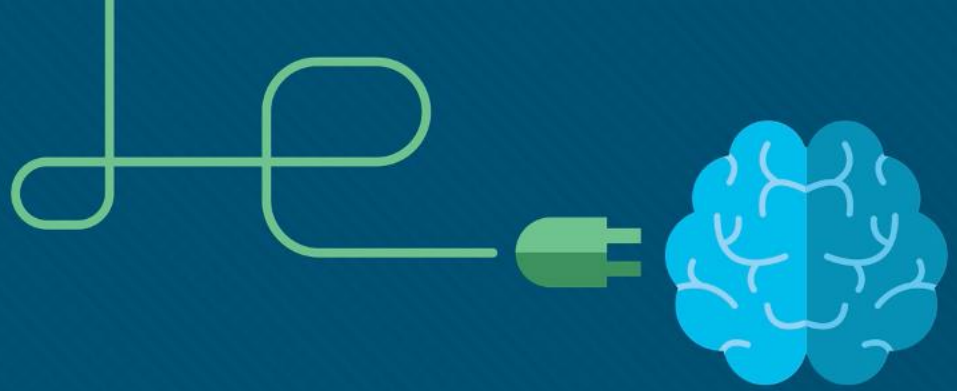


Módulo 4: Protegendo a Organização

Introdução à Cibersegurança

Objetivos do Módulo

Título do Módulo: Protegendo a Organização

Objetivo do Módulo: Explicar como as empresas podem proteger suas operações contra esses ataques.

Título do Tópico	Objetivo do Tópico
Dispositivos e Tecnologias de Cibersegurança	Explicar os diferentes firewalls, dispositivos de segurança e software usados por profissionais de segurança cibernética que protegem a rede, os dados e os equipamentos de uma empresa.
Abordagem comportamental à segurança cibernética	Explicar como detectar uma ameaça cibernética por meio de abordagens de segurança baseadas em comportamento.
Abordagem da Cisco à segurança cibernética	Explicar a abordagem da Cisco para a segurança cibernética, incluindo a equipe de CSIRT e o manual de segurança.

4.1 Dispositivos e Tecnologias de Segurança Cibernética

Dispositivos de Segurança

- Os dispositivos de segurança podem ser dispositivos autônomos, como um roteador ou ferramentas de software executadas em um dispositivo de rede. Eles se enquadram em seis categorias gerais.

  - **Roteadores:** Embora o uso principal de um roteador seja interconectar vários segmentos de rede, eles geralmente fornecem recursos básicos de filtragem de tráfego. Essas informações podem ajudá-lo a definir quais computadores de um determinado segmento de rede podem se comunicar com quais segmentos de rede.

  - **Os firewalls** podem examinar mais profundamente o tráfego da rede para bloquear comportamentos maliciosos. Os firewalls podem ter políticas de segurança sofisticadas aplicadas ao tráfego que passa por eles.

  - **Sistema de prevenção de intrusões**: Os sistemas IPS utilizam um conjunto de assinaturas de tráfego que combinam e bloqueiam tráfego e ataques maliciosos.

Dispositivos de Segurança (Cont.)

- **Redes privadas virtuais:** os sistemas VPN permitem que funcionários remotos usem um túnel criptografado seguro a partir de seus computadores móveis e se conectem com segurança à rede da organização. Os sistemas de VPN também podem interconectar com segurança filiais com a rede da central.

- **Antimalware or antivirus:** Esses sistemas usam assinaturas ou análises comportamentais das aplicações para identificar e bloquear a execução de códigos mal-intencionados.

- **Other security devices:** Outros dispositivos de segurança incluem dispositivos de segurança para web e e-mail, dispositivos de descriptografia, servidores de controle de acesso de clientes e sistemas de gerenciamento de segurança.

Firewalls

- Em redes de computadores, um firewall é projetado para controlar ou filtrar quais comunicações são permitidas dentro e quais são permitidas fora de um dispositivo ou rede. Você pode instalar um firewall em um único computador com o objetivo de proteger aquele computador (firewall baseado em host) ou pode ser um dispositivo de rede autônomo que protege uma rede inteira de computadores e todos os dispositivos host nessa rede (firewall baseado em rede).

- À medida que os ataques a computadores e redes se tornam mais sofisticados, serão desenvolvidos novos tipos de firewalls, que atendem a finalidades diferentes.

    - **Firewall da camada de rede**: filtra as comunicações com base nos endereços IP de origem e destino.

    - **Firewall da camada de transporte:** Filtra as comunicações com base nas portas de dados de origem e destino e nos estados de conexão.

Firewalls (cont.)

- **Firewall da camada de aplicativo:** Filtra as comunicações com base em um aplicativo, programa ou serviço.
- **Firewall de camada sensível ao contexto:** filtra as comunicações com base no usuário, dispositivo, função, tipo de aplicativo e perfil de ameaça
- **Servidor proxy:** filtra solicitações de conteúdo da web como URLs, nomes de domínio e tipos de mídia.
- **Servidor proxy reverso:** colocados na frente dos servidores web, os servidores proxy reversos protegem, ocultam, descarregam e distribuem o acesso aos servidores web.
- **Firewall de tradução de endereço de rede (NAT):** Este firewall oculta ou mascara os endereços privados dos hosts da rede.
- **Firewall baseado em host**: Filtra portas e chamadas de serviço do sistema em um único sistema operacional de computador.

Varredura de Porta

- Na rede, cada aplicativo em execução em um dispositivo recebe um identificador ou número de porta. Este número de porta é usado em ambas as extremidades da transmissão para passar os dados corretos para o aplicativo correto. A varredura de portas investiga um computador, servidor ou outro host de rede em busca de portas abertas. Ele pode ser usado maliciosamente como uma ferramenta de reconhecimento para identificar o sistema operacional e os serviços em execução em um computador ou host, ou pode ser usado de forma inofensiva por um administrador de rede para verificar as políticas de segurança da rede.

- Baixe e inicie uma ferramenta de varredura de portas como Zenmap. Digite o endereço IP do seu computador, escolha um perfil de digitalização padrão e pressione ‘scan’.

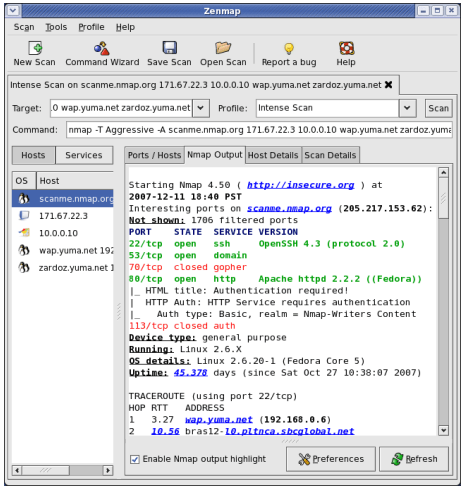
- A varredura reportará todos os serviços em execução, como serviços da Web ou de e-mail, e seus números de porta.

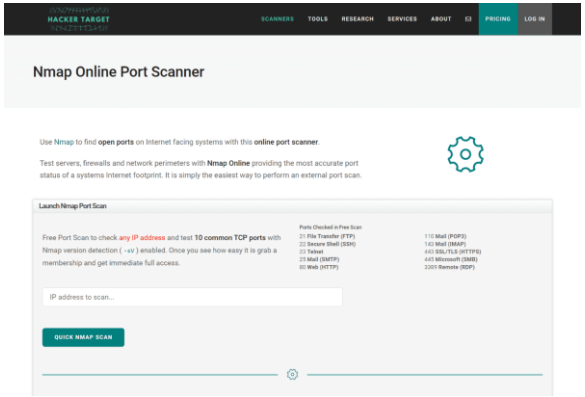
Escaneamento de Portas (Cont.)

- A verificação também irá relatar uma das seguintes respostas:
  - ‘Aberto’ ou ‘Aceito’ significa que outros dispositivos de rede podem acessar a porta ou serviço em execução no computador.
  - ‘Fechado’, ‘Negado’ ou ‘Não escutando’ significa que a porta ou serviço não está em execução no computador e, portanto, não pode ser explorado.
  - ´Filtrado’, ‘Descartado’ ou ‘Bloqueado’ significa que um firewall bloqueia o acesso à porta ou serviço e não pode explorá-lo.

Escaneamento de Portas (Cont.)

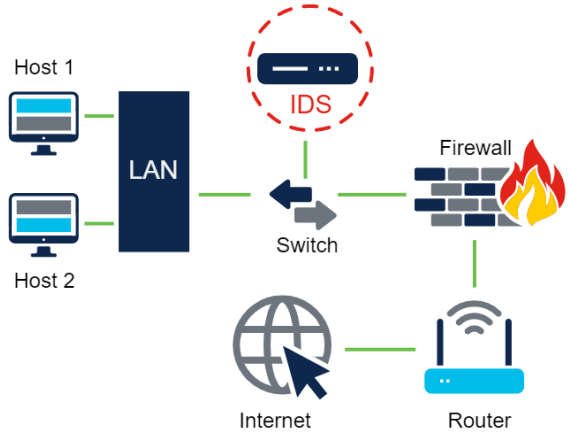
- Para executar uma varredura de porta fora da sua rede, você deve executá-la no firewall ou no endereço IP público do roteador.
- Insira a pergunta "qual é o meu endereço IP?" em um mecanismo de pesquisa como o Google para descobrir essas informações.
- Acesse o Nmap Online Port Scanner, digite seu endereço IP público na caixa de entrada e pressione “Quick Nmap Scan”. Se a resposta estiver aberta para as portas 21, 22, 25, 80, 443 ou 3389, provavelmente o encaminhamento de porta foi habilitado em seu roteador ou firewall e você está executando servidores em sua rede privada.





Sistemas de Detecção e Prevenção de Intrusão

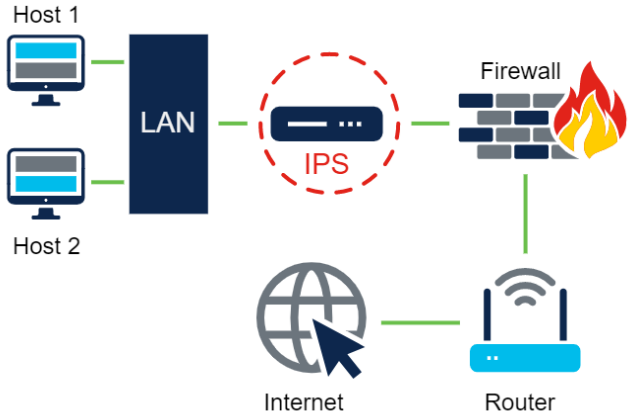
- Sistemas de detecção de intrusão (IDSs) e sistemas de prevenção de intrusão (IPSs) são medidas de segurança implantadas em uma rede para detectar e prevenir atividades maliciosas.
- Um IDS pode ser um dispositivo de rede dedicado ou uma das várias ferramentas em um servidor, firewall ou até mesmo um sistema operacional de computador host, como Windows ou Linux, que faz a varredura de dados em um banco de dados de regras ou assinaturas de ataque, em busca de tráfego malicioso.
- Se uma correspondência for detectada, o IDS registrará a detecção de registro e criará um alerta para um administrador de rede. Ela não tomará nenhuma ação e, portanto, não impedirá que os ataques aconteçam. O trabalho do IDS é detectar, registrar e relatar.



- A varredura realizada pelo IDS deixa a rede mais lenta (conhecido como latência). Colocar um IDS off-line, separado do tráfego normal da rede, evita atrasos na rede. Dados são copiados ou espelhados por um switch e então encaminhados para o IDS para a detecção off-line.

Sistemas de Detecção e Prevenção de Intrusão (Cont.)

- Um IPS pode bloquear ou negar tráfego com base em uma regra positiva ou correspondência de assinatura. Um dos sistemas mais conhecidos de IPS/IDS é o Snort. A versão comercial do Snort é o Sourcefire da Cisco. Sourcefire pode realizar tráfego em tempo real e análise de portas, registro, pesquisa e correspondência de conteúdo, detectar sondagens e ataques e executar varreduras de portas. Ele também se integra a ferramentas de relatórios, desempenho e análise de log de terceiros.



Detecção em Tempo Real

- Muitas organizações hoje não conseguem detectar ataques até dias ou até meses após sua ocorrência.

- A detecção de ataques em tempo real requer uma verificação ativa de ataques usando firewalls e dispositivos de rede IDS/IPS. Ajudaria se você também usasse a detecção de malware de cliente e servidor de última geração com conexões a centros de ameaças globais on-line. Atualmente, os softwares e dispositivos de varredura ativos devem detectar anomalias de rede usando a detecção de comportamento e análise baseada em contexto.

- DDoS é um dos ataques mais potentes que requer detecção e resposta em tempo real. Para muitas organizações, os ataques DDoS prejudicam regularmente os servidores da Internet e a disponibilidade da rede. Esses ataques são extremamente difíceis de se defender porque os ataques se originam de centenas, até mesmo milhares, de hosts zumbis, e os ataques aparecem como tráfego legítimo.

Proteção Contra Malware

- Uma forma de se defender contra ataques de dia zero e ameaças persistentes avançadas (APTs) é usar uma solução empresarial de detecção de malware, como o **Advanced Malware Protection (AMP) Threat Grid** da Cisco.

- Este software cliente/servidor pode ser implementado em endpoints de host, como um servidor independente ou em outros dispositivos de segurança de rede. Ele analisa milhões de arquivos e os correlaciona com centenas de milhões de outros artefatos de malware interpretados em busca de comportamentos que revelam uma APT. Essa abordagem fornece uma visão global de ataques, campanhas e distribuição de malware.

    - **Equipe do Secure Operations Center:** O Threat Grid permite que a equipe do Cisco Secure Operations Center reúna dados mais precisos e acionáveis.
    - **Equipe de resposta a incidentes:** A equipe de resposta a incidentes tem acesso a informações úteis do ponto de vista forense, a partir das quais pode analisar e compreender mais rapidamente comportamentos suspeitos.

Proteção Contra Malware (Cont.)

- **Equipe de inteligência de ameaças:** Usando essa análise, a equipe de inteligência de ameaças pode melhorar proativamente a infraestrutura de segurança da organização.
- **Equipe de Engenharia de Infraestrutura de Segurança:** No geral, a equipe de Engenharia de Infraestrutura de Segurança pode consumir e agir com base em informações sobre ameaças com mais rapidez, geralmente de forma automatizada.

Melhores Práticas de Segurança

- Muitas empresas e profissionais publicaram listas das melhores práticas de segurança. Você pode encontrar algumas das diretrizes mais úteis em repositórios organizacionais, como o Centro de Recursos de Segurança de Computadores do Instituto Nacional de Padrões e Tecnologia (NIST).
  - **Realize uma avaliação de risco:** Conhecer e compreender o valor daquilo que você está protegendo ajudará a justificar os gastos com segurança.
  - **Crie uma política de segurança:** Descreve claramente as regras, funções, responsabilidades e expectativas dos funcionários da organização.
  - **Medida de segurança física:** Restringir o acesso a armários de rede e locais de servidores e supressão de incêndio.

Melhores Práticas de Segurança de Rede (Cont.)

- **Medidas de segurança de recursos humanos:** A conclusão das verificações de antecedentes deve ser para todos os funcionários.
- **Execute e teste backups:** Faça backup de informações regularmente e teste a recuperação de dados de backups.
- **Mantenha patches e atualizações de segurança:** Atualize regularmente os sistemas operacionais e programas de servidores, clientes e dispositivos de rede.
- **Empregue controles de acesso:** Configure funções de usuário e níveis de privilégio e autenticação forte de usuário.
- **Teste regularmente a resposta a incidentes:** Empregar uma equipe de resposta a incidentes e testar cenários de resposta a emergências.

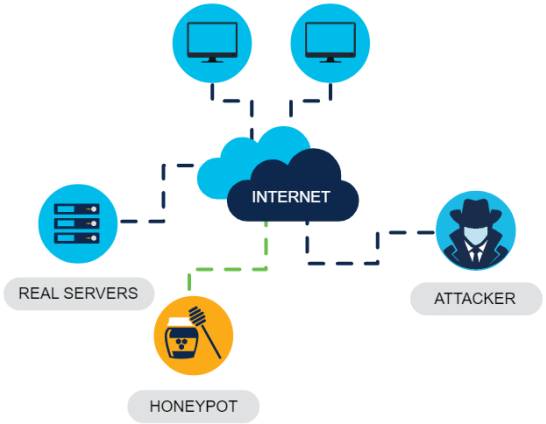
Melhores Práticas de Segurança de Rede (Cont.)

- **Implemente uma ferramenta de monitoramento, análise e gerenciamento de rede:** Escolha uma solução de monitoramento de segurança que se integre a outras tecnologias.
- **Implemente dispositivos de segurança de rede:** Use roteadores, firewalls e outros dispositivos de segurança da seguinte geração.
- **Implemente uma solução abrangente de segurança de endpoint:** Use software antimalware e antivírus de nível empresarial.
- **Eduque os usuários:** Forneça treinamento aos funcionários em procedimentos de segurança. Uma das empresas mais conhecidas e respeitadas para o treinamento de segurança cibernética é o Instituto SANS. Clique aqui para saber mais sobre SANS e os tipos de treinamento e certificações disponíveis.
- **Criptografar dados:** Criptografe todos os dados organizacionais confidenciais, incluindo e-mail.

4.2 Abordagem Comportamental à Cibersegurança

Segurança Baseada em Comportamento

- A segurança baseada em comportamento é uma forma de detecção de ameaças que captura e analisa o fluxo de comunicação entre um usuário na rede local e um destino local ou remoto. Quaisquer alterações nos padrões normais de comportamento são consideradas anomalias e podem indicar um ataque.

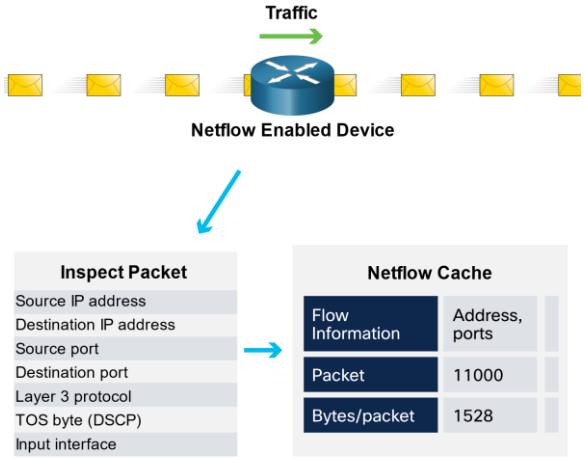


  - **Honeypots:** Um honeypot é uma ferramenta de detecção baseada em comportamento que atrai invasores apelando para seu padrão previsto de comportamento malicioso. Quando o invasor estiver dentro do honeypot, o administrador de rede poderá capturar, registrar e analisar o comportamento dele para que possa construir uma defesa melhor.

- **Arquitetura de solução de defesa contra ameaças cibernéticas da Cisco:** Essa arquitetura de segurança usa detecção e indicadores baseados em comportamento para fornecer maior visibilidade, contexto e controle. O objetivo é saber quem está realizando o ataque, que ataque está realizando e onde, quando e como o ataque está ocorrendo. Essa arquitetura de segurança usa muitas tecnologias de segurança para atingir esse objetivo.

NetFlow

- O uso da tecnologia NetFlow visa coletar informações sobre o fluxo de dados através de uma rede, incluindo quem e quais dispositivos estão na rede e quando e como os usuários e dispositivos acessam a rede.
- NetFlow é um componente essencial na detecção e análise baseada em comportamento. Switches, roteadores e firewalls equipados com NetFlow podem relatar informações sobre dados que entram, saem e trafegam pela rede.
- Essas informações são enviadas aos coletores NetFlow que coletam, armazenam e analisam dados do NetFlow para estabelecer comportamentos de linha de base em mais de 90 atributos, como endereço IP de origem e destino.



Teste de Penetração

- O teste de penetração, comumente conhecido como teste de penetração, avalia um sistema de computador, rede ou organização em busca de vulnerabilidades de segurança. Um pen test busca violar sistemas, pessoas, processos e códigos que possam explorar vulnerabilidades. Estas informações melhoram as defesas do sistema para garantir que ele seja mais capaz de resistir a ataques cibernéticos no futuro.

    - **Passo 1. Planejamento:** O pen tester reúne o máximo de informações possível sobre um sistema ou rede alvo, suas vulnerabilidades potenciais e explorações para usar contra ele. Isto envolve a realização de vigilância passiva ou activa (footprinting) e investigação de vulnerabilidades.

Teste de Penetração (Cont.)

- **Etapa 2: Verificação:** O pen tester realiza reconhecimento ativo para sondar um sistema ou rede alvo e identificar potenciais pontos fracos que, se explorados, poderiam dar acesso a um invasor.

- A vigilância ativa pode incluir:

  - varredura de portas para identificar possíveis pontos de acesso em um sistema de destino
  - verificação de vulnerabilidades para identificar vulnerabilidades potencialmente exploráveis de um alvo específico
  - Ele estabelece uma conexão ativa com um destino (enumeração) para identificar as contas de usuário, sistema e administrador.

Teste de Penetração (Cont.)

- **Etapa 3: Obtendo acesso:** O pen tester tentará obter acesso a um sistema de destino e detectar o tráfego de rede, usando vários métodos para explorar o sistema, incluindo:
  - lançar um exploit com um payload no sistema
  - violar barreiras físicas a ativos
  - engenharia social
  - explorando vulnerabilidades de sites
  - explorando vulnerabilidades ou configurações incorretas de software e hardware
  - Violando a segurança dos controles de acesso
  - Quebrar Wi-Fi com criptografia fraca.

Teste de Penetração (Cont.)

- **Etapa 4:** Manter o acesso: O pen tester manterá o acesso ao alvo para descobrir quais dados e sistemas estão vulneráveis à exploração. Eles devem permanecer indetectados, normalmente usando backdoors, cavalos de Tróia, rootkits e outros canais secretos para ocultar sua presença.

- Quando essa infraestrutura estiver instalada, o pen tester coletará os dados que considera valiosos.

- **Etapa 5:** Análise e relatórios: O pen tester fornecerá feedback por meio de um relatório recomendando atualizações de produtos, políticas e treinamento para melhorar a segurança de uma organização.

Redução do Impacto

- Embora a maioria das organizações hoje esteja ciente das ameaças comuns à segurança e faça esforços consideráveis para evitá-las, nenhuma prática de segurança é infalível. Therefore, organizations must prepare to contain the damage if a security breach occurs. E devem agir rápido!

  - **Comunique o problema:** A comunicação cria transparência, o que é fundamental nesta situação.
    - Informar todos os funcionários e comunicar um apelo à ação claro deve ocorrer internamente.
    - A informação a todos os clientes através de comunicação direta e anúncios oficiais deverá ocorrer externamente.

  - **Seja sincero e responsável:** Responda à violação de forma honesta e genuína, assumindo a responsabilidade quando a culpa for da organização.

Redução do Impacto (Cont.)

- **Forneça detalhes:** Esteja aberto e explique por que a violação ocorreu e quais informações foram comprometidas. As organizações geralmente cuidam de quaisquer custos do cliente associados aos serviços de roubo de identidade exigidos como resultado de uma violação de segurança.

- **Encontre a causa:** Tome medidas para entender o que causou e facilitou a violação. Isso pode envolver a contratação de especialistas forenses para pesquisar e descobrir os detalhes.

- **Aplicar as lições aprendidas:** Certifique-se de que todas as lições aprendidas nas investigações forenses sejam aplicadas para evitar a ocorrência de violações semelhantes.

- **Verifique e verifique novamente:** Os invasores geralmente tentam deixar um backdoor para facilitar futuras violações. Para evitar isso, você deve garantir que todos os sistemas estejam limpos, sem backdoors de desinstalação e não comprometam mais nada.

- **Educar:** Conscientizar, treinar e educar funcionários, parceiros e clientes sobre como prevenir futuras violações

O Que é Gestão de Riscos?

- **Gestão de riscos:** O processo formal de identificação e avaliação contínua de riscos para reduzir o impacto de ameaças e vulnerabilidades. Não é possível eliminar o risco, mas é possível determinar níveis aceitáveis ponderando o impacto de uma ameaça com o custo de implementação de controlos para a mitigar. O custo da energia deve ser sempre, no máximo, o valor do recurso que você está protegendo.

    - **Enquadrar o risco:** Identifique as ameaças que aumentam o risco. As ameaças podem incluir processos, produtos, ataques, possíveis falhas ou interrupções de serviços, percepção negativa da reputação de uma organização, possíveis responsabilidades legais ou perda de propriedade intelectual.

    - **Avalie o risco:** Determine a gravidade que cada ameaça representa. Por exemplo, algumas ameaças podem paralisar toda uma organização, enquanto outras podem ser apenas pequenos inconvenientes. Você pode priorizar o risco avaliando o impacto financeiro (uma análise quantitativa) ou o efeito em escala na operação de uma organização (pesquisa qualitativa).

O que é Gestão de Riscos? (Cont.)

- **Responder ao risco:** Desenvolva um plano de ação para reduzir a exposição geral ao risco da organização, detalhando onde o risco pode ser eliminado, mitigado, transferido ou aceito.

- **Monitore o risco:** Revise continuamente qualquer risco reduzido por meio de ações de eliminação, mitigação ou transferência. Lembre-se, você não pode eliminar todos os riscos, então você deve monitorar de perto as ameaças.

4.3 Abordagem da Cisco à Cibersegurança

CSIRT da Cisco

- Muitas empresas de grande porte têm uma equipe de resposta a incidentes de segurança computacional (CSIRT-Computer Security Incident Response Team) para recepção, análise e resposta de incidentes de segurança de computador. O Cisco CSIRT vai um passo além e fornece avaliação proativa de ameaças, planejamento de mitigação, análise de tendências de incidentes e revisão da arquitetura de segurança para evitar a ocorrência de incidentes de segurança.

- O CSIRT da Cisco adota uma abordagem proativa, colaborando com o Fórum de Equipes de Segurança e Resposta a Incidentes (FIRST), o National Safety Information Exchange (NSIE), o Defense Security Information Exchange (DSIE) e o DNS Operations Analysis and Research Center (DNS- OARC). Isso garante que estamos atualizados com os novos desenvolvimentos.

- Várias organizações CSIRT nacionais e públicas, como a Divisão CERT do Instituto de Engenharia de Software da Universidade Carnegie Mellon, estão disponíveis para ajudar organizações e CSIRT nacionais a desenvolver, operar e melhorar as suas capacidades de gestão de incidentes.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

computer emergency response team | CERT-EU
for the EU institutions, bodies and agencies

FIRST
Improving Security Together

APCERT
Asia Pacific Computer Emergency Response Team

Software Engineering Institute
Carnegie Mellon University

Manual de Segurança

Uma das melhores maneiras de se preparar para uma violação de segurança é evitá-la. As empresas devem orientar sobre o seguinte:

- como identificar os riscos de segurança digital para sistemas, ativos, dados e recursos
- a implementação de proteções e treinamento de pessoal
- um plano de resposta flexível que minimiza o impacto e os danos em caso de violação de segurança
- a colocação de medidas e processos de segurança deve acontecer após uma violação de segurança.

Todas estas informações devem ser compiladas em um manual de segurança.

Manual de Segurança (Cont.)

Um manual de segurança é uma coleção de consultas ou relatórios repetíveis que descrevem um processo padronizado de detecção e resposta a incidentes. Idealmente, um manual de segurança deve:

- destacar como identificar e automatizar a resposta a ameaças comuns, como a detecção de máquinas infectadas por malware, atividade de rede suspeita ou tentativas de autenticação irregular
- Descrever e definir claramente o tráfego de entrada e saída
- Fornecer informações resumidas, incluindo tendências, estatísticas e contagens
- Fornecer acesso utilizável e rápido às principais estatísticas e métricas
- Correlacionar eventos em todas as fontes de dados relevantes.

Ferramentas para Prevenção e Detecção de Incidentes

Estas são algumas das ferramentas usadas para detectar e prevenir incidentes de segurança:

- Um sistema **Security Information and Event Management (SIEM)** coleta e analisa alertas de segurança, logs e outros dados históricos e em tempo real de dispositivos de segurança na rede para facilitar a detecção precoce de ataques cibernéticos.

- Um sistema de **Data Loss Prevention (DLP)** é projetado para impedir que dados confidenciais sejam roubados ou escapem de uma rede. Ele monitora e protege dados em três estados diferentes: dados em uso (acessando dados por um usuário), dados em movimento (dados viajando pela rede) e dados em repouso (dados armazenados em uma rede ou dispositivo de computador).

Cisco ISE e TrustSec

O Cisco Identity Services Engine (ISE) e o TrustSec reforçam o acesso do usuário aos recursos de rede ao criar políticas de controle de acesso por função.

4.4 Questionário do Módulo

O que Aprendi Neste Módulo?

- Os dispositivos de segurança podem ser dispositivos autônomos, como um roteador, ou ferramentas de software executadas em um dispositivo de rede.
- Nas redes de computadores, um design de firewall controla ou filtra quais comunicações são permitidas dentro e fora de um dispositivo ou rede.
- A varredura de portas investiga um computador, servidor ou outro host de rede em busca de portas abertas.
- Sistemas de detecção de intrusão (IDSs) e sistemas de prevenção de intrusão (IPSs) são medidas de segurança implantadas em uma rede para detectar e prevenir atividades maliciosas.
- A detecção de ataques em tempo real requer uma verificação ativa de ataques usando firewalls e dispositivos de rede IDS/IPS.
- A segurança baseada em comportamento é uma forma de detecção de ameaças que captura e analisa o fluxo de comunicação entre um usuário na rede local e um destino local ou remoto.
- O NetFlow é um componente importante na análise e detecção baseada em comportamento.

O que Aprendi Neste Módulo? (Cont.)

- Um pen test busca violar sistemas, pessoas, processos e códigos para descobrir vulnerabilidades exploráveis.
- **A gestão de riscos** é o processo formal de identificação e avaliação contínua de riscos para reduzir o impacto de ameaças e vulnerabilidades.
- Um manual de segurança é uma coleção de consultas ou relatórios repetíveis que descrevem um processo padronizado de detecção e resposta a incidentes.