TEMA 04
Identificação de Vulnerabilidades

Habilidades:

- Entender as principais ameaças e vulnerabilidades atuais.
- Identificar fatores de riscos digitais e humanos.
- Entender sistemas de defesa e resolução de falhas digitais e humanas.

É inevitável não falarmos sobre vulnerabilidades quando mencionamos a Segurança da Informação e Cyber Security. Com o aumento e agressividade dos ataques a cada dia, o profissional de S.I. sempre deve estar atento a todo o ambiente.
A **identificação de vulnerabilidades** é um processo essencial na área de Segurança da Informação. Por meio desse processo, é possível identificar falhas, fraquezas e lacunas nos sistemas, redes e aplicativos, o que permite que medidas de proteção sejam tomadas antes que sejam exploradas por ameaças maliciosas. Esta apostila fornecerá uma visão geral dos elementos fundamentais da identificação de vulnerabilidades.
É preciso **compreender como identificar e categorizar uma vulnerabilidade, pressentir as prováveis ameaças que ela pode trazer**, gerando riscos em potencial aos ativos de informação.

O que são vulnerabilidades?

São pontos fracos em sistemas ou redes que podem ser explorados por ameaças para comprometer a Segurança da Informação. Essas vulnerabilidades podem incluir **falhas de software, configurações incorretas, deficiências na infraestrutura de rede e outros fatores que podem ser explorados para obter acesso não autorizado**, comprometer a integridade dos dados ou interromper os serviços.

Importância da identificação de vulnerabilidades

A identificação de vulnerabilidades é crucial para a Segurança da Informação, pois facilita que as organizações ajam proativamente para mitigar riscos e evitar possíveis ataques. Ao identificar e corrigir vulnerabilidades, é possível reduzir as chances de violações de segurança, minimizar impactos negativos e proteger ativos críticos de informações.

Métodos de identificação de vulnerabilidades

Existem **diferentes métodos e ferramentas disponíveis** para a identificação de vulnerabilidades.

Alguns dos métodos comumente utilizados incluem:

- **Scanners de vulnerabilidades:** Ferramentas automatizadas que examinam sistemas, redes ou aplicativos em busca de vulnerabilidades conhecidas.
- **Testes de penetração:** Processo controlado que simula um ataque real para identificar e explorar vulnerabilidades existentes.
- **Análise de código:** Revisão do código-fonte de um software em busca de falhas e vulnerabilidades.
- **Análise de configuração:** Avaliação das configurações de sistemas e redes para identificar erros de configuração que possam criar vulnerabilidades.

Ciclo de Identificação de Vulnerabilidades

O ciclo de identificação de vulnerabilidades envolve as seguintes etapas:

- **Planejamento:** Definição de escopo, objetivos e métodos para a identificação de vulnerabilidades.

- **Coleta de informações:** Reunião de dados relevantes sobre os sistemas, redes e aplicativos a serem analisados.
- **Análise:** Avaliação das informações coletadas para identificar vulnerabilidades e determinar seu impacto potencial.
- **Classificação:** Classificação das vulnerabilidades identificadas com base em sua gravidade e prioridade.
- **Relatório:** Elaboração de um relatório detalhado que descreve as vulnerabilidades identificadas, suas possíveis consequências e recomendações para mitigação.

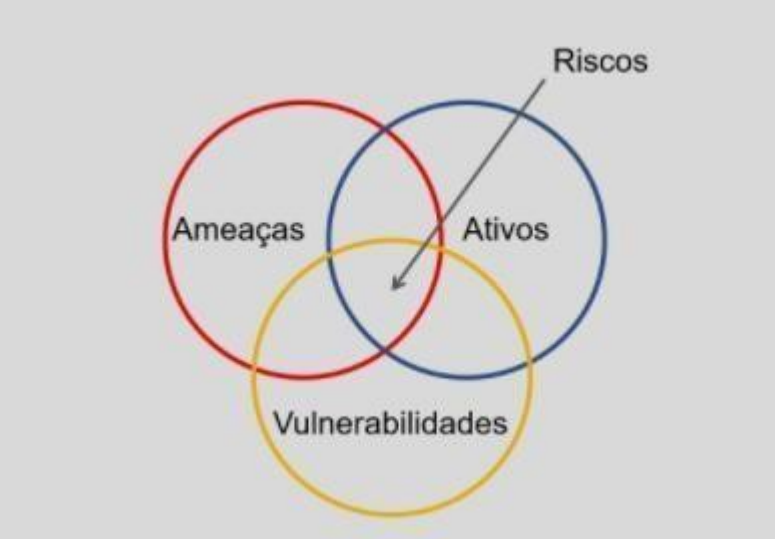
Ameaças

As **ameaças** são os resultados das vulnerabilidades. Seja de modo intencional ou acidental, elas exploram as brechas, o que pode causar danos aos ativos de informação.

Riscos

Os **riscos** são as possíveis resultantes das ameaças caso estas sejam realmente iminentes. É a futura concretização do dano, acesso não autorizado ou destruição dos ativos na hipótese que estes não sejam mitigados e tratados.

A lógica é a seguinte: Se você tem um ativo que está sendo ameaçado devido a uma vulnerabilidade, logo o ativo está em risco. A fórmula usada para contextualizar é:



Sendo assim, podemos concluir que o risco é o resultado de uma ameaça que abusa de uma vulnerabilidade. Se não existirem vulnerabilidades, dificilmente haverá riscos.

A identificação das vulnerabilidades servirá, justamente, às correções das brechas e falhas que foram antecipadamente analisadas e classificadas pelo profissional de S.I. Estas correções irão partir de uma estratégia operacional e educacional que implementará todas as medidas necessárias para tratar este ambiente e torná-lo mais robusto a novas vulnerabilidades que possam surgir no futuro. Ela garantirá a saúde da infraestrutura e aplicações da empresa de modo geral.

Mas, afinal, como identificamos vulnerabilidades?

Identificação de Vulnerabilidades

Antes de tudo, devemos nos atentar e estudar as fragilidades do ambiente organizacional.

Partimos, a princípio, do levantamento dos ativos de informação e sua análise total. Desde os próprios dados e informações armazenados, como os servidores e outros equipamentos. Após isso, abordaremos o ambiente da organização para identificar as falhas. Alguns apontamentos que podemos realizar são os seguintes:

Gestão humana – Uma empresa não é feita simplesmente de equipamentos e aplicações. Precisamos de colaboradores que realizem sua função de maneira segura e exatamente de acordo com o que lhe foi ensinado e instruído. Por isso, devemos nos atentar em alguns pontos:

- Analisar a conduta dos usuários ao utilizarem sistemas operacionais;
- Checar se há um controle hierárquico de acessos, sejam eles virtuais ou físicos;
- Ver se a empresa oferece treinamentos para que os usuários utilizem ferramentas e sistemas;
- Analisar o cotidiano para checar se estas condutas e orientações são realmente feitas ou se há más práticas que devem ser revistas.

Softwares e Hardwares desatualizados – A organização deve sempre estar atenta aos sistemas e dispositivos operadores. A falta de reparos e atualizações acarreta em diversas vulnerabilidades, já que, ao longo do tempo, novas tecnologias mais seguras tomam conta do mercado e as antigas perdem suporte e se tornam obsoletas e inseguras. Veja abaixo alguns pontos:

- Checar qual sistema operacional está instalado nos computadores e se estão com as atualizações em dia;
- Avaliar as condições físicas dos equipamentos como computadores e servidores, e se necessitam de reparos, upgrades, limpeza ou substituição;
- Verificar se existe um Firewall e/ou antivírus em todos os equipamentos;
- Analisar se há um monitoramento na infraestrutura de rede;
- Verificar se a empresa está conforme a legislação vigente no âmbito da Segurança da Informação.

Ambiente

Por incrível que pareça, **fatores ambientais podem incidir em vulnerabilidades**. Veja alguns levantamentos de ambiente abaixo:

- Analisar as condições de temperatura para o pleno funcionamento de dispositivos informáticos como computadores e servidores;
- Verificar as condições de estrutura do local para desastres naturais como incêndios e enchentes;
- Analisar se a empresa possui algum tipo de controle perante quedas súbitas de energia.

Após identificarmos as vulnerabilidades, devemos categorizá-las para modelar e arquitetar as estratégias às devidas resoluções. Há **diversas maneiras de categorizar e avaliar vulnerabilidades**. Iremos utilizar o **Microsoft Stride**, pois é o mais popular.
O método Stride utiliza seu nome para definir seu conceito. Cada letra aponta a uma ameaça em potencial causada por uma vulnerabilidade e que traz os riscos de violação.

S – *Spoofing*: falsificação de identidade e dados.
T – *Tampering*: Adulteração de dados e informações.
R – *Repudiation*: Repúdio.
I – *Information Disclosure*: Exposição de dados e informações confidenciais.
D – *Denial of Service*: Ataques voltados à negação de serviço.
E – *Elevation of privilege*: Elevação de privilégio.

Com essa modelagem, os profissionais poderão analisar e enumerar as ameaças e vulnerabilidades e priorizar as que demandam mais urgência.
Após realizarmos o procedimento de identificação e categorização das vulnerabilidades, poderemos remediá-las e tomar medidas de conscientização a partir das políticas de Segurança da Informação, que já aprendemos anteriormente. Assim, os profissionais de T.I. irão conseguir investigar e reduzir

as vulnerabilidades, as ameaças e os riscos, e resolvê- los o mais breve possível.
Lembre-se que cada organização possui um ambiente diferente e pendências de segurança diferentes a serem resolvidas, ou seja, as medidas que devem ser tomadas poderão ter o leque aberto ou específico para cada situação.

Algumas medidas que podemos tomar após levantarmos as vulnerabilidades são:

- Criar ou atualizar políticas de segurança com foco em resolver vulnerabilidades
- Investimento no treinamento dos usuários em geral, para nivelar o conhecimento e tratar os maus hábitos;
- Implantar ou rever o monitoramento para controle dos sistemas, aplicações e infraestrutura de redes, com profissionais qualificados;
- Manter os dispositivos e sistemas atualizados com antivírus e firewall de qualidade;
- Padronizar todo o ambiente para que respeite as leis vigentes.

Desafios cibernéticos: Através da análise, planejamento e execução de boas práticas, o profissional de S.I. diminui exponencialmente os riscos e ameaças que circundam uma aplicação, infraestrutura ou um ambiente corporativo inteiro.

ATENÇÃO: https://www.zaproxy.org/
ZAP, anteriormente conhecido como OWASP ZAP, é um scanner de segurança de aplicativos da web de código aberto. Ele deve ser usado tanto por iniciantes em segurança de aplicativos quanto por testadores de penetração profissionais.

OWASP ZAP (Zed Attack Proxy) pode ser considerado tanto um scanner de vulnerabilidades quanto uma ferramenta de teste de penetração. Ele possui funcionalidades que abrangem ambos os aspectos:

Scanner de Vulnerabilidades
Como scanner de vulnerabilidades, OWASP ZAP:

1. **Exploração Automática:** Possui mecanismos automatizados, como o spidering, para explorar a aplicação e identificar pontos de entrada.
2. **Escaneamento de Vulnerabilidades:** Realiza escaneamentos ativos e passivos para detectar vulnerabilidades conhecidas, como SQL Injection, Cross-Site Scripting (XSS), entre outras.
3. **Relatórios de Vulnerabilidades:** Gera relatórios detalhados das vulnerabilidades encontradas, categorizando-as por severidade e oferecendo recomendações para correção.

Teste de Penetração
Como ferramenta de teste de penetração, OWASP ZAP:

1. **Interatividade:** Permite que os testadores interajam manualmente com a aplicação, manipulando e analisando requisições HTTP/HTTPS.
2. **Interceptação de Tráfego:** Funciona como um proxy intermediário, permitindo a captura e modificação de requisições e respostas para testar a robustez da aplicação.
3. **Ferramentas Avançadas:** Inclui ferramentas como o fuzzing, que envia dados aleatórios ou malformados para a aplicação, ajudando a identificar falhas de segurança não triviais.
4. **Scripts Personalizados:** Suporta scripts personalizados que podem ser usados para realizar testes de penetração específicos e avançados.

Conclusão

OWASP ZAP é uma ferramenta versátil que pode ser usada para ambos os propósitos:

- **Scanner de Vulnerabilidades:** Ideal para uma análise automatizada e contínua de vulnerabilidades.
- **Teste de Penetração:** Útil para uma análise mais profunda e interativa, onde um testador pode explorar manualmente a aplicação e identificar falhas de segurança que um scanner automatizado pode não detectar.

Essa dualidade faz do OWASP ZAP uma ferramenta valiosa tanto para desenvolvedores quanto para profissionais de segurança que desejam garantir a robustez e a segurança de suas aplicações web.

RESUMO

Com o avanço da tecnologia e a crescente digitalização, as ameaças e vulnerabilidades têm se intensificado, e variam de invasões cibernéticas, ataques de phishing, ransomware, até a exploração de vulnerabilidades em softwares e hardware. Por outro lado, fatores de risco humano, como a falta de treinamento adequado e comportamentos de risco, como o uso de senhas fracas ou a abertura de e-mails desconhecidos, também permitem o acesso não autorizado aos sistemas. Além disso, a implementação de tecnologias emergentes, como a Internet das Coisas (IoT) e a Inteligência Artificial (IA), aumenta a superfície de ataque, e exigem uma compreensão mais profunda dos riscos digitais associados.

Na luta contra estas ameaças, a adoção de sistemas de defesa robustos é fundamental. Isso inclui a implementação de firewalls, programas antivírus, sistemas de detecção e prevenção de intrusões, bem como a criptografia de dados. Sem contar, estratégias de defesa em profundidade, como a segmentação de redes, podem minimizar o impacto de um ataque. Do lado humano, a educação e o treinamento em segurança cibernética são fundamentais para minimizar os riscos.

ATIVIDADES

1. O que são vulnerabilidades de segurança da informação?

Vulnerabilidades de segurança da informação são pontos fracos em sistemas ou redes que podem ser explorados por ameaças para comprometer a segurança da informação. Essas vulnerabilidades podem incluir falhas de software, configurações incorretas, deficiências na infraestrutura de rede e outros fatores que podem ser explorados para obter acesso não autorizado, comprometer a integridade dos dados ou interromper os serviços.

2. Qual é a importância da identificação de vulnerabilidades em um ambiente de Segurança da Informação?

A identificação de vulnerabilidades é crucial para a segurança da informação, pois permite que as organizações ajam proativamente para mitigar riscos e evitar possíveis ataques. Ao identificar e corrigir vulnerabilidades, é possível reduzir as chances de violações de segurança, minimizar impactos negativos e proteger ativos críticos de informações. Isso ajuda a manter a integridade, confidencialidade e disponibilidade dos dados e sistemas.

3. Quais são algumas das principais consequências de não identificar e corrigir vulnerabilidades em um sistema?

- **Acesso não autorizado:** Invasores podem explorar vulnerabilidades para obter acesso não autorizado a sistemas e dados sensíveis.
- **Comprometimento da integridade dos dados:** Dados podem ser alterados, corrompidos ou excluídos por atacantes.
- **Interrupção dos serviços:** Ataques podem causar a interrupção de serviços críticos, resultando em perda de produtividade e receita.
- **Roubo de informações:** Dados confidenciais podem ser roubados, levando a violações de

privacidade e danos à reputação.

- **Custos elevados:** A resposta a incidentes de segurança e a recuperação de ataques podem ser caros e consumir muitos recursos.

4. Explique a diferença entre scanners de vulnerabilidades e testes de penetração. Quando cada um desses métodos é mais adequado para identificar vulnerabilidades?

- **Scanners de vulnerabilidades:** São ferramentas automatizadas que examinam sistemas, redes ou aplicativos em busca de vulnerabilidades conhecidas. Eles são rápidos e podem cobrir uma ampla gama de sistemas e dispositivos. São mais adequados para a identificação inicial de vulnerabilidades e para realizar verificações regulares.
- **Testes de penetração:** São processos controlados que simulam ataques reais para identificar e explorar vulnerabilidades existentes. Eles são realizados manualmente por profissionais qualificados e fornecem uma visão mais profunda e detalhada das vulnerabilidades, incluindo aquelas que podem não ser detectadas por scanners automatizados. São mais adequados para avaliações detalhadas e para confirmar a eficácia das medidas de segurança implementadas.

5. Cite três exemplos de informações que podem ser coletadas durante a fase de coleta de informações no processo de identificação de vulnerabilidades. Por que essas informações são relevantes para a análise de vulnerabilidades?

- **Configurações de sistemas e redes:** Informações sobre configurações de firewall, políticas de senha, configurações de segurança do sistema operacional, entre outros. Estas informações são relevantes porque configurações inadequadas podem criar vulnerabilidades.
- **Versões de software e firmware:** Informações sobre as versões dos sistemas operacionais, aplicativos e firmware dos dispositivos. Estas informações são relevantes porque versões desatualizadas podem conter vulnerabilidades conhecidas que foram corrigidas em versões mais recentes.
- **Logs de atividade e eventos de segurança:** Informações de logs de eventos de segurança e atividades de usuários e sistemas. Estas informações são relevantes porque podem indicar tentativas de exploração de vulnerabilidades, bem como fornecer contexto sobre como as vulnerabilidades podem ser exploradas.