Resumo Prova 2
Segurança da Informação

9 de setembro de 2024

0.1 Aulas

0.1.1 Aula 5.0 - Ataques Maliciosos, Ameaças e Vulnerabilidades

Segurança está na proteção de ativos de algum invasor

- Ativo é qualquer item que tenha valor para uma organização, sendo eles:
- **TI e infraestrutura de rede** - Hardware, software e serviços.
- **Propriedade intelectual** - Dados confidenciais como patentes, código-fonte, fórmulas ou projetos de engenharia.
- **Finanças e dados financeiros** - Contas bancárias, dados de cartão de crédito e de transações financeiras.
- **Disponibilidade e produtividade de serviços** - A capacidade de serviços computacionais e de software em dar suporte à produtividade para humanos e máquinas
- **Reputação** - Conformidade corporativa e imagem da marca.

O termo Hacker pode ser dividido em 3 categorias, sendo elas:

- **Hacker Black-Hat** : Alguém que invade sistemas de forma maliciosa, para roubar informações e obter algum ganho pessoal. Eles não tem a permissão para acessar os sistemas.
- **Hacker White-Hat** : Conhecidos também como hackers éticos. São pessoas contratadas para identificar falhas no sistema através de testes de invasão. Depois dos testes é gerado um relatório das vulnerabilidade existes e repassado para a organização.
- **Hacker Gray-Hat** : São os hacker que ficam entre o Black-hat e White-hat. É alguém que invade os sistemas sem permissão, mas geralmente sem intenção maliciosa, apenas para explorar as vulnerabilidades. Podem divulgar o não as vulnerabilidade existes para a organização.
- Já um **Cracker** é alguém com intenção hostil, possui habilidade sofisticadas e pode estar interessado em ganho financeiro.
- Existe também os chamados **Script Kiddie** que são pessoas com pouca habilidade, que apenas seguem seguem instruções para realizar um ataque

Ferramentas utilizadas por indivíduos maliciosos

- Varredura de vulnerabilidades(Scanner), Programas de varredura de portas, Farejadores(Sniffers), Programa para captura de teclado(Keyloggers).

O que é uma brecha de segurança

- Qualquer evento que resulte em uma violação de qualquer um dos princípios de segurança é uma brecha de segurança
- Pode ser acidental ou maliciosa, e pode afetar a capacidade de uma organização realizar negócios.
- **Common Vulnerabilities and Exposures - CVE** - Sistema de nomenclatura e identificação de vulnerabilidades de segurança em software, mantido pela Mitre Corporation e padroniza a referência de vulnerabilidades. Quando uma vulnerabilidade é descoberta ela recebe um número de identificação único no CVE. Ex: CVE-2021-1234.

Atividades que podem causar uma brecha de segurança

- Ataques de negação de serviço, onde é apenas um computador realizando o ataque**(Denial of Service - DOS)**
- Ataques de negação de serviço distribuidos onde são vários computadores realizando o ataque a um serviço **Distributed Denial of Service - DDoS**

  Ataques de negação de serviço podem ser **Lógicos** - Usam falhas de software para arruinar o desempenho de servidores remotos. Ou **Inundação** - Comprometem a CPU, memória e recursos de rede do computador-vítima com o envio de pacotes SYN.
- Comportamento inaceitável de navegador web.
- Uso de backdoor(porta de entrada) para acessar recursos.
- Modificações acidentais em dados.
- **SPAM** é uma mensagem de e-mail ou mensagens instantâneas indesejadas, basicamente contem anúncios comerciais.
- **Hoax** ou (boato) é um ato com intenção de enganar alguém ou defraudar o receptor.
- **Cookies** é um arquivo com detalhes colhidos em visitas anteriores a um sítio web. Pode conter nome de usuários, informações pessoais e outros.

Vulnerabilidades e Ameaças

- Uma **Ameaça** é qualquer ação que possa danificar um ativo.

  Ameaças mais comuns são: Software malicioso, Falha de hardware ou software, atacante interno, roubo de equipamento, atacante externo, desastre natural, espionagem industrial, terrorismo

– Uma **Vulnerabilidade** é qualquer ponto fraco em um sistema que possibilite que uma ameaça causa danos a ele.

Ataque

– Existem 4 categorias de ataque

– **Fabricação** - Criação de uma fraude de modo a enganar o usuário

– **Interceptação** - Escuta transmissões e redireciona para uso não autorizado.

– **Interrupção** - Causa uma quebra em um canal de comunicação

– **Modificação** - Alteração dos dados contidos em transmissões ou arquivos.

0.2 Listas

0.2.1 Lista 05 - Ataques Maliciosos, Ameaças e Vulnerabilidades

1. O principal objetivo de um ciberataque é afetar um ou mais ativos de TI.
   (a) Verdadeiro
   (b) Falso
2. Qual dos seguintes descreve melhor a propriedade intelectual?
   (a) Os itens que uma empresa protegeu por direitos autorais.
   (b) Todas as patentes pertencentes a uma empresa.
   (c) O conhecimento exclusivo que uma empresa possui.
   (d) O pessoal engajado em uma pesquisa exclusiva.
3. Qual dos seguintes termos descreve melhor uma pessoa com muito pouca habilidade?
   (a) Hacker
   (b) Script kiddie
   (c) Cracker
   (d) Aspirante
4. Um(a) Spyware é um software que captura tráfego enquanto ele atravessa uma rede.
5. Qual tipo de ataque resulta em usuários legítimos sem acesso a um recurso de sistema?

(a) DoS

(b) IPS

(c) Homem no meio

(d) Cavalo de Troia

6. Um ataque de inundação de SYN inunda um alvo com pacotes de rede inválidos.

   (a) Verdadeiro

   (b) Falso

7. Qual das seguintes medidas pode proteger melhor seu computador contra worms?

   (a) Instalar software antimalware

   (b) Configurar um firewall para bloquear todas as portas

   (c) Criptografar todos os discos

   (d) Impor senhas fortes para todos os usuários

8. Um ataque de dicionário é um ataque simples, que conta principalmente com usuários que escolhem senhas fracas.

   (a) Verdadeiro

   (b) Falso

9. Qual tipo de ataque envolve capturar pacotes de dados de uma rede e retransmiti-los mais adiante para produzir um efeito não autorizado?

   (a) Homem no meio

   (b) Inundação de SYN

   (c) Retransmissão (replay)

   (d) Smurf

10. Um(a) Ameaça é qualquer ação que possa danificar um ativo.

11. Um(a) Vulnerabilidade é qualquer falha que torne possível para uma ameaça causar danos a um computador ou uma rede.

12. Qual tipo de malware é um programa autocontido que se replica e envia cópias de si mesmo para outros computadores, geralmente por uma rede?

    (a) Vírus

    (b) Verme

    (c) Cavalo de Troia

    (d) Rootkit

0.2.2 Lista 06 - de Controle de Acesso

1. Qual resposta descreve melhor o componente de autorização de controle de acesso?

   (a) Autorização é o método que um sujeito utiliza para solicitar acesso a um sistema.

   (b) Autorização é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

   (c) Autorização é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   (d) Autorização é o processo de determinar quem está aprovado para acesso para quais recursos.

2. Qual resposta descreve melhor o comportamento de identificação de controle de acesso?

   (a) Identificação é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   (b) Identificação é o método que um sujeito utiliza para solicitar acesso a um sistema.

   (c) Identificação é o processo de determinar quem está aprovado para acesso e para quais recursos.

   (d) Identificação é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

3. Qual resposta descreve melhor o componente de autenticação de controle de acesso?

   (a) Autenticação é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

   (b) Autenticação é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

   (c) Autenticação é o processo de determinar quem está aprovado para acesso e para quais recursos.

   (d) Autenticação é o método que um sujeito utiliza para solicitar acesso a um sistema.

4. Qual resposta descreve melhor o componente de responsabilização de controle de acesso?

   (a) Responsabilização é a validação ou prova de que o sujeito que recebeu o acesso foi o mesmo que o solicitou.

(b) Responsabilização é o método que um sujeito utiliza para solicitar acesso a um sistema.

(c) Responsabilização é o processo de criar e manter as políticas e os procedimentos necessários para garantir que informação apropriada esteja disponível quando uma organização for auditada.

(d) Responsabilização é o processo de determinar quem está aprovado para acesso e para quais recursos.

5. Quando acessa uma rede, você recebe uma combinação de nome de usuário, senha, token, cartão inteligente ou biometria. Você, então, terá acesso autorizado ou negado pelo sistema. Este é um exemplo de .

   (a) Controles de acesso físico.

   (b) Controles de acesso lógico.

   (c) Política de inclusão de grupo.

   (d) Nenhuma das alternativas anteriores.

6. Acesso físico, contorno de segurança e interceptação são exemplos de como os controles de acesso podem ser .

   (a) Roubados

   (b) Comprometidos

   (c) Auditados

   (d) Autorizados

7. Desafios de controle de acesso incluem qual dos seguintes?

   (a) Perda de laptop

   (b) Exploração de hardware

   (c) Interceptação

   (d) Exploração de aplicativos

   (e) Todas as alternativas anteriores

8. Analise:

   - I. Segurança física está associada à proteção de recursos através de controles como guardas, iluminação e detectores de movimento.
   - II. Controle de acesso através de usuário e senha específicos em um determinado software aplicativo pode ser caracterizado como um controle físico.
   - III. A segurança física está associada ao ambiente e a segurança lógica aos programas.
   - IV. A segurança lógica deve ocorrer após a segurança física, através de softwares e protocolos.

São corretas as afirmações:

(a) somente I, II e III
(b) somente I, II e IV
(c) somente II, III e IV
(d) somente I, III e IV
(e) I, II, III e IV

9. A respeito do controle de acesso a redes e aplicações, assinale, dentre as alternativas a seguir, a única que contém a ordem correta dos procedimentos lógicos atravessados por um usuário para acessar um recurso:

(a) Autenticação, Identificação, Autorização e Auditoria.
(b) Identificação, Autenticação, Autorização e Auditoria.
(c) Autorização, Identificação, Autenticação e Auditoria.
(d) Autorização, Autenticação, Identificação e Auditoria.
(e) Bloqueio, Autenticação, Autorização e Auditoria.

10. A biometria se refere a várias técnicas de autenticação, para distinguir um indivíduo do outro, baseando-se nas características:

(a) comportamentais, somente.
(b) físicas e/ou lógicas.
(c) físicas e/ou comportamentais.
(d) físicas, somente.
(e) lógicas, somente.

11. Obter confiança sobre a identidade de agentes ou integridade de dados em comunicação, baseando-se na posse de informação sigilosa (senha), dispositivos (smartcard), dado biométrico (impressão digital, retinal, etc) ou nas combinações destes elementos, trata-se do conceito de:

(a) criptografia.
(b) autenticação.
(c) assinatura digital.
(d) certificado digital.
(e) função de hash.

12. Na ausência temporária do operador, o acesso ao computador por pessoa não autorizada pode ser evitado, de forma ideal, com a utilização de:

(a) uma senha inserida na proteção de tela do Windows.
(b) uma senha inserida no boot do computador.

(c) uma senha inserida para acesso ao disco rígido.

(d) desligamento do monitor, após alguns minutos de inatividade.

(e) desligamento do computador, sempre que o operador se retirar.

13. Os métodos para implementação de um controle de acesso efetivo envolvem:

(a) política de senhas, adoção de antivírus e firewall.

(b) identificação, autenticação, autorização e auditoria.

(c) assinatura digital, detecção de intrusão e criptografia.

(d) política de senhas, plano de bloqueio e liberação.

(e) processo de login e rotinas de backup.

0.2.3 Lista 07 - Gerenciamento de Riscos e Plano de Continuidade de Negócios

1. De acordo com o PMI, qual termo descreve a lista de riscos identificados?

(a) Lista de verificação de riscos

(b) Registrador de riscos

(c) Metodologia de riscos

(d) Lista de atenuação

2. Que tipo de análise de risco usa fórmulas e valores numéricos para indicar seriedade de risco?

(a) Análise objetiva de risco

(b) Análise qualitativa de risco

(c) Análise subjetiva de risco

(d) Análise quantitativa de risco

3. Qual tipo de análise de risco usa classificação relativa?

(a) Análise objetiva de risco

(b) Análise qualitativa de risco

(c) Análise subjetiva de risco

(d) Análise quantitativa de risco

4. Qual valor de análise de risco representa a probabilidade anual de uma perda?

(a) EF

(b) SLE

(c) ALE

(d) ARO

5. Qual opção de resposta a risco descreveria melhor a realização de um seguro contra incêndio?

   (a) Aceitar
   (b) Atenuar
   (c) Transferir
   (d) Evitar

6. Qual resposta a risco seria mais apropriada se a possibilidade do impacto de um risco se tornar realidade for desprezível?

   (a) Aceitar
   (b) Atenuar
   (c) Transferir
   (d) Evitar

7. Qual das seguintes afirmações descreve melhor a relação entre um BCP e um DRP?

   (a) Um BCP é obrigatório, mas um DRP não.
   (b) Um DRP é um componente de um BCP.
   (c) Um DRP é obrigatório, mas um BCP não.
   (d) Um BCP é um componente de um DRP.

8. Qual termo é usado para indicar a quantidade de perda de dados aceitável?

   (a) RAI
   (b) ROI
   (c) RTO
   (d) RPO

9. Qual metodologia de avaliação de risco é comercializada como abordagem autodirecionada e tem duas edições diferentes para organizações de tamanhos diferentes?

   (a) CRAMM
   (b) OCTAVE
   (c) NIST
   (d) EBIOS

10. Um Analista de Segurança de Informações do Tribunal de Justiça está redigindo um documento que estabelece ações de monitoração de riscos e prevenção de problemas, de forma a evitar interrupções em operações do negócio. Esse documento será parte integrante

(a) do Plano de Recuperação de Desastres.

(b) do Plano de Continuidade dos Negócios.

(c) do Plano de Segurança da Informação.

(d) da Estratégia de Serviços de TI.

11. No que se refere ao plano de continuidade de negócios, assinale a opção correta.

(a) Os objetivos do plano em tela incluem evitar a interrupção das atividades do negócio, proteger os processos críticos contra o acesso de pessoas estranhas ao ambiente e assegurar a retomada dos processos em tempo hábil, caso necessário.

(b) A existência de um gestor específico para cada plano de continuidade é desvantajoso, visto que causa aumentos significativos dos custos dos planos como um todo.

(c) Os planos de continuidade do negócio devem ser testados e atualizados infrequentemente, já que a realização regular dessas ações acarreta o aumento significativo dos custos dos planos.

(d) A estrutura de planejamento para continuidade de negócios deve abranger os ativos e os recursos críticos para uma eventual utilização dos procedimentos de emergência, recuperação e ativação.

12. O plano de continuidade do negócio deve

(a) ter a mesma definição e desenvolvimento para todas as organizações e utilizar uma abordagem genérica, já que dessa forma poderá abranger todos os aspectos críticos que causam impactos negativos ao negócio.

(b) ser eficiente e eficaz, ser mantido atualizado e ser testado periodicamente contando com a participação de todos os envolvidos.

(c) ser do conhecimento apenas da alta administração que deve conhecer e aprovar as ameaças e riscos que estão fora do escopo do plano.

(d) ser elaborado de forma que possibilite seu funcionamento em condições perfeitas, em nível otimizado, garantindo que não haja a possibilidade de incidentes que gerem impactos financeiros ou operacionais.

13. O Plano de Continuidade do Negócio:

(a) não precisa ser testado antes que se torne realmente necessário, pois testes por si só implicam em riscos aos ativos de informação.

(b) prioriza e estabelece as ações de implantação como resultado de uma ampla análise de risco.

(c) define uma ação de continuidade imediata e temporária.

(d) precisa ser contínuo, evoluir com a organização, mas não precisa ser gerido sob a responsabilidade de alguém como os processos organizacionais.

14. Considerando a TI, as empresas devem ter constante preocupação com os riscos, que se concretizados, podem vir a prejudicar suas atividades. Dessa forma, a gestão de riscos é uma atividade de grande importância na condução dos negócios de uma empresa. Na maioria dos casos, a primeira etapa a ser realizada na gestão de riscos é a identificação dos riscos, que consiste em

    (a) elaborar os planos de contingência, cujo objetivo é obter um controle preciso dos riscos presentes.

    (b) minimizar os problemas que possam surgir, eventualmente, em função dos riscos existentes.

    (c) detectar os perigos potenciais que possam vir a prejudicar as operações da empresa, como a execução de um projeto de TI.

    (d) registrar todas as ações tomadas no decorrer da concretização de um risco de forma a evitar problemas semelhantes no futuro.

0.2.4 Lista 08 - Auditoria de Sistemas

1. Qual dos seguintes é um exemplo de um nível de permissividade?

    (a) Prudente

    (b) Permissivo

    (c) Paranóico

    (d) Promíscuo

    (e) Todas as alternativas anteriores

2. Uma auditoria examina se os controles de segurança são apropriados, estão instalados corretamente e são/estão .

    (a) Atualizados

    (b) Cuidando de seu objetivo

    (c) Autorizados

    (d) Econômicos

3. Uma é um padrão usado para medir quão efetivo seu sistema é em relação a expectativas do setor.

    (a) Objetivo de controle

    (b) Configuração

    (c) Padrão de referência (benchmark)

    (d) Política

4. Atividades de pós-auditoria incluem qual das seguintes?

    (a) Apresentar descobertas à gerência

(b) Analisar dados

(c) Entrevistas de saída

(d) Análise de descobertas do auditor

(e) Todas as alternativas anteriores

5. é usado quando não é tão crítico detectar e responder a incidentes imediatamente.

   (a) Monitoramento que não seja em tempo real

   (b) Um controle de acesso lógico

   (c) Monitoramento em tempo real

   (d) Nenhuma das alternativas anteriores

6. Uma plataforma comum para capturar e analisar entradas de histórico é .

   (a) Sistema de detecção de intrusos (IDS)

   (b) Honeypot

   (c) Informação de Segurança e Gerenciamento de Evento (SIEM - Security Information and Event Management)

   (d) HIPAA

7. Em métodos ., o IDS compara tráfego atual com padrões de atividade consistente com aqueles de uma intrusão de rede conhecida via casamento de padrão e casamento de estado.

   (a) Baseados em assinatura

   (b) Baseados em anomalia

   (c) De varredura heurística

   (d) Todas as alternativas anteriores

8. Isolamento de computador é o isolamento de redes internas e o estabelecimento de um(a) .

   (a) HIDS

   (b) DMZ

   (c) IDS

   (d) IPS

9. A análise do sistema para descobrir o máximo possível sobre a organização, seus sistemas e redes é conhecida como .

   (a) Teste de penetração

   (b) Teste de vulnerabilidade

   (c) Mapeamento de rede

   (d) Reconhecimento