Estratégia Concursos

Aula 00

CAGEPA - Segurança da Informação (Parte do Conhecimentos Complementares para Cargos de TI) - 2024 (Pós-Edital)

Autor:
André Castro

13 de Janeiro de 2025

Índice

Índice

APRESENTAÇÃO

Olá, pessoal! Como estão? Espero que bem e animados para essa jornada.

Aqui é o André Castro, professor de Redes de Computadores e Segurança da Informação do Estratégia Concursos. Sou formado em Engenharia de Redes de Comunicação pela Universidade de Brasília – UnB e pós-graduado na área de Segurança e Administração de Redes também pela UnB.

Atualmente, após um ciclo de 14 anos no serviço público como servidor público, fiz uma transição de carreira para o setor privado. Hoje, estou exercendo a função de Estrategista de Governo e Especialista em Transformação Digital na Microsoft Brasil, em Brasília.

Na trajetória de Governo, exerci o último cargo de Analista em Tecnologia do Ministério da Economia ou atual Ministério da Gestão e Inovação, tendo exercido cargos de relevância à frente de unidades de tecnologia do Governo Federal. No último ciclo de Governo, estive como Assessor Especial de Tecnologia na AGU e antes disso, atuei como Subsecretário/CIO de Tecnologia da Informação do Ministério da Educação.

Fui aprovado ainda nos concursos de Analista Administrativo da Câmara dos Deputados, realizado em 2011 e aprovado no concurso de Analista para o Banco Central do Brasil em 2013. Exerci ainda atividades de instrução e apoio em alguns cursos na área de Redes e Segurança pela Escola Superior de Redes – ESR, da Rede Nacional de Pesquisa – RNP, além de outros projetos relacionados a concursos públicos, incluindo aulas presenciais.

Para você que se prepara para concursos públicos na área de tecnologia... Pois bem... preparei um material muito bacana e bem completo sobre os assuntos voltados para a nossa temática, que possuem algumas variações a depender do cargo e do concurso, e por isso buscamos trazer uma abordagem bem completa e eficiente para não deixar lacunas e não exceder conteúdos desnecessariamente.

A ideia é que você possa conhecer os tópicos mais importantes e ter uma abordagem diferenciada e com didática adequada para sua preparação. O meu foco é sempre buscar ser o mais preciso possível nos assuntos, otimizando e muito o seu tempo de preparação. Você perceberá isso ao longo do curso.

Abraço,

Prof. André Castro

@profandrecastro

Instagram YouTube

andrecastroprofessor@gmail.com
/professorandrecastro

Também gostaria de convidá-lo a conhecer alguns projetos da equipe de TI:

//estratégia tech ESTRATEGIA	**Nosso podcast alternativo:** *https://anchor.fm/estrategia-tech*
Telegram a new era of messaging	**Nosso grupo do Telegram:** ***https://t.me/estrategia_ti***
Instagram	**Perfil no Instagram:** *http://instagram.com/estrategiaconcursosti*

Informações Gerais

É nítida a evolução conjunta das partes envolvidas em concursos públicos, uma vez que temos provas cada vez mais difíceis, com um nível maior de inteligência e preparação das questões, bem como o surgimento constante de novos conceitos e abordagens.

Além disso, o nível dos candidatos que têm concorrido às vagas de cargos públicos tem aumentado e tende a continuar aumentando, como se pode verificar pela simples análise das melhores notas obtidas em diversos concursos.

A preparação para concursos considerados de médio e alto nível demanda tempo e dedicação prévia.

Quando você tiver se preparando para o seu concurso, seja com edital ou não, tenho a intenção de possibilitar ao candidato a preparação, especificamente para o propósito a que propomos, bem como para os mais diversos editais na área de TI. A minha expectativa é que os nossos alunos estejam passos à frente dos demais candidatos nessa fase de preparação.

Informações Sobre o Curso

Abordaremos nesse curso todos os tópicos apresentados em nosso cronograma. Faremos juntos muitos exercícios para fixação do conteúdo ao final de cada aula, sempre de forma objetiva, prática e complementar.

Entretanto, gostaria de lembrar da dificuldade de esgotar as possibilidades de cada assunto até o seu nível máximo de detalhe em cada aula por se tratar de assuntos demasiadamente extensos.

O ponto chave de cada assunto é entender o perfil da banca e o perfil do órgão para o qual a banca está prestando o serviço. Diante disso, buscarei estar alinhado a esses pontos para direcioná-los da melhor forma possível, realizando diversos exercícios, principalmente dos últimos concursos ou concursos equivalentes. Contem comigo para isso!

Ressalto ainda o meu compromisso de buscar cumprir o cronograma da melhor maneira possível. No entanto, ao longo do curso, posso identificar alguns ajustes na ordem da apresentação dos conteúdos ou ainda a necessidade de adaptação a alguma alteração do Edital em caso de divulgação, portanto, digo a vocês que o cronograma não é de todo rígido.

Desde já eu agradeço a confiança de cada um de vocês e tenham certeza que esse curso irá auxiliá-los bastante nessa jornada. Não deixem de me procurar no fórum para esclarecimentos de dúvidas, por favor!

Não deixem acumular lacunas em seu aprendizado pois a "*lei de Murphy*" se aplica aqui...!!! Vai ser exatamente essa lacuna que será cobrada na prova e você vai se arrepender depois de não ter perguntado. *Digo por experiência própria!*

Críticas, reclamações, sugestões, comentários ou identificação de erros de digitação podem ser enviados para o nosso fórum. Tentarei responder com a maior brevidade possível.

Informações Sobre as Aulas

Apresento a vocês algumas metodologias adotadas em nossas aulas que aprendi ao estudar para concursos e que me ajudaram bastante, bem como no compartilhamento de experiências com outros professores:

1 - Parágrafos curtos e objetivos: Sempre que possível, os parágrafos serão reduzidos para facilitar a leitura e não a tornar cansativa, buscando sempre maior fluidez. O cronograma também segue esse princípio, deixando as aulas objetivas e eficazes em termos de organização e extensão do conteúdo. *De repente vocês terão tempo até para estudar as demais outras matérias...!!!*

2 - Entender o Básico (Princípios e Fundamentos): *Isso não é óbvio André?* Não, não é! Muitas das vezes nos preocupamos em aprender ou "decorar" os detalhes de determinada disciplina ou matéria, buscar tabelas e figuras para memorizar e esquecemos os princípios, o básico, aquilo que com certeza te ajudará a entender os detalhes. Portanto, estejam atentos a isso, por favor, ok?

3 - Linguagem Comum: Tentarei fazer com que a sua leitura se aproxime de um diálogo ou uma aula expositiva e presencial. O objetivo é não deixar a leitura cansativa para aqueles que talvez tenham dificuldades com leituras extensas, como eu. Combinado?

4 - Exercícios: Ler por si só já é bem cansativo. Imagina leituras bibliográficas, como o livro do Tanembaum, Forouzan ou Kurose com mais de 600 páginas? Convenhamos, né? Na maioria das vezes não vale a pena, a não ser para dúvidas pontuais e consolidação de determinado conteúdo. Além disso, deixe esse trabalho comigo, a não ser que você tenha tempo sobrando. Invista seu tempo em uma boa leitura do material e principalmente na resolução de exercícios!!!

A essência dos exercícios muitas vezes se repete, portanto, se você já tiver feito muitos, mas muitos exercícios, é provável que você se depare com questões iguais ou semelhantes nas provas seguintes.

Utilizarei exercícios também para esclarecer ou mencionar algum ponto que tenha passado na parte teórica. Vamos nos esforçar para que você precise de apenas mais uma prova para sua aprovação, certo?

Focaremos nos exercícios da Banca Examinadora do Concurso. Porém, sempre que houver necessidade, seja para complementarmos o conteúdo ou por falta de exercícios da banca sobre determinada matéria, utilizaremos exercícios de outras bancas também.

5 - Artifícios Complementares: O conteúdo de redes possui a vantagem de ter muita figura ilustrativa, o que nos ajuda a entender o conteúdo. Então sempre buscarei trazer figuras, imagens, tabelas e diagramas para tornar a leitura mais saudável e clara. Geralmente, é mais fácil memorizar uma figura ilustrativa do que puramente o conteúdo escrito.

6 - Linhas Destacadas em vermelho: Utilizarei esse recurso de destaque em negrito e vermelho das palavras e frases que são mais importantes dentro de alguns parágrafos para uma posterior leitura vertical (Segunda leitura do material com o objetivo de revisão dos pontos destacados).

7 - Revisão em Exercícios: Pessoal, a tendência é que nos assuntos iniciais, façamos a leitura e façamos os exercícios com um bom índice de acerto, pois você ainda estará com a memória fresca. Porém, tal índice nem sempre se mantém após semanas da leitura daquele conteúdo.

Portanto, é muito importante que estejam sempre voltando e fazendo alguns exercícios avulsos para fixar o conhecimento, além do que, será a oportunidade para descobrir onde você está tendo mais dificuldade de memorização e aprendizado.

ATENÇÃO

As videoaulas estão sendo constantemente gravadas e, dessa forma, não há garantia de que teremos todo o conteúdo disponível em vídeo. Então seu curso pode ou não ter as gravações a depender do edital.

Mas tenham certeza de que tudo e mais um pouco estará em seus PDF's.

Ufa, chega de apresentações e informações, certo? Vamos ao que interessa! Procurem estar descansados e tranquilos com vistas a obter uma leitura suave do conteúdo para otimizarmos os resultados das nossas aulas.

ESTRATÉGIA FLASHCARDS

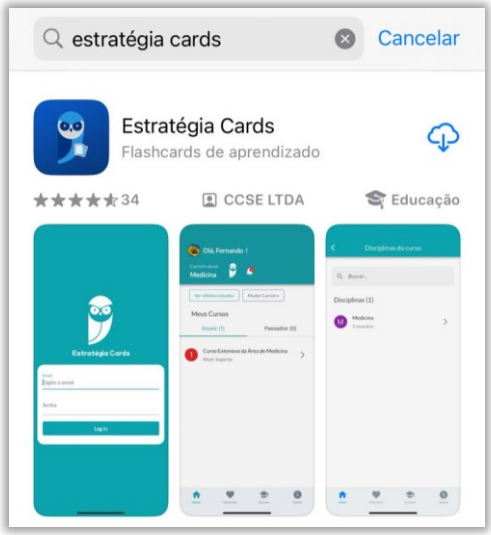
📚 Você tem dificuldade de estudar, memorizar e revisar os conteúdos que estuda em nossas aulas? Então nós temos a ferramenta perfeita para você!

Apresentamos o **Estratégia Cards**: app de flashcards que vai revolucionar sua forma de **estudar** e **revisar** conteúdos de provas de concurso público. Com nossa tecnologia inovadora e interface amigável, você dominará os tópicos mais complexos de maneira eficiente e divertida.

✨ Recursos do Estratégia Cards:

Curadoria de Flashcards	Flashcards criados e revisados por professores especializados em cada área, com qualidade e voltados para concursos públicos.
Flashcards Personalizados	Crie seus próprios flashcards, cobrindo os principais tópicos e matérias dos concursos públicos.
Repetição Espaçada	Técnica de aprendizagem que envolve revisar informações em intervalos crescentes para melhorar a retenção de longo prazo e combater o esquecimento.
Estatísticas Personalizadas	Visualize graficamente o percentual de acertos, erros ou dúvidas dos decks estudados.
Modo Offline	Estude em qualquer lugar, mesmo sem conexão à internet, fazendo o download dos decks.
Estudo por Áudio	*Está dirigindo ou fazendo esteira e quer continuar estudando?* Basta utilizar a opção "Escutar".
Decks Favoritos	Você pode escolher decks específicos como favoritos e visualizá-los em uma aba separada do app.
Opções de Estudo	Você poderá estudar todos os cards de um deck; ou apenas os que você errou; ou apenas os que você não estudou ainda; entre outras opções.

E como eu consigo baixar?



É muito fácil! Basta pesquisar por "Estratégia Cards" na loja oficial do seu smartphone.

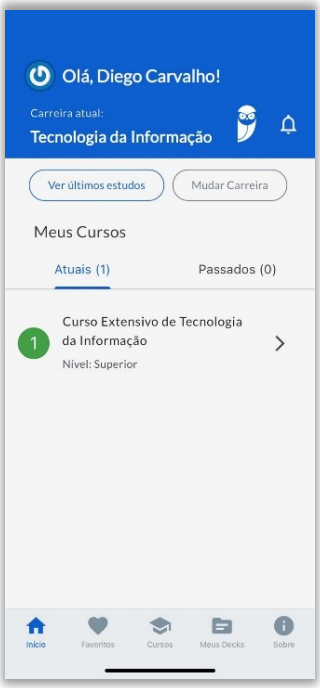
Se você tiver um Android, basta acessar a **Google Play**;

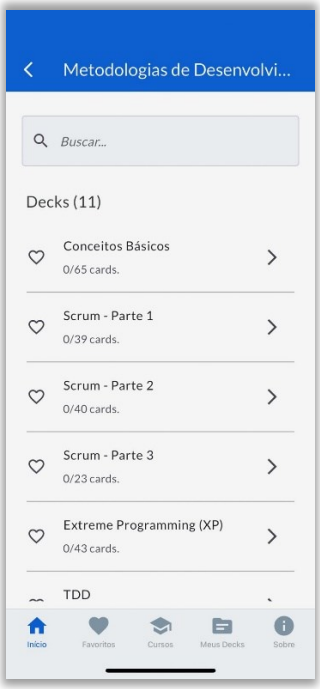
Se for tiver um iPhone, basta acessar a **App Store (iOS)**.

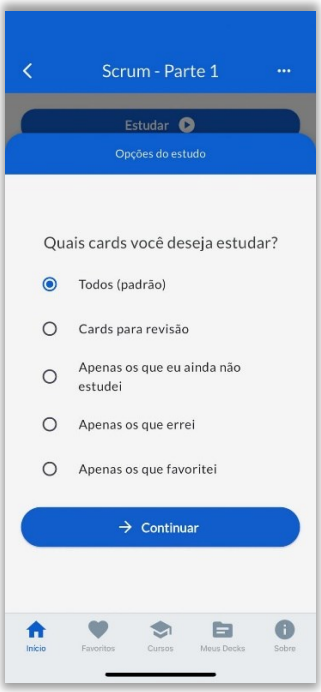
E para acessar?

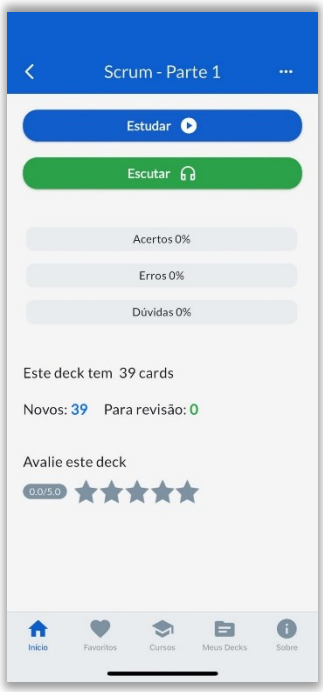
Para acessar, basta ter uma conta no Estratégia Concursos. Em seguida, utilize suas credenciais de login e senha para acessar o aplicativo. Por fim, acessa a carreira de Tecnologia da Informação.

Como utilizar o app:









Princípios de Segurança

Considerando a era da Informação em que nos encontramos atualmente, aspectos de Segurança da Informação são fundamentais em qualquer ambiente.

Diversas são as empresas e organizações que mantêm toda a sua vantagem competitiva, base de negócios, investimentos, entre outros pontos extremamente importantes ancorados em suas informações ou dados. A informação e seus ativos são, de fato, os elementos mais importantes de uma organização.

Desse modo, tais instituições necessariamente devem se resguardar de diversas formas de possíveis problemas relacionados a esse tópico.

Nesse sentido, aplicam-se muitos conceitos e padrões de segurança que visam amenizar os problemas atrelados de alguma forma a esse assunto.

Para iniciarmos, de fato, o referido assunto, vamos definir os três principais pilares que compõem a base da Segurança da Informação, quais sejam:

- Confidencialidade – Aqui temos o princípio que visa zelar pela privacidade e sigilo dos dados de tal modo que estes devem ser acessados e visualizados somente por aqueles de direito, ou seja, a informação só deve estar disponível para aqueles com a devida autorização.

Desse modo, a título de analogia, caso alguém envie uma carta dentro de um envelope e alguma pessoa indevidamente tenha acesso ao envelope, até então não temos problemas.

Referenciamos tal fato como interceptação dos dados. Entretanto, caso a pessoa mal-intencionada coloque o envelope contra a luz e verifique o conteúdo da carta, aí sim teremos a violação do princípio da confidencialidade.

Ano: 2021 Banca: CESPE Órgão: UFES Prova: Analista em TI

Segundo Machado (2014), o princípio fundamental de segurança da informação que é definido como a capacidade de garantir que o nível necessário de sigilo seja aplicado aos dados, tratando-se da prevenção contra a divulgação não autorizada desses dados

A) integridade.

B) disponibilidade.

C) criptografia.

D) privacidade.

E) confidencialidade.

Comentários:

Primeira questão da nossa sequência de conteúdo a ser abordado. Pessoal, percebam que o foco no enunciado é justamente o sigilo e prevenção contra a divulgação não autorizada. Vimos que duas palavras chaves do princípio da confidencialidade são SIGILO e PRIVACIDADE.

Muito cuidado, pois, a privacidade é uma característica do princípio da CONFIDENCIALIDADE.

Gabarito: E

- Integridade (Confiabilidade) – No segundo princípio, temos como objetivo garantir que os dados trafegados sejam os mesmos do início ao fim de um determinado trecho, ou seja, que a mesma mensagem gerada na origem chegue ao destino de forma intacta.

Ora, considerando o exemplo anterior, após a leitura indevida dos dados, a pessoa mal-intencionada poderia entregar o envelope com a carta para o destinatário. Logo, a mensagem é a mesma que foi gerada pela origem, certo? Exato! Dessa forma, não tivemos violação do princípio da integridade.

Agora, caso a pessoa altere a mensagem, teremos sim um problema de integridade dos dados.

Importante destacar que também há a perspectiva dos dados em repouso, isto é, armazenado em algum local. Nessa condição, também deverá ser observado o princípio da integridade. Na prática, caso este arquivo armazenado sofra algum tipo de modificação não autorizada, também teremos uma violação do princípio.

Um exemplo que gosto de citar para materializar um pouco algum interesse difuso nesse aspecto seria alguém conseguir acessar os dados e arquivos de um contador. Nos referidos documentos, consta uma planilha de controle com a relação de empresas e referidas contas bancárias gerenciadas pelo profissional. Na ocasião, o usuário que está com má intenção realizará a alteração das contas no documento para que ele possa se beneficiar de alguma forma nesse processo.

- Disponibilidade – Neste princípio, temos como principal objetivo o fato de determinado recurso poder ser utilizado quando este for requisitado em um determinado momento,

considerando a devida autorização do usuário requisitante. Desse modo, quando tentamos acessar o site da Receita Federal, por exemplo, no primeiro dia de declaração de Imposto de Renda, teremos a experiência por diversos usuários da violação do princípio da disponibilidade caso estes não consigam acessar o site ou enviar suas requisições por falha no sistema ou volume de acesso que consomem todos os recursos disponíveis, impedindo a utilização por novos usuários.

Ademais, outros conceitos também surgem com grande relevância, senão vejamos:

- Autenticidade – O princípio da autenticidade busca garantir que determinada pessoa ou sistema é, de fato, quem ela diz ser. Ou seja, quando utilizamos o simples recurso de inserir as informações de login e senha em um computador, estamos dizendo ao computador que realmente somos o usuário, pois ele assume que somente o usuário legítimo em questão possui a informação de login e senha.

Importante informar que nesse processo, para a devida realização da autenticação, é necessário cumprir a etapa preliminar de identificação, onde será possível coletar as informações necessárias sobre o usuário para posteriormente, validá-lo.

Nesta etapa de identificação, temos muitos exemplos de cunho mais prático do nosso dia a dia, seja pela utilização de uma impressão digital ou reconhecimento facial, logins e senhas tradicionais, utilização de cartões físicos ou digitais de acesso, entre muitos outros.

CESPE-2020 - SEFAZ/AL - Auditor de Finanças e Controle

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

Tranquilo, certo pessoal? Mencionamos a importância do processo de identificação preliminarmente, para posterior realização do processo de autenticação. Um peque destaque que deixo nessa questão, que abordaremos mais à frente da nossa aula é a questão das permissões e autorizações de acesso. Vejam que a questão não tratou a identificação e autenticação como garantidores dessa permissão, mas como pré-requisitos apenas.

Veremos mais à frente que o processo de autenticação é complementado pela etapa de autorização, que será responsável por gerenciar as credenciais e permissões de acesso.

Gabarito: C

- Não-Repúdio (Irretratabilidade) – Neste princípio, busca-se garantir que o usuário não tenha condições de negar ou contrariar o fato de que foi ele quem gerou determinado conteúdo ou informação, ou ainda que determinado receptor tenha, de fato, recebido certa mensagem. Tal princípio se aplica, por exemplo, na geração de uma autorização para compra de determinado produto e depois, o gestor responsável queira negar a autorização. Entretanto, utiliza-se mecanismos para que não haja possibilidade de haver a referida negação.

Stallings traz ainda a seguinte definição:

"A irretratabilidade impede que o emissor ou o receptor negue uma mensagem transmitida. Assim, quando uma mensagem é enviada, o receptor pode provar que o emissor alegado de fato enviou a mensagem. De modo semelhante, quando uma mensagem é recebida, o emissor pode provar que o receptor alegado de fato recebeu a mensagem."

(Ano: 2022 Banca: FGV Órgão: TJDFT Prova: Suporte em TI) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

A) confidencialidade;

B) autenticidade;

C) integridade;

D) disponibilidade;

E) irretratabilidade.

Comentários:

Exatamente como vimos na nossa explanação. Tenham muito cuidado na leitura da questão, pois, conforme este caso, o aluno poderia marcar a opção autenticidade por observar as menções no enunciado de reconhecer o usuário. Mas percebam que o foco é justamente na incapacidade de Lucas negar que tenha realizado tal operação.

Gabarito: E

- Irretroatividade – Um outro princípio importante diretamente associado ao processo de autenticidade, integridade e não repúdio é a Irretroatividade, ou seja, não é possível reverter o ato ou questionar a data/momento da sua realização. Na prática, ela estabelece que não é possível reverter um evento ou ação uma vez que ele tenha sido executado e registrado. Este princípio é importante para garantir a integridade dos dados e a confiabilidade dos sistemas de informação.

Podemos citar como exemplos:

- Uma vez que uma transação é registrada em um blockchain, não é possível alterá-la ou excluí-la.
- Uma vez que um certificado digital é emitido, não é possível revogá-lo retroativamente.
- Uma vez que um documento é assinado com certificado digital e assinatura digital, não é possível revertê-lo em termos do ato e do tempo.

- Legalidade – O aspecto de legislação e normatização é fundamental nos processos relacionados à Segurança da Informação. Desse modo, respeitar a legislação vigente é um aspecto fundamental e serve, inclusive, como base para o aprimoramento e robustez dos ambientes.

FGV - 2021 - IMBEL - Supervisor - Tecnologia da Informação

Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção. Assinale o atributo que não é parte desse grupo.

A) Autenticidade.

B) Completude.

C) Confidencialidade.

D) Disponibilidade.

E) Integridade.

Comentários:

Sem muito segredo até aqui, certo? Acabamos de destacar as características dos principais princípios: Autenticidade; Confidencialidades; Disponibilidade; Integridade.

Gabarito: B

Tranquilo até aqui pessoal? Esses conceitos são extremamente importantes. Quero aproveitar para registrar alguns conceitos complementares previstos na norma de referência X.800 que trata da Segurança de arquiteturas, principalmente no que tange a soluções de rede distribuídas. Vamos conhecê-los:

- Autenticação de entidade Parceiras
  - Usada em associação com uma conexão lógica com a capacidade de prover confiabilidade a respeito da identidade das entidades conectadas.
- Autenticação da origem dos Dados

- Considerando uma transferência sem conexão entre as partes, visa assegurar que a origem dos dados recebidos é quem ela afirma ser.

- Confidencialidade de campo seletivo
  - Busca-se manter a confidencialidade de campos específicos dentro do volume de dados de um usuário em uma conexão.
- Confidencialidade do fluxo de tráfego
  - Busca-se gerar a confidencialidade sob a perspectiva do fluxo, ou seja, a simples análise do fluxo de dados não deve ser capaz de gerar informações indevidas.
- Integridade de conexão com recuperação
  - Como o próprio nome diz, é capaz de detectar qualquer modificação, inserção, deleção ou repetição de quaisquer dados dentro de uma sequência de dado. Além disso, é capaz de recuperar a intervenção realizada.
- Integridade de conexão sem recuperação
  - Como vimos, neste caso, não há capacidade de recuperação, mas tão somente de detecção.
- Integridade de conexão de campo seletivo
  - Assim como a confidencialidade seletiva, aqui, busca-se garantir a integridade de áreas e dados específicos. Assim, busca-se avaliar se houve modificação, inserção, eliminação ou repetição dessa parcela.
- Integridade sem conexão
  - Considera a capacidade de prover a integridade de dados em um ambiente sem conexão. Possui o foco na detecção de modificações e uma capacidade limitada de detectar repetições.
- Integridade de campo seletivo sem conexão
  - Mesma condição do tipo acima, porém, de áreas de dados específicos ou seletivos.
- Irretratabilidade de origem
  - É o padrão que vimos, uma vez que é possível provar que a mensagem foi enviada por determinada parte.
- Irretratabilidade de destino
  - A perspectiva aqui é diferente. Consegue-se provar que o destinatário recebeu determinada mensagem.

Segurança de Redes

O Cert.br, principal órgão do Brasil responsável pelo fomento à Segurança da Informação, nos traz alguns conceitos que são constantemente explorados pelas bancas examinadoras. Nesse sentido, vamos conhecê-los:

- Furto de dados: informações pessoais e outros dados podem ser obtidos tanto pela interceptação de tráfego como pela exploração de possíveis vulnerabilidades existentes em seu computador;
- Uso indevido de recursos: um atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo para a prática de atividades maliciosas, como obter arquivos, disseminar spam, propagar códigos maliciosos, desferir ataques e esconder a real identidade do atacante;
- Varredura: um atacante pode fazer varreduras na rede, a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades;
- Interceptação de tráfego: um atacante, que venha a ter acesso à rede, pode tentar interceptar o tráfego e, então, coletar dados que estejam sendo transmitidos sem o uso de criptografia;
- Exploração de vulnerabilidades: por meio da exploração de vulnerabilidades, um computador pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados e ser usado para a propagação de códigos maliciosos. Além disso, equipamentos de rede (como modems e roteadores) vulneráveis também podem ser invadidos, terem as configurações alteradas e fazerem com que as conexões dos usuários sejam redirecionadas para sites fraudulentos;
- Ataque de negação de serviço: um atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar;
- Ataque de força bruta: computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta. Muitos computadores, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes;
- Ataque de personificação: um atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.


Segurança da Informação
Furto de dados: dados podem ser obtidos pela interceptação de tráfego
Ataque de personificação: atacante pode introduzir ou substituir um dispositivo de rede para induzir outros a se conectarem a este
Ataque de força bruta: computadores conectados à rede e que usem senhas como métodos de autenticação estão expostos a ataques de força bruta
Ataque de negação de serviço: atacante pode usar a rede para enviar grande volume de mensagens para um computador, até torná-lo inoperante ou incapaz de se comunicar
Exploração de vulnerabilidades: computador pode ser infectado ou invadido
Interceptação de tráfego: atacante pode tentar interceptar o tráfego e coletar dados que estejam sendo transmitidos sem o uso de criptografia
Varredura: atacante pode fazer varreduras na rede, a fim de descobrir outros computadores
Uso indevido de recursos: atacante pode ganhar acesso a um computador conectado à rede e utilizá-lo

Questões Comentadas - Princípios de Segurança - CESPE

1. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

São princípios da segurança da informação, entre outros, a confidencialidade, a integridade e a disponibilidade.

Comentários:

Questão bem básica, e que traz, de fato, alguns dos principais princípios. Da base principal, ficou de fora apenas a autenticidade.

Gabarito: C

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A integridade é uma propriedade que visa aplicar conhecimentos e habilidades para garantir a assinatura digital.

Comentários:

Temos uma inversão de conceitos. Na prática, a assinatura digital é que garante a autenticidade e integridade.

Gabarito: E

3. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

A confidencialidade trata da proteção de dados contra ataques passivos e envolve mecanismos de controle de acesso e criptografia.

Comentários:

Importante a gente lembrar que os ataques passivos são aqueles que não alteram ou interferem no fluxo de dados. Ou seja, escutas ou interceptações apenas para coleta e leitura das informações, sem sua alteração, caracteriza esse tipo de ataque.

Já a confidencialidade é aquele princípio que justamente visa garantir o sigilo dos dados. Então, a questão está adequada em seus conceitos, e também na referência a práticas de segurança como os controles de acesso e criptografia, que visam restringir o acesso às informações e/ou, ainda que alguém tenha acesso, não consiga interpretá-las.

Alguns exemplos de ataques passivos:

Exemplos:

- Eavesdropping: Interceptação de dados em redes sem fio ou com fio.
- Análise de tráfego: Monitoramento de pacotes de rede para identificar informações confidenciais.
- Ataques de sniffing: Captura de dados em redes utilizando ferramentas específicas.

Gabarito: C

4. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

Para determinar o grau de sigilo da informação, é necessário que sejam observados o interesse público da informação e a utilização do critério menos restritivo possível.

Comentários:

Muita atenção e cuidado nessa questão. Na prática, temos aqui uma referência a prática de classificação da informação, ou seja, quando se define níveis de acesso e, quem pode ou não acessar as informações.

Mas vejam que a questão traz a perspectiva de acesso amplo, ou seja, direito público de acesso. Logo, se há interesse público, há o princípio da transparência. Isso é preconizado na LEI DE ACESSO À INFORMAÇÃO, no artigo 24:

§ 5º Para a classificação da informação em determinado grau de sigilo, deverá ser observado o interesse público da informação e utilizado o critério menos restritivo possível,

Então vejam que, evitar estabelecer critérios restritivos para os casos de informações abertas e públicas é sim uma prática recomendada. Muito cuidado pois em alguma medida entra em conflito com tudo que trabalhamos sobre sigilo e restrição. Mas nesses casos, as informações, de fato, são restritas, e por isso, deve-se aumentar o grau de restrição.

São duas perspectivas distintas.

Gabarito: C

5. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em uma conexão criptografada, o princípio da disponibilidade é, de fato, atingido.

Comentários:

A criptografia está majoritariamente associada ao princípio da confidencialidade. Lembrando que ela também poderá estar associada ao princípio da autenticidade ao considerar a ordem das chaves a ser utilizada.

Gabarito: E

6. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A confidencialidade é uma propriedade segundo a qual as informações não podem ser disponibilizadas a indivíduos, entidades ou processos que não estejam previamente autorizados.

Comentários:

Sem muito o que acrescentar pessoal. A autorização de acesso é o recurso chave para garantir a restrição de acesso às informações confidenciais.

Gabarito: C

7. CEBRASPE (CESPE) - Ana Reg (AGER MT)/AGER MT/Ciências da Computação e Sistemas de Informação/2023

Funções de hash são muito utilizadas para verificação da propriedade básica da segurança da informação denominada

a) disponibilidade.

b) confidencialidade.

c) não-repúdio.

d) integridade.

e) perímetro.

Comentários:

O HASH sem dúvida está associado ao princípio da integridade. Lembrando que, por exemplo, na assinatura digital, temos a combinação da criptografia assimétrica com o HASH, onde a primeira técnica garante a autenticidade e a segunda, o HASH, garante a integridade. Por isso temos que a assinatura digital garante a autenticidade e a integridade.

Gabarito: D

8. CESPE / CEBRASPE - 2022 - APEX Brasil - Perfil 5: Tecnologia da Informação e Comunicação (TIC) - Especialidade: Infraestrutura e Operações de TIC

A característica de servidores de alta disponibilidade que permite a alternância imediata para uma rede em espera quando a rede principal falha denomina-se

A) balanceamento de carga.

B) failover.

C) nuvem privada escalável.

D) cluster.

Comentários:

A disponibilidade da informação é um dos princípios da segurança que vimos. E para isso, os sistemas e serviços, bem como o acesso à informação não pode deixar de acontecer.

Como prática de continuidade de negócios, sem dúvida, a técnica de FAILOVER é uma das principais. Ela diz respeito justamente à capacidade de um novo serviço, recurso, sistema, ou um DATACENTER completo começar a funcionar de forma subsidiária a partir do momento que a estrutura principal parou de funcionar.

Gabarito: B

9. Ano: 2021 Banca: CESPE Órgão: UFES Prova: Analista em TI

Segundo Machado (2014), o princípio fundamental de segurança da informação que é definido como a capacidade de garantir que o nível necessário de sigilo seja aplicado aos dados, tratando-se da prevenção contra a divulgação não autorizada desses dados

A) integridade.

B) disponibilidade.

C) criptografia.

D) privacidade.

E) confidencialidade.

Comentários:

Primeira questão da nossa sequência de conteúdo a ser abordado. Pessoal, percebam que o foco no enunciado é justamente o sigilo e prevenção contra a divulgação não autorizada. Vimos que duas palavras chaves do princípio da confidencialidade são SIGILO e PRIVACIDADE.

Muito cuidado, pois, a privacidade é uma característica do princípio da CONFIDENCIALIDADE.

Gabarito: E

10. CESPE-2020 - SEFAZ/AL - Auditor de Finanças e Controle

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

Tranquilo, certo pessoal? Mencionamos a importância do processo de identificação preliminarmente, para posterior realização do processo de autenticação. Um peque destaque que deixo nesta questão, que abordaremos mais à frente da nossa aula é a questão das permissões e autorizações de acesso. Vejam que a questão não tratou a identificação e autenticação como garantidores dessa permissão, mas como pré-requisitos apenas.

Veremos mais à frente que o processo de autenticação é complementado pela etapa de autorização, que será responsável por gerenciar as credenciais e permissões de acesso.

Gabarito: C

11. CESPE – Banco da Amazônia/Técnico Científico – Segurança da Informação/2013

A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação

Comentários:

Como vimos, estes são os principais pilares da Segurança da Informação.

Gabarito: C

---

12. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de
recuperação, é a integridade

a) conexão com recuperação.

b) autenticação da origem de dados.

c) entidade par a par.

d) conexão com campo selecionado.

e) fluxo de tráfego.

Comentários:

Pessoal, os únicos itens que tratam da integridade são as letras “A” e “D”. As letras “B” e “C” tratam do princípio da autenticidade, enquanto a letra “E” de confidencialidade.

Assim, para a letra "A", temos o grande diferencial que é a capacidade de detecção e recuperação de todos os dados. Para a letra "D", temos que será aplicado o princípio de monitoramento em uma parcela específica, ou seja, uma área selecionada dos dados. Percebam que nesse caso não há recuperação, mas tão somente detecção.

Gabarito: A

---

13. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam violação da autenticidade das informações.

Comentários:

O princípio descrito está relacionado à disponibilidade e não à autenticidade.

Gabarito: E

---

14. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se, para cometer o incidente, um colaborador usou software sem licenciamento regular e sem autorização formal da política de segurança da organização, então houve violação da integridade das informações da organização.

Comentários:

O princípio da integridade visa garantir que os dados originados de um determinado ponto chegaram ao destino sem serem violados e adulterados. Uma típica utilização para essa finalidade é por intermédio de funções HASH.

Gabarito: E

---

15. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

Comentários:

Temos aqui um exemplo de acesso a dados que não deveriam ser acessados pelo usuário em tela. Ou seja, se o dado foi acessado de forma indevida por algum ente sem autorização, nitidamente temos a violação do princípio da confidencialidade.

Gabarito: C

---

16. (CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2013) Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

Comentários:

Pessoal, muita atenção aqui. Se devemos garantir que a informação não esteja disponível para aqueles que não possuem autorização, queremos garantir que a informação não seja acessada de forma indevida, logo, estamos falando da propriedade da confidencialidade.

Gabarito: C

---

17. (CESPE – TCE-RO/Analista de Informática/2013) Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

Comentários:

Mais uma questão bacana do CESPE. Temos descrito aqui a violação do princípio da confidencialidade quando a assertiva afirma que "o seu conteúdo tenha sido visualizado". Entretanto, a informação se manteve íntegra pois não houve alteração de seu conteúdo, não havendo, portanto, a violação do princípio da integridade.

Gabarito: E

---

18. (CESPE – TCE-RO/Analista de Informática/2013) Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

Comentários:

Se usuários legítimos não estão conseguindo usufruir dos serviços oferecidos, temos, de fato, a violação do princípio da disponibilidade.

Gabarito: C

---

19. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013)A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

Comentários:

Sem dúvida, todos esses elementos devem ser protegidos no que tange à proteção de recursos computacionais, pois, todos podem ser vetores de ataques ou de vazamento de dados.

Gabarito: C

---

20. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

Comentários:

Não, né pessoal? Se restringimos o acesso somente às pessoas autorizadas, temos o princípio da confidencialidade.

Gabarito: E

---

21. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

Comentários:

A informação é a base para qualquer organização, sendo ela e seus ativos de informação, sem dúvida, os elementos mais importantes.

Gabarito: E

---

22. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

Comentários:

Temos aqui a descrição de Integridade, certo?

Gabarito: E

---

23. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

Comentários:

Houve violação do princípio da integridade e não da disponibilidade, considerando que o arquivo, ainda que alterado, esteja disponível.

Gabarito: E

---

24. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

Comentários:

Ora, com a criptografia, temos que os dados poderão até ser acessados, porém, não poderão ser lidos ou interpretados de forma não autorizada. Assim, temos a garantia do princípio da confidencialidade, que é uma forma de aumentar a segurança da informação.

Gabarito: C

---

25. (CESPE - TCE-ES/Informática/2013) Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

a) Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.

b) No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.

c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.

d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.

e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

Comentários:

Vamos aos itens:

a) Temos que os principais princípios ou atributos da Segurança da Informação são a disponibilidade, integridade e confidencialidade. Muitos já complementam com a autenticidade, formando a nossa DICA. INCORRETO

b) À época, diversas foram a ocorrência de vulnerabilidade e invasões a sites do Governo e de empresas brasileiras. INCORRETO

c) A privacidade é um conceito diretamente ligada ao aspecto da confidencialidade e que muitas vezes são tratados como sinônimos para fins de comunicação dos dados. INCORRETO

d) Não né pessoal? Temos aí uma violação à classificação da informação ou da diferenciação de níveis de acesso considerando o grau de sigilo ou proteção dos dados ou ativos em um determinado ambiente. INCORRETO

e) Ainda que tivéssemos dúvida em algum dos itens acima, essa questão nos traz a tranquilidade na resposta, certo? Temos os três princípios relacionados à Segurança da Informação. CORRETO

Gabarito: E

---

26. (CESPE - TCE-RO/Ciências da Computação/2013) As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

Comentários:

Lembremos sempre de ficarmos atentos a essas afirmações restritivas. No caso em questão, temos o termo "ESTRITAMENTE". Não né pessoal? O simples princípio da autenticidade ficou de fora da lista.

Gabarito: E

---

27. (CESPE - SUFRAMA/Analista de Sistemas/2014) A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

Comentários:

Podemos usar o mesmo exemplo que demos logo acima. O fato de você criptografar um disco com dados não impede que ele seja destruído e os dados sejam perdidos. Assim, apesar de usar a criptografia, os dados não estarão mais disponíveis.

Gabarito: E

---

28. (CESPE - SUFRAMA/Analista de Sistemas/2014) A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

Comentários:

Se tivermos problemas com acessos gerando dificuldades no acesso e utilização dos recursos da página, temos um problema de disponibilidade e não confidencialidade.

O problema de confidencialidade existiria se alguém invadisse a página e conseguisse acesso às informações de usuário e senha de outros usuários, por exemplo.

Gabarito: E

---

29. (CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013) Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi

a) a disponibilidade

b) a autenticidade

c) o não repúdio

d) a confidencialidade

e) a integridade

Comentários:

Quando falamos de acesso indevido a informações ou dados, estamos falando de violação do princípio da confidencialidade. Atenção para o fato de que a questão deixou claro que o invasor não fez qualquer alteração no conteúdo da planilha, ou seja, não houve prejuízo à integridade desta planilha.

Gabarito: D

---

30. (CESPE – ANCINE/Analista Administrativo/2013) No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

Comentários:

Temos aí a descrição do princípio da irretratabilidade ou não repúdio pessoal.

Gabarito: E

---

31. (CESPE – ANTAQ/Analista de Infraestrutura/2014) A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

Comentários:

Duas observações nessa questão. Primeiro, se estamos falando de alteração de documento, estamos falando da integridade e não confidencialidade. Em relação ao tópico de criptografia, na prática se utiliza funções HASH que possuem um caráter um pouco diferente. Veremos isso com mais calma em um outro momento.

Gabarito: E

---

32. (CESPE – DEPEN/Área 07/2015) O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.

Comentários:

Temos aí a simples apresentação dos princípios que formam o nosso principal mnemônico: DICA.

Gabarito: C

---

33. (CESPE – TCU/Auditor Federal de Controle Externo – TI/2015) Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.

Comentários:

Questão bem tranquila por ser do TCU. O erro da questão se encontra no segundo trecho ao se descrever o princípio da disponibilidade e não integridade. Gostaria apenas de destacar o trecho de "usuários autorizados tenham acesso". Qual é a ideia aqui pessoal?

Se eu tenho um sistema interno que somente os usuários de gestão devem acessar, caso esse sistema fique fora do ar e ninguém tente acessar nesse período ou caso um técnico financeiro não autorizado tente acessar e verifique o sistema fora do ar, não poderemos dizer que houve indisponibilidade, pois não houve pessoas autorizadas tentando acessar o sistema no período de indisponibilidade. Certo?

Gabarito: E

---

34. (CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação) Uma auditoria no plano de continuidade de negócios de uma organização precisa verificar se o plano é exequível e se o pessoal está treinado para executá-lo.

Comentários:

Como mencionamos, a auditoria pode atuar em qualquer etapa, fase ou tipo de processo, recurso (inclusive humano) ou documento.

Desta feita, é recomendado que se avalie a exequibilidade dos planos gerados na empresa, bem como se as equipes estão aptas a executarem os mesmos.

Gabarito: C

QUESTÕES COMENTADAS - PRINCÍPIOS DE SEGURANÇA - FCC

1. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

No âmbito da segurança da informação em bancos de dados, as dimensões privacidade de comunicação, armazenamento seguro de dados sensíveis, autenticação de usuários e controle de acesso granular são pertinentes ao aspecto

a) confidencialidade.

b) rastreabilidade.

c) integridade.

d) permissibilidade.

e) disponibilidade.

Comentários:

Vejam que todos os itens estão preocupados em garantir a restrição e eventual sigilo dos dados. Logo, o princípio associado é o da confidencialidade. Cuidado para não vincular autenticação a autenticidade de forma imediata. Nesse caso, a autenticação está associada ao requisito necessário para um acesso controlado.

Gabarito: A

---

2. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

3. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

Comentário:

Vimos todas essas características no início do nosso conteúdo de princípios de segurança. Vale mencionar que no item IV, temos a descrição tanto da autenticidade quanto da integridade.

Gabarito: E

---

4. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2015) Em relação à segurança da informação, considere:

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

Comentário:

Reforçando os conceitos que vimos previamente. Observemos que, no item II, o examinador destaca o aspecto de alteração não autorizada, ou seja, impactando o princípio de integridade.

Gabarito: A

---

5. (FCC – TRE-CE/Técnico Judiciário – Programação de Sistemas/2012) A propriedade que garante que nem o emissor nem o destinatário das informações possam negar a sua transmissão, recepção ou posse é conhecida como

a) autenticidade.

b) integridade.

c) irretratabilidade.

d) confidenciabilidade.

e) acessibilidade.

Comentário:

Pessoal, temos aqui uma abordagem um pouco mais ampla do conceito de não-repúdio ou irretratabilidade.

Gabarito: C

---

6. (FCC – TJ-AP/Analista Judiciário – Banco de Dados/2014) O controle de acesso à informação é composto por diversos processos, dentre os quais, aquele que identifica quem efetua o acesso a uma dada informação. Esse processo é denominado

A) autenticação.

B) auditoria.

C) autorização.

D) identificação.

E) permissão.

Comentário:

Lembrando que o controle de acesso envolve tanto a autenticação quanto a autorização. Entretanto, o processo de identificação está relacionado à autenticação.

Gabarito: A

QUESTÕES COMENTADAS - PRINCÍPIOS DE SEGURANÇA - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

A empresa Progseg foi contratada via processo licitatório para a modernização das aplicações utilizadas no Tribunal de Justiça do Rio Grande do Norte. Aurélio, chefe do Departamento de Tecnologia, conduzirá junto à empresa o retrofit, que terá como foco a melhoria na segurança dos sistemas.

Os requisitos mandatórios dessa modernização são:

- Assegurar que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados; e

- Verificar que os usuários são quem dizem ser.

O requisito desejável dessa modernização é:

- Ser capaz de associar uma violação de segurança a uma parte responsável.

Com base nos requisitos citados, a Progseg deverá implementar, respectivamente:

a) confidencialidade, autenticidade, responsabilização;

b) disponibilidade, autenticidade, privacidade;

c) não repúdio, integridade de sistemas, confidencialidade;

d) integridade, disponibilidade, responsabilização;

e) autenticidade, integridade de dados, integridade de sistemas.

Comentários:

Questão bem prática e tranquila a respeito dos conceitos, certo?

O primeiro, tem foco no sigilo, logo, confidencialidade. Aqui, já teríamos resolvido a questão. O ponto de atenção fica pelo item de accountability ou responsabilização. Que é justamente você conseguir associar alguém a determinado ato para fins de registro.

Gabarito: A

2. (FGV - Aud Est (CGE SC)/CGE SC/Ciências da Computação/2023)

Para o caso hipotético descrito a seguir, somente informações corretas são consideradas disponíveis.

Um determinado funcionário atende um pedido por telefone de alguém que se identifica como o cliente A. Essa pessoa explica que seus dados cadastrais estão errados e pede que seja feito um novo cadastro com as informações que ela está passando. O funcionário atende ao pedido e atualiza o sistema da empresa removendo o cadastro antigo e criando um novo.

Dias depois, ao tentar emitir uma fatura, a empresa nota que os dados do cliente A não estão completos e resolve abrir uma investigação. Durante a investigação descobre-se que os dados passados pela pessoa ao telefone eram falsos e que é portanto necessário refazer o cadastro.

Neste caso, avalie se, durante o processo de atendimento mencionado, ocorreu um incidente com quebra da

I. Confidencialidade dos dados do cliente A.

II. Disponibilidade dos dados do cliente A.

III. Integridade dos dados do cliente A.

Está correto o que se afirma em

a) I, apenas.

b) II, apenas.

c) III, apenas.

d) I e II, apenas.

e) II e III, apenas.

Comentários:

Essa questão traz uma visão moderna, e que eu gosto muito, a respeito da associação entre a integridade e disponibilidade. Vejam que houve alteração indevida dos dados gravados, o que, por si só, afetou a integridade. O ponto adicional é que, em momento posterior, houve necessidade de consumo da informação, e esta estava com problema de integridade, o que acabou gerando indisponibilidade do dado.

Ainda, em nenhum momento, conforme enunciado, as informações originais que foram sobrescritas foram vazadas ou informadas sem autorização, o que não gerou problema com a confidencialidade.

Gabarito: E

3. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Tânia trabalha em uma prestadora de serviços de Internet. Equivocadamente, ela enviou ao servidor um comando UPDATE, o qual alterou indevidamente a base de dados, não permitindo mais seu acesso. De forma a ocultar seu erro, Tânia descobriu um post-it sob o teclado com a

senha de um dos técnicos que trabalhava com ela. Então, utilizando a senha, entrou no sistema e efetuou novas modificações, de forma que a culpa recaísse sobre o técnico.

No incidente relatado, houve a quebra do(a):

a) confidencialidade e autenticidade;

b) integridade e autenticidade;

c) irretratabilidade e disponibilidade;

d) não repúdio e confidencialidade;

e) confidencialidade e integridade.

Comentários:

Com o comando UPDATE, houve a alteração do dado indevidamente, o que gerou problema de integridade.

O segundo ponto, houve quebra da autenticidade, pois houve vazamento de senha e agora não é possível garantir a autoria da ação, pois estará associado ao usuário que nem sequer estava no local.

Gabarito: B

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã

A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista.

Assinale o significado do princípio da Irretratabilidade.

A Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.

B Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.

C Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.

D Preservação fidedigna das informações.

E Restrição de acesso às informações apenas aos autorizados.

Comentário:

Vamos aos itens:

a) Estamos falando aqui da prática de controle de acesso com autenticação e autorização. INCORRETO

b) Exatamente pessoal. Lembrando que a irretratabilidade também se aplica ao destinatário, no sentido dele não ser capaz de negar o recebimento da informação. CORRETO

c) Estamos falando aqui de processo de cultura organizacional. INCORRETO

d) Temos o princípio da integridade. INCORRETO

e) Novamente, controle de acesso, associado à confidencialidade. INCORRETO

Gabarito: B

---

5. (Ano: 2022 Banca: FGV Órgão: TJDFT Prova: Suporte em TI) Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

A) confidencialidade;

B) autenticidade;

C) integridade;

D) disponibilidade;

E) irretratabilidade.

Comentários:

Exatamente como vimos na nossa explanação. Tenham muito cuidado na leitura da questão, pois, conforme este caso, o aluno poderia marcar a opção autenticidade por observar as menções no enunciado de reconhecer o usuário. Mas percebam que o foco é justamente na incapacidade de Lucas negar que tenha realizado tal operação.

Gabarito: E

6. FGV - 2021 - IMBEL - Supervisor - Tecnologia da Informação

Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção. Assinale o atributo que não é parte desse grupo.

A) Autenticidade.

B) Completude.

C) Confidencialidade.

D) Disponibilidade.

E) Integridade.

Comentários:

Sem muito segredo até aqui, certo? Acabamos de destacar as características dos principais princípios: Autenticidade; Confidencialidades; Disponibilidade; Integridade.

Gabarito: B

Lista de Questões - Princípios de Segurança - CESPE

1. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

São princípios da segurança da informação, entre outros, a confidencialidade, a integridade e a disponibilidade.

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A integridade é uma propriedade que visa aplicar conhecimentos e habilidades para garantir a assinatura digital.

3. CEBRASPE (CESPE) - Per Crim (POLC AL)/POLC AL/Análise de Sistemas, Ciências da Computação, Informática. Processamento de Dados ou Sistemas da Informação/2023

A confidencialidade trata da proteção de dados contra ataques passivos e envolve mecanismos de controle de acesso e criptografia.

4. CEBRASPE (CESPE) - Tec (CNMP)/CNMP/Apoio Técnico Administrativo/Segurança Institucional/2023

Para determinar o grau de sigilo da informação, é necessário que sejam observados o interesse público da informação e a utilização do critério menos restritivo possível.

5. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em uma conexão criptografada, o princípio da disponibilidade é, de fato, atingido.

6. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

A confidencialidade é uma propriedade segundo a qual as informações não podem ser disponibilizadas a indivíduos, entidades ou processos que não estejam previamente autorizados.

7. CEBRASPE (CESPE) - Ana Reg (AGER MT)/AGER MT/Ciências da Computação e Sistemas de Informação/2023

Funções de hash são muito utilizadas para verificação da propriedade básica da segurança da informação denominada

a) disponibilidade.

b) confidencialidade.

c) não-repúdio.

d) integridade.

e) perímetro.

8. CESPE / CEBRASPE - 2022 - APEX Brasil - Perfil 5: Tecnologia da Informação e Comunicação (TIC) - Especialidade: Infraestrutura e Operações de TIC

A característica de servidores de alta disponibilidade que permite a alternância imediata para uma rede em espera quando a rede principal falha denomina-se

A) balanceamento de carga.

B) failover.

C) nuvem privada escalável.

D) cluster.

9. Ano: 2021 Banca: CESPE Órgão: UFES Prova: Analista em TI

Segundo Machado (2014), o princípio fundamental de segurança da informação que é definido como a capacidade de garantir que o nível necessário de sigilo seja aplicado aos dados, tratando-se da prevenção contra a divulgação não autorizada desses dados

A) integridade.

B) disponibilidade.

C) criptografia.

D) privacidade.

E) confidencialidade.

10. CESPE-2020 - SEFAZ/AL - Auditor de Finanças e Controle

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

11. CESPE – Banco da Amazônia/Técnico Científico – Segurança da Informação/2013

A segurança da informação pode ser entendida como uma atividade voltada à preservação de princípios básicos, como confidencialidade, integridade e disponibilidade da informação.

12. (CESPE – TCE-PR/Analista de Controle – Área TI/2016) A integridade de dados que detecta modificação, inserção, exclusão ou repetição de quaisquer dados em sequência, com tentativa de
recuperação, é a integridade

a) conexão com recuperação.

b) autenticação da origem de dados.

c) entidade par a par.

d) conexão com campo selecionado.

e) fluxo de tráfego.

13. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Possíveis dificuldades apresentadas por colaboradores para acessar as informações do sistema da organização por mais de dois dias indicam violação da autenticidade das informações.

14. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se, para cometer o incidente, um colaborador usou software sem licenciamento regular e sem autorização formal da política de segurança da organização, então houve violação da integridade das informações da organização.

15. (CESPE – TJDFT/Analista Judiciário – Análise de Sistemas/2015) Se um colaborador conseguiu visualizar informações das quais ele não possuía privilégios, então houve violação da confidencialidade das informações.

16. (CESPE – ANTAQ/Analista Administrativo – Infraestrutura de TI/2013) Confidencialidade diz respeito à propriedade da informação que não se encontra disponível a pessoas, entidades ou processos não autorizados.

17. (CESPE – TCE-RO/Analista de Informática/2013) Considere que um arquivo que esteja sendo transferido entre dois usuários tenha sido interceptado e seu conteúdo tenha sido visualizado e encaminhado a outros usuários. Nessa situação, caracterizou-se a ocorrência do comprometimento da integridade do arquivo

18. (CESPE – TCE-RO/Analista de Informática/2013) Se um sítio da web sofrer comprometimento devido a problemas de hardware no servidor, impossibilitando a visualização do conteúdo pelos usuários, esse fato poderá ser considerado como comprometimento da disponibilidade do serviço.

19. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013)A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

20. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) O princípio da autenticidade é garantido quando o acesso à informação é concedido apenas a pessoas explicitamente autorizadas.

21. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)Na atualidade, os ativos físicos de uma organização são mais importantes para ela do que os ativos de informação.

22. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012)O termo de confidencialidade, de acordo com norma NBR ISO/IEC, representa a propriedade de salvaguarda da exatidão e completude de ativos.

23. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Considere que um usuário armazenou um arquivo nesse servidor e, após dois dias, verificou que o arquivo está modificado, de forma indevida, uma vez que somente ele tinha privilégios de gravação na área em que armazenou esse arquivo. Nessa situação, houve problema de segurança da informação relacionado à disponibilidade do arquivo.

24. (CESPE – TRE-RJ/Analista Judiciário – Análise de Sistemas/2012) Se as mídias das cópias de segurança são enviadas para outro local, fisicamente distante do servidor de arquivos, pelo

menos uma vez a cada cinco dias úteis e tendo em vista que o transporte desses dados é feito por uma empresa terceirizada, uma forma de aumentar a segurança dessa informação é efetuar procedimento para criptografar os dados armazenados nas mídias.

25. (CESPE - TCE-ES/Informática/2013) Tendo em vista que a segurança da informação tem importância estratégica, contribuindo para garantir a realização dos objetivos da organização e a continuidade dos negócios, assinale a opção correta.

a) Os principais atributos da segurança da informação são a autenticidade, a irretratabilidade e o não repúdio.

b) No contexto atual do governo e das empresas brasileiras, a segurança da informação tem sido tratada de forma eficiente, não permitindo que dados dos cidadãos ou informações estratégicas sejam vazados.

c) A privacidade constitui uma preocupação do comércio eletrônico e da sociedade da informação, não estando inserida como atributo de segurança da informação, uma vez que é prevista no Código Penal brasileiro.

d) A área de segurança da informação deve preocupar-se em proteger todos os ativos de informação de uma organização, governo, indivíduo ou empresa, empregando, em todas as situações, o mesmo nível de proteção.

e) Entre as características básicas da segurança da informação estão a confidencialidade, a disponibilidade e a integridade.

26. (CESPE - TCE-RO/Ciências da Computação/2013) As ações referentes à segurança da informação devem focar estritamente a manutenção da confidencialidade e a integridade e disponibilidade da informação.

27. (CESPE - SUFRAMA/Analista de Sistemas/2014) A utilização de algoritmos de criptografia garante a disponibilidade e a autenticidade de informações em ambientes de tecnologia da informação.

28. (CESPE - SUFRAMA/Analista de Sistemas/2014) A lentidão e a paralisação do funcionamento de um sítio de comércio eletrônico que provê transações para venda de produtos é considerado incidente que viola a confidencialidade das informações do sítio.

29. (CESPE - TRT8/Analista Judiciário - Tecnologia da Informação/2013) Considere que, em uma organização, uma planilha armazenada em um computador (o servidor de arquivos) tenha sido acessada indevidamente por usuários que visualizaram as informações contidas na planilha, mas não as modificaram. O princípio da segurança da informação comprometido com esse incidente foi

a) a disponibilidade

b) a autenticidade

c) o não repúdio

d) a confidencialidade

e) a integridade

30. (CESPE – ANCINE/Analista Administrativo/2013) No que tange à autenticação, a confiabilidade trata especificamente da proteção contra negação, por parte das entidades envolvidas em uma comunicação, de ter participado de toda ou parte desta comunicação.

31. (CESPE – ANTAQ/Analista de Infraestrutura/2014) A utilização adequada dos mecanismos de criptografia permite que se descubra qualquer alteração em um documento por partes não autorizadas, o que garante a confidencialidade do documento.

32. (CESPE – DEPEN/Área 07/2015) O principal objetivo da segurança da informação é preservar a confidencialidade, a autenticidade, a integridade e a disponibilidade da informação.

33. (CESPE – TCU/Auditor Federal de Controle Externo – TI/2015) Confidencialidade é a garantia de que somente pessoas autorizadas tenham acesso à informação, ao passo que integridade é a garantia de que os usuários autorizados tenham acesso, sempre que necessário, à informação e aos ativos correspondentes.

34. (CESPE - 2018 - EBSERH - Analista de Tecnologia da Informação) Uma auditoria no plano de continuidade de negócios de uma organização precisa verificar se o plano é exequível e se o pessoal está treinado para executá-lo.

GABARITO

GABARITO

1. C
2. E
3. C
4. C
5. E
6. C
7. D
8. B
9. E
10. C
11. C
12. A
13. E
14. E
15. C
16. C
17. E
18. C
19. C
20. E
21. E
22. E
23. E
24. C
25. E
26. E
27. E
28. E
29. D
30. E
31. E
32. C
33. E
34. C

Lista de Questões - Princípios de Segurança - FCC

1. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

No âmbito da segurança da informação em bancos de dados, as dimensões privacidade de comunicação, armazenamento seguro de dados sensíveis, autenticação de usuários e controle de acesso granular são pertinentes ao aspecto

a) confidencialidade.

b) rastreabilidade.

c) integridade.

d) permissibilidade.

e) disponibilidade.

2. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

3. (FCC – TRE-RR/Analista Judiciário/2015)

O processo de proteção da informação das ameaças caracteriza-se como Segurança da Informação. O resultado de uma gestão de segurança da informação adequada deve oferecer suporte a cinco aspectos principais:

I. Somente as pessoas autorizadas terão acesso às informações.

II. As informações serão confiáveis e exatas. Pessoas não autorizadas não podem alterar os dados.

III. Garante o acesso às informações, sempre que for necessário, por pessoas autorizadas.

IV. Garante que em um processo de comunicação os remetentes não se passem por terceiros e nem que a mensagem sofra alterações durante o envio.

V. Garante que as informações foram produzidas respeitando a legislação vigente.

Os aspectos elencados de I a V correspondem, correta e respectivamente, a:

a) autenticidade -integridade -disponibilidade - legalidade -confidencialidade.

b) autenticidade -confidencialidade -integridade - disponibilidade -legalidade.

c) integridade -disponibilidade -confidencialidade - autenticidade -legalidade.

d) disponibilidade -confidencialidade -integridade - legalidade -autenticidade.

e) confidencialidade -integridade -disponibilidade - autenticidade -legalidade.

4. (FCC – TRE-CE/Analista Judiciário – Análise de Sistemas/2015) Em relação à segurança da informação, considere:

I. Capacidade do sistema de permitir que alguns usuários acessem determinadas informações, enquanto impede que outros, não autorizados, sequer as consultem.

II. Informação exposta, sob risco de manuseio (alterações não aprovadas e fora do controle do proprietário da informação) por pessoa não autorizada.

III. O sistema deve ter condições de verificar a identidade dos usuários, e este ter condições de analisar a identidade do sistema.

Os itens I, II e III, associam-se, direta e respectivamente, aos princípios de

a) confidencialidade, integridade e autenticidade.

b) autenticidade, confidencialidade e irretratabilidade.

c) confidencialidade, confidencialidade e irretratabilidade.

d) autenticidade, confidencialidade e autenticidade.

e) integridade, confidencialidade e integridade.

5. (FCC – TRE-CE/Técnico Judiciário – Programação de Sistemas/2012) A propriedade que garante que nem o emissor nem o destinatário das informações possam negar a sua transmissão, recepção ou posse é conhecida como

a) autenticidade.

b) integridade.

c) irretratabilidade.

d) confidenciabilidade.

e) acessibilidade.

6. (FCC – TJ-AP/Analista Judiciário – Banco de Dados/2014) O controle de acesso à informação é composto por diversos processos, dentre os quais, aquele que identifica quem efetua o acesso a uma dada informação. Esse processo é denominado

A) autenticação.

B) auditoria.

C) autorização.

D) identificação.

E) permissão.

GABARITO

GABARITO

1. A
2. E
3. E
4. A
5. C
6. A

Lista de Questões - Princípios de Segurança - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

A empresa Progseg foi contratada via processo licitatório para a modernização das aplicações utilizadas no Tribunal de Justiça do Rio Grande do Norte. Aurélio, chefe do Departamento de Tecnologia, conduzirá junto à empresa o retrofit, que terá como foco a melhoria na segurança dos sistemas.

Os requisitos mandatórios dessa modernização são:

- Assegurar que informações privadas e confidenciais não estejam disponíveis nem sejam reveladas para indivíduos não autorizados; e

- Verificar que os usuários são quem dizem ser.

O requisito desejável dessa modernização é:

- Ser capaz de associar uma violação de segurança a uma parte responsável.

Com base nos requisitos citados, a Progseg deverá implementar, respectivamente:

a) confidencialidade, autenticidade, responsabilização;

b) disponibilidade, autenticidade, privacidade;

c) não repúdio, integridade de sistemas, confidencialidade;

d) integridade, disponibilidade, responsabilização;

e) autenticidade, integridade de dados, integridade de sistemas.

2. (FGV - Aud Est (CGE SC)/CGE SC/Ciências da Computação/2023)

Para o caso hipotético descrito a seguir, somente informações corretas são consideradas disponíveis.

Um determinado funcionário atende um pedido por telefone de alguém que se identifica como o cliente A. Essa pessoa explica que seus dados cadastrais estão errados e pede que seja feito um novo cadastro com as informações que ela está passando. O funcionário atende ao pedido e atualiza o sistema da empresa removendo o cadastro antigo e criando um novo.

Dias depois, ao tentar emitir uma fatura, a empresa nota que os dados do cliente A não estão completos e resolve abrir uma investigação. Durante a investigação descobre-se que os dados passados pela pessoa ao telefone eram falsos e que é portanto necessário refazer o cadastro.

Neste caso, avalie se, durante o processo de atendimento mencionado, ocorreu um incidente com quebra da

I. Confidencialidade dos dados do cliente A.

II. Disponibilidade dos dados do cliente A.

III. Integridade dos dados do cliente A.

Está correto o que se afirma em

a) I, apenas.

b) II, apenas.

c) III, apenas.

d) I e II, apenas.

e) II e III, apenas.

3. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Tânia trabalha em uma prestadora de serviços de Internet. Equivocadamente, ela enviou ao servidor um comando UPDATE, o qual alterou indevidamente a base de dados, não permitindo mais seu acesso. De forma a ocultar seu erro, Tânia descobriu um post-it sob o teclado com a senha de um dos técnicos que trabalhava com ela. Então, utilizando a senha, entrou no sistema e efetuou novas modificações, de forma que a culpa recaísse sobre o técnico.

No incidente relatado, houve a quebra do(a):

a) confidencialidade e autenticidade;

b) integridade e autenticidade;

c) irretratabilidade e disponibilidade;

d) não repúdio e confidencialidade;

e) confidencialidade e integridade.

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual - Manhã

A administração de dados deve observar princípios básicos que são largamente adotados pela comunidade segurança da informação. Além da Confidencialidade, Integridade, Disponibilidade e Autenticidade, o princípio da Irretratabilidade completa a lista.

Assinale o significado do princípio da Irretratabilidade.

A) Garantia de que os usuários que originam as informações são conhecidos e autorizados, de modo que não possam se passar por terceiros.

B) Impossibilidade de negação de que uma pessoa tenha sido autora de uma determinada informação.

C) Obrigatoriedade dos agentes pelo zelo com todas as informações coletadas.

D) Preservação fidedigna das informações.

E) Restrição de acesso às informações apenas aos autorizados.

5. (Ano: 2022 Banca: FGV Órgão: TJDFT Prova: Suporte em TI)

Lucas é um trader profissional que trabalha em uma corretora de valores. Ele efetua muitas operações durante o período em que a bolsa negocia seus ativos. Após fazer uma revisão em suas operações do dia, não validou, como sendo efetuadas por ele, algumas das operações que obtiveram prejuízo. Lucas, então, entrou em contato com a corretora e esta demonstrou, a partir de registros de auditoria e garantia de identidade, que as operações em questão realmente foram executadas por ele.

Para que a corretora prove que foi Lucas quem realmente executou as operações, ela deve fazer uso do conceito de segurança chamado:

A) confidencialidade;

B) autenticidade;

C) integridade;

D) disponibilidade;

E) irretratabilidade.

6. FGV - 2021 - IMBEL - Supervisor - Tecnologia da Informação

Segundo padrões internacionais, a Segurança da Informação distingue quatro atributos básicos que orientam a implementação de políticas e procedimentos de proteção. Assinale o atributo que não é parte desse grupo.

A) Autenticidade.

B) Completude.

C) Confidencialidade.

D) Disponibilidade.

E) Integridade.

GABARITO

GABARITO

1. A
2. E
3. B
4. B
5. E
6. B

Segurança Física, Lógica e Controle de Acesso

Quando falamos de Segurança da Informação, há uma diferenciação clássica no que tange às características dos elementos e ferramentas utilizadas para esta finalidade.

Seguimos aqui o mesmo princípio visto na nossa aula de topologia de redes em que diferenciamos os conceitos de implementação física e lógica.

Lembrando que a física diz respeito aos aspectos tangíveis e que, de fato, podem ser tocados, enquanto a lógica está relacionada aos dados em seu formato analógico ou digital, tanto no aspecto de transmissão, processamento e armazenamento.

Segurança Física

Podemos citar diversos elementos que são considerados como recursos para a segurança física. Vamos conhecer alguns:

- Unidade de Alimentação Ininterrupta (UPS) – São sistemas munidos de baterias que são capazes de armazenar energia e fornecer corrente elétrica aos demais equipamentos por um período limitado. Assim, em caso de ausência de energia, esses equipamentos possibilitam o funcionamento dos equipamentos por um período suficiente em que os administradores da rede podem atuar com vistas a mitigar perdas.

- Gerador – Seguindo a mesma linha do IPS, o gerador também tem como propósito manter o sistema em operação frente à eventual falta de energia. Entretanto, estamos falando de um período muito mais de sustentação podendo ser prolongado facilmente, uma vez que se utiliza combustível como fonte de energia.

- Site físico redundante – Busca-se criar outro ambiente que seja capaz de assumir a operação em caso de catástrofe que prejudique o ambiente principal. Para tanto, é muito importante que os dados sejam armazenados e replicados, seja online, ou em fitas e equipamentos disponibilizados em outro local.

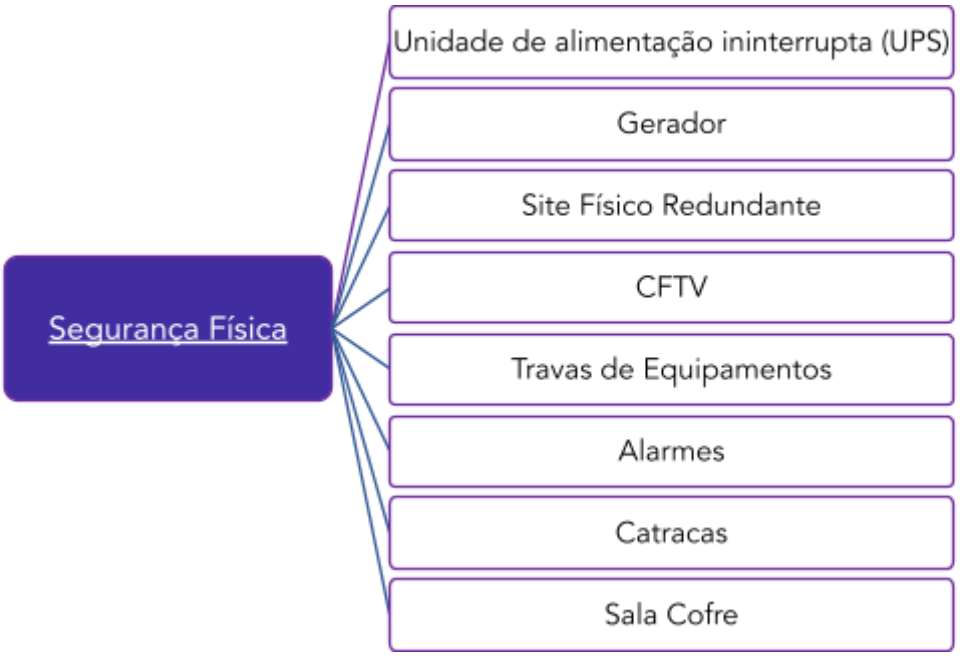
- CFTV – Temos aqui a utilização de câmeras para registro e visualização dos ambientes de uma organização. É um meio eminentemente reativo, uma vez que, na maioria das vezes, é utilizado para gravar o vídeo e ser utilizado posteriormente para análise e auditoria.

- Travas de Equipamentos – As referidas travas podem ser utilizadas tanto para impedir a utilização de determinados recursos, como bloqueio de portas USB ou unidades de DVD, de forma física, como também no intuito de não possibilitar o furto de notebooks, por exemplo, através das conhecidas chaves kensington, que, literalmente, "prendem" o equipamento em uma localidade.

- Alarmes – Temos aqui um sistema de aviso que pode ser considerado no seu aspecto físico, como alarmes de incêndio, como no aspecto lógico, como alarmes lógicos de rede.

- Catracas – A partir da utilização de senhas, crachás, smart cards, entre outros, pode-se restringir o acesso somente a pessoas autorizadas em determinados locais.

- Sala Cofre – As Salas Cofre são criadas para serem um ambiente seguro para datacenters, implementando diversos tipos de controles de segurança, de acesso, mecanismos de reação a catástrofes, entre outros.



FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A radiofrequência.

B infravermelho.

C ultravioleta.

D raio-X.

E ultrassom.

Comentários:

O mecanismo de detecção por aproximação em crachás, como o descrito, está baseado em radiofrequência. Essa tecnologia é comumente conhecida como RFID (Radio-Frequency Identification). Os crachás de identificação são equipados com uma pequena antena e um chip que emite sinais de radiofrequência quando aproximados de um leitor compatível. O leitor, que está integrado à catraca ou ao sistema de controle de acesso, captura esses sinais e autentica o usuário, permitindo ou negando o acesso com base nas informações contidas no crachá

Gabarito: A

Segurança Lógica

A segurança lógica possui diversas vertentes que podem ser consideradas. Podemos considerar a segurança a nível de um servidor de rede e serviços, por exemplo, em que devemos considerar a proteção dos recursos computacionais em todas as suas camadas, desde a linguagem de máquina e Kernel do SO, passando pelo próprio sistema operacional, arquivos, aplicações, dados, entre outros.

Podemos considerar a segurança lógica a nível da rede em que devemos inserir elementos que visam controlar o tráfego e impedir o acesso indevido aos dados trafegados ou ainda impedir que determinados tipos de fluxos passem pela rede. Neste cenário, pode-se utilizar firewalls, IDS, IPS, Proxies, entre outros elementos.

Podemos contemplar ainda as autorizações de usuários específicos e sistemas que podem acessar e utilizar determinados recursos na rede, sendo esse mecanismo conhecido como autorização.

Mencionamos ainda os registros e logs dos diversos equipamentos, sistemas e aplicações em um parque tecnológico. Tais registros são fundamentais para processos de auditoria, sendo, portanto, um recurso de segurança lógica.

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

As boas práticas da gestão dos controles de acesso lógico de uma organização incluem atribuir direitos de acesso aos usuários, conforme necessidades reais de seu trabalho ou cargo, disponibilizar contas de usuários apenas a pessoas autorizadas, armazenar senhas criptografadas e usar técnicas visíveis de identificação.

Comentários:

Muito cuidado pessoal. A questão traz uma boa narrativa que convence. Mas nem todos os itens elencados são boas práticas. O item que fica fora dessa lista é a técnica de armazenamento de senhas criptografadas. Na prática, uma forma de deixar os servidores e os dados armazenados neste equipamento mais seguros é por meio do armazenamento dos HASHES das senhas. O HASH, nada mais é do que uma função unidirecional que gera um resumo do conteúdo de entrada com tamanho físico.

Nosso objetivo não é aprender sobre HASH nessa aula, mas saber que ele é uma boa prática associada ao armazenamento de senhas.

Os demais itens, lembrando, estão aderentes às boas práticas a serem adotadas.

Gabarito: E

Outro conceito interessante que surge a esse respeito é o de HARDENING. A ideia do HARDENING é, de fato, "endurecer" um servidor de tal modo a deixá-lo mais robusto e seguro.

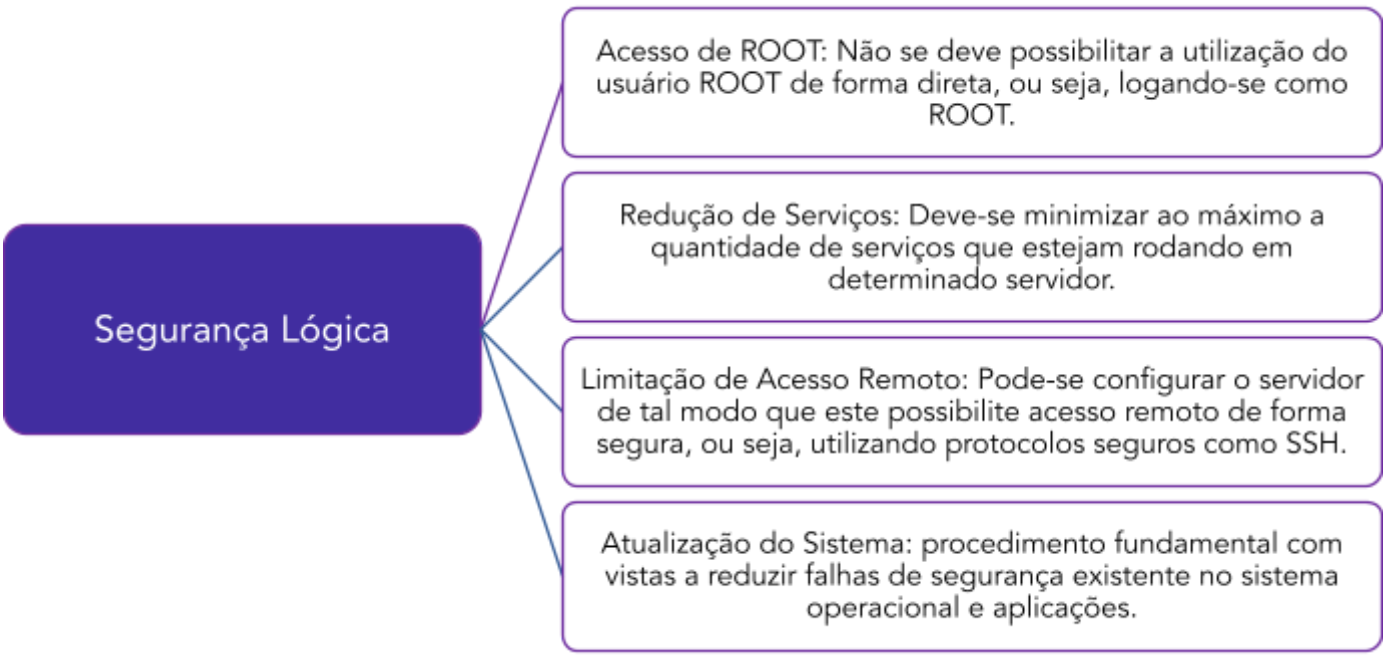
Diversos são os métodos ou regras a serem implementadas. Buscarei elencar algumas e complementaremos, eventualmente, nos exercícios:

- Acesso de ROOT – Não se deve possibilitar a utilização do usuário ROOT de forma direta, ou seja, logando-se como ROOT. Para tanto, deve-se utilizar apenas o método de escalação de privilégios, ou seja, deve-se logar como determinado usuário para posterior mudança de privilégio e consequente execução de comandos ou aplicações. Isto possibilita a geração de lastros e trilhas de auditorias, além de ser mais uma camada de segurança.

- Redução de Serviços – Deve-se minimizar ao máximo a quantidade de serviços que estejam rodando em determinado servidor. Isto tem o intuito de reduzir a possibilidade de vulnerabilidades existentes nas aplicações e serviços, bem como aumentar o desempenho do servidor. Portanto, deve-se manter apenas os serviços e aplicações necessárias, nada mais.

- Limitação de Acesso Remoto – Pode-se configurar o servidor de tal modo que este possibilite acesso remoto de forma segura, ou seja, utilizando protocolos seguros como SSH. Além disso, pode-se restringir a máquinas ou redes específicas que poderão acessar o referido servidor.

- Atualização do Sistema – É um procedimento fundamental com vistas a reduzir falhas de segurança existentes no sistema operacional e aplicações. Assim, deve-se manter e instalar as últimas versões e mais atualizadas.



HORA DE PRATICAR!

Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI

Suponha que um Analista do Tribunal Regional Federal da 4ª Região – TRF4 se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das informações no ambiente do Tribunal. Para isso, ele levantou os seguintes requisitos:

I. Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do Tribunal.

II. Os usuários não podem executar transações de TI incompatíveis com sua função.

III. Apenas usuários autorizados devem ter acesso de uso dos sistemas e aplicativos.

IV. Proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

O Analista classificou correta e respectivamente os requisitos de I a IV como segurança

A) física, física, lógica e física.

B) física, lógica, lógica e física.

C) lógica, física, lógica e física.

D) lógica, física, física e lógica.

E) física, lógica, física e lógica.

Comentários:

Pessoal, lembrem-se da dica no sentido de entenderem se o item é tangível, ou seja, algo que se toca, ou não. Caso seja o primeiro, estamos falando de segurança física. Caso seja o segundo, estamos falando de segurança lógica.

I – Trata-se se segurança física, pois a itenção é não permitir o acesso direto ao equipamento, no caso, o Access Point.

II – Estamos falando de transações, ou seja, operações nos sistemas. Neste aspecto, estamos no mundo lógico.

III – Novamente, estamos falando de acesso lógicos, em sistemas e aplicativos. E não acesso a equipamentos. Logo, também é lógico.

IV – Vejam que o interesse é em proteção de local, além de acesso aos computadores e impressoras, que também são itens materiais. Logo, segurança física.

Gabarito: B

Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI

O conceito de hardening caracteriza-se principalmente por medidas e ações que visam:

A) permitir a recuperação de sistemas computacionais na sequência de um desastre natural;

B) criar ambientes similares ao de servidores físicos, de modo que sistemas computacionais operem independentes do hardware;

C) mapear ameaças, mitigar riscos e tornar sistemas computacionais preparados para enfrentar tentativas de ataque;

D) distribuir a carga de trabalho uniformemente entre dois ou mais computadores para aumentar a confiabilidade através da redundância;

E) construir sistemas computacionais sem preocupação com a infraestrutura em que esses sistemas estão rodando.

Comentários:

Vejam que a questão traz alguns pontos que devem ser observados previamente à realização das ações de HARDENING propriamente dito. Então, quando se fala em mapear ameaças para mitigar riscos, naturalmente devemos realizar ações que tornarão os sistemas computacionais mais seguros e isso quer dizer que eles precisam ter maior robustez frente às suas configurações e serviços habilitados.

Gabarito: C

Controle de Acesso

Temos aqui um método aplicado tanto no contexto físico e lógico, com vistas a estabelecer barreiras que podem restringir determinados acessos a locais, equipamentos, serviços e dados a pessoas. O controle de acesso está diretamente ligado ao princípio da autenticidade e autorização.

1. Considerando o controle de acesso físico, temos então a primeira barreira a ser implementada. Nessa etapa pode-se diferenciar funcionários que são da organização ou não, usuários da organização que possuem autorização para acessar determinadas localidades, entre outros.

Assim, como exemplo, para um usuário acessar fisicamente o ambiente de datacenter de uma empresa, ele necessitará passar por diversos fatores de controle de acesso, como a cancela de entrada para o veículo, portaria e catraca na entrada do edifício, autenticação e autorização por algum mecanismo, como o de biometria para a sala, possuir alguma chave específica para acessar determinado rack com os servidores, e por aí vai.

Além disso, pode-se implementar recursos para controle de acesso lógico. Entre eles podemos citar a restrição de acesso por IP a determinado serviço, necessidade de login e senha, tanto para o usuário quanto para o root, entre outros.

Existem quatro técnicas de controle e gerenciamento de acesso que são amplamente utilizadas nos ambientes de tecnologia da informação.

1. Mandatory Access Control (MAC) – O administrador do sistema é responsável por atribuir as devidas permissões para os usuários. Este modelo utiliza o conceito de "label" para identificar o nível de sensibilidade a um determinado objeto. O label do usuário é verificado pelo gerenciador de acesso e através desta avaliação, é verificado o nível de acesso do usuário e quais recursos ele é capaz de usar.

2. Discretionary Access Control (DAC) – Este é um modelo mais flexível quando comparado com o MAC e considerando o usuário que necessita compartilhar o recurso com outros usuários. Nesta técnica, o usuário tem o controle de garantir privilégios de acesso a recursos aos que estão sob seu domínio. Como exemplo desta técnica, podemos citar o próprio sistema de permissão do linux ou windows, por exemplo, em que o próprio usuário pode determinar as permissões do arquivo em que ele tem a posse.

3. Role-Based Access Control (RBAC) – Também conhecido como controle baseado em papéis. Nesta técnica, o administrador garante privilégios de acordo com a função exercida pelo usuário. Esta estratégia simplifica o gerenciamento das permissões dadas aos usuários. Algumas questões têm trazido uma perspectiva mais aprofundada desse modelo. Portanto, vejamos os níveis de configuração que são possíveis com diferentes níveis de gerenciamento e atribuições:

    - RBAC 0: Esse modelo não possui hierarquia de papéis, o que significa que cada usuário teria que ter permissões específicas configuradas individualmente. Isso seria inviável em um ambiente com muitos usuários e diferentes níveis de acesso.
    - RBAC 1: Esse modelo introduz a hierarquia de papéis, permitindo que os administradores definam conjuntos de permissões que podem ser atribuídos a diferentes grupos de usuários. No entanto, o RBAC 1 não permite a delegação de permissões, o que pode ser uma limitação em ambientes complexos
    - RBAC 2: Esse modelo é o mais adequado para ambientes corporativos em geral. Ele permite a definição de hierarquias de papéis, a delegação de permissões e a restrição de acesso a recursos específicos. Isso oferece maior flexibilidade e granularidade no controle de acesso.
    - RBAC 3: Esse modelo é uma extensão do RBAC 2 que inclui suporte para controle de acesso baseado em tempo e em contexto. Estamos diante de um recurso de maior complexidade e que envolve um contexto corporativo mais maduro e gerenciável.
    - RBAC 4: Esse modelo é uma proposta recente que ainda não está totalmente implementada. Ele oferece recursos adicionais de segurança e flexibilidade, mas pode ser mais complexo de gerenciar.

4. Attribute-Based Access Control (ABAC) – É uma técnica de controle de acesso que concede ou nega acesso a recursos com base em atributos do sujeito, objeto e contexto. A principal diferença entre ABAC e RBAC é que ABAC é mais flexível e granular do que RBAC. ABAC permite que os administradores de segurança atribuam direitos de acesso com base em uma ampla gama de atributos, incluindo: Identidade do sujeito; Função do sujeito; Localização do sujeito; Tempo ; Tipo de recurso ; Critérios de segurança

    Por exemplo, imagine um sistema de gerenciamento de documentos com ABAC. Uma política ABAC poderia ser: "Permitir que usuários do departamento de vendas acessem documentos de vendas apenas durante horário comercial e a partir do escritório". Nesse caso, os atributos seriam a identidade do usuário, o departamento, o horário e a localização, e a decisão de acesso dependerá de como esses atributos se relacionam com a política.

FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

Comentários:

Conforme vimos em nossa teoria, estamos mais próximos da configuração tipo 2, que é, de fato, o modelo mais usual e que traz um equilíbrio entre controle, segurança e esforço para consolidar e implantar.

Gabarito: C

Ano: 2019 Banca: CESPE / CEBRASPE Órgão: TCE-RO

O modelo de controle de acesso que permite níveis de interação e acesso aos recursos dos sistemas de acordo com as funções que os usuários desempenham na organização é o

A) discricionário.

B) embasado em papéis.

C) em matriz.

D) embasado em regras.

E) mandatório.

Comentários:

Vejam a palavra chave, pessoal. De acordo com as suas funções ou papeis. Logo, temos o modelo RBAC, que é embasado em papéis.

Gabarito: B

(Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Para o controle de acesso a sistemas de informação, podem ser adotadas diferentes formas de controle de acesso lógico, com vistas à segurança de um recurso. Quanto a essas formas de controle, assinale a opção correta.

A) Do ponto de vista do usuário, um controle discricionário é, em geral, menos flexível que um mandatório.

B) Em geral, é mais difícil auditar sistemas que operam com controle de acesso discricionário do que sistemas com controle de acesso mandatório.

C) Como regra geral, no controle de acesso mandatório, os donos e usuários de recursos podem conceder acesso além dos limites declarados pela política da empresa.

D) No controle discricionário, podem ser transferidos para terceiros os direitos de acesso, mas não a propriedade de um recurso.

E) Em um sistema mandatório, o acesso é concedido com base na avaliação das funções dos sujeitos em relação às reivindicações relacionadas ao seu papel no sistema de informação.

Comentários:

Cobrança direta do conteúdo que acabamos de ver. Vamos aos itens:

A) Vimos que o controle mandatório é o mais rígido, logo, menos flexível, e não o discricionário como apresenta o item.

B) Exatamente pessoal. Como o mandatório tem a visão centralizada, a partir do admin da rede, há menos variação nas pastas e objetos. Logo, de fato, é mais fácil de se auditar.

C) Questão invertida. Tem-se a descrição do controle discricionário.

D) O erro está em afirmar que não se pode transferir a propriedade. Ela é possível também de ser transferida.

E) Aqui, temos o descritivo do modelo RBAC, dado o trecho focado nas funções ou papeis dos sujeitos.

Gabarito: B

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - CESPE Órgão: PG-DF

1. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

Para reduzir vulnerabilidades, os controles de acesso devem liberar a propriedade do registro para que usuário possa criar, ler, atualizar ou excluir qualquer registro.

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

O uso de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso para usuários é considerado uma boa prática de segurança da informação.

3. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

O emprego de controles apropriados para o acesso físico de pessoas a ambientes seguros de processamento de informações tem como principal finalidade

a) organizar a emissão de identidades funcionais permanentes e credenciais temporárias para o público externo.

b) criar um banco de dados de clientes, com foco em relacionamento corporativo.

c) assegurar que somente pessoas autorizadas tenham acesso permitido.

d) viabilizar e acelerar o acesso de fornecedores e prestadores de serviços em emergências.

e) estabelecer um histórico de todos os acessos, para fins logísticos e estatísticos.

4. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em função de sua codificação mais robusta, os firmwares de IoT são mais sofisticados que os sistemas operacionais executados em computadores e smartphones, o que os torna imunes a falhas consequentes das vulnerabilidades conhecidas.

5. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

As boas práticas da gestão dos controles de acesso lógico de uma organização incluem atribuir direitos de acesso aos usuários, conforme necessidades reais de seu trabalho ou cargo, disponibilizar contas de usuários apenas a pessoas autorizadas, armazenar senhas criptografadas e usar técnicas visíveis de identificação.

6. (CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012)

Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

7. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Suponha que um Analista do Tribunal Regional Federal da 4ª Região – TRF4 se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das informações no ambiente do Tribunal. Para isso, ele levantou os seguintes requisitos:

I. Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do Tribunal.

II. Os usuários não podem executar transações de TI incompatíveis com sua função.

III. Apenas usuários autorizados devem ter acesso de uso dos sistemas e aplicativos.

IV. Proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

O Analista classificou correta e respectivamente os requisitos de I a IV como segurança

A) física, física, lógica e física.

B) física, lógica, lógica e física.

C) lógica, física, lógica e física.

D) lógica, física, física e lógica.

E) física, lógica, física e lógica.

8. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

O conceito de hardening caracteriza-se principalmente por medidas e ações que visam:

A) permitir a recuperação de sistemas computacionais na sequência de um desastre natural;

B) criar ambientes similares ao de servidores físicos, de modo que sistemas computacionais operem independentes do hardware;

C) mapear ameaças, mitigar riscos e tornar sistemas computacionais preparados para enfrentar tentativas de ataque;

D) distribuir a carga de trabalho uniformemente entre dois ou mais computadores para aumentar a confiabilidade através da redundância;

E) construir sistemas computacionais sem preocupação com a infraestrutura em que esses sistemas estão rodando.

9. Ano: 2019 Banca: CESPE / CEBRASPE Órgão: TCE-RO

O modelo de controle de acesso que permite níveis de interação e acesso aos recursos dos sistemas de acordo com as funções que os usuários desempenham na organização é o

A) discricionário.

B) embasado em papéis.

C) em matriz.

D) embasado em regras.

E) mandatório.

10. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Para o controle de acesso a sistemas de informação, podem ser adotadas diferentes formas de controle de acesso lógico, com vistas à segurança de um recurso. Quanto a essas formas de controle, assinale a opção correta.

A) Do ponto de vista do usuário, um controle discricionário é, em geral, menos flexível que um mandatório.

B) Em geral, é mais difícil auditar sistemas que operam com controle de acesso discricionário do que sistemas com controle de acesso mandatório.

C) Como regra geral, no controle de acesso mandatório, os donos e usuários de recursos podem conceder acesso além dos limites declarados pela política da empresa.

D) No controle discricionário, podem ser transferidos para terceiros os direitos de acesso, mas não a propriedade de um recurso.

E) Em um sistema mandatório, o acesso é concedido com base na avaliação das funções dos sujeitos em relação às reivindicações relacionadas ao seu papel no sistema de informação.

11. (CESPE – TJ-AC/Técnico Judiciário – Informática/2012)

Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

GABARITO

GABARITO

1. E
2. E
3. C
4. E
5. E
6. C
7. B
8. C
9. B
10. B
11. C

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FCC

1. (FCC – TRF 4ª Região / Analista Judiciário – Informática/2014) José deve estabelecer uma política de segurança e implantar os mecanismos de segurança para o TRF da 4a Região. Dentre os mecanismos para a segurança física, José deve escolher o uso de

A) senha de acesso ao computador do TRF.

B) Token criptográfico para autenticar os dados acessados no computador do TRF.

C) senha de acesso às páginas web do TRF.

D) cartão de acesso para as pessoas que entram no TRF.

E) criptografia na troca de informações entre os computadores do TRF.

Comentário:

Pessoal, o problema nessa questão está nos itens "B" e "D", pois, ambos são itens utilizados para segurança física. Entretanto, no item "B", temos a descrição incorreta pois não se objetiva autenticar os dados e sim a pessoa.

Gabarito: D

---

2. (FCC – SABESP/Analista de Gestão – Sistemas/2014) Todos os procedimentos de segurança listados abaixo referem-se a controles de acesso lógico, EXCETO:

A) utilizar mecanismos de time-out automático, isto é, desativar a sessão após um determinado tempo sem qualquer atividade no terminal ou computador. Para restaurá-la, o usuário é obrigado a fornecer novamente seu ID e senha.

B) definir o controle de acesso nas entradas e saídas através de travas, alarmes, grades, vigilante humano, vigilância eletrônica, portas com senha, cartão de acesso e registros de entrada e saída de pessoas e objetos.

C) utilizar logs como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando.

D) definir as permissões e os privilégios de acesso para cada recurso ou arquivo no sistema. Quando um usuário tenta acessar um recurso, o sistema operacional verifica se as definições de acesso desse usuário e do recurso desejado conferem. O usuário só conseguirá o acesso se essa verificação for positiva.

E) limitar o número de tentativas de logon sem sucesso e limitar o horário de uso dos recursos computacionais de acordo com a real necessidade de acesso aos sistemas. Pode-se, por exemplo, desabilitar o uso dos recursos nos fins de semana ou à noite.

Comentário:

O item "B" nos traz uma lista de itens que fazem parte da segurança física de qualquer ambiente. Questão bem extensa, porém, bem tranquila.

Gabarito: B

---

3. (FCC – TRT – 6ª Região (PE)/Analista Judiciário - TI/2018) A gerência de riscos na segurança da informação inclui o uso de diversos tipos e recursos de segurança. Um recurso de segurança categorizado como mecanismo de controle de acesso lógico é

a) a função hash.

b) o sistema biométrico.

c) a catraca eletrônica.

d) o sistema de detecção de intrusão.

e) o sniffer.

Comentários:

Questão bem tranquila, certo pessoal? Vimos que um dos mecanismos de controle de acesso é o sistema biométrico. Nele podemos controlar o acesso a partir de ALGO QUE VOCÊ É.

a) Algoritmo utilizado para fins de integridade. ERRADO

c) Controle de acesso físico. ERRADO

d) Ferramenta para gerenciamento de segurança de redes de computadores. ERRADO

e) Ferramenta utilizada para capturar e analisar dados lógicos (pacotes) que trafegam na rede. ERRADO

Gabarito: B

---

4. (FCC - 2013 - SEFAZ-SP - Agente Fiscal de Rendas - Gestão Tributária - Prova 3)

A auditoria da segurança da informação avalia a política de segurança e os controles relacionados adotados em cada organização. Nesse contexto, muitas vezes, as organizações não se preocupam, ou até negligenciam, um aspecto básico da segurança que é a localização dos equipamentos que podem facilitar a intrusão. Na auditoria de segurança da informação, esse aspecto é avaliado no Controle de :

a) acesso lógico.

b) acesso físico.

c) programas.

d) conteúdo.

e) entrada e saída de dados.

Comentários:

Percebam que a questão aborda a questão da "Localização dos equipamentos". Ora, estamos falando, portanto, das questões atreladas ao controle físico.

Gabarito: B

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

Comentários:

Estamos mais próximos da configuração tipo 2, que é, de fato, o modelo mais usual e que traz um equilíbrio entre controle, segurança e esforço para consolidar e implantar.

RBAC 2: Esse modelo é o mais adequado para ambientes corporativos em geral. Ele permite a definição de hierarquias de papéis, a delegação de permissões e a restrição de acesso a recursos específicos. Isso oferece maior flexibilidade e granularidade no controle de acesso.

Gabarito: C

2. FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A radiofrequência.

B infravermelho.

C ultravioleta.

D raio-X.

E ultrassom.

Comentários:

O mecanismo de detecção por aproximação em crachás, como o descrito, está baseado em radiofrequência. Essa tecnologia é comumente conhecida como RFID (Radio-Frequency Identification). Os crachás de identificação são equipados com uma pequena antena e um chip que emite sinais de radiofrequência quando aproximados de um leitor compatível. O leitor, que está integrado à catraca ou ao sistema de controle de acesso, captura esses sinais e autentica o usuário, permitindo ou negando o acesso com base nas informações contidas no crachá

Gabarito: A

3. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e

No contexto da Segurança da Informação, o primeiro controle de acesso a ser estabelecido, isto é, a primeira barreira de segurança deve ser o controle de acesso

A lógico.

B físico.

C por nome de usuário (login) e senha.

D por DMZ.

E por criptografia.

Comentário:

Pessoal, sem dúvida, a boa prática traz a primeira camada física de proteção como referência. Estamos falando aqui de controles em portarias, hall de entrada, garagens, seja com estruturas que envolvem pessoas ou não. Todas as demais são recursos a serem implantados em novas camadas de segurança.

Gabarito: B

QUESTÕES COMENTADAS - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - CESPE

1. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

Para reduzir vulnerabilidades, os controles de acesso devem liberar a propriedade do registro para que usuário possa criar, ler, atualizar ou excluir qualquer registro.

Comentários:

Os controles de acesso devem restringir as permissões dos usuários, permitindo apenas as operações necessárias para suas funções. Liberar a propriedade do registro para criar, ler, atualizar ou excluir qualquer registro aumenta as vulnerabilidades.

Gabarito: E

2. CEBRASPE (CESPE) - Ana (SERPRO)/SERPRO/Tecnologia/2023

Acerca de conceitos relacionados a controle de acesso, julgue o item a seguir.

O uso de processos e ferramentas para criar, atribuir, gerenciar e revogar credenciais de acesso para usuários é considerado uma boa prática de segurança da informação.

Comentários:

O uso de processos e ferramentas para gerenciar credenciais de acesso é uma boa prática de segurança da informação, pois garante que apenas usuários autorizados tenham acesso aos recursos e que as credenciais sejam gerenciadas de forma segura.

Gabarito: E

3. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

O emprego de controles apropriados para o acesso físico de pessoas a ambientes seguros de processamento de informações tem como principal finalidade

a) organizar a emissão de identidades funcionais permanentes e credenciais temporárias para o público externo.

b) criar um banco de dados de clientes, com foco em relacionamento corporativo.

c) assegurar que somente pessoas autorizadas tenham acesso permitido.

d) viabilizar e acelerar o acesso de fornecedores e prestadores de serviços em emergências.

e) estabelecer um histórico de todos os acessos, para fins logísticos e estatísticos.

Comentários:

Conforme vimos, o foco não se trata de aspectos de identificação, mas sim, indicar quem pode fazer algo nesse contexto. Essa é a essência da autorização e controle de acesso.

Gabarito: C

4. CEBRASPE (CESPE) - Ana TI (DATAPREV)/DATAPREV/Segurança Cibernética/2023

Em função de sua codificação mais robusta, os firmwares de IoT são mais sofisticados que os sistemas operacionais executados em computadores e smartphones, o que os torna imunes a falhas consequentes das vulnerabilidades conhecidas.

Comentários:

Os sistemas operacionais tradicionais são muito mais robustos do que os firmware que operam nesses hardwares de IoT. Lembrando que IoT é Internet das Coisas, ou seja, aquele conceito onde praticamente tudo se torna digital, e portanto, controlável e acessado pelas redes de computadores.

Esse novo contexto e realidade gera desafios imensos de segurança, justamente porque todo dispositivo conectado na rede ou internet passa a ser alvo de atacantes, e pode, inclusive, virar vetor para realização de outros ataques.

Gabarito: E

5. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

As boas práticas da gestão dos controles de acesso lógico de uma organização incluem atribuir direitos de acesso aos usuários, conforme necessidades reais de seu trabalho ou cargo, disponibilizar contas de usuários apenas a pessoas autorizadas, armazenar senhas criptografadas e usar técnicas visíveis de identificação.

Comentários:

Muito cuidado pessoal. A questão traz uma boa narrativa que convence. Mas nem todos os itens elencados são boas práticas. O item que fica fora dessa lista é a técnica de armazenamento de senhas criptografadas. Na prática, uma forma de deixar os servidores e os dados armazenados neste equipamento mais seguros é por meio do armazenamento dos HASHES das senhas. O HASH, nada mais é do que uma função unidirecional que gera um resumo do conteúdo de entrada com tamanho físico.

Nosso objetivo não é aprender sobre HASH nessa aula, mas saber que ele é uma boa prática associada ao armazenamento de senhas.

Os demais itens, lembrando, estão aderentes as boas práticas a serem adotadas.

Gabarito: E

6. (CESPE – TJ-ES/Analista Judiciário – Análise de Sistemas/2012)

Para o controle lógico do ambiente computacional, deve-se considerar que medidas de segurança devem ser atribuídas aos sistemas corporativos e aos bancos de dados, formas de proteção ao código-fonte, preservação de arquivos de log de acesso ao sistema, incluindo-se o sistema de autenticação de usuários.

Comentários:

Dos elementos apresentados, o que não apresentamos como recurso de segurança lógica na nossa teoria é a proteção de código fonte. Existem algumas ferramentas, como ofuscadores de código ou a própria criptografia que visam tornar o código fonte mais seguro, impossibilitando o acesso ou visualização por parte de usuários mal intencionados.

Gabarito: C

7. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Suponha que um Analista do Tribunal Regional Federal da 4ª Região – TRF4 se depare com uma situação em que deve implantar mecanismos de proteção interna voltados à segurança física e lógica das informações no ambiente do Tribunal. Para isso, ele levantou os seguintes requisitos:

I. Não instalar em áreas de acesso público equipamentos que permitam o acesso à rede interna do Tribunal.

II. Os usuários não podem executar transações de TI incompatíveis com sua função.

III. Apenas usuários autorizados devem ter acesso de uso dos sistemas e aplicativos.

IV. Proteger o local de armazenamento das unidades de backup e restringir o acesso a computadores e impressoras que possam conter dados confidenciais.

O Analista classificou correta e respectivamente os requisitos de I a IV como segurança

A) física, física, lógica e física.

B) física, lógica, lógica e física.

C) lógica, física, lógica e física.

D) lógica, física, física e lógica.

E) física, lógica, física e lógica.

Comentários:

Pessoal, lembrem-se da dica no sentido de entenderem se o item é tangível, ou seja, algo que se toca, ou não. Caso seja o primeiro, estamos falando de segurança física. Caso seja o segundo, estamos falando de segurança lógica.

I – Trata-se se segurança física, pois a itenção é não permitir o acesso direto ao equipamento, no caso, o Access Point.

II – Estamos falando de transações, ou seja, operações nos sistemas. Neste aspecto, estamos no mundo lógico.

III – Novamente, estamos falando de acesso lógicos, em sistemas e aplicativos. E não acesso a equipamentos. Logo, também é lógico.

IV – Vejam que o interesse é em proteção de local, além de acesso aos computadores e impressoras, que também são itens materiais. Logo, segurança física.

Gabarito: B

8. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

O conceito de hardening caracteriza-se principalmente por medidas e ações que visam:

A) permitir a recuperação de sistemas computacionais na sequência de um desastre natural;

B) criar ambientes similares ao de servidores físicos, de modo que sistemas computacionais operem independentes do hardware;

C) mapear ameaças, mitigar riscos e tornar sistemas computacionais preparados para enfrentar tentativas de ataque;

D) distribuir a carga de trabalho uniformemente entre dois ou mais computadores para aumentar a confiabilidade através da redundância;

E) construir sistemas computacionais sem preocupação com a infraestrutura em que esses sistemas estão rodando.

Comentários:

Vejam que a questão traz alguns pontos que devem ser observados previamente à realização das ações de HARDENING propriamente dito. Então, quando se fala em Mapear ameaças para mitigar riscos, naturalmente devemos realizar ações que tornarão os sistemas computacionais mais seguros e isso quer dizer que eles precisam ter maior robustez frente às suas configurações e serviços habilitados.

Gabarito: C

9. Ano: 2019 Banca: CESPE / CEBRASPE Órgão: TCE-RO

O modelo de controle de acesso que permite níveis de interação e acesso aos recursos dos sistemas de acordo com as funções que os usuários desempenham na organização é o

A) discricionário.

B) embasado em papéis.

C) em matriz.

D) embasado em regras.

E) mandatório.

Comentários:

Vejam a palavra chave, pessoal. De acordo com as suas funções ou papeis. Logo, temos o modelo RBAC, que é embasado em papéis.

Gabarito: B

10. (Ano: 2021 Banca: CESPE Órgão: PG-DF Prova: Técnico Jurídico – TI)

Para o controle de acesso a sistemas de informação, podem ser adotadas diferentes formas de controle de acesso lógico, com vistas à segurança de um recurso. Quanto a essas formas de controle, assinale a opção correta.

A) Do ponto de vista do usuário, um controle discricionário é, em geral, menos flexível que um mandatório.

B) Em geral, é mais difícil auditar sistemas que operam com controle de acesso discricionário do que sistemas com controle de acesso mandatório.

C) Como regra geral, no controle de acesso mandatório, os donos e usuários de recursos podem conceder acesso além dos limites declarados pela política da empresa.

D) No controle discricionário, podem ser transferidos para terceiros os direitos de acesso, mas não a propriedade de um recurso.

E) Em um sistema mandatório, o acesso é concedido com base na avaliação das funções dos sujeitos em relação às reivindicações relacionadas ao seu papel no sistema de informação.

Comentários:

Cobrança direta do conteúdo que acabamos de ver. Vamos aos itens:

A) Vimos que o controle mandatório é o mais rídigo, logo, menos flexível, e não o discricionário como a presenta o item.

B) Exatamente pessoal. Como o mandatório tem a visão centralizada, a partir do admin da rede, há menos variação nas pastas e objetos. Logo, de fato, é mais fácil de se auditar.

C) Questão invertida. Tem-se a descrição do controle discricionário.

D) O erro está em afirmar que não se pode transferir a propriedade. Ela é possível também de ser transferida.

E) Aqui, temos o descritivo do modelo RBAC, dado o trecho focado nas funções ou papeis dos sujeitos.

Gabarito: B

11. (CESPE – TJ-AC/Técnico Judiciário – Informática/2012)

Para garantir a segurança da informação, é recomendável não apenas a instalação de procedimentos relacionados a sistemas e manipulação de dados eletrônicos, mas também daqueles pertinentes ao controle de acesso físico.

Comentários:

Nada mais é do que implementar de fato os aspectos de segurança física e lógica, certo pessoal?

Gabarito: C

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FCC

1. (FCC – TRF 4ª Região / Analista Judiciário – Informática/2014) José deve estabelecer uma política de segurança e implantar os mecanismos de segurança para o TRF da 4a Região. Dentre os mecanismos para a segurança física, José deve escolher o uso de

A) senha de acesso ao computador do TRF.

B) Token criptográfico para autenticar os dados acessados no computador do TRF.

C) senha de acesso às páginas web do TRF.

D) cartão de acesso para as pessoas que entram no TRF.

E) criptografia na troca de informações entre os computadores do TRF.

2. (FCC – SABESP/Analista de Gestão – Sistemas/2014) Todos os procedimentos de segurança listados abaixo referem-se a controles de acesso lógico, EXCETO:

A) utilizar mecanismos de time-out automático, isto é, desativar a sessão após um determinado tempo sem qualquer atividade no terminal ou computador. Para restaurá-la, o usuário é obrigado a fornecer novamente seu ID e senha.

B) definir o controle de acesso nas entradas e saídas através de travas, alarmes, grades, vigilante humano, vigilância eletrônica, portas com senha, cartão de acesso e registros de entrada e saída de pessoas e objetos.

C) utilizar logs como medidas de detecção e monitoramento, registrando atividades, falhas de acesso (tentativas frustradas de logon ou de acesso a recursos protegidos) ou uso do sistema operacional, utilitários e aplicativos, e detalhando o que foi acessado, por quem e quando.

D) definir as permissões e os privilégios de acesso para cada recurso ou arquivo no sistema. Quando um usuário tenta acessar um recurso, o sistema operacional verifica se as definições de acesso desse usuário e do recurso desejado conferem. O usuário só conseguirá o acesso se essa verificação for positiva.

E) limitar o número de tentativas de logon sem sucesso e limitar o horário de uso dos recursos computacionais de acordo com a real necessidade de acesso aos sistemas. Pode-se, por exemplo, desabilitar o uso dos recursos nos fins de semana ou à noite.

3. (FCC – TRT – 6ª Região (PE)/Analista Judiciário - TI/2018) A gerência de riscos na segurança da informação inclui o uso de diversos tipos e recursos de segurança. Um recurso de segurança categorizado como mecanismo de controle de acesso lógico é

A) a função hash.

B) o sistema biométrico.

C) a catraca eletrônica.

D) o sistema de detecção de intrusão.

E) o sniffer.

4. (FCC - 2013 - SEFAZ-SP - Agente Fiscal de Rendas - Gestão Tributária - Prova 3)

A auditoria da segurança da informação avalia a política de segurança e os controles relacionados adotados em cada organização. Nesse contexto, muitas vezes, as organizações não se preocupam, ou até negligenciam, um aspecto básico da segurança que é a localização dos equipamentos que podem facilitar a intrusão. Na auditoria de segurança da informação, esse aspecto é avaliado no Controle de :

A) acesso lógico.

B) acesso físico.

C) programas.

D) conteúdo.

E) entrada e saída de dados.

GABARITO

GABARITO

1. D
2. B
3. B
4. B

Lista de Questões - SEGURANÇA FÍSICA, LÓGICA E CONTROLE DE ACESSO - FGV

1. (FGV - Ana (DPE RS)/DPE RS/Apoio Especializado (TI)/Infraestrutura e Redes/2023)

Aurélio está implementando o controle de acesso à rede wi-fi da Defensoria Pública do Estado do Rio Grande do Sul (DPE/RS). Ele se baseou no modelo de referência do RBAC (Role Based Access Control) para a definição dos perfis. O perfil mais restrito possui as permissões básicas para cada servidor e, a partir dele, o acesso vai se incrementando. Os servidores do Departamento de Segurança devem ter as permissões mais básicas, além de acrescentar restrições, que restringem os modos de configuração possíveis.

Com base nesse modelo de referência, Aurélio deverá atribuir para o Departamento de Segurança o modelo RBAC:

a) 0;

b) 1;

c) 2;

d) 3;

e) 4.

2. FGV - 2023 - Banco do Brasil - Técnico Atendimento

A catraca de controle de acesso é um dispositivo de segurança utilizado para dificultar o acesso não-autorizado a determinadas áreas de uma empresa, bem como possibilita monitorar o próprio fluxo de pessoal nessas áreas restritas.

O controle do acesso propriamente dito pode ser feito a partir da checagem de algum dado do usuário, como, por exemplo, a aproximação do seu crachá de identificação.

O mecanismo de detecção por aproximação em crachás está baseado em

A) radiofrequência.

B)infravermelho.

C) ultravioleta.

D) raio-X.

E ultrassom.

3. FGV - 2018 - AL-RO - Analista Legislativo - Infraestrutura de Redes e

No contexto da Segurança da Informação, o primeiro controle de acesso a ser estabelecido, isto é, a primeira barreira de segurança deve ser o controle de acesso

A) lógico.

B) físico.

C) por nome de usuário (login) e senha.

D) por DMZ.

E) por criptografia.

GABARITO

GABARITO

1. C
2. A
3. B

AUTENTICAÇÃO E SEUS MECANISMOS

Os mecanismos de autenticação são procedimentos, rotinas, ferramentas ou soluções que implementam, de fato, o princípio de autenticação com o devido controle de acesso. Estes podem ser subdivididos em três grandes grupos, quais sejam:

- Algo que você sabe

Nesta categoria, busca-se determinar a autenticidade dos usuários baseado em alguma informação que seja de conhecimento único daquele usuário. Podemos utilizar, como exemplo clássico, a nossa senha de acesso à rede corporativa do local onde trabalhamos. Ora, assume-se que a informação de senha seja de conhecimento apenas do dono da conta.

- Algo que você tem

Quando se vincula a autenticação a alguma coisa que esteja sob a posse exclusiva do usuário, temos a aplicação desta categoria. Temos diversos exemplos, entre eles, a utilização de um token, crachá, smart card.

- Algo que você é

Temos aqui, em regra, o mecanismo mais robusto na garantia do princípio da autenticidade. Aqui, uma característica específica e exclusiva dos usuários é utilizada como parâmetro. Os exemplos clássicos que se aplicam aqui é a utilização da biometria.

Um detalhe importante a se mencionar é que a biometria não se restringe à impressão digital. Pode-se utilizar a informação da Íris, padrão de voz, imagem da face, entre outros.

Avançando a nossa discussão, temos ainda que o serviço de autenticação traz consigo outras funções e recursos muito importantes, como a autorização e a auditabilidade. O primeiro corresponde ao fato de que determinado usuário ou serviço dependerá da devida validação de suas credenciais para verificar se este pode ou não acessar determinado recurso. Ou seja, agora, não basta simplesmente ser um usuário válido no sentido de autenticação, mas deve-se ter autorização para tal recurso.

Como exemplo, podemos citar o fato de se ter permissão para ler informações de um diretório, porém, não há permissão para modificar ou criar informações em um diretório.

Conforme mencionamos, temos ainda o aspecto da auditabilidade que permite o registro das ações dos usuários de tal forma que permita o rastreamento para identificação de falhas ou atos indevidos com seus respectivos responsáveis.

> O conjunto dessas três características conceitua o termo AAA (authentication, authorization e accounting).

É pacífica a ideia de que a segurança não é 100% confiável. Entretanto, utilizam-se meios diversos para tentar se aproximar desse percentual, ou seja, de dificultar o processo de quebra. No aspecto da autenticação não é diferente.

Nesse sentido surge o conceito de autenticação forte ou de dois fatores (duas etapas) ou ainda, duplo fator de autenticação (2FA). Como o próprio nome sugere, nada mais é do que dividir a fase de autenticação em duas etapas. Destaca-se que esse processo deve, necessariamente, envolver a combinação de ALGO QUE VOCÊ SABE, ALGO QUE VOCÊ TEM ou ALGO QUE VOCÊ É.

Muito cuidado com essa combinação.

Um exemplo que temos é: na primeira etapa, em regra, tem-se a inserção das informações de usuário e senha. Em seguida, utilizando-se de algum outro meio (sms, email, aplicativo de celular), o usuário receberá uma outra senha aleatória ou código que deverá ser inserido na aplicação inicial para acessar o recurso, sendo esta a segunda etapa.

Percebam que esse código funciona como se fosse uma chave de sessão, ou seja, servirá para aquele acesso durante um período específico. Se você tentar, em um segundo momento, acessar de novo a sua conta, um novo código será gerado. Esse exemplo contemplou os fatores de ALGO QUE VOCÊ SABE com ALGO QUE VOCÊ TEM.

Algumas aplicações utilizam esse recurso: BB CODE do banco do Brasil; Steam Guard para Games; Gmail quando se habilita a funcionalidade. Basicamente as principais aplicações WEB suportam esse recurso.

Reparem que nesse caso, assumindo que sua senha foi violada, o invasor não conseguirá acessar sua conta uma vez que dependerá do código aleatório que será enviado na segunda etapa de autenticação.

Por fim, merece destacar também a existência do MULTIFATOR de autenticação, ou MFA, que segue o mesmo princípio, e pode ter 2 ou mais fatores.

Ainda no contexto do MFA, temos a Autenticação Multifator Adaptativa (MFA Adaptativa), que é uma forma avançada de autenticação multi fator que ajusta dinamicamente os requisitos de autenticação com base no contexto e no comportamento do usuário. Em vez de aplicar os mesmos fatores de autenticação para todos os usuários em todas as situações, a MFA adaptativa analisa diversos parâmetros para determinar o nível apropriado de segurança necessário para cada tentativa de login.

A MFA adaptativa utiliza informações contextuais e padrões de comportamento do usuário para avaliar o risco associado a uma tentativa de login. Alguns dos fatores considerados incluem:

1. Localização: Onde o usuário está tentando se conectar.

2. Dispositivo: O dispositivo usado para fazer login.
3. Horário: O horário em que a tentativa de login está sendo feita.
4. Rede: Se a conexão está sendo feita a partir de uma rede privada ou pública.
5. Tentativas de Login: O número de tentativas de login falhadas.

Com base nesses parâmetros, a MFA adaptativa pode exigir diferentes níveis de autenticação. Por exemplo, se um usuário tenta fazer login de um local desconhecido ou em um horário incomum, o sistema pode solicitar uma verificação adicional, como um código enviado por SMS ou uma autenticação biométrica.

CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

No controle de acesso, somente os usuários que tenham sido especificamente autorizados podem usar e receber acesso às redes e aos seus serviços.

Comentários:

Exatamente pessoal. É importante sempre lembrar essa diferença básica da autenticação e autorização.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-CE

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Comentários:

Exatamente pessoal. Típica questão conceito. Veremos mais à frente algumas questões mais práticas sobre o funcionamento desses aplicativos? Mas tenho certeza que muitos de vocês já usaram, como o Google Authenticator, por exemplo, ou algum serviço semelhante, onde são geradas senhas para cada usuário. Agora é importante destacar que aqui nós temos o modelo de algo que você sabe, com algo que você possui.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Para acessar a intranet corporativa, um colaborador informa seu CPF, senha pessoal e um código enviado para o seu celular cadastrado.

O mecanismo de reforço implementado nessa intranet para confirmar a identidade do usuário contra acessos indevidos é a autenticação:

A) biométrica;

B) Kerberos;

C) Oauth2;

D) 2FA;

E) Openid.

Comentários:

Conforme nós vimos pessoal, há a necessidade de conhecimento de algo que VOCÊ SABE (CPF + senha), com ALGO QUE VOCÊ POSSUI (celular). Logo, temos aí o 2FA.

Gabarito: D

Um outro tópico que surge ainda no mundo da autenticação é o conceito de Single Sign On (SSO). A ideia básica e simplista aqui é possibilitar a determinado usuário consumir recursos de diversos sistemas e serviços a partir de uma única camada de autenticação.

Ou seja, no seu serviço por exemplo, uma vez que você chegou e acessou a sua máquina com login e senha, a partir de então, você será capaz acessar os recursos de ponto eletrônico, email, serviço de diretórios, outros sistemas internos, sem ser necessário digitar novamente o login e a senha. Importante destacar que é um serviço que permite a integração de sistemas independentes.

O principal protocolo que roda por trás desse recurso é o LDAP, no âmbito corporativo. Uma implementação mais simples é por intermédio dos cookies dos browsers dos dispositivos. O conceito de Single Sign OFF também se aplica no sentido inverso.

Ano: 2020 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

A dinâmica é sempre essa pessoal. A autenticação é o ato final de reconhecimento do usuário ou sistema. Fato é que, para autenticar, devemos identificar. E esse processo pode acontecer de diferentes formas. Ainda, após o processo de identificação e autenticação, temos a autorização, recebendo esses dois pré-requisitos.

Gabarito: C

SAML - Security Assertion Markup Language

Avançando um pouco mais na nossa conversa a respeito de processos de identificação e acesso, é importante falarmos sobre o SAML. Esse assunto tem sido cobrado cada vez mais em provas, trazendo um contexto de aplicação para ambientes corporativos com alta e média complexidade.

Importante destacar que o SAML não é uma tecnologia em si, mas sim, um padrão aberto que permite com que provedores de serviços e recursos de identidade passe credenciais de autorização para provedores de serviços. Vejam que na sua própria definição, há instância e regimes de competências a serem observados. Então se aplica aqui o contexto de simplicidade de implementação quando falamos de logins centralizados e unificados.

A título de referência sobre esse serviço e o Single-Sign-On, temos a própria camada de login único criado pelo Governo Federal, conhecido como Acesso.gov, da plataforma Gov.br. Basicamente, a partir deste serviço, busca-se eliminar a múltiplas instâncias de identidade de diferentes órgãos e serviços, passando a responsabilidade pelo processo de gestão de identidade de forma centralizada, e, a partir daí, uma vez que o usuário é reconhecido, cabe a cada serviço ou dono do produto (no caso os ministérios), definirem se o mesmo possui ou não acesso para tal.

Importante destacar ainda que tal gestão de identidade pode alcançar diferentes níveis de abordagem. Podemos ter, a partir dessa estrutura centralizada, usuários com processos de validação e credenciamento que foram mais criteriosos ou não, e isso determinar o nível de acesso a soluções. Novamente, vou trazer um contexto muito prático do nosso dia a dia, no mesmo regime de serviços do Governo Federal.

Atualmente, os serviços do Acesso.Gov, que atua com instância de login único, se utilizam de processos variados de reconhecimento de credenciais dos usuários para compor sua base. Nesse aspecto, há três formas básicas (espécie de categoria). Elas são bronze, prata e ouro. Tal definição reside basicamente do nível de confiabilidade que foi gerado no cadastramento e reconhecimento do usuário.

O nível bronze contempla usuários que cadastraram seu e-mail, responderam algumas perguntas básicas derivadas de uma inteligência de cruzamento de bases do Governo Federal, tendo gerado login e senha. Exemplo, no ato do cadastro, são perguntas de registro do último emprego, data de nascimento, nome da mãe, e outras informações que o Governo Federal possui para reconhecer um cidadão. Caso todas essas perguntas sejam respondidas durante o processo de validação, tem-se um cadastro nível bronze.

Percebam que há um modelo federado no fornecimento de informações e bases para a gestão de identidades. Seguindo esse raciocínio, tem-se ainda o nível prata, que basicamente utiliza o conceito de reconhecimento do usuário por meio da comprovação de documentos, sejam físicos

ou digitais. Assim, caso haja esse reconhecimento em alguma medida, o usuário terá sua credencial nível prata.

Por fim, o nível Ouro, que envolve reconhecimento biométrico. Basicamente, o principal provedor dessa informação atualmente é o Tribunal Superior Eleitoral, que disponibiliza sua base biométrica para todo o Governo Federal.

Dessa forma, a partir dessa base centralizada de gestão de acesso e credenciais, os demais serviços do Governo Federal podem realizar seus critérios para definição do nível desejado para determinado tipo de serviço. A sensibilidade fica por conta do órgão, ao considerar o tipo de transação que pode ser feita. A título de exemplo, caso seja um serviço de consulta a informações de cunho social ou ainda o status de alguma requisição, pode-se aceitar o nível bronze.

Agora, caso seja um serviço por exemplo, de declaração de Imposto de Renda, com alta sensibilidade e criticidade, exige-se o nível Ouro, e por aí vai. Ficou claro pessoal a lógica da gestão de identidades?

Nesse contexto, as definições e padrões são fundamentais nesse processo. E aí onde o SAML exerce um papel fundamental. Suas transações geralmente usam XML. Assim, por meio do SMAL, é possível prover serviços como SaaS, com um ambiente gerenciável e seguro, integrando e ativando recursos diversos de SSO, com logins únicos e sessões compartilhadas, a partir de sua reutilização.

O SAML trabalha transmitindo informações sobre usuários, logins e atributos entre o provedor de identidade e os provedores de serviços. Cada usuário efetua login uma única vez com o provedor de identificação e, em seguida, o provedor de identificação pode passar os atributos de SAML para o provedor de serviços, que solicita a autorização e a autenticação. Como ambos os sistemas falam a mesma linguagem – SAML -, o usuário só precisa efetuar login uma vez.

O SAML está na versão 2.0, e, em suas especificações, define basicamente 3 papéis:

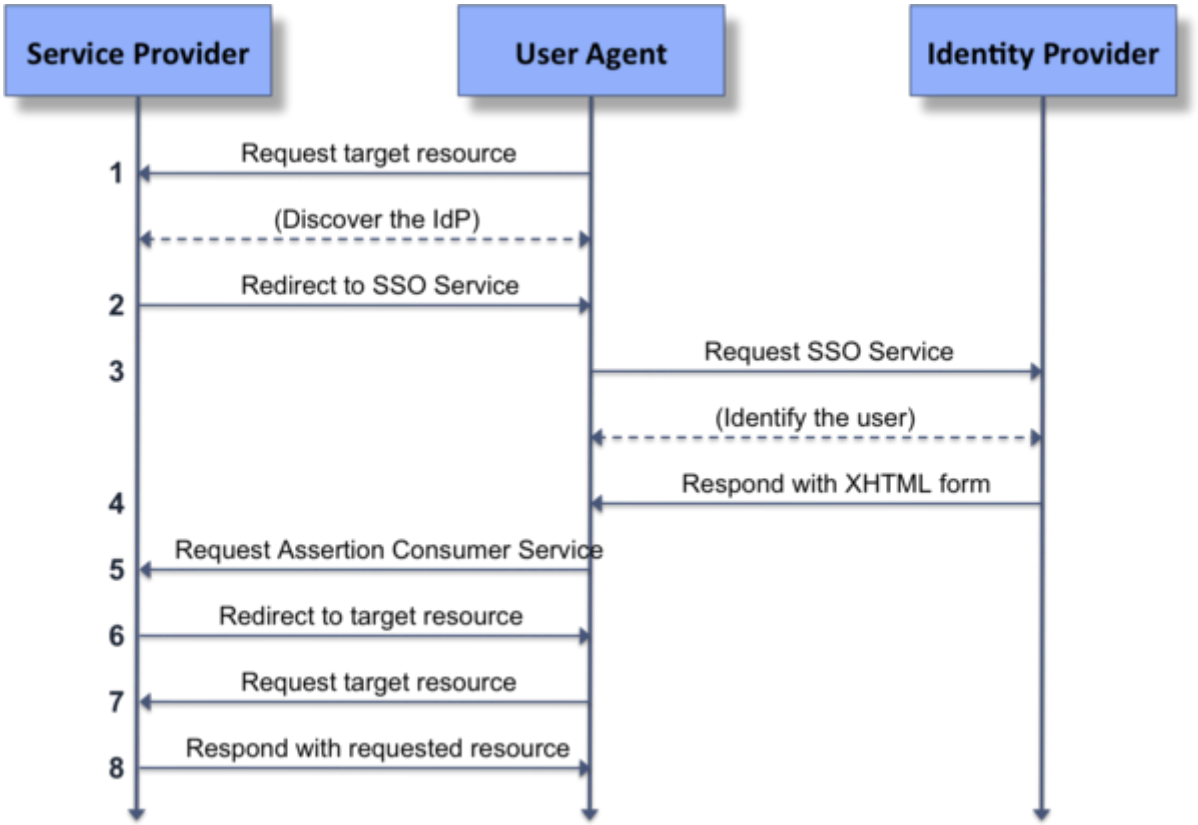
1. O principal (tipicamente um humano);
2. O Provedor de Identidades (Identity Provider - IDP)
3. O Provedor de Serviços (Service Provider - SP)

Em uma rotina básica de fluxo, tem-se que o Principal, portanto, acessa ou solicita os recursos ao Provedor de Serviços. Este então, precisa reconhecer o usuário a partir de sua autorização. Tal processo é feito com uma chamada do Provedor de Serviços ao Provedor de Identidades. Este último, solicita então ao Principal, que insira suas informações de Login e Senha, no mínimo, para ser reconhecido, e liberar acesso aos recursos.

Importante destacar que o SAML não especifica ou define um método específico de autenticação no âmbito do Provedor de Identidade. Pode usar o modelo de Login e Senha mencionado anteriormente, ou qualquer outro modo de autenticação, inclusive, incorporando as técnicas de

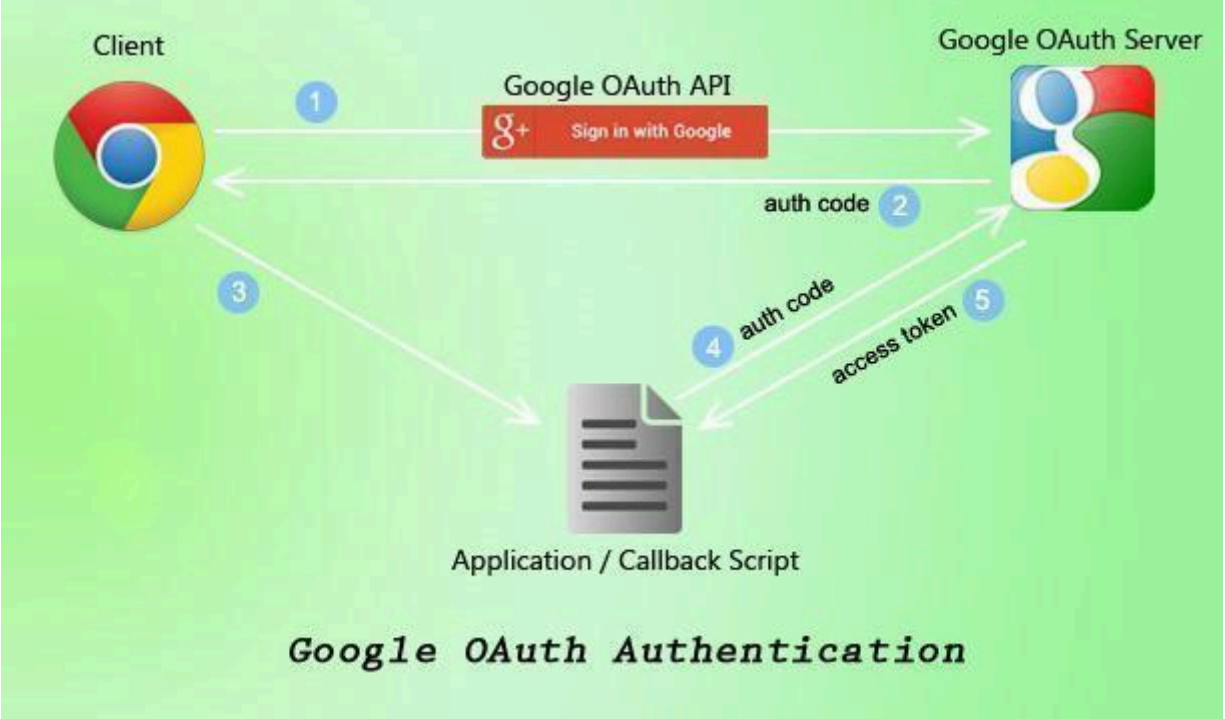
múltiplo fator de autenticação (MFA). Então, para cada serviço que se deseje utilizar, todo o processo do MFA deve ser realizado, ou, no mínimo, a confirmação da segunda camada de segurança. Ainda, a título de exemplo, pode-se utilizar serviços como RADIUS, LDAP ou ainda Active Directory da Microsoft. Nesse aspecto, já começamos a introduzir também a capacidade de autenticação por meio de serviços de terceiros, como Google, Facebook, Twitter, o qual detalharemos a seguir no padrão OAuth.

A imagem a seguir representa em fluxo, de forma simplificada, esse processo:



OAuth

Seguindo a nossa estrutura de gestão de identidade e credenciais, temos agora o Oauth. Tal padrão foi concebido no nicho privado, em conjunto pela Google e pelo Twitter, permitindo assim logins simplificados e integrados a múltiplos serviços na Internet. O processo por trás é muito semelhante ao SAML que mencionamos.



A figura acima ilustra um processo base de quando efetuamos logins por meio do OAuth da Google. Creio que muitos estão familiarizados com a imagem vermelha do centro, certo? Basicamente, estamos autorizando a aplicação ou serviço que estamos consumindo a realizar troca de informações com os servidores e provedores de credenciais da Google para reconhecimento da nossa identidade. A partir da chamada do serviço, no passo 2, a aplicação recebe o código de autenticação gerado pelo servidor Oauth do Google e por meio de processos em background e serviços próprios, realiza o processo de checagem para liberação de acesso com o recebimento de um token.

Nosso intuito não é entrar no detalhe de implementação do OAuth, por ser um aspecto de cobrança mais associado a itens de desenvolvimento ao considerar bibliotecas JWT e outros. Aqui, estamos focando nos conceitos das soluções e ferramentas, além de processos que garantem a gestão de identidade e credenciais.

O OAuth atualmente está em sua versão 2.0 e possui compatibilidade completa com sua versão 1.0. Nesse processo, são definidos 4 papéis básicos. São eles:

1. Resource Owner - Basicamente é a pessoa que concede acesso aos seus dados. Quando clicamos na opção de login integrado com o Google, por exemplo, teremos que incluir nosso login e senha do google, a partir da chamada de serviço. Caso você tenha uma sessão já aberta do serviço, essa etapa não será necessária. O ponto é, após a inclusão das informações de login

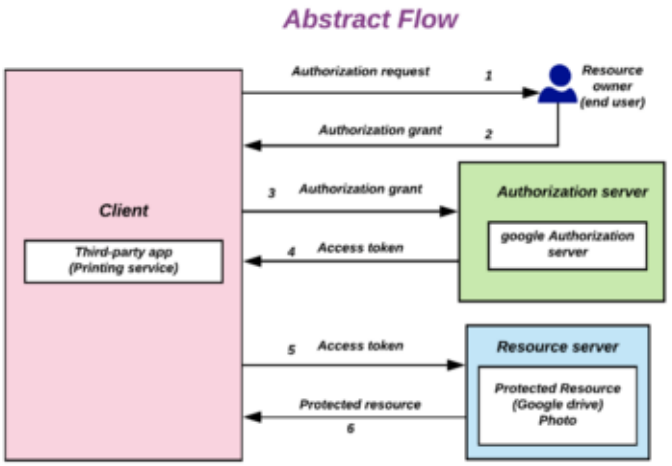
e senha, tem-se um processo de autorização, em que você autoriza a aplicação ou serviço, a obter suas informações do servidor OAuth. Na prática, temos aqui o DONO DO RECURSO.

2. Resource Server - Em resumo, é a camada de serviço/integração disponibilizada pelo provedor de identidades. Este serviço, com as devidas camadas de segurança, está exposto para a Internet, caso seja uma API Pública, a exemplo da Google, Twitter, Facebook, ou pode estar em um contexto mais restrito, como foi o caso do serviço do Acesso.Gov que mencionamos, que pode ser utilizado apenas por órgãos de Governo. O que importa é que, nesse processo, é necessário que o serviço que realiza chamada a essa API tenha um token emitido pelo servidor de autorização, que mencionaremos a seguir.

3. Authorization Server - Responsável por autenticação e emissão dos tokens de acesso (Access Token) para os Clients (aplicação requisitante). Estes recursos possuem informações dos Resource Owner (Usuários) e expõe no formato de Claims através do Bearer Token. Autentica e interage com o usuário após identificar e autorizar o client. Não vamos entrar em detalhes técnicos de implementação, mas registro apenas que o Bearer Token é referenciado em chamadas nos cabeçalhos HTTP e pode ser implementado de diferentes formas. No caso, tais chamadas são sempre realizadas por meio de HTTPS, uma vez que o token é passado de forma aberta no cabeçalho HTTP. Esse ponto é fundamental para garantir a segurança do Oauth2.0.

4. Client - É a aplicação que interage com o Resource Owner. No caso de uma App Web, seria a aplicação do Browser. Na prática, é a camada que oferece os serviços requisitados pelos usuários.

A imagem a seguir representa bem a execução desses papéis e respectivos fluxos, vejamos:



A partir do momento, portanto, que um usuário acessa um site e solicita o acesso ou tenta realizar o login, inicia-se o processo

ETAPA 1 - A aplicação (cliente) solicita autorização para o usuário, para que a aplicação possa interagir e solicitar informações de suas credenciais junto ao provedor de identidade.

ETAPA 2 - O Dono do Recurso (resource owner) realiza a autorização.

ETAPA 3 - De posse da autorização, esta é encaminhada pelo cliente ao Servidor de Autorização, responsável por viabilizar a passagem das credenciais de acesso aos serviços do provedor.

ETAPA 4 - O provedor de credenciais passa o TOKEN, por meio de uma comunicação segura. De posse desse token, a aplicação poderá acessar os recursos do usuário requisitante. Aqui é onde temos a referência ao nosso BEARER TOKEN, que também será utilizado na etapa 5. São as credenciais em si usadas para acessar os recursos protegidos.

ETAPA 5 - Passa-se o token aos provedores de serviços que detêm os recursos protegidos dos usuários. Na imagem em questão, temos exemplos de serviços da google como o Google Drive ou Google Photo, que passa a ser acessado pelo Client com a devida autorização do usuário Dono do Recurso, realizado no passo 2.

ETAPA 6 - As informações e recursos protegidos são compartilhados com o Cliente. É nessa etapa que é possível, por exemplo, já ter a sua foto integrada com o serviço web requisitado, outras informações, como e-mail, dados de telefone, recursos específicos no Drive, lista de amigos e contatos, entre muitos outros.

Ano: 2024 Banca: CESPE / CEBRASPE Órgão: TCDF

Os tokens de acesso devem ser lidos e interpretados pelo cliente OAuth, que é o público-alvo do token.

Comentários:

Há uma série de propriedades de tokens de acesso que são fundamentais para o modelo de segurança do OAuth. Os tokens de acesso não devem ser lidos ou interpretados pelo cliente OAuth. O cliente OAuth não é o público-alvo do token.

Gabarito: E

Algumas bancas começam a trazer uma visão mais técnica para o conteúdo do OAUTH, exigindo do candidato um conhecimentos mais aprofundados de parâmetros, bibliotecas e itens de configuração, de uma forma geral. Esse mesmo assunto também é abordado pela nossa equipe de professores de desenvolvimento.

Entretanto, vou trazer alguns pontos relevantes aqui nesse contexto para garantir a visibilidade de vocês desses temas.

1. Tipos de Clientes:

No OAuth 2.0, existem dois tipos de clientes: confidenciais e públicos. Vamos entender as diferenças:

a) Clientes Confidenciais:

Estes tipos de clientes são registrados com um segredo do cliente. Com isso, podem manter a confidencialidade de suas credenciais.

Como exemplos, podemos citar as integrações entre serviços da organização ou aplicativos que consomem APIs internas. Esses clientes podem armazenar e proteger suas credenciais de acesso.

b) Clientes Públicos:

Em uma outra perspectiva, estes não conseguem manter a confidencialidade de suas credenciais. Por isso, são usados em cenários como aplicativos móveis ou baseados em navegador, justamente por não possuírem um segredo do cliente.

Assim, como requisito, temos que as credenciais do cliente não precisam ser mantidas em sigilo.

2. TIPOS DE TOKENS

a) Bearer Tokens:

São usados para acessar recursos protegidos em nome de um usuário. Neste contexto, o portador apresenta um token válido para obter acesso. Tem como vulnerabilidade ou ponto de atenção o fato de não haver verificação da legitimidade do remetente. Logo, pode ser vulnerável se cair em mãos não autorizadas.

b) Sender-Constrained Tokens (Mutual TLS):

Garantem que o remetente seja legítimo. Para tanto, são vinculados à conexão TLS mútua entre cliente e servidor de autorização. O servidor de recursos verifica o certificado do cliente, o que, na prática, traz uma burocracia para o processo justamente pela necessidade da Infraestrutura de chaves públicas e certificados do cliente.

O token inclui o hash do certificado (por exemplo, no JWT). O remetente deve provar que possui a chave privada do certificado vinculado.

c) ID Tokens:

Fornecem informações sobre o usuário autenticado. Como o próprio nome já diz, o ID, vem justamente de Identificação, sendo essas informações emitidas pelo provedor de identidade.

Contêm detalhes como ID do usuário e escopo. Justamente por tratar somente da camada de identificação e não de autenticação/autorização, propriamente ditos, acabam por não serem usados para acessar recursos protegidos.

d) Refresh Tokens:

Permitem obter novos *access tokens* sem novo login. São mais duradouros que os access tokens e geralmente são usados para renovar tokens expirados. Falaremos mais dele no tópico a seguir.

3. REFRESH TOKEN

Um Refresh Token é uma sequência (string) que o cliente OAuth pode usar para obter um novo access token sem a interação do usuário, tendo como premissa a autorização inicial que ele obteve na primeira requisição ao usuário.

Tanto clientes públicos quanto confidenciais podem usar refresh tokens. Se um refresh token emitido para um cliente público for roubado, o atacante pode se passar pelo cliente e usar o refresh token sem ser detectado.

Quando inicialmente se recebe o access token, ele pode incluir um refresh token e um tempo de expiração. Vejam que é um item opcional e configurável.

Com isso, é possível atualizar o conteúdo ou o recurso sem nova solicitação ou interação com o Dono do Recurso, sendo processado tudo em background dos sistemas envolvidos.

O valor "expires_in" indica quantos segundos o access token será válido.

É possível usar esse timestamp para atualizar os access tokens antes que eles expirem, evitando falhas em chamadas de API.

Para fins práticos, caso queira utilizar o refresh token, basta fazer uma solicitação POST para o endpoint de token com *grant_type=refresh_token*, incluindo o refresh token e as credenciais do cliente, se necessário:

POST /oauth/token HTTP/1.1

Host: authorization-server.com

grant_type=refresh_token

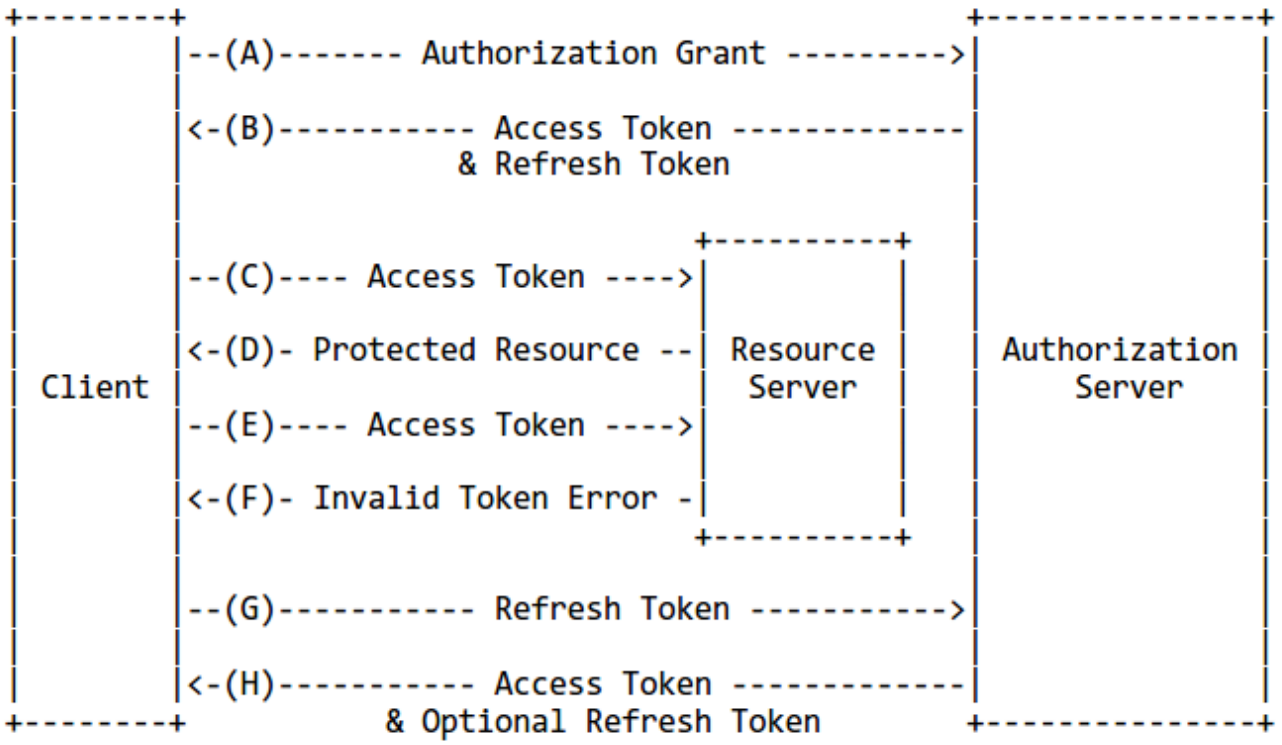
&refresh_token=xxxxxxxxxx

&client_id=xxxxxxxxxx

&client_secret=xxxxxxxxxx

A resposta incluirá um novo access token e, opcionalmente, um novo refresh token.

A imagem abaixo nos traz essa dinâmica em diagrama de fluxos de mensagens, extraído diretamente da documentação oficial do OAUTH. Reparem que, após o acesso ao recurso protegido, na etapa D, uma nova tentativa de uso do Token anterior é feita em E, porém, o token não é mais válido em F. Com isso, pode-se utilizar o Refresh Token em G para a geração de um novo TOKEN em H sem a interação com o usuário, bastante a interação com o Authorization Server.



Ano: 2024 Banca: CESPE / CEBRASPE Órgão: TCDF

Os tokens Sender-constrained exigem que, para usar o token de acesso, o cliente OAuth prove, de alguma forma, a posse de uma chave privada, de modo que o token de acesso por si só não seja utilizável.

Comentários:

Exatamente a camada adicional de segurança que comentamos em nossa teoria, que incorpora a infraestrutura de chaves públicas e certificados digitais, com a posse da chave privada..

Gabarito: C

Um ponto importante que tem aparecido em prova dentro deste tópico são as abordagens de boas práticas de configuração e perspectivas de segurança. Dessa forma, vamos trabalhar ainda alguns conceitos:

Boas Práticas de Segurança para JWT

1. Use Algoritmos Seguros:
    - Prefira algoritmos como HS256 ou RS256 para assinar seus tokens.
2. Mantenha as Chaves Secretas Seguras:
    - Armazene as chaves secretas em locais seguros e nunca as exponha no código-fonte.
3. Defina um Tempo de Expiração Curto:
    - Configure um tempo de expiração curto para os tokens (exp claim) para minimizar o impacto de um token comprometido.
4. Revogação de Tokens:
    - Implemente um mecanismo para revogar tokens, como uma lista de tokens revogados.
5. Validação de Tokens:
    - Sempre valide o token no servidor, verificando a assinatura e as claims.
6. Use HTTPS:
    - Transmita tokens apenas por conexões seguras (HTTPS) para evitar ataques de interceptação.
7. Minimize as Claims:
    - Inclua apenas as informações necessárias nas claims do token para reduzir o risco de exposição de dados sensíveis.
8. Verificação de Origem:
    - Verifique a origem do token (iss claim) para garantir que ele foi emitido por uma fonte confiável.

Boas Práticas de Configuração para JWT

1. Configuração de Claims:
    - Defina claims padrão como iss (issuer), sub (subject), aud (audience) e exp (expiration).
2. Uso de Bibliotecas Confiáveis:
    - Utilize bibliotecas bem mantidas e confiáveis para a geração e validação de JWTs.
3. Rotação de Chaves:
    - Implemente a rotação periódica de chaves para aumentar a segurança.
4. Escopo e Permissões:
    - Defina escopos e permissões claras dentro do token para controlar o acesso aos recursos.

5. Monitoramento e Logs:
    - Monitore e registre o uso de tokens para detectar e responder a atividades suspeitas.
6. Política de Renovação de Tokens:
    - Estabeleça uma política clara para a renovação de tokens, garantindo que os usuários obtenham novos tokens antes que os antigos expirem.

Manipulação de Tokens Sem Estado de Curta Duração

1. Tokens de Curta Duração:
    - Utilize tokens de curta duração para minimizar o impacto de um token comprometido. Tokens de curta duração são ideais para aplicações sem estado, onde o servidor não mantém informações sobre o estado do cliente entre as requisições.
2. Renovação de Tokens:
    - Implemente um mecanismo de renovação de tokens, onde um token de curta duração pode ser trocado por um novo token antes de expirar. Isso pode ser feito através de um endpoint de renovação seguro.
3. Tokens de Atualização (Refresh Tokens):
    - Utilize tokens de atualização para emitir novos tokens de curta duração. Os tokens de atualização devem ser armazenados de forma segura e transmitidos apenas por conexões seguras.
4. Verificação de Expiração:
    - Sempre verifique a expiração (exp claim) dos tokens de curta duração no servidor para garantir que apenas tokens válidos sejam aceitos.
5. Desempenho e Escalabilidade:
    - Tokens sem estado de curta duração são leves e não requerem armazenamento no servidor, o que melhora o desempenho e a escalabilidade da aplicação.

Biometria

Algumas questões tratam os aspectos de BIOMETRIA de uma maneira mais detalhada. Por esse motivo, reservamos essa seção para isso

Para balizarmos o nosso princípio, ao analisarmos a etimologia da palavra temos: BIO (VIDA) + METRIA (MEDIDA). Podemos traduzir isso também como a forma de identificar de maneira única um indivíduo por meio de suas características físicas ou comportamentais.

Trazendo um pouco mais de história em nosso estudo, é importante citar a importância de FRANCIS DALTON, considerado um dos fundadores do processo de biometria. Seu estudo era baseado na identificação de características e traços genéticos. Em 1982, GALTON inventou o primeiro sistema moderno de IMPRESSÕES DIGITAIS, e que fora amplamente utilizado nos departamentos de polícia.

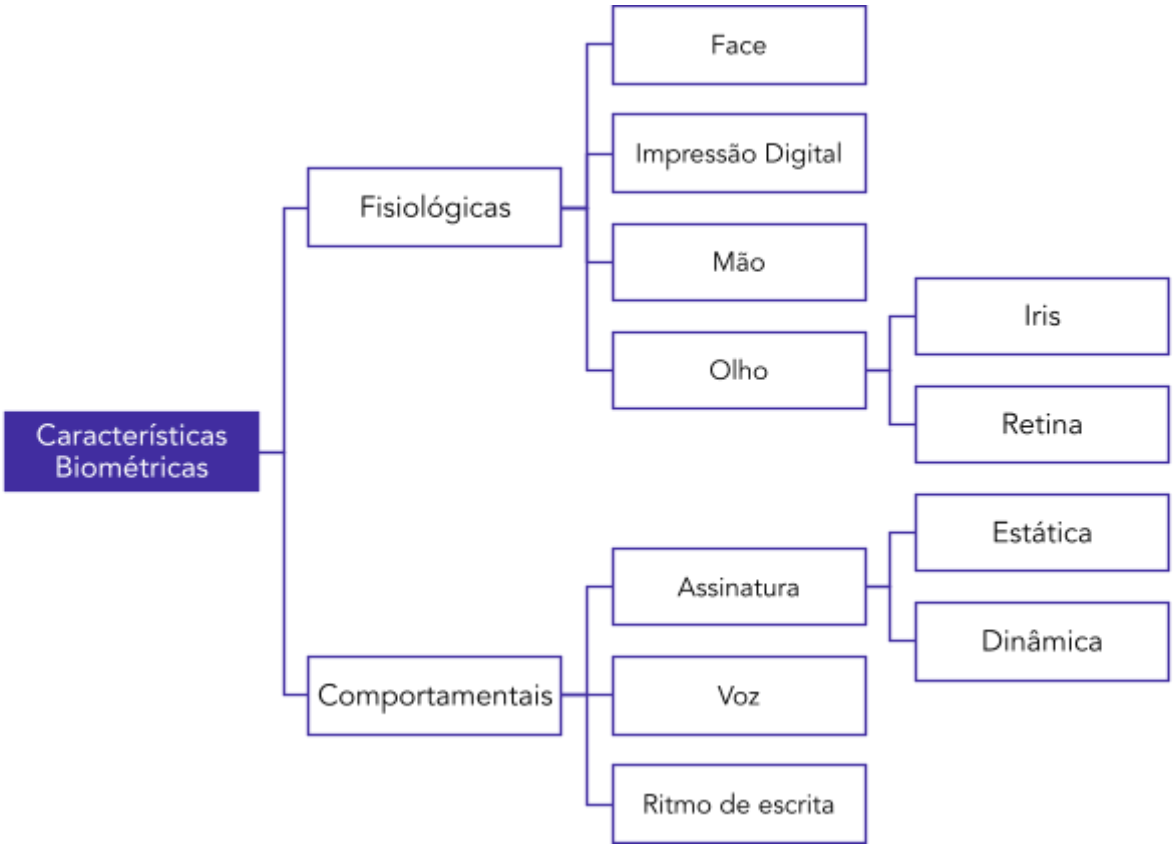
Como vimos anteriormente, o processo de biometria está atrelado à fase de autenticação e autorização, principalmente, para fins de controle de acesso.

Desse modo, quando falamos de ALGO QUE VOCÊ É, podemos utilizar alguns recursos para tal finalidade, como por exemplo:

1. Impressão Digital
2. Palma da mão
3. Imagem da Face
4. Retina ou íris dos olhos (a retina analisa o fundo do olho, enquanto a retina analisa os anéis coloridos do olho, sendo este mais rápido que aquele)
5. Reconhecimento de voz

Desse modo, os filmes futuristas, bem como aqueles que retratam assaltos a cofres muito seguros, necessariamente passam pelo processo de biometria.

A imagem abaixo nos traz uma visão agregada das principais técnicas de biometria:



Fonte: http://www.sinfic.pt

Nesse sentido, a biométrica zela pelos princípios de unicidade abaixo:

1. Universalidade – Significa que todas as pessoas devem possuir a característica;
2. Singularidade – Indica que esta característica não pode ser igual em pessoas diferentes;
3. Permanência – Significa que a característica não deve variar com o tempo;
4. Mensurabilidade – Indica que a característica pode ser medida quantitativamente;

Analisando a estrutura de um sistema biométrico, podemos elencar ainda as etapas desses sistemas:

1. Captura – Aquisição da amostra biométrica;
2. Extração – Remoção da amostra com informações únicas para posterior análise;
3. Comparação – Comparação com as informações armazenadas em uma base de dados. Caso a comparação seja positiva, tem-se um "match", dando o resultado como positivo.

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

O uso de senhas ou a adoção de identificação física, como biometrias, são formas de autenticação para fins de identificação única e exclusiva de usuários.

Comentários:

Pessoal, a questão retrata, de fato, as finalidades de senhas associadas a biometrias. A exclusividade, como vimos é um princípio da biometria. No trecho, vimos o termo SINGULARIDADE.

Gabarito: C

Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Uma das condições para a autenticação é que o sinal biométrico apresenta correspondência exata entre o sinal biométrico recebido pelo sistema e o gabarito armazenado.

Comentários:

Pessoal, vimos que existem os modelos comportamentais, certo? Esses modelos, também são sinais biométricos e trabalham com referências variáveis, mas dentro de um padrão aceitável, com taxa de similaridade e equivalência alto. Agora, dizer que o gabarito tem que ser exato, não é uma verdade para sua generalização.

Gabarito: E

CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

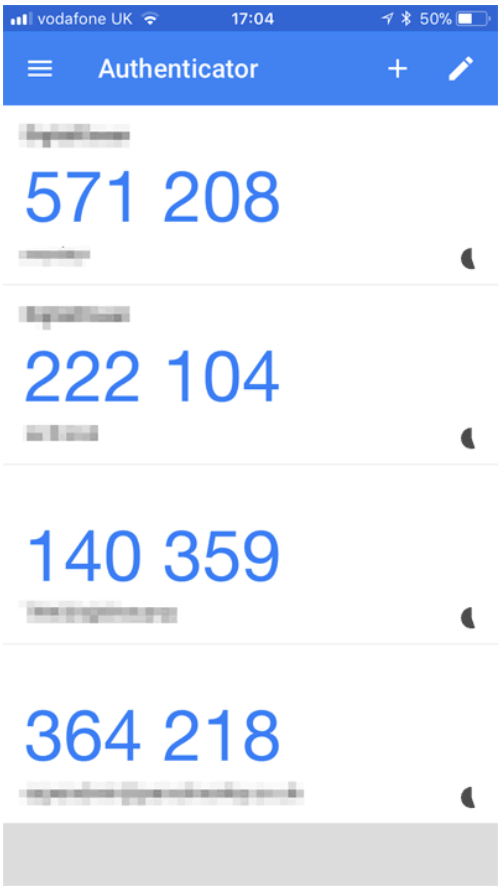
Comentários:

Conforme vimos, de fato, estes são os três principais métodos.

Gabarito: C

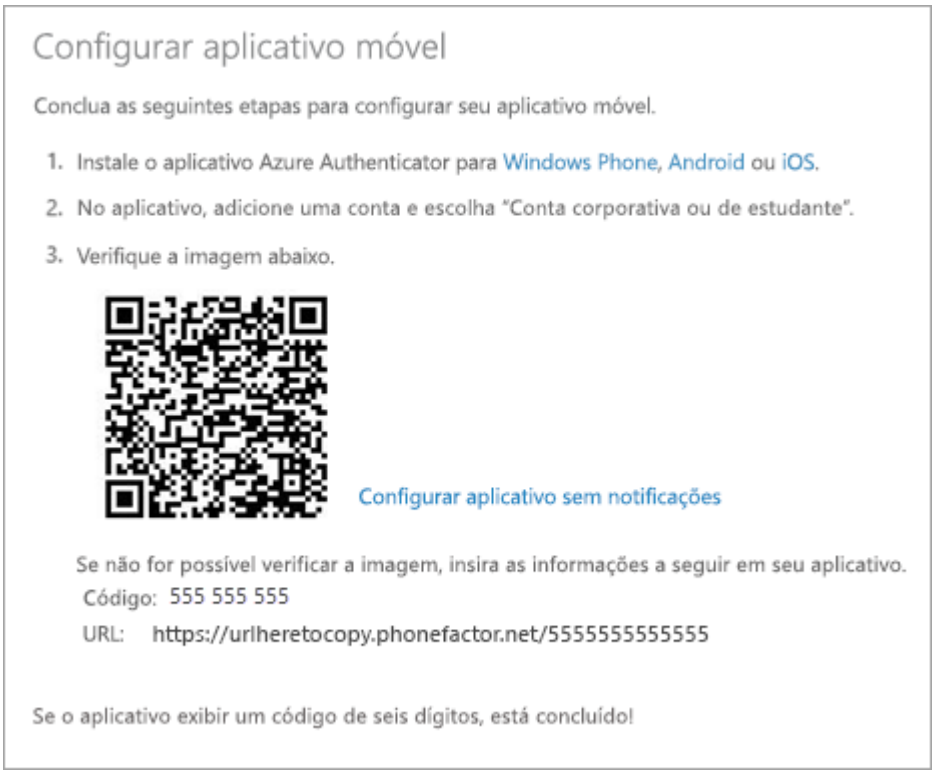
Um outro mecanismo interessante que surge é por meio de autenticadores em dispositivos móveis. Por vezes, também conhecidos como tokens de segurança ou chaves de sessão, podem ser efetivados por meio de aplicativos próprios que permitem a vinculação a determinados serviços e seus usuários.

Antes de explicarmos seu funcionamento, vamos citar alguns deles:


vodafone UK
17:04
50%
Authenticator
571 208
222 104
140 359
364 218


12:30
AWS
amazon
web services
AWS TOKEN IS:
7294528
AWS
john@gmail.com
Gmail
johnro...@gmail.com
Dropbox
jonathan.robertso...
Evernote
Digital Ocean
johnrob...@gmail.com
Facebook
jonatha...@gmail.com
Github
johndoe@gmail.com
Coinbase
Gmail
johnro...domine.com


Microsoft
Authenticator



Apresentei uma lista de três aplicativos distintos. O fluxo base de configuração é o mesmo. O site específico do serviço gerará um QRCODE para que seja lido pelo aplicativo. Neste momento, haverá a vinculação da conta e site, junto ao aplicativo. A partir deste instante, todo acesso dependerá de algum nível de aprovação no aplicativo como segundo fator de autenticação, ou ainda, será necessária a extração de uma informação dos códigos de cada aplicativo gerado no aplicativo. Esses códigos são dinâmicos e de tempos em tempos, geralmente 30 segundos, são alterados.

OPENID Connect - OIDC

Aqui temos um conceito associado à criação da camada que atua sobre as soluções de gestão de identidade (OAUTH).

Ela permite aos clientes/aplicações a verificação da identidade do usuário final integrado aos recursos do Servidor de Autorização.

O OpenID Connect (OIDC) é um protocolo de autenticação que permite que usuários se autentiquem em um serviço usando suas credenciais de um provedor de identidade (IDP). O OIDC é um protocolo leve e flexível que pode ser integrado a uma ampla gama de serviços.

As principais características do OIDC são:

- Autenticação baseada em tokens: O OIDC usa tokens para autenticar usuários. Esses tokens são emitidos pelo IDP e são usados pelo serviço para verificar a identidade do usuário.
- Autorização baseada em declarações: O OIDC usa declarações para autorizar usuários a acessar recursos. Essas declarações são emitidas pelo IDP e são usadas pelo serviço para determinar quais recursos o usuário pode acessar.
- Descentralização: O OIDC é um protocolo descentralizado. Isso significa que não há um único ponto de falha ou controle.

Ainda, o OIDC oferece uma série de vantagens em relação a outras tecnologias de autenticação, incluindo:

- Simplicidade: O OIDC é um protocolo simples e fácil de implementar.
- Flexibilidade: O OIDC pode ser integrado a uma ampla gama de serviços.
- Segurança: O OIDC usa criptografia para proteger os dados do usuário.
- Interoperabilidade: O OIDC é um protocolo interoperável que pode ser usado com uma ampla gama de IDPs. Opera por meio de API/RESTFULL e tem como característica o fato de ser Multiplataforma.

KeyCloak

Na mesma linha, temos aqui uma ferramenta muito importante e de código aberto (opensource) de Gerenciamento de Acesso e Identidade.

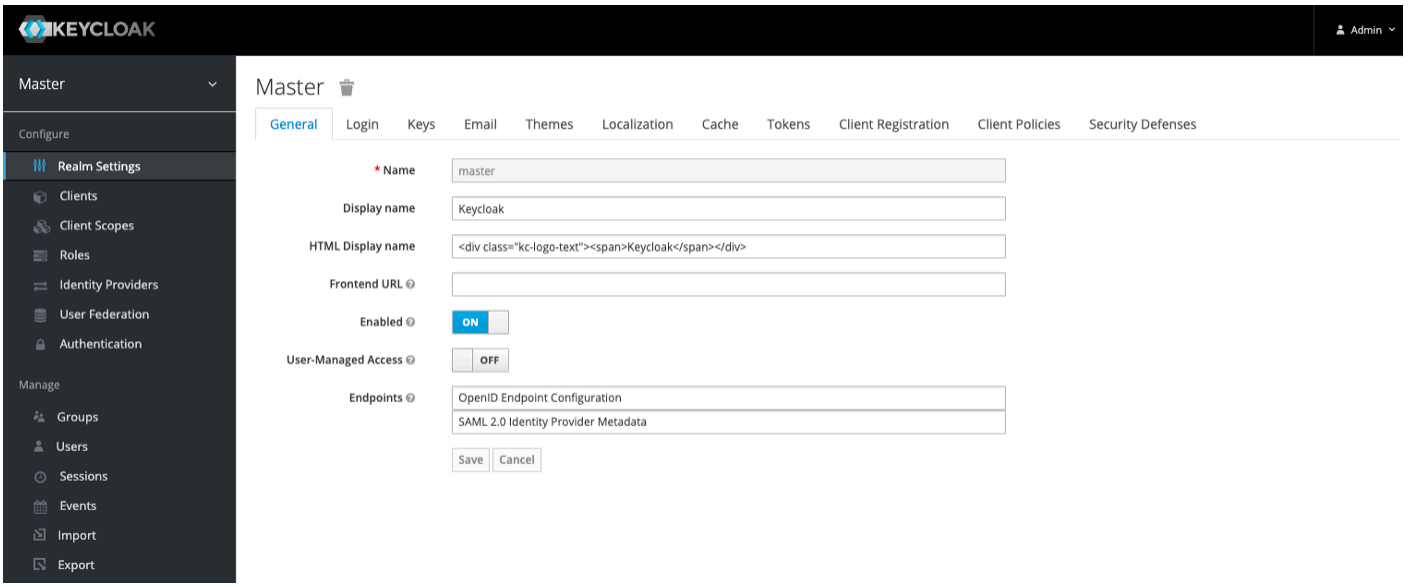
Sendo muito fácil de configurar e implantar a gestão de identidade, o KeyCloak vem sendo usado cada vez mais pelas instituições.

A ferramenta, assim como o OPENID Connect é baseada em API-Restfull, tendo as seguintes características:

- Fornece telas de login personalizáveis
- Recursos de Recuperação de Senhas
- Termos de uso
- Ausência de necessidade de codificação

- Recurso de MFA
- Isolamento da aplicação com a camada de autenticação
- Visualização dos tokens do KeyCloak
- Recursos de SSO
- Utiliza OAUTH2.0 + OpenID
- Possui banco de dados próprio
- Pode integrar com AD ou LDAP

A seguir, temos uma tela exemplo da ferramenta e seu painel de gerenciamento e configuração:



FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

Marcia decidiu padronizar o mecanismo de autenticação de suas APIs RESTful e armazenar com segurança as credenciais de usuários e suas respectivas permissões. Para isso, ela deseja utilizar uma ferramenta de código aberto.

A ferramenta que tem por principal finalidade o gerenciamento de identidade e acesso que Márcia deve escolher é

A JBoss.

B Keycloak.

C Kibana.

D RabbitMQ.

E Wildfly.

Comentários:

Temos aí pessoal uma questão que traz a forma de abordagem da solução KeyCloak. Apenas para validarmos as outras tecnologias/ferramentas:

JBoss - Um servidor de aplicação Java EE de código aberto, desenvolvido pela Red Hat. Oferece uma plataforma para construir, implementar e executar aplicações empresariais. Suporte a diversas tecnologias, como EJB, CDI, JPA e JSF.

Kibana: Uma ferramenta de visualização de dados e interface de usuário do Elastic Stack. Permite explorar, analisar e visualizar dados armazenados no Elasticsearch. Utilizada para monitoramento, análise de logs e business intelligence.

RabbitMQ: Um message broker de código aberto que implementa o protocolo Advanced Message Queuing Protocol (AMQP). Facilita a comunicação entre aplicações através de mensagens assíncronas. Oferece alta disponibilidade e escalabilidade.

Wildfly: Anteriormente conhecido como JBoss AS, é um servidor de aplicação Java EE de código aberto. Desenvolvido pela Red Hat, permite a criação e implantação de aplicações empresariais. Suporta diversas tecnologias, como EJB, CDI, JPA e JSF.

Gabarito: B

Questões Comentadas - Autenticação e seus Mecanismos - CESPE

1. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

Em situações de gerenciamento de acesso de usuários a sistemas críticos, o uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado é restrito aos administradores do sistema.

Comentários:

O uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado não se restringe apenas aos administradores do sistema, mas pode ser estendido a outros usuários que acessam sistemas críticos, dependendo da política de segurança da organização.

Gabarito: E

---

2. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

No Single Sign-On, a funcionalidade em que as informações de login e senha permitem um melhor controle da equipe de TI é

a) a autenticação multifator.

b) o gerenciamento interno de credenciais.

c) a velocidade na recuperação de senhas.

d) o ponto único para reinserir senha.

e) a melhor aplicação da política de senha.

Comentários:

No Single Sign-On, o gerenciamento interno de credenciais é a funcionalidade que permite um melhor controle da equipe de TI, pois centraliza o gerenciamento das credenciais dos usuários, facilitando o controle de acesso e a revogação de permissões. Vejam que a questão não restringe qualquer aspecto de função ou privilégio.

Gabarito: B

---

3. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

No controle de acesso, somente os usuários que tenham sido especificamente autorizados podem usar e receber acesso às redes e aos seus serviços.

Comentários:

Exatamente pessoal. É importante sempre lembrar essa diferença básica da autenticação e autorização.

Gabarito: C

---

4. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-CE

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Comentários:

Exatamente pessoal. Típica questão conceito. Veremos mais à frente algumas questões mais práticas sobre o funcionamento desses aplicativos? Mas tenho certeza que muitos de vocês já usaram, como o Google Authenticator, por exemplo, ou algum serviço semelhante, onde são geradas senhas para cada usuário. Agora é importante destacar que aqui nós temos o modelo de algo que você sabe, com algo que você possui.

Gabarito: C

---

5. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Para acessar a intranet corporativa, um colaborador informa seu CPF, senha pessoal e um código enviado para o seu celular cadastrado.

O mecanismo de reforço implementado nessa intranet para confirmar a identidade do usuário contra acessos indevidos é a autenticação:

A) biométrica;

B) Kerberos;

C) Oauth2;

D) 2FA;

E) Openid.

Comentários:

Conforme nós vimos, há a necessidade de conhecimento de algo que VOCÊ SABE (CPF + senha), com ALGO QUE VOCÊ POSSUI (celular). Logo, temos aí o 2FA.

Gabarito: D

---

6. Ano: 2020 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

Comentários:

A dinâmica é sempre essa pessoal. A autenticação é o ato final de reconhecimento do usuário ou sistema. Fato é que, para autenticar, devemos identificar. E esse processo pode acontecer de diferentes formas. Ainda, após o processo de identificação e autenticação, temos a autorização, recebendo esses dois pré-requisitos.

Gabarito: C

---

7. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

O uso de senhas ou a adoção de identificação física, como biometrias, são formas de autenticação para fins de identificação única e exclusiva de usuários.

Comentários:

Pessoal, a questão retrata, de fato, as finalidades de senhas associadas a biometrias. A exclusividade, como vimos, é um princípio da biometria. No trecho, vimos o termo SINGULARIDADE.

Gabarito: C

---

8. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Uma das condições para a autenticação é que o sinal biométrico apresente correspondência exata entre o sinal biométrico recebido pelo sistema e o gabarito armazenado.

Comentários:

Pessoal, vimos que existem os modelos comportamentais, certo? Esses modelos, também são sinais biométricos e trabalham com referências variáveis, mas dentro de um padrão aceitável, com taxa de similaridade e equivalência alto. Agora, dizer que o gabarito tem que ser exato, não é uma verdade para sua generalização.

Gabarito: E

9. CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

Comentários:

Conforme vimos, de fato, estes são os três principais métodos.

Gabarito: C

---

10. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

Comentários:

Lembremos que autenticação biométrica está baseada no mecanismo de "algo que você é". Como sabemos, esse é um procedimento de segurança da informação.

Gabarito: C

---

11. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

Comentários:

Vimos que os três principais tipos de autenticação e também de controle de acesso estão amparados em: algo que você sabe (necessidade de saber), algo que você tem (necessidade de ter) e algo que você é (necessidade de ser).

Gabarito: E

---

12. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

Comentários:

Conforme vimos, de fato, estes são os três principais métodos.

Gabarito: C

---

13. (CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014)

O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

Comentários:

Duas observações nessa questão. Primeiro, que o controle de acesso se aplica a pessoas de uma organização. E segundo, que se deve considerar também, além da autenticidade, a autorização.

Gabarito: C

Questões Comentadas - Autenticação e seus Mecanismos - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

Considere as seguintes medidas de segurança:

I. Centralizar o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.

II. Usar Single-Factor Authentication (SFA) para todas as contas de acesso administrativo, em todos os ativos corporativos, sejam estes gerenciados no site local ou por meio de um provedor terceirizado, pois esta é a medida de acesso seguro mais usada atualmente nas organizações.

III. Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

IV. Estabelecer e seguir um processo, de preferência manual, para manter o acesso aos ativos corporativos, por meio da ativação de contas antigas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

São medidas recomendadas e adequadas para a gestão do controle de acesso o que se afirma APENAS em

a) I e III.

b) II e IV.

c) I.

d) III e IV.

e) II.

Comentários:

Vamos aos itens:

I - Correto. Conforme vimos, o SSO é, sem dúvida, uma boa prática a ser implantada.

II - Incorreto. A recomendação é o MFA e não o SFA.

III - Correto. Estamos falando do RBAC. Lembrando que atualmente já temos o ABAC que é ainda mais recomendado.

IV- Incorreto. Processo manual? Forçando a barra. Ainda, deve-se desativar as contas antigas, e não ativar.

Gabarito: A

---

2. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Um serviço da web RESTful autentica solicitações antes de enviar uma resposta, usando métodos de autenticação. O método que combina senhas e tokens para acesso de login seguro, no qual primeiro o servidor solicita uma senha e, depois, um token adicional para concluir o processo de autorização, é o

a) API Key Security.

b) RSA Authentication.

c) Webhook.

d) Swagger SSO.

e) OAuth.

Comentários:

Vimos que o processo de troca de tokens (Bearer Token), é característico do OAUTH, correto? Apenas para validarmos os demais:

a) A autenticação por chave de API é um método que utiliza uma chave única (token) para autenticar um usuário ou aplicativo. No entanto, ela não combina senhas e tokens para acesso de login seguro. A chave de API é geralmente usada para identificar o aplicativo que faz a chamada da API, mas não é considerada segura para autenticação de usuários.

b) A autenticação RSA é um método de autenticação que utiliza criptografia de chave pública para autenticar usuários. Ela não combina senhas e tokens para acesso de login seguro. Em vez disso, usa um par de chaves pública e privada para autenticação.

c)Webhook é uma função de callback baseada em HTTP que viabiliza a comunicação entre duas interfaces de programação de aplicações (APIs). Ele não é um método de autenticação, mas sim um meio de enviar dados em tempo eal entre dois sistemas ou aplicativos distintos.

d) Swagger SSO (Single Sign-On) é um recurso do SwaggerHub On-Premise que suporta autenticação de usuários via Okta (SAML 2.0), Active Directory, OpenLDAP e GitHub. No entanto, ele não combina senhas e tokens para acesso de login seguro. Em vez disso, ele permite que os usuários façam login usando suas contas existentes nesses provedores de identidade.

Gabarito: E

---

3. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

Um Analista está utilizando o protocolo OAuth2 (RFC 6749) e, após realizar todos os passos para obtenção e geração de um access token em condições ideais, recebeu o seguinte retorno:

{

"access_token": "57f10f0e-3d2e-311f-a797-4011f66e1cbf",

" I ": "ca81cb16-43e4-3e96-aaea-4861e7791dc7",

"token_type": "access_token",

"expires_in": 3600

}

Considerando que a lacuna I se refere ao campo que poderá ser utilizado para atualizar um access token que tenha expirado, esta é corretamente denominada:

a) refresh_token

b) redirect_uri

c) extraInfo

d) expired_token

e) redirect_token

Comentários:

Vejam que a estrutura da questão assusta, pode imaginarmos que temos que saber codificar. Mas aqui o nosso conhecimento dos conceitos da base teórica são suficientes. Vimos que na Etapa 4 do fluxo do OAUTH, há o envio do TOKEN e do REFRESH TOKEN, este último sendo útil para geração de um novo TOKEN caso o primeiro expire.

Além disso, os demais parâmetros basicamente indicam o tipo de TOKEN e o prazo de validade. Em relação aos tipos de token temos:

Bearer: Este é o tipo de token mais comum. Qualquer parte que possua o token (um "portador") pode usar o token da mesma maneira que qualquer outra parte que o possua. Usar um token do tipo "Bearer" não requer que o portador prove a posse de material criptográfico (prova de posse).

MAC: Se você escolher o tipo MAC e sign_type (padrão hmac-sha-1 na maioria das implementações), o token de acesso é gerado e mantido como segredo no gerenciador de chaves como um atributo, e um segredo criptografado é enviado de volta como access_token.

Em relação aos outros itens:

b) redirect_uri: Este é o URI para o qual o cliente é redirecionado após a conclusão da autorização. Não é usado para atualizar um access_token.

c) extraInfo: Este não é um campo padrão no OAuth2. Pode ser usado para informações adicionais, mas não para atualizar um access_token.

d) expired_token: Este não é um campo padrão no OAuth2. O access_token expirado é inútil e não pode ser usado para obter um novo access_token.

e) redirect_token: Este não é um campo padrão no OAuth2. O redirect_uri do item B é usado no fluxo de autorização, mas não há redirect_token no OAuth2.

Gabarito: A

4. (FCC – TRF – 4ª Região/Técnico Judiciário/2014) Os sistemas de identificação biométricos funcionam através da comparação de características físicas apresentadas por um usuário com as correspondentes armazenadas em um determinado banco de dados, identificando-o ou não como um dos usuários cadastrados, dificultando sobremaneira as fraudes praticadas contra as várias formas de verificação de identidades. O sistema de identificação biométrica que utiliza a parte do fundo do olho como identificador é conhecido como identificação

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

Comentários:

Como vimos em nossa teoria:

1. Retina – Analisa os vasos sanguíneos do fundo do olho;
2. Íris – Analise os anéis coloridos do olho;

Gabarito: C

Questões Comentadas - Autenticação e seus Mecanismos - FGV

1. FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

Marcia decidiu padronizar o mecanismo de autenticação de suas APIs RESTful e armazenar com segurança as credenciais de usuários e suas respectivas permissões. Para isso, ela deseja utilizar uma ferramenta de código aberto.

A ferramenta que tem por principal finalidade o gerenciamento de identidade e acesso que Márcia deve escolher é

A JBoss.

B Keycloak.

C Kibana.

D RabbitMQ.

E Wildfly.

Comentários:

Temos aí pessoal uma questão que traz a forma de abordagem da solução KeyCloak. Apenas para validarmos as outras tecnologias/ferramentas:

JBoss - Um servidor de aplicação Java EE de código aberto, desenvolvido pela Red Hat. Oferece uma plataforma para construir, implementar e executar aplicações empresariais. Suporte a diversas tecnologias, como EJB, CDI, JPA e JSF.

Kibana: Uma ferramenta de visualização de dados e interface de usuário do Elastic Stack. Permite explorar, analisar e visualizar dados armazenados no Elasticsearch. Utilizada para monitoramento, análise de logs e business intelligence.

RabbitMQ: Um message broker de código aberto que implementa o protocolo Advanced Message Queuing Protocol (AMQP). Facilita a comunicação entre aplicações através de mensagens assíncronas. Oferece alta disponibilidade e escalabilidade.

Wildfly: Anteriormente conhecido como JBoss AS, é um servidor de aplicação Java EE de código aberto. Desenvolvido pela Red Hat, permite a criação e implantação de aplicações empresariais. Suporta diversas tecnologias, como EJB, CDI, JPA e JSF.

Gabarito: B

2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Segurança da Informação

Um pequeno dispositivo que contém um código de proteção precisa necessariamente ficar conectado à porta USB do computador para que determinado software possa ser utilizado.

Esse dispositivo utilizado para prevenir o uso não autorizado de determinado software é conhecido como:

A Vault;

B Keycloak;

C KeePass;

D Keylogger;

E Hardlock.

Comentário:

Um dongle (HARDLOCK) de proteção de software é um dispositivo de proteção eletrônica contra cópia e proteção de conteúdo. Quando conectados a um computador ou outros eletrônicos, eles desbloqueiam a funcionalidade do software ou decodificam o conteúdo. Ele funciona como uma "chave" que autentica o usuário e protege o software contra cópias e uso não autorizado.

Vamos aos demais itens:

A) INCORRETO. "Vault" geralmente se refere a um local seguro para armazenar informações sensíveis, como senhas e chaves criptográficas.

B) INCORRETO. "Keycloak" é um software de gerenciamento de identidade e acesso de código aberto, que fornece serviços de autenticação e autorização.

C) INCORRETO. "KeePass" é um gerenciador de senhas de código aberto que armazena credenciais de usuário criptografadas. Embora possa ajudar a proteger informações de acesso, não se refere a um dispositivo físico que precisa ser conectado à porta USB para utilizar um software específico.

D) INCORRETO. "Keylogger" é um tipo de software ou hardware malicioso que registra as teclas pressionadas pelos usuários, com o objetivo de roubar informações confidenciais, como senhas e números de cartão de crédito.

Gabarito: E

3. FGV - 2020 - IBGE - Agente Censitário Operacional - Reaplicação

Considere as seguintes regras para a composição de senhas de 4 caracteres:

I. Dois dígitos numéricos + duas letras maiúsculas;

II. Quatro letras minúsculas;

III. Quatro dígitos numéricos;

IV. Três letras minúsculas + um dígito numérico;

V. Uma letra minúscula + três dígitos numéricos.

A regra que permite a criação de senhas mais fortes é:

A I;

B II;

C III;

D IV;

E V.

Comentário:

Temos aqui muito mais uma questão de probabilidade e estatística, do que de segurança em si.

Pessoal, quanto mais possibilidade temos de gerar caracteres diferentes e na combinação deles, senhas diferentes, teremos maior robustez.

Sendo assim, quando indicamos que um campo suporta apenas números, temos 10 opções (0 a 10). Quando falamos de letras, temos 26 possibilidades de minúsculas e outras 26 de maiúsculas, a depender do alfabeto suportado. Sendo assim, quando colocamos quatro opções de letras minúsculas, teremos 26x26x26x26 como total de combinações possíveis.

Gabarito: B

4. FGV - 2018 - MPE-AL - Técnico do Ministério Público - Tecnologia da Informação

Em muitas transações financeiras realizadas pela Internet é necessário que o usuário, além de fornecer o seu e-mail e senha, digite um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como

A biometria.

B cartão inteligente.

C certificado digital.

D criptografia.

E token de segurança.

Comentário:

Estamos falando dos recursos associados aos múltiplos fatores de segurança da informação. Assim, quando se tem uma mensagem enviada ao celular, estamos tratando de uma camada de segurança de algo que você tem, sendo também referenciado como token de segurança para validação do usuário.

Gabarito: E

5. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O reconhecimento biométrico consiste em reconhecer um indivíduo com base nas suas características físicas ou comportamentais.

A técnica adotada pelo sistema de identificação biométrico que implica em detectar e comparar a posição das minúcias (minutiae), também conhecida como características de Galton, é utilizada no reconhecimento da

A impressão digital.

B íris.

C retina.

D face.

E voz.

Comentário:

Vamos aos itens:

A) CORRETO. A técnica que detecta e compara a posição das minúcias (minutiae) ou características de Galton é utilizada no reconhecimento de impressões digitais. As minúcias são pontos específicos das impressões digitais, como bifurcações e terminações de cristas, que são únicos para cada indivíduo e podem ser utilizados para identificá-los de forma confiável.

B) INCORRETO. O reconhecimento da íris se baseia na análise das características únicas da íris de um indivíduo, como padrões de cores, estruturas e texturas. Essa técnica não utiliza minúcias para realizar a identificação.

C) INCORRETO. O reconhecimento de retina envolve a análise dos padrões de vasos sanguíneos da retina, que são únicos para cada indivíduo. A técnica de minúcias não é aplicada nesse método de reconhecimento biométrico.

D) INCORRETO. O reconhecimento facial analisa características faciais específicas, como distâncias entre os olhos, formato do nariz e contorno dos lábios. A técnica de minúcias não é empregada nesse tipo de reconhecimento biométrico.

E) INCORRETO. O reconhecimento de voz utiliza características comportamentais, como a frequência, tom e ritmo da fala, para identificar um indivíduo. A técnica de minúcias não é relevante para o reconhecimento de voz.

Gabarito: B

Lista de Questões - Autenticação e seus Mecanismos - CESPE

1. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

Em situações de gerenciamento de acesso de usuários a sistemas críticos, o uso de ferramentas de segundo fator de autenticação e gerenciamento de acesso privilegiado é restrito aos administradores do sistema.

2. CEBRASPE (CESPE) - Ana Sist (EMPREL)/EMPREL/2023

No Single Sign-On, a funcionalidade em que as informações de login e senha permitem um melhor controle da equipe de TI é

a) a autenticação multifator.

b) o gerenciamento interno de credenciais.

c) a velocidade na recuperação de senhas.

d) o ponto único para reinserir senha.

e) a melhor aplicação da política de senha.

3. CESPE / CEBRASPE - 2022 - TCE-SC - Auditor Fiscal de Controle Externo - Ciência da Computação

No controle de acesso, somente os usuários que tenham sido especificamente autorizados podem usar e receber acesso às redes e aos seus serviços.

4. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-CE

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

5. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Para acessar a intranet corporativa, um colaborador informa seu CPF, senha pessoal e um código enviado para o seu celular cadastrado.

O mecanismo de reforço implementado nessa intranet para confirmar a identidade do usuário contra acessos indevidos é a autenticação:

A) biométrica;

B) Kerberos;

C) Oauth2;

D) 2FA;

E) Openid.

6. Ano: 2020 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

Identificação e autenticação são requisitos de segurança da informação que consistem em identificar usuários do sistema e verificar as suas identidades, como pré-requisito para permitir o acesso desses usuários ao sistema.

7. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: SEFAZ-AL

O uso de senhas ou a adoção de identificação física, como biometrias, são formas de autenticação para fins de identificação única e exclusiva de usuários.

8. Ano: 2021 Banca: CESPE / CEBRASPE Órgão: PG-DF

Uma das condições para a autenticação é que o sinal biométrico apresente correspondência exata entre o sinal biométrico recebido pelo sistema e o gabarito armazenado.

9. CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

10. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Considere que uma empresa tenha introduzido sistema de autenticação biométrica como controle de acesso de seus funcionários às suas instalações físicas. Nessa situação, o uso desse tipo de controle é um procedimento de segurança da informação.

11. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Separação de tarefas, privilégio mínimo e necessidade de saber são conceitos que identificam os três principais tipos de controle de acesso.

12. (CESPE – TJ-SE/Analista Judiciário – Segurança da Informação/2014)

Os métodos de autenticação comumente empregados fundamentam-se na clássica divisão entre o que você sabe (senha ou número PIN); o que você tem (token ou um smart card); e o que você é (íris, retina e digitais).

13. (CESPE – SUFRAMA/Analista de Sistemas – Desenvolvimento/2014)

O controle de acesso refere-se à verificação da autenticidade de uma pessoa ou de dados. As técnicas utilizadas, geralmente, formam a base para todas as formas de controle de acesso a sistemas ou dados da organização.

GABARITO

GABARITO

1. E
2. B
3. C
4. C
5. D
6. C
7. C
8. E
9. C
10. C
11. E
12. C
13. C

Lista de Questões - Autenticação e seus Mecanismos - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

Considere as seguintes medidas de segurança:

I. Centralizar o controle de acesso para todos os ativos corporativos por meio de um serviço de diretório ou provedor de SSO, onde houver suporte.

II. Usar Single-Factor Authentication (SFA) para todas as contas de acesso administrativo, em todos os ativos corporativos, sejam estes gerenciados no site local ou por meio de um provedor terceirizado, pois esta é a medida de acesso seguro mais usada atualmente nas organizações.

III. Definir e manter o controle de acesso baseado em funções, determinando e documentando os direitos de acesso necessários para cada função dentro da organização para cumprir com sucesso suas funções atribuídas.

IV. Estabelecer e seguir um processo, de preferência manual, para manter o acesso aos ativos corporativos, por meio da ativação de contas antigas imediatamente após o encerramento, revogação de direitos ou mudança de função de um usuário.

São medidas recomendadas e adequadas para a gestão do controle de acesso o que se afirma APENAS em

a) I e III.

b) II e IV.

c) I.

d) III e IV.

e) II.

2. (FCC - TJ TRT18/TRT 18/Apoio Especializado/Tecnologia da Informação/2023)

Um serviço da web RESTful autentica solicitações antes de enviar uma resposta, usando métodos de autenticação. O método que combina senhas e tokens para acesso de login seguro, no qual primeiro o servidor solicita uma senha e, depois, um token adicional para concluir o processo de autorização, é o

a) API Key Security.

b) RSA Authentication.

c) Webhook.

d) Swagger SSO.

e) OAuth.

3. (FCC - AM (MPE PB)/MPE PB/Analista de Sistemas/Administrador de Banco de Dados/2023)

Um Analista está utilizando o protocolo OAuth2 (RFC 6749) e, após realizar todos os passos para obtenção e geração de um access token em condições ideais, recebeu o seguinte retorno:

{

"access_token": "57f10f0e-3d2e-311f-a797-4011f66e1cbf",

" I ": "ca81cb16-43e4-3e96-aaea-4861e7791dc7",

"token_type": "access_token",

"expires_in": 3600

}

Considerando que a lacuna I se refere ao campo que poderá ser utilizado para atualizar um access token que tenha expirado, esta é corretamente denominada:

a) refresh_token

b) redirect_uri

c) extraInfo

d) expired_token

e) redirect_token

4. (FCC – TRF – 4ª Região/Técnico Judiciário/2014) Os sistemas de identificação biométricos funcionam através da comparação de características físicas apresentadas por um usuário com as correspondentes armazenadas em um determinado banco de dados, identificando-o ou não como um dos usuários cadastrados, dificultando sobremaneira as fraudes praticadas contra as várias formas de verificação de identidades. O sistema de identificação biométrica que utiliza a parte do fundo do olho como identificador é conhecido como identificação

a) datiloscópica ou fingerprint.

b) da íris

c) da retina.

d) cognitiva.

e) teclar.

GABARITO

GABARITO

1. A
2. E
3. A
4. C

Lista de Questões - Autenticação e seus Mecanismos - FGV

1. FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

Marcia decidiu padronizar o mecanismo de autenticação de suas APIs RESTful e armazenar com segurança as credenciais de usuários e suas respectivas permissões. Para isso, ela deseja utilizar uma ferramenta de código aberto.

A ferramenta que tem por principal finalidade o gerenciamento de identidade e acesso que Márcia deve escolher é

A) JBoss.

B) Keycloak.

C) Kibana.

D) RabbitMQ.

E) Wildfly.

2. FGV - 2021 - Banestes - Analista em Tecnologia da Informação - Segurança da Informação

Um pequeno dispositivo que contém um código de proteção precisa necessariamente ficar conectado à porta USB do computador para que determinado software possa ser utilizado.

Esse dispositivo utilizado para prevenir o uso não autorizado de determinado software é conhecido como:

A) Vault;

B) Keycloak;

C) KeePass;

D) Keylogger;

E) Hardlock.

3. FGV - 2020 - IBGE - Agente Censitário Operacional - Reaplicação

Considere as seguintes regras para a composição de senhas de 4 caracteres:

I. Dois dígitos numéricos + duas letras maiúsculas;

II. Quatro letras minúsculas;

III. Quatro dígitos numéricos;

IV. Três letras minúsculas + um dígito numérico;

V. Uma letra minúscula + três dígitos numéricos.

A regra que permite a criação de senhas mais fortes é:

A) I;

B) II;

C) III;

D) IV;

E) V.

4. FGV - 2018 - MPE-AL - Técnico do Ministério Público - Tecnologia da Informação

Em muitas transações financeiras realizadas pela Internet é necessário que o usuário, além de fornecer o seu e-mail e senha, digite um código gerado ou recebido em seu celular. Essa tecnologia é conhecida como

A) biometria.

B) cartão inteligente.

C) certificado digital.

D) criptografia.

E) token de segurança.

5. FGV - 2017 - SEPOG - RO - Analista em Tecnologia da Informação e Comunicação

O reconhecimento biométrico consiste em reconhecer um indivíduo com base nas suas características físicas ou comportamentais.

A técnica adotada pelo sistema de identificação biométrico que implica em detectar e comparar a posição das minúcias (minutiae), também conhecida como características de Galton, é utilizada no reconhecimento da

A) impressão digital.

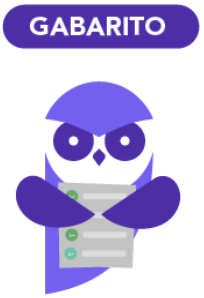
B) íris.

C) retina.

D) face.

E) voz.

GABARITO



1. B
2. E
3. B
4. E
5. B

RECURSO PARA GESTÃO DE ACESSO

IAM – Identity Access Management

PAM – Privileged Access Management

NTLM - Windows NT LAN Manager

Já vimos em momentos anteriores os desafios de se gerenciar os processos e etapas de autenticação e autorização, mantendo toda a rastreabilidade necessária nesse processo. Passamos pela referência prática do AAA.

Sendo assim, vamos tratar agora desses dois instrumentos que são de suma importância para a gestão de acesso nas organizações. Estamos falando do IAM e PAM.

De forma bem direta, vamos desde já diferenciá-los. O IAM possui foco na gestão de acessos de uma forma geral aos serviços e ambientes da organização. O PAM traz um olhar mais qualificado ao tratar as políticas de acesso para usuários privilegiados, ou seja, aqueles usuários que precisam interagir com áreas mais sensíveis da organização

Nesse contexto, ainda aparece o NTLM como solução mais antiga, porém, ainda com propósito de providenciar modelos de autenticação com base em modelo de desafio e resposta, algo semelhante ao que se pratica nas soluções de IPSeC, por exemplo.

Sendo assim, de forma bem objetiva, é importante termos a clareza dos três instrumentos:

- **IAM (Gerenciamento de Identidade e Acesso)** é um termo amplo que abrange uma variedade de tecnologias e processos para gerenciar identidades de usuário e acesso a sistemas e recursos. O IAM pode ser usado para autenticar usuários, autorizar seu acesso a recursos específicos e gerenciar suas permissões ao longo do tempo.
- **PAM (Gerenciamento de Acesso Privilegiado)** é um subconjunto do IAM que se concentra no gerenciamento do acesso de usuários privilegiados, como administradores e contas de serviço. O PAM pode ser usado para restringir o uso de contas privilegiadas, monitorar sua atividade e impedir acesso não autorizado.
- **NTLM (NT LAN Manager)** é um protocolo de autenticação mais antigo que é baseado em autenticação por desafio-resposta. O NTLM é considerado inseguro e não é recomendado para uso em novos sistemas. Se ancorava nas soluções Windows com o Kerberos para gestão de tokens de acesso.

Um ponto que se destaca nesses serviços, principalmente no modelo de PAM, é a gestão de segredos e/ou senhas. Essas soluções possuem a capacidade de se integrar diretamente aos serviços e recursos com vistas a gerar novas senhas dinamicamente para os usuários. Sendo assim, para cada novo acesso, é gerado uma nova senha e o usuário específico somente saberá no momento de solicitação do uso. Com isso, é possível

criar diversas políticas, incluindo aquelas que observam o horário de serviço do profissional, o local de acesso, entre muitas outras. Práticas como essa são conhecidas como acesso “just-in-time”.

Ainda, na ótica de capacidades, carece destacar que essas soluções podem incluir e excluir usuários, incorporar práticas de múltiplos fatores de autenticação, entre outros. Eles visam garantir que os usuários tenham o acesso certo com base em suas funções, responsabilidades e no princípio do menor privilégio. São soluções necessárias para uma arquitetura de segurança que se baseie na prática de Zero Trust.

Evoluindo o nível de controle exigido pelas soluções de PAM, é fundamental saber exatamente o que foi executado por um usuário com conta privilegiada. Nessa ótica, ainda são incorporadas funcionalidades de monitoramento das sessões, com controle de práticas e ações, com algum nível de alçada de aprovação ou notificação de grupos de administradores compartilhados para gestão do risco.

Aqui estão alguns exemplos específicos de ferramentas e recursos que podem ser usados em cada solução:

IAM:

- ***Gerenciamento de identidades:*** *ferramentas de gerenciamento de identidade como Active Directory, Okta e OneLogin.*
- ***Gerenciamento de acesso:*** *ferramentas de gerenciamento de acesso como Azure Active Directory, AWS Identity and Access Management (IAM) e Google Cloud Identity and Access Management (IAM).*
- ***Auditoria de acesso:*** *ferramentas de auditoria de acesso como Microsoft Advanced Auditing, AWS CloudTrail e Google Cloud Audit Logging.*

PAM:

- **Controle de acesso privilegiado:** ferramentas de controle de acesso privilegiado como CyberArk Privileged Access Management, BeyondTrust PowerBroker e Centrify Privileged Access Management.
- **Monitoramento de atividade privilegiada:** ferramentas de monitoramento de atividade privilegiada como CyberArk Privileged Session Manager, BeyondTrust PowerBroker Reporting e Centrify Privileged Access Audit.
- **Prevenção de acesso não autorizado:** ferramentas de prevenção de acesso não autorizado como CyberArk Privileged Identity Firewall, BeyondTrust Privileged Password Manager e Centrify Password Vault.

NTLM:

- **Autenticação por desafio-resposta:** o protocolo NTLM é integrado ao Windows e está disponível em todos os sistemas operacionais Windows.

SEGURANÇA EM ENDPOINTS

Primeira coisa para validarmos e lembrarmos para esse capítulo é o conceito de ENDPOINT. Basicamente, quando falamos de **ENDPOINTS,** referenciamos os equipamentos finais que ficam nas mãos dos usuários finais (computadores, laptops, smartphones, entre outros). A segurança desses equipamentos busca evitar ataques cibernéticos, detectar atividades maliciosas e fornecer recursos de correção instantânea, entre outros.

Importante destacar que estamos na era da Internet das Coisas, diretamente associada ao conceito de **BYOD (bring your own device)**, além de toda dinâmica associada ao trabalho remoto potencializado pela pandemia. Com esses conceitos modernos e dinâmica de utilização dos equipamentos, fica evidente a necessidade de aprimoramento dos aspectos voltados para segurança destes dispositivos.

Um outro ponto que merece destaque a respeito da dinâmica de uso dos dados e serviços corporativos está associado ao **princípio de desoneração** de recursos locais nas **máquinas e dispositivos**, com a potencialização do uso de recursos em nuvem, até mesmo explorando conceitos de Desktops Virtuais Corporativos.

A título de referência, podemos extrair de um dos grandes fornecedores de soluções de segurança a nível mundial, a Mcafee, que extrapola ainda mais o conceito de **Endpoints:**

Na prática, se o dispositivo está conectado à rede em alguma medida, com a capacidade de **processar informação e trafegar dados**, poderá ser classificado como um ENDPOINT.

Basicamente, ao longo das diversas disciplinas do Curso de Segurança, diversas ações que contribuem para esse processo são tratadas e detalhadas. Entretanto, reforçaremos alguns conceitos. Destaco também que muitos destes são tratados em diretrizes e ações como a **ISO 27002** e **Medidas de Controle de Segurança diversos**, definidos em **Frameworks de referência como o CIS CONTROLS ou NIST.**

Primeiro ponto a ser observado é o **conceito de camada e plataforma**. É importante que tais defesas contemplem as camadas horizontais (camadas da arquitetura TCP/IP), camadas horizontais (envolvem as etapas de pré-execução, execução e pós-execução de malwares ou ações maliciosas em geral), além de serem multiplataformas como diferentes linguagens de programação de sistemas e softwares, sistemas operacionais, entre outros. Lembrando que no bojo das plataformas, devemos considerar também soluções mobile, que envolvem, por exemplo, iOS e Android.

Dentre alguns recursos e contextos de aplicação das soluções voltadas para segurança em EndPoints, podemos citar **Antivírus, Antimalwares, firewalls, HIDS e HIPS, Atualizações diversas de drivers, softwares e S.O.,** entre outros. Vamos reforçar alguns recursos e conceitos para cada um desses aspectos.

Uso de Assinaturas e Inteligência Artificial

Sem dúvida, o uso de assinaturas de códigos e programas sempre foram a **linha de base** de identificação de quaisquer **malwares** em equipamentos. Entretanto, diversas técnicas de ofuscação de código podem ser implementadas, de tal modo que reduzem, sobremaneira, a eficiência dessa técnica de identificação.

Destaca-se que há compartilhamentos de múltiplas bases de assinaturas e identificação desses softwares que não se restringem necessariamente a fabricantes ou provedores de tecnologia especificamente. Esse arranjo ajuda a fortalecer a capacidade de identificação por meio da disseminação de informações. Entretanto, mesmo essas medidas não são suficientes no processo.

Assim, surgem as técnicas de análise de comportamento por meio de inteligência artificial e aprendizado de máquina que traçam linhas de base com base em heurísticas, redes neurais e muitas outras técnicas, para tentar prever determinados malwares e outras ações.

Importante destacar que ataques como **ZERO-DAY**, onde não são conhecidos em nenhuma assinatura, somente poderão ser detectados preventivamente por meio dessas técnicas ou ações manuais. Lembrando que ataques ZERO-DAY basicamente são aqueles que ainda **não foram descobertos** pelas **comunidades e provedores** de soluções de segurança, ou ainda, pelo donos das soluções e produtos, para que possam implementar as medidas de segurança ou correções necessárias para eliminar a vulnerabilidade.

Nesse ponto, além dos recursos já mencionados na introdução, merece comentar também recursos voltados para atuação no ambiente de pré-inicialização do Sistema Operacional, para monitoramento da integridade do firmware por meio do UEFI (Interface de Firmware Extensível Unificada.

Monitoramento de Processos, Serviços e Memória

Um outro recurso interessante que se conecta com o recurso de inteligência é justamente o monitor de eventos e comportamentos, que atua nos processos, serviços e memórias dos equipamentos.

Ataques mais modernos se utilizam da memória para poderem acelerar seu poder de fogo e reduzir a capacidade de detecção, uma vez que não passa por arquivos em disco, não havendo, nesse caso persistência.

Assim, entender o **comportamento da memória** é importante no contexto atual para se prevenir e tentar combater esse tipo de ataque.

Monitoramento de Atualizações e Patches de Segurança

Apesar de trivial, mas nem sempre é feito de forma efetiva e de forma automática. Garantir com que os sistemas operacionais, softwares instalados, drivers dos dispositivos, entre outros, possuam as últimas atualizações instaladas é de suma importância.

Os **Patches** de atualização geralmente agregam recursos de Segurança e eliminação de vulnerabilidades identificadas.

Área segura e virtualizada para execução de arquivos (sandbox)

Um outro recurso importante que também é incorporado nas múltiplas ferramentas elencadas acima é o **SANDBOX**. Tal recurso se trata, basicamente, de uma área virtualizada criada com a capacidade de isolar o processamento de determinado arquivo.

Na prática, cria-se um contexto virtual capaz de emular todos os recursos de uma máquina, para avaliar o comportamento do software. Muitas das vezes, há trechos no código que não são reconhecidos e gera-se dúvidas sobre sua forma de atuação e potenciais resultados derivados. Basicamente tem-se a questão da ofuscação do código ou trecho dele que procederá exatamente com as funcionalidades maliciosas.

Nesse contexto, portanto, dentro de uma sandbox, **pode-se executar o código e avaliar o comportamento** e, caso seja, de fato, um software malicioso, o dano será gerado apenas em estruturas virtuais, que podem ser facilmente excluídas posteriormente e não havendo qualquer propagação para as estruturas do Sistema Operacional base.

Tal técnica é a mesma utilizada, por exemplo, quando se deseja navegar em redes não confiáveis, ou ainda, a deep web. Nesse caso, não se trata de uma instância simplificada criada pelas ferramentas de antivírus ou antimalware, por exemplo, mas sim, uma ferramenta de virtualização, de fato, de máquinas, como Virtual Box ou Virtual Machine. Assim, a partir das instâncias virtualizadas criadas, pode-se navegar em redes inseguras sem colocar em risco, da mesma forma, o próprio Sistema Operacional.

Navegação Segura e e-mails seguros

Já adiantamos o assunto na seção anterior, e é importante reforçar a dinâmica de navegação na WEB por parte desses endpoints. Desta feita, **utiliza-se técnicas** como proxies e outros recursos a **nível da camada de aplicação** que são capazes de promover uma **navegação segura e controlada,** inclusive, trabalhando com práticas de blacklists e whitelists.

Ações proativas em torno da navegação são fundamentais nesse processo.

No mesmo contexto, pode-se implementar técnicas e soluções associadas aos clientes de e-mail que eventualmente sejam instalados e utilizados nos Endpoints, ou ainda, clientes web que também sejam acessados. Nesse ponto, destaca-se a possibilidade de utilização da tecnologia **MFA (Multi Factor Authentication).**

Gerenciamento Centralizado

Um outro recurso que pode ser utilizado associado à segurança de endpoints é um gerenciamento centralizado. Com isso, é possível incluir tanto equipamentos corporativos como equipamentos particulares que possuem acesso aos recursos corporativos. Desse modo, a partir do **gerenciamento Centralizado**, é possível estabelecer **policies diversas**, com categorias e tipos de **uso dos equipamentos**, garantindo baselines de configuração, com a possibilidade de varreduras e ações remotas de forma automática nesses equipamentos.

Trata-se de um recurso que impõe uma **dinâmica**, por vezes, invasivas, principalmente quando se fala de inclusão de **dispositivos pessoais** neste monitoramento. Mas é sempre um trade off quando se trata de privacidade e comodidade, para unificar procedimentos e soluções em torno da vida pessoal e necessidades particulares em conjunto com o contexto corporativo.

(FGV/CGU/2022) Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

A) redução de custos e facilidade de atualização;

B) configuração simplificada e fácil instalação de API;

C) monitoramento completo e antivírus atualizado;

D) administração descentralizada e facilidade de integração com novas tecnologias;

E) bloqueio de ações indesejadas e controle no lado do usuário.

Comentários:

Essa foi uma questão extremamente polêmica, pessoal. É um desafio para os candidatos lidarem com assuntos novos, pois não se tem muito parâmetro de como esse assunto será cobrado. E nesse contexto, foi exatamente o que aconteceu. A Banca utilizou uma referência extremamente frágil na perspectiva de um

fabricante sem relevância, e trouxe como gabarito a alternativa A. Agora, há de se destacar que há diversas outras fontes de outros fabricantes, que também trazem as perspectivas das alternativas B e C.

Então focando nos comentários dos itens isolados, temos:

- Redução de custos pois concentra o regime de oferta de soluções, não implicando em custos avulsos e descentralizados para os endpoints.

- Facilidade de Atualização traz a perspectiva de você manter uma base centralizada com as versões e bases de conhecimento para combate a ataques diversos. Então torna-se um processo automático e simples.

Agora os outros itens:

- Configuração simplificada seria um item também viável, pois as soluções de Segurança em Endpoints precisam ser usáveis e simples, permitindo a implantação em qualquer dispositivo.

- Fácil instalação de API, diz respeito ao fato de que múltiplas soluções não são completas em si e abarcam todas as frentes de segurança, cabendo modelos de integração e troca de informações entre soluções distintas

- Monitoramento Completo abarca o contexto e capacidade da ferramenta/solução extrair a visão completa dos fluxos de trabalho e processos dos equipamentos por meio de agendas e troca de informações, resguardando assim os endpoints.

- Antivírus atualizado é o mínimo que se espera de uma solução que busca estabelecer parâmetros mínimos de segurança para seus equipamentos.

Gabarito: A (Gabarito do Professor: Anulação)

QUESTÕES COMENTADAS - SEGURANÇA EM ENDPOINTS - FGV

1. FGV/CGU/2022 Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

A) redução de custos e facilidade de atualização;

B) configuração simplificada e fácil instalação de API;

C) monitoramento completo e antivírus atualizado;

D) administração descentralizada e facilidade de integração com novas tecnologias;

E) bloqueio de ações indesejadas e controle no lado do usuário.

Comentários:

Essa foi uma questão extremamente polêmica, pessoal. É um desafio para os candidatos lidarem com assuntos novos, pois não se tem muito parâmetro de como esse assunto será cobrado. E nesse contexto, foi exatamente o que aconteceu. A Banca utilizou uma referência extremamente frágil na perspectiva de um fabricante sem relevância, e trouxe como gabarito a alternativa A. Agora, há de se destacar que há diversas outras fontes de outros fabricantes, que também trazem as perspectivas das alternativas B e C.

Então focando nos comentários dos itens isolados, temos:

- Redução de custos pois concentra o regime de oferta de soluções, não implicando em custos avulsos e descentralizados para os endpoints.

- Facilidade de Atualização traz a perspectiva de você manter uma base centralizada com as versões e bases de conhecimento para combate a ataques diversos. Então torna-se um processo automático e simples.

Agora os outros itens:

- Configuração simplificada seria um item também viável, pois as soluções de Segurança em Endpoints precisam ser usáveis e simples, permitindo a implantação em qualquer dispositivo.

- Fácil instalação de API, diz respeito ao fato de que múltiplas soluções não são completas em si e abarcam todas as frentes de segurança, cabendo modelos de integração e troca de informações entre soluções distintas

- Monitoramento Completo abarca o contexto e capacidade da ferramenta/solução extrair a visão completa dos fluxos de trabalho e processos dos equipamentos por meio de agendas e troca de informações, resguardando assim os endpoints.

- Antivírus atualizado é o mínimo que se espera de uma solução que busca estabelecer parâmetros mínimos de segurança para seus equipamentos.

Gabarito: A (Gabarito do Professor: Anulação)

Lista de Questões - Segurança em Endpoints - FGV

1. FGV/CGU/2022 Roberto é funcionário de um órgão público e está trabalhando em home office devido ao cenário pandêmico. Para que não haja perda de produtividade, Roberto precisa acessar a rede interna do órgão onde trabalha. Para isso, Roberto irá utilizar um computador considerado um endpoint, por se tratar de um dispositivo final que se conecta fisicamente a uma rede interna do órgão. Para que o órgão público em que Roberto trabalha possa confiar em conexões externas com a rede interna, soluções de segurança de endpoints precisam ser implementadas e ter como características:

A) redução de custos e facilidade de atualização;

B) configuração simplificada e fácil instalação de API;

C) monitoramento completo e antivírus atualizado;

D) administração descentralizada e facilidade de integração com novas tecnologias;

E) bloqueio de ações indesejadas e controle no lado do usuário.

GABARITO

GABARITO

1. A (Gabarito do Professor: Anulação)

AUDITORIA E CONFORMIDADE

Outros assuntos que constantemente caem em prova em termos conceituais e suas aplicações, é a **auditoria** e **conformidade.**

Já mencionamos na aula de hoje alguns instrumentos e mecanismos utilizados para fins de auditoria.

Em um conceito básico, temos que

> A **auditoria** em tecnologia da informação diz respeito à análise **cuidadosa e sistemática** dos **recursos de TI**, pessoas, documentos, sistemas, entre outros, no intuito de se averiguar se estes estão de acordo com aquilo que fora planejado ou em relação às atividades e comportamentos definidos como padrão. Avalia-se quanto à sua eficácia e eficiência em torno dos objetivos e resultados esperados.

Geralmente, lembramos de auditoria em ações que buscam evidenciar aspectos para fins de apuração de algum tipo de desvio ou comportamento indesejado.

Uma outra definição para a auditoria de **Segurança da Informação**, trazida pelo TCU é:

> Avaliação se a gestão da segurança da informação, o controle dos ativos e os riscos envolvidos são considerados de **forma efetiva pela organização.** A auditoria de SI visa avaliar a gestão da organização com relação à segurança. Aborda aspectos de confidencialidade, integridade e disponibilidade embutidos nos conceitos de segurança lógica e física.

Quando falamos que devemos registrar os acessos dos usuários, por exemplo, tem-se como pano de fundo o fato de que, em um eventual problema de vazamento de dados, novamente, como exemplo, pode-se avaliar as informações e identificar o responsável por tal ação. Isso está muito atrelado ao conceito do **AAA – Autenticação, Autorização e Auditoria.**

Assim, uma auditoria de TI deve ter um escopo bem definido que contemple a identificação e avaliação de controles que possa afetar a segurança da informação, tanto em um contexto macro, quanto micro (mais aprofundado e técnico) a depender da intenção e necessidade de análise.

Falando um pouco sobre **conformidade,** podemos definir como:

> Conceito relacionado à adesão dos **sistemas de informação** às **políticas** e às normas organizacionais de segurança da informação.

Conforme veremos mais à frente, há diversas normas e padrões, além de políticas diversas que apresentam as melhores práticas e aspectos para certificações nos mais distintos nichos e contextos da segurança da informação. Assim, quando uma empresa prima pelas boas práticas, ela deve estar aderente, ou seja, em conformidade com os referidos padrões.

Importante destacar que os critérios de conformidade **não se restringem** a essas normas e padrões **internacionais.** Trazendo a nossa análise para o contexto do próprio Governo, uma vez que estamos falando de concursos públicos, há órgãos diversos do Governo capazes de gerar normas, manuais, políticas, boas práticas e diretrizes a serem seguidas pelos órgãos da administração pública. Sem contar as leis e Decretos que devem ser seguidos.

Assim, espera-se que os órgãos estejam em conformidade com essas questões que mencionamos.

(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Comentários:

Questão tranquila, certo pessoal? Já vimos a importância dos referidos registros e logs para as auditorias e investigações.

Questões Comentadas - Noções Básicas de Continuidade de Negócios - CESPE

(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

Comentários:

Questão tranquila, certo pessoal? Já vimos a importância dos referidos registros e logs para as auditorias e investigações.

Gabarito: errada.

Lista de Questões - Noções Básicas de Continuidade de Negócios - CESPE

(CESPE - 2014 - TJ-SE - Analista Judiciário - Segurança da Informação) Atividades de usuários, exceções e outros eventos são registros ou logs de eventos produzidos e mantidos pela instituição, mas, por constituírem eventos qualitativos, não são objetos apropriados para futuras investigações ou auditorias.

GABARITO

GABARITO

1. Errada

NOÇÕES BÁSICAS DE CONTINUIDADE DE NEGÓCIOS

Nada melhor do que avaliarmos os conceitos estabelecidos nas normas. Nesse caso, vamos ver o que a **ISO 27002** nos traz a respeito do **objetivo da Gestão da Continuidade de Negócios:**

"não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua **retomada em tempo hábil**, se for o caso"

Ou seja, é uma questão de sobrevivência de uma empresa. Quando há falhas ou desastres significativos, estamos falando inclusive de catástrofes, como enxurradas, terremotos, entre outros. Falaremos um pouco mais sobre isso depois.

Nesse contexto, a criticidade do negócio varia caso a caso. Uma coisa é falarmos de uma estrutura para continuidade de negócios de empresas como a GOOGLE, AMAZON, entre outros.... Nesses casos, **minutos são críticos** para gerar qualquer tipo de **indisponibilidade dos serviços.**

Agora para as demais empresas, esses **parâmetros** devem ser avaliados **caso a caso**, justamente para se chegar ao **ponto de equilíbrio** em que a prevenção ou gestão/controle se torne tão onerosa a ponto de não se sustentarem.

Não temos como deixar de mencionar um caso clássico de exemplo desse aspecto que é o infeliz atentado de 11 de setembro.

Sem entrar no mérito da causa e, obviamente, ciente de que as vidas eram os bens mais precioso nesse contexto, vamos focar na nossa análise de Continuidade de Negócio.

Nesse momento da foto, várias empresas e negócios já estavam sofrendo com dados e informações perdidas, estruturas de Datacenter danificados. Nesse contexto, uma alternativa era colocar uma **redundância** ou **Backup** (solução alternativa para funcionar no caso de parada da principal) no prédio ao lado. Mas todos nós já sabemos o fim que se deu. A gestão da continuidade do negócio não considerou algo que parecia ser impossível, um atentado quase que simultâneo nas duas torres.

É nessa mesma toada que muitas empresas não enviam seus conselhos e executivos nos mesmos aviões e em mesmos horários, pois em caso de acidente de um, ainda se tem o restante da equipe para continuar girando os negócios.

A título de curiosidade, para você se divertir após passar a sua prova, veja o seriado "DESIGNATED SURVIVOR", que nos retrata um pouco sobre essas alternativas em casos extremos de catástrofes.

Fato é que o atentado foi um momento em que grandes empresas e bancos passaram a reavaliar seus processos de gestão de continuidade de negócios. **Muitas empresas** até tinham seus **planos e soluções** alternativas, mas sofreram para **voltarem ao seu funcionamento.**

Aqui cabe mais um caso clássico que é o uso de nobreaks e geradores em soluções de redundância e backup. Mas de nada adianta se não houver uma manutenção desses equipamentos para manter as células de bateria carregadas ou o combustível disponível. Nesse aspecto, auditorias constantes nos planos e soluções ajudam a manter um ambiente estável e "pronto" para eventuais catástrofes.

Nesse contexto surge o **PCN – Plano de Continuidade de Negócios**. Este é o documento responsável por consolidar as ações para continuidade do negócio. Todos os **riscos envolvidos**, no que tange às suas probabilidades e impactos devem ser analisados. O PCN possui como foco tanto o capital intelectual (informações), bem como suas instalações.

Se o PCN não estiver atualizado e for constantemente revisado e internalizado pelas equipes, com certeza haverá uma grande dificuldade no restabelecimento dos serviços e do negócio nos casos de necessidade. Por isso, pensar nas pessoas e testar esses planos, por intermédio de questionários e teorias, e até simulações práticas, é de suma importância.

O PCN deve então contemplar as estratégias e planos de ação com vistas a manter os serviços essenciais ativos. Obviamente, tem-se uma **etapa prévia** que é a **identificação** desses **serviços essenciais.**

Neste plano terá todos os detalhamentos dos procedimentos a serem seguidos, bem como as devidas matrizes de responsabilidades e ações por componente e recurso envolvido.

Alguns exemplos de **cenários e eventos** que podem ser considerados em um **PCN:**

1. Falhas humanas;

2. Falhas das soluções e componentes de TI;

3. Fenômenos da natureza que geram acidentes e catástrofes (furação, tempestades, maremotos);

4. Interrupções de abastecimento;

5. Distúrbios civis (greves, vandalismos);

6. Malwares e Vírus;

7. Sabotagem;

8. Terrorismo, etc.

Assim, fechamos essa parte de noções básicas de Continuidade de Negócios.

NOÇÕES DE GESTÃO DE RISCOS

Costumeiramente ouvimos falar dessa palavrinha tão comum no meio de segurança da informação, que é RISCO! Sem dúvida, considerá-la é fundamental na implantação de qualquer ambiente que trate a informação de alguma forma.

Entretanto, o que vem a ser, de fato, risco? Antes de definirmos propriamente o risco, vamos trabalhar alguns conceitos prévios.

Primeiramente, vamos falar da **VULNERABILIDADE**. A vulnerabilidade, segundo a norma ISO 27002, "é a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças". Portanto, temos uma situação ou condição que poderá ser um meio, um vetor, uma entrada para um eventual problema de segurança. Como exemplo, podemos citar o fato de não termos uma rede estabilizada e aterrada.

Surge então um segundo conceito, que é o **de AMEAÇA.** Este conceito nada mais é do que um fator, elemento, causa que poderá explorar uma determinada vulnerabilidade. Segundo a ISO 27002, temos que a ameaça é a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Percebam, portanto, que não devemos vincular o conceito de AMEAÇA a alguém mal-intencionado com o objetivo de vazar informações ou gerar algum dano. A simples existência de períodos chuvosos com raios pode ser uma ameaça para a vulnerabilidade que utilizamos como exemplo anteriormente, pois, neste caso, poderá gerar descarga nos equipamentos e queimá-los, gerando indisponibilidade dos serviços.

Avançando um pouco mais, temos o conceito de **IMPACTO,** que considera o resultado gerado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos. Na maioria das vezes, este resultado está atrelado a algum dano ou prejuízo gerado quando uma ameaça explora determinada vulnerabilidade.

Culminou então **no conceito de RISCO** que é a probabilidade potencial associada à exploração de uma ou mais vulnerabilidades por parte de uma ou mais ameaças, capazes de gerar determinado IMPACTO para a organização. Percebam que o RISCO está atrelado a todos os demais conceitos que vimos anteriormente.

Resumindo, portanto, temos:

- **RISCO**: probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização;
- **AMEAÇA:** Causa potencial de um incidente indesejado.
- **VULNERABILIDADE:** Fragilidade de um ativo que pode ser explorada por uma ou mais ameaças
- **IMPACTO:** Resultado gerado por uma ameaça ao explorar uma vulnerabilidade.

É importante aproveitarmos o contexto para definir, segundo a ISO 27001, o **conceito de incidente:**

> "Incidente de segurança da informação é indicado por um simples ou por uma série de **eventos** de segurança da informação **indesejados ou inesperados**, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação".

Muita atenção para o fato de ser indesejado e inesperado, pois são esses elementos que o diferenciam do evento, como veremos em algumas questões.

Existem algumas formas básicas de como a organização deve reagir aos riscos. Pode-se tomar basicamente quatro tipos de ação, quais sejam:

- **Evitar –** Busca-se ações com vistas a prevenir a ocorrência de determinado risco. Como exemplo, pode-se bloquear o acesso de determinado usuário à internet. Isso poderia evitar que este acesse serviços remotamente e vaze dados pela Internet.
- **Transferir –** Busca-se transferir o risco para uma terceira parte. Nesse caso, a terceira parte assume a responsabilidade das ações frente ao risco, bem como custos e outros fatores. Analogia simples ao seguro de carro que fazemos, passando o risco de acidente e roubo para a seguradora.
- **Mitigar –** Objetiva-se atuar em prol da minimização dos riscos. Como exemplo, pode-se restringir o acesso de determinados usuários a sites controlados.
- **Aceitar ou Reter –** Determinados riscos não valem a penas ser evitados, mitigados ou transferidos por agregar custos ou esforços extremamente elevados que, em termos quantitativos, são maiores que os dados ou informação em análise. Desse modo, aceita-se o risco em caso de ocorrência.

(FCC – TCE-GO/Analista de Controle Externo/2014) Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

A) aceitação do risco.

B) transferência do risco.

C) eliminação do risco.

D) especificação do risco.

E) mitigação do risco.

Comentários:

Quando se criar um ambiente replicado, temos uma redução do risco de perda de dados em caso de falhas ou catástrofes. Entretanto, pessoal, isso não evita ou elimina o risco, pois, ainda assim, pode-se ter uma catástrofe que impacte os dois ambientes.

Gabarito: E

Questões Comentadas - Noções Básicas de Gestão de Riscos - FCC

1. (FCC – TCE-GO/Analista de Controle Externo/2014) Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

A) aceitação do risco.

B) transferência do risco.

C) eliminação do risco.

D) especificação do risco.

E) mitigação do risco.

Comentários:

Quando se cria um ambiente replicado, temos uma redução do risco de perda de dados em caso de falhas ou catástrofes. Entretanto, pessoal, isso não evita ou elimina o risco, pois, ainda assim, pode-se ter uma catástrofe que impacte os dois ambientes.

Gabarito: E

Lista de Questões - Noções Básicas de Gestão de Riscos - FCC

1. (FCC – TCE-GO/Analista de Controle Externo/2014) Pedro trabalha na área que cuida da Segurança da Informação de uma empresa. Frente ao risco de indisponibilidade de uma aplicação, criou um servidor de backup para tentar garantir que as informações sejam replicadas, automaticamente, do servidor principal para o servidor backup de forma redundante. A estratégia utilizada por Pedro para tratar o risco é considerada como

A) aceitação do risco.

B) transferência do risco.

C) eliminação do risco.

D) especificação do risco.

E) mitigação do risco.

GABARITO

GABARITO

1. E

Diretrizes para o Desenvolvimento de Software Seguro

Quando falamos de Segurança da Informação, devemos nos preocupar com todas as camadas, objetos, recursos, locais, entre outros, que de alguma forma tratará os dados em uma comunicação, ou seja, que manipulará a informação em algum momento.

Desse modo, aplicações e softwares estão diretamente envolvidos nesse processo. Portanto, é fundamental estabelecer diretrizes, regras, rotinas e boas práticas que de alguma forma visam tornar o processo de desenvolvimento das aplicações mais seguro e consequentemente obter um software mais seguro

Esses softwares devem ser capazes de aplicar regras de controle de acesso, gerar registros e logs que possibilitem verificar as trilhas de auditoria e, obviamente, serem robustos com vistas a manter a disponibilidade dos recursos.

É importante destacar que os aspectos de segurança da informação, em um modelo ideal, devem ser incorporados aos requisitos de desenvolvimento, além de participar em todas as fases de desenvolvimento do software, desde a modelagem, passando pela etapa de desenvolvimento, testes, instalação e homologação.

Veremos então neste tópico diversos aspectos que devem ser considerados para tal finalidade.

- Senhas Fortes

A utilização de senhas fortes é amplamente difundida no mundo da Segurança da Informação. Entretanto, é extremamente negligenciado pelos usuários. Quantos de vocês realmente têm essa preocupação? Buscam utilizar senhas diferentes para cada aplicação? Utilizam números, letras maiúsculas e minúsculas, caracteres especiais, entre outros

Creio que a maioria reconheceu que não.. e acabam por estar na lista daqueles que negligenciam esse ponto.

Desse modo, as aplicações atuais buscam "obrigar" o usuário a cadastrar senhas que tenham parâmetros mínimos de segurança, conforme elencamos, além de considerar os tamanhos das senhas. Recomenda-se um tamanho mínimo de 8 caracteres, apesar de diversas aplicações aceitarem como quantidade razoável 6 caracteres.

Atualmente, existem diversas soluções de mercado que permite a utilização de cofres de senhas. Tais cofres podem ser instalados em uma máquina ou servidor e gerenciar as diversas senhas do usuário, além de prover um armazenamento seguro e criptografado na máquina. Além disso, são capazes também de gerar senhas extremamente fortes para os usuários.

- Atualização de aplicações

Temos aqui mais um ponto amplamente difundido, entretanto, mais uma vez, negligenciado pelos usuários. É importante lembrar que as atualizações disponibilizadas pelos fabricantes não se restringem ao acréscimo de novas funcionalidades e recursos, mas também contemplam correções de bugs, falhas de segurança, entre outros.

Assim, não basta que o software seja seguro por si próprio se softwares complementares e integrados ou sistemas operacionais não se encontram atualizados, com diversas brechas de segurança.

- Fuzzing

Esta é uma técnica utilizada para testar erros em aplicações. É amplamente utilizado no processo de desenvolvimento de softwares seguros devido sua capacidade de detectar defeitos que usuários não descobrem com facilidade. Assim, caso este seja descoberto em ambiente de produção, pode gerar grandes danos aos usuários de determinada aplicação.

A referida técnica consiste, basicamente, em enviar entradas randômicas para a aplicação. Por este motivo, também é conhecida como injeção de falhas, teste de validação robusta, teste de sintaxe ou teste de negação.

Como exemplo, podemos citar um formulário que foi criado com a expectativa de receber determinado conjunto de caracteres e dados, como informações de telefone, CEP, entre outros.

Assim, o Fuzzing injetará informações incomuns como tamanhos diferenciados, caracteres não utilizados e, paralelamente, monitorará o comportamento da aplicação, pois esta poderá travar ou vazar dados de forma indevida.

- Boas práticas de Código Seguro

Diversas aplicações necessitam ser desenvolvidas dentro de prazos específicos e muitas vezes, arrojados. Assim, cumprir prazo e entregar o produto é a principal prioridade e, por muitas vezes, amplifica o surgimento de novas falhas, vulnerabilidades, entre outros. Neste sentido, temos diversas boas práticas que podem ser seguidas no desenvolvimento dessas aplicações, quais sejam:

Documentação – A documentação pode ser extremamente importante no diagnóstico e resolução de forma mais fácil e rápida de problemas.

Validação de Entrada – Este processo consiste em inserir dados em pontos de entrada da aplicação e verificar se o comportamento está de acordo com o esperado pelo desenvolvedor, documentando todo o processo. Um típico exemplo é a utilização de máscaras que obrigam o usuário de inserir dados no formato esperado, como o CPF.

Manipulação de Erros – O tratamento de erros é um ponto muito importante no desenvolvimento de aplicações seguras. Essas aplicações sempre estarão sujeitas a erros e, por medida de segurança, é importante que haja um padrão de mensagem de erro para o usuário que não vaze informações a respeito da aplicação, evitando assim que um atacante obtenha essas informações para aprimorar seus ataques. Sob a perspectiva do desenvolvedor em utilizar tais mensagens para correção, recomenda-se que este utilize logs das aplicações e controle de forma segura em um ambiente seguro.

- Baseline de Configuração de Aplicação

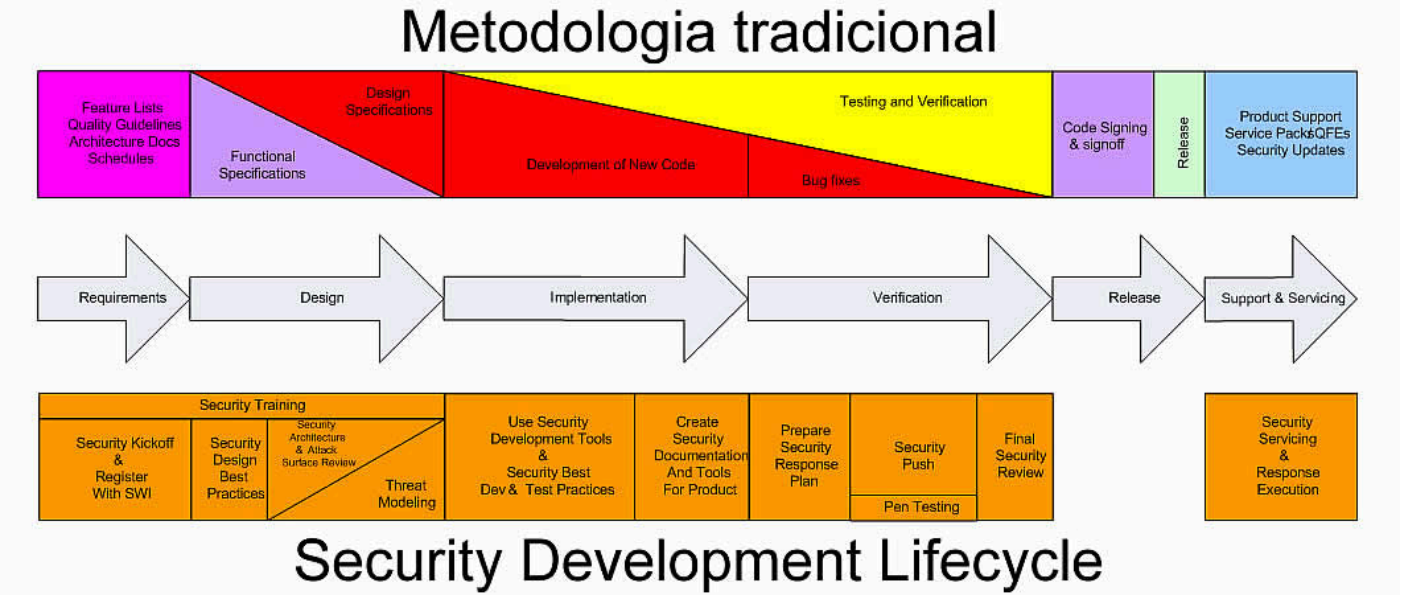
As aplicações podem utilizar diversos componentes pelos quais possuem dependências para seu funcionamento. É importante identificar esses componentes e entender como as aplicações fazem uso dessas. A partir de então, pode-se trabalhar em cima dessas aplicações com configurações seguras que darão a devida base e sustentação da aplicação principal.

SDL (Security Development Lifecycle)

Falando um pouco mais sobre segurança no processo de desenvolvimento, vamos abordar agora o SDL (Security Development Lifecycle ou Ciclo de Vida do Desenvolvimento Seguro).

É uma metodologia criada pela Microsoft para o desenvolvimento de softwares que precisam suportar ataques de usuários mal-intencionados.

O processo engloba a adição de uma série de atividades e produtos concentrados na segurança em cada fase do processo de desenvolvimento de software da Microsoft. Essas atividades e esses produtos incluem o desenvolvimento de modelos de ameaças durante o design do software, o uso de ferramentas de verificação de código de análise estática durante a implementação e a realização de revisões de código e testes de segurança durante um "esforço de segurança" direcionado.



SDL tem relação direta com as fases do ciclo de vida para desenvolvimento de software. Esse processo segue o modelo espiral para aqueles que já estudaram metodologias de desenvolvimento de software.

Nesse modelo, a MICROSOFT criou os princípios de segurança no desenvolvimento conhecido como SD3 + C:

a) Secure by Design (Seguro por Desenho)

A arquitetura, o design e a implementação do software devem ser executados de forma a protegê-lo e proteger as informações que ele processa, além de resistir a ataques.

b) Secure by Default (Seguro por Padrão)

Na prática, o software não atingirá uma segurança perfeita; portanto, os designers devem considerar a possibilidade de haver falhas de segurança. Para minimizar os danos que ocorrem quando invasores miram nessas falhas restantes, o estado padrão do software deve aumentar a segurança.

Por exemplo, o software deve ser executado com o privilégio mínimo necessário, e os serviços e os recursos que não sejam amplamente necessários devem ser desabilitados por padrão ou ficar acessíveis apenas para uma pequena parte dos usuários.

c) Secure by Deployment (Seguro na Implantação)

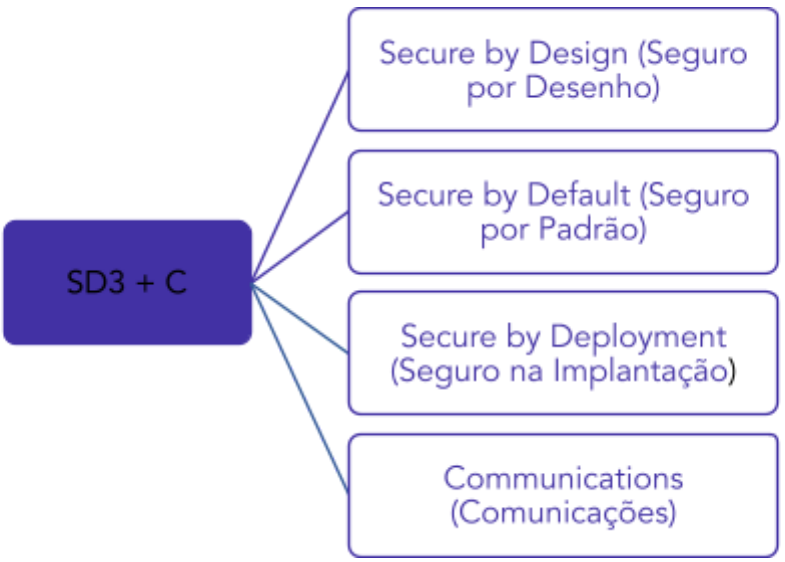
O software deve conter ferramentas e orientação que ajudem os usuários finais e/ou administradores a usá-lo com segurança. Além disso, a implantação das atualizações deve ser fácil.

d) Communications (Comunicações)

Os desenvolvedores de software devem estar preparados para a descoberta de vulnerabilidades do produto e devem comunicar-se de maneira aberta e responsável com os usuários finais e/ou com os administradores para ajudá-los a tomar medidas de proteção (como instalar patches ou implantar soluções alternativas).

Destes, considera-se que os dois primeiros são os que possuem a maior capacidade de agregar segurança no software.

Vamos explorar um pouco mais os aspectos de segurança considerados em cada uma das fases.



1. FASE DE REQUISITOS

Durante a fase de requisitos, a equipe de produto entra em contato com a equipe de segurança central para solicitar a designação de um supervisor de segurança (chamado de o "cara da segurança" na implementação do SDL na Microsoft) que serve como um ponto de contato, pesquisa e orientação durante o planejamento.

O supervisor de segurança também serve como ponto de contato entre a equipe de segurança e a gerência da equipe de produto, e aconselha a gerência da equipe quanto ao controle do elemento de segurança de seus projetos, de forma a evitar surpresas relacionadas à segurança posteriormente durante o processo.

A fase de requisitos é a oportunidade para a equipe de produto considerar como a segurança será integrada no processo de desenvolvimento, identificar os objetivos-chave de segurança e maximizar a segurança de software, minimizando a quebra de planos e cronogramas.

Como parte desse processo, a equipe precisa considerar como os recursos de segurança e as medidas de controle de seu software serão integrados com outros softwares que provavelmente serão usados com ele.

A perspectiva geral da equipe de produto sobre os objetivos, os desafios e os planos de segurança devem se refletir nos documentos de planejamento produzidos durante a fase de requisitos. Embora os planos estejam sujeitos a alterações conforme o andamento do projeto, a articulação precoce desses planos ajuda a garantir que nenhum requisito seja desconsiderado ou estabelecido na última hora.

2. FASE DE DESIGN

Nesta fase, tem-se a identificação da estrutura e os requisitos gerais do software. Na perspectiva de segurança, os elementos-chave dessa fase são:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

3. FASE DE IMPLEMENTAÇÃO

Durante a fase de implementação, a equipe de produto gera o código, testa e integra o software.

Os resultados da modelagem de ameaças fornecem uma orientação particularmente importante durante a fase de implementação. Os desenvolvedores dedicam atenção especial em corrigir o código de modo a atenuar as ameaças de alta prioridade e os testadores concentram seus testes na garantia de que essas ameaças estejam de fato bloqueadas ou atenuadas.

Os elementos do SDL considerados nessa fase são:

- Aplicar padrões de codificação e teste.
- Aplicar ferramentas de testes de segurança, incluindo ferramentas de difusão.
- Aplicar ferramentas de verificação de código de análise estática.
- Realizar revisões de código.

A atenção especial fica em relação ao fato de que não se considera a aplicação de ferramentas de verificação de código de análise dinâmica nessa fase.

4. FASE DE VERIFICAÇÃO

A fase de verificação é o ponto em que o software está funcionalmente concluído e entra em testes beta por usuários. Durante essa fase, enquanto o software passa por testes beta, a equipe de produto realiza um "esforço de segurança" que inclui revisões do código de segurança além das concluídas na fase de implementação, bem como testes de segurança direcionados.

5. FASE DE SUPORTE E MANUTENÇÃO

Apesar da aplicação do SDL durante o desenvolvimento, as práticas de desenvolvimento mais avançadas ainda não dão suporte ao fornecimento de software completamente livre de vulnerabilidades, e há bons motivos para acreditarmos que isso nunca acontecerá.

Mesmo que o processo de desenvolvimento pudesse eliminar todas as vulnerabilidades do software fornecido, novos ataques seriam descobertos e o software que era "seguro" estaria vulnerável. Assim, as equipes de produto devem se preparar para responder a vulnerabilidades recém-descobertas no software fornecido aos clientes.

Parte do processo de resposta envolve a preparação para avaliar relatórios de vulnerabilidades e lançar orientações e atualizações de segurança quando apropriado. O outro componente do processo de resposta é a condução de um post-mortem das vulnerabilidades relatadas e a adoção de medidas, conforme necessário.

As medidas em resposta a uma vulnerabilidade variam de emitir uma atualização para um erro isolado até atualizar as ferramentas de verificação de código e iniciar revisões do código dos principais subsistemas.

O objetivo durante a fase de resposta é aprender a partir dos erros e utilizar as informações fornecidas em relatórios de vulnerabilidade para ajudar a detectar e eliminar mais vulnerabilidades antes que sejam descobertas no campo e utilizadas para colocar os clientes em risco.

O processo de resposta também ajuda a equipe de produto e a equipe de segurança a adaptar processos de forma que erros semelhantes não sejam introduzidos no futuro

Referência:

https://learn.microsoft.com/pt-br/compliance/assurance/assurance-microsoft-security-development-lifecycle

CLASP (Comprehensive, Lightweight Application Security Process)

O CLASP (Comprehensive, Lightweight Application Security Process) é uma metodologia de desenvolvimento seguro de software orientada a atividades e papéis, que descreve melhores práticas para projetos novos ou em andamento.

São propostas 24 atividades divididas em componentes de processos discretos ligados a um ou mais papéis de um projeto. Desta forma, o CLASP provê um guia para participantes de um projeto: gerentes, auditores de segurança, desenvolvedores, arquitetos e testadores, entre outros.

A estrutura do processo é dividida em cinco perspectivas, denominadas Visões CLASP. Cada Visão, por sua vez, é dividida em atividades, que contém os componentes do processo. São as Visões:

- Visão Conceitual
- Visão de Papéis
- Visão de Avaliação de Atividade
- Visão de Implementação de Atividade
- Visão de Vulnerabilidades

As visões também são referenciadas como Conjuntos de Taxonomias de vulnerabilidades a serem consideradas no desenvolvimento do software.

A Visão Conceitual apresenta uma visão geral de como funciona o processo CLASP e como seus componentes interagem. São introduzidas as melhores práticas, a interação entre o CLASP e as políticas de segurança, alguns conceitos de segurança e os componentes do processo.

A Visão de Papéis introduz as responsabilidades básicas de cada membro do projeto (gerente, arquiteto, especificador de requisitos, projetista, implementador, analista de testes e auditor de segurançA) relacionando-os com as atividades propostas, além de especificar quais são os requerimentos básicos para que cada função seja desempenhada.

A Visão de Avaliação de Atividades descreve o propósito de cada atividade, bem como os responsáveis, contribuidores, a aplicabilidade, o impacto relativo, os riscos em caso de omissão da atividade, a frequência da atividade e sugere uma aproximação do valor para homens/hora.

A Visão de Implementação descreve o conteúdo das 24 atividades de segurança definidas pelo CLASP e identifica os responsáveis pela implementação, bem como as atividades relacionadas.

A Visão de Vulnerabilidades possui um catálogo que descreve 104 tipos de vulnerabilidades no desenvolvimento de software, divididas em 5 categorias:

- Erros de Tipo e Limites de Tamanho
- Problemas do Ambiente
- Erros de Sincronização e Temporização
- Erros de Protocolo
- Erros lógicos em geral.

Referência(s):

1. https://www.firemountaingems.com/learn/categories/jewelry-medium/bead-stringing/about-bead-stringing/8B6H-article.html
2. https://github.com/google/clasp

OWASP SAMM (Software Assurance Maturity Model)

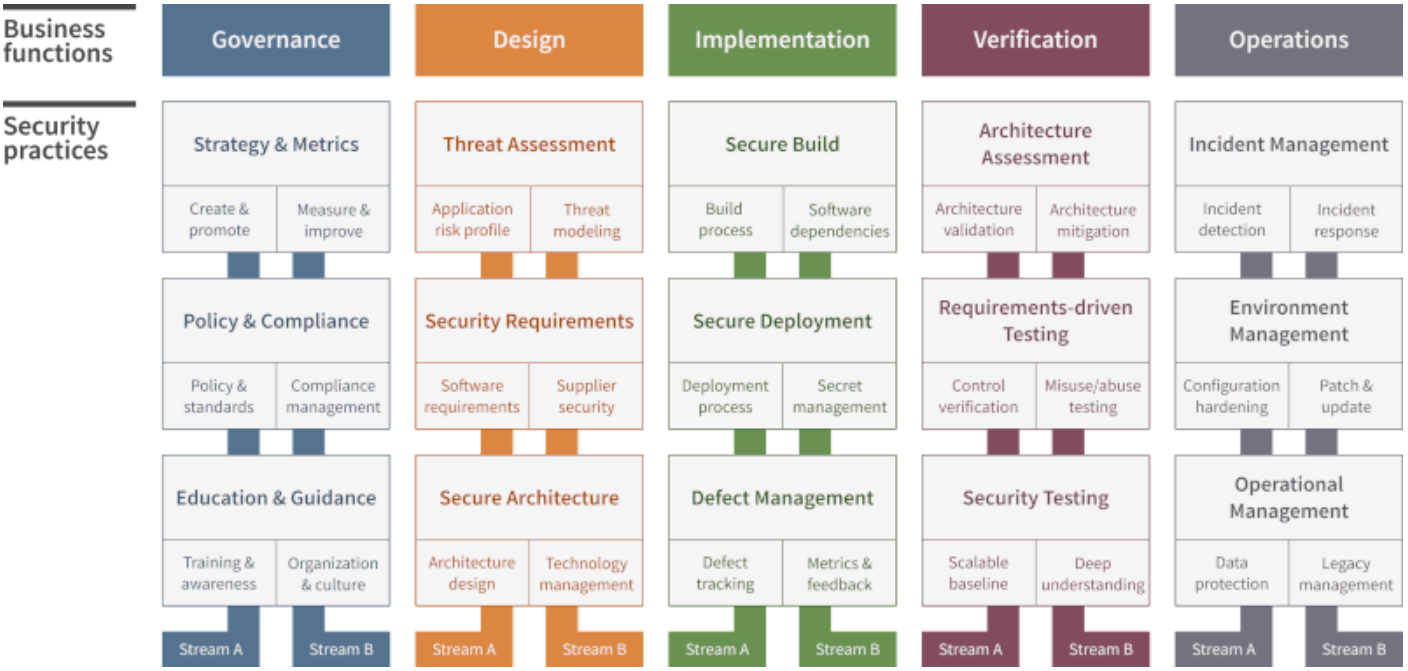
O OWASP SAMM (Software Assurance Maturity Model) é um modelo aberto que auxilia organizações a formular e implementar uma estratégia para a segurança de software, adaptada aos riscos específicos enfrentados pela organização. O modelo é agnóstico em relação a tecnologias e processos, orientado por riscos e evolução, apoiando o ciclo de vida completo do desenvolvimento e aquisição de software.

Como já vimos em diferentes contextos, a segurança de software é um componente crítico no desenvolvimento de sistemas confiáveis. O OWASP SAMM oferece um caminho estruturado para organizações melhorarem suas práticas de segurança de software.

Observando as suas principais características, portanto, vale destacar que o SAMM permite que as organizações:

- Avaliem suas práticas existentes de segurança de software.
- Construam um programa equilibrado de garantia de segurança em iterações bem definidas.
- Demonstrem melhorias concretas no programa de garantia de segurança.
- Definam e meçam atividades relacionadas à segurança em toda a organização.

O SAMM é dividido em cinco áreas de negócio, cada uma com três objetivos de segurança.



Para cada objetivo, há três níveis de maturidade, fornecendo um total de 45 atividades de segurança. As organizações podem usar o SAMM para criar um roteiro de melhorias incrementais, medindo o progresso ao longo do tempo.

Trazendo uma perspectiva de vantagens a respeito do seu uso, destaca-se a capacidade de personalizar a abordagem de segurança para atender às necessidades específicas da organização e a possibilidade de medir a maturidade da segurança de software de forma eficaz. Os desafios podem incluir a necessidade de comprometimento organizacional e recursos para implementar e manter o programa.

Comparado a outros modelos como o BSIMM, que é descritivo e baseado em práticas observadas, o SAMM é prescritivo, oferecendo um caminho estruturado para melhorar a segurança de software. Enquanto o BSIMM pode ser usado para benchmarking e referência, o SAMM fornece um roteiro para ação.

- ESTRUTURA DE FUNCIONAMENTO

Conforme já vimos na introdução, o OWASP SAMM (Software Assurance Maturity Model) é estruturado em torno de cinco pilares de negócio, cada um abrangendo práticas de segurança específicas. Vamos trazer um resumo dos principais pontos em cada um deles:

1. Governança (Governance):
    - Estratégia e Métricas: Estabelecer e manter uma estratégia de segurança de software alinhada com os objetivos de negócio.
    - Educação e Orientação: Assegurar que todos os envolvidos compreendam suas responsabilidades relacionadas à segurança de software.
    - Política e Conformidade: Desenvolver e aplicar políticas de segurança de software que estejam em conformidade com os requisitos legais e regulatórios.

2. Desenho (Design):
    - Requisitos de Segurança: Identificar e incorporar requisitos de segurança durante a fase de design.
    - Arquitetura de Segurança: Definir e manter uma arquitetura de software que suporte os requisitos de segurança.
    - Modelagem de Ameaças: Realizar análises de ameaças para identificar e mitigar riscos potenciais.

3. Implementação (Implementation):
    - Padrões de Codificação Segura: Utilizar e aplicar padrões de codificação segura para reduzir vulnerabilidades.
    - Revisão de Código de Segurança: Realizar revisões de código para identificar e corrigir problemas de segurança.
    - Teste de Segurança do Software: Testar o software para garantir que os requisitos de segurança sejam atendidos.

4. Verificação (Verification):
    - Revisão de Requisitos de Segurança: Verificar se todos os requisitos de segurança foram atendidos.
    - Teste de Segurança: Executar testes de segurança abrangentes para identificar e mitigar vulnerabilidades.
    - Análise de Segurança Operacional: Avaliar a segurança do software em seu ambiente operacional.

5. Operações (Operations):
    - Gerenciamento de Incidentes: Estabelecer e manter um processo eficaz para a detecção e resposta a incidentes de segurança.
    - Gerenciamento de Ambiente: Proteger o ambiente operacional contra ameaças de segurança.
    - Melhoria Operacional: Implementar processos para garantir a melhoria contínua da segurança do software.

Cada pilar e seus respectivos objetivos são fundamentais para a construção de um programa de segurança de software robusto e eficaz.

- NÍVEIS DE MATURIDADE

O OWASP SAMM define três níveis de maturidade para cada prática de segurança, que são generalizados como fundacional, maduro e avançado. Esses três níveis são divididos para cada um dos objetivos, conforme um dos exemplos abaixo:

Governance

Activities Overview

Stream A **Create & Promote**	Stream B **Measure & Improve**
Maturity level 1 Identify objectives and means of measuring effectiveness of the security program.	
Identify organization drivers as they relate to the organization's risk tolerance.	Define metrics with insight into the effectiveness and efficiency of the Application Security Program.
Maturity level 2 Establish a unified strategic roadmap for software security within the organization.	
Publish a unified strategy for application security.	Set targets and KPI's for measuring the program effectiveness.
Maturity level 3 Align security efforts with the relevant organizational indicators and asset values.	
Align the application security program to support the organization's growth.	Influence the strategy based on the metrics and organizational needs.

Sendo assim, para um conhecimento aprofundado e detalhados, não há outra alternativa a não ser ler o documento em sua íntegra no link:

https://owaspsamm.org/model/

https://drive.google.com/file/d/1cI3Qzfrly_X89z7StLWI5p_Jfqs0-OZv/view?usp=sharing

Trazendo um resumo sobre os diferentes níveis, podemos dizer que cada nível possui objetivos progressivamente mais sofisticados, atividades específicas e métricas de sucesso mais rigorosas. Assim são os três níveis de maturidade:

1. Nível Fundacional (Nível 1):
    - Objetivo: Estabelecer as bases para a segurança de software.
    - Atividades: Implementar práticas básicas de segurança e conscientização.
    - Métricas: Foco em alcançar a conformidade com requisitos mínimos de segurança.
2. Nível Maduro (Nível 2):
    - Objetivo: Desenvolver e aprimorar processos de segurança de software.
    - Atividades: Integrar segurança de forma mais profunda no ciclo de vida do desenvolvimento.
    - Métricas: Medir a eficácia das práticas de segurança e fazer melhorias contínuas.
3. Nível Avançado (Nível 3):
    - Objetivo: Otimizar e liderar com práticas de segurança inovadoras.
    - Atividades: Implementar processos de segurança sofisticados e proativos.
    - Métricas: Buscar a excelência em segurança e ser um modelo para outras organizações.

Esses níveis de maturidade ajudam as organizações a avaliar onde estão em termos de segurança de software e a planejar melhorias incrementais para alcançar uma postura de segurança mais robusta e eficaz.

Referência:

https://owasp.org/www-project-samm/

BSIMM - Building Security in Maturity Model

O BSIMM, ou Building Security in Maturity Model, atualmente em sua versão 14, é um modelo descritivo que fornece uma linha de base de atividades observadas para iniciativas de segurança de software. Este modelo não é um padrão ou uma lista de verificação, mas sim um reflexo das práticas atuais observadas em programas reais de segurança de software. Tal análise é composta por diferentes perfis, mas há um destaque de centenas de milhares de desenvolvedores e algumas dezenas de milhares de profissionais de segurança da informação.

No mundo do desenvolvimento de software, o BSIMM ajuda a analisar e comparar programas de segurança de software contra mais de 130 organizações em vários setores industriais, fornecendo uma análise objetiva e baseada em dados para tomar decisões sobre recursos, tempo, orçamento e prioridades na melhoria da postura de segurança.

O BSIMM mede a maturidade de um programa de segurança de software contra 126 atividades específicas, permitindo que as organizações avaliem seu nível de maturidade e comparem suas necessidades e capacidades de segurança com outros programas de segurança de software. Diferentemente de outros frameworks, o BSIMM é descritivo, não prescritivo, documentando práticas atuais em vez de prescrever o que um pequeno grupo de especialistas acredita que deveria ser feito.

Conforme já antecipamos, o BSIMM ajuda as organizações a entenderem seus pontos fortes e fracos e quais áreas priorizar com base em riscos e capacidades específicas da organização. O próximo passo é desenvolver um Plano de Ação de Maturidade (MAP) com etapas detalhadas para atender aos objetivos de segurança de software da organização.

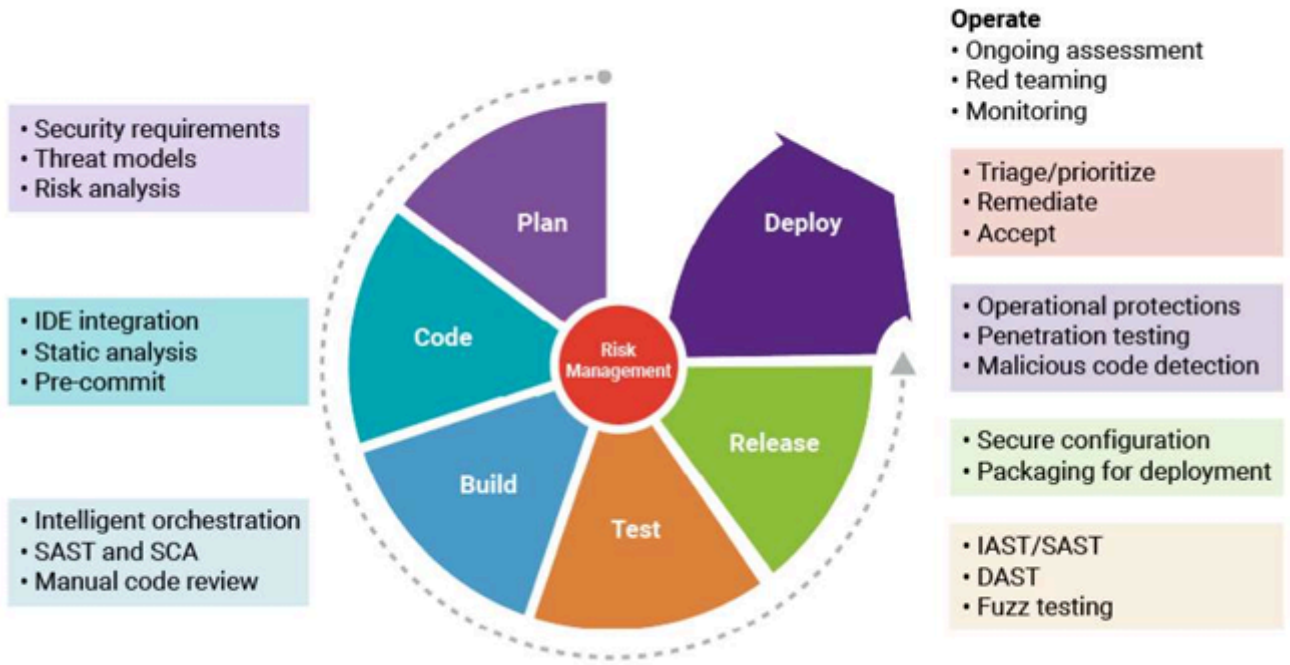
As vantagens do BSIMM incluem a capacidade de compartilhar rapidamente a postura de segurança de software com as partes interessadas, oferecendo detalhes concretos para mostrar a executivos, membros do conselho, clientes, parceiros e reguladores como os esforços estão fazendo a diferença na postura de segurança da organização. Os desafios podem incluir a necessidade de adaptar as práticas observadas às necessidades específicas da organização e garantir que as atividades de segurança sejam integradas ao ciclo de vida do desenvolvimento de software.

Enquanto o BSIMM fornece um modelo baseado em dados para iniciativas de segurança de software, outras tecnologias e frameworks, como o OWASP SAMM (Software Assurance Maturity Model), também oferecem abordagens para avaliar e melhorar a segurança de software. O OWASP SAMM, por exemplo, é um framework prescritivo que fornece um caminho para organizações implementarem práticas de segurança de software de acordo com os melhores padrões da indústria.

Caso você ainda esteja se perguntando a diferença prática de frameworks descritivos e prescritivos,temos que os frameworks descritivos focam sobre entender e relatar o que acontece, com base em análise de contextos e focos de observação, sem julgamentos e com capacidade dinâmica e rápida de atualização. Já os prescritivos são sobre estabelecer como as coisas devem ser feitas, trazendo uma visão de normatização ou padronização melhores definidas, e por esse motivo, são mais rígidas no processo. Ambas as abordagens têm suas vantagens e são escolhidas com base nos objetivos e necessidades específicas

Trazendo uma questão mais específica do framework e do relatório, observamos:

1. SBOMs - Software Bill of Materials: Também pode ser entendido como componentes que são utilizados na estrutura de desenvolvimento de código como bibliotecas e dependências de software em geral. O relatório aponta um crescimento de 22% deste tipo de recurso, o que implica em uma necessidade de tratamento desse tipo de solução, e buscar um amplo domínio de seu inventário de software.
2. Gestão de Risco de OSS: Crescimento de 10% nas atividades de gestão de risco de software de código aberto. Isso traz ações específicas de gestão de riscos com softwares abertos para identificação e controle destes riscos como camada básica.
3. Segurança na Nuvem: Ferramentas de segurança na nuvem são essenciais para melhorar a postura de segurança.
4. Testes Contínuos: Importância de testes contínuos em múltiplos pontos do pipeline, totalmente aderentes à evolução do produto junto ao negócio a ser aplicado. Espera-se a utilização de ferramentas para escalar esses testes conforme necessidade, com recursos de automação e orquestração das soluções.



Referência(a):

https://www.synopsys.com

OWASP Secure Coding Practices

Antes de iniciarmos esse bloco, é importante conceituar o que vem a ser o OWASP (Open Web Application Security Project). O OWASP é uma fundação sem fins lucrativos que trabalha para melhorar a segurança de softwares. É uma referência global em vários eixos de atuação, e tem sido referenciado diretamente e explicitamente em provas, e também em questões. Suas atuações são diversas frente ao escopo de atuação. Sem dúvida, seu grande destaque é o monitoramento e geração de relatórios dos conhecidos TOP 10 ataques e vulnerabilidades exploradas, ano após ano.

Entretanto, este não será o assunto do bloco, mas sim, as suas referências práticas para desenvolvimento de códigos seguros.

A OWASP, reforçando, é uma comunidade aberta dedicada a permitir que as organizações concebam, desenvolvam, adquiram, operem e mantenham aplicativos confiáveis. Todos os projetos, ferramentas, documentos, fóruns e capítulos são gratuitos e abertos a qualquer pessoa interessada em melhorar a segurança de aplicativos. A Fundação OWASP foi lançada em 1° de dezembro de 2001, tornando-se uma instituição de caridade sem fins lucrativos dos Estados Unidos em 21 de abril de 2004.

Voltando o nosso foco às práticas seguras de desenvolvimento, destacamos primeiramente a sua característica agnóstica, ou seja, não há vínculo ou restrição com tecnologias específicas. Trata-se de um checklist que pode ser integrado em qualquer ciclo de desenvolvimento. Na sua concepção, o objetivo foi gerar um documento simples e enxuto, capaz de ser facilmente compreendido e absorvido pelas instituições.

Abaixo, você encontra o link com todas as práticas que são recomendadas nesse escopo.

https://www.owasp.org/index.php/Testing_Guide_Introduction#Principles_of_Testing

Referência(a):

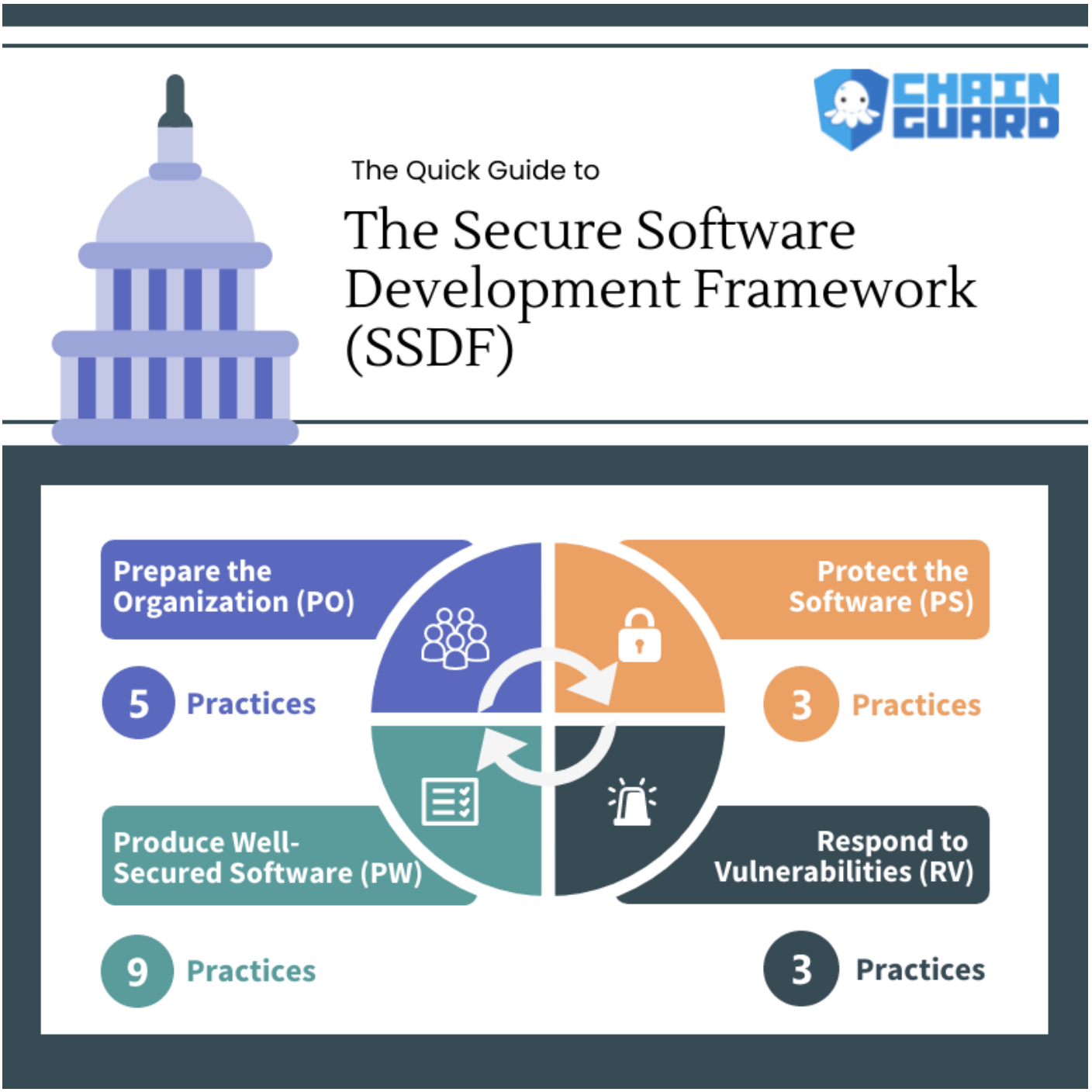
https://www.owasp.org/index.php/Testing_Guide_Introduction#Principles_of_Testing

NIST SSDF - Secure Software Development Framework

O NIST SSDF é um conjunto de práticas recomendadas para desenvolvimento de software seguro, publicado pelo NIST. Ele visa ajudar os desenvolvedores a reduzir vulnerabilidades em software, mitigando os riscos de exploração e abordando as causas raízes dessas vulnerabilidades.

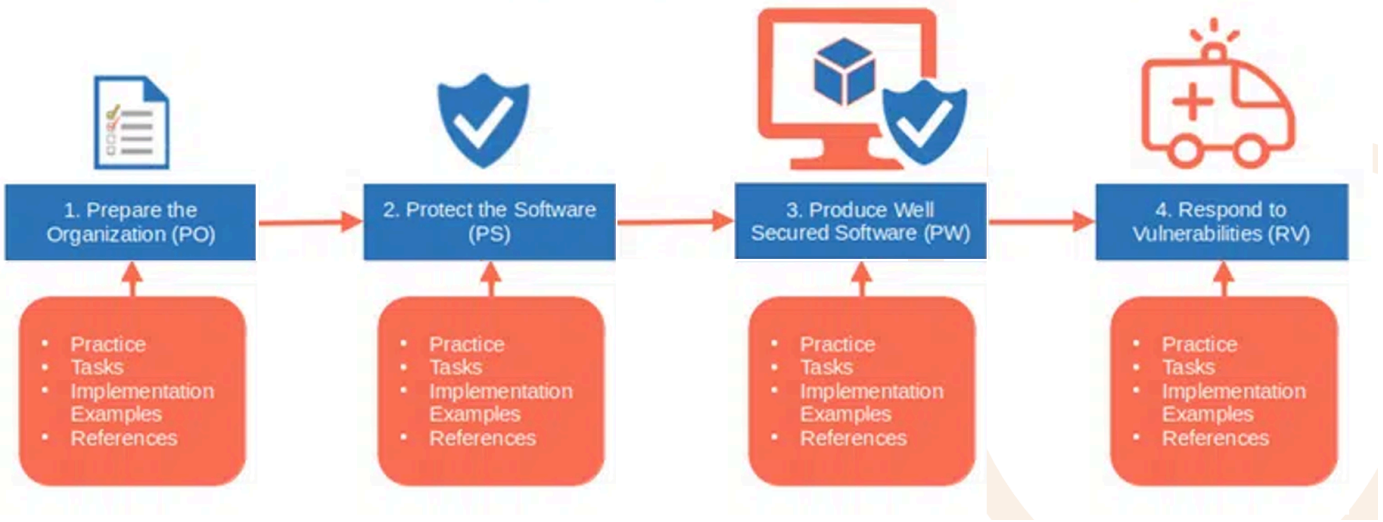
O SSDF é organizado em quatro grupos principais de práticas:

1. *Prepare the Organization (PO) - Prepare sua Organização*
   - Objetivo: Preparar a organização, seus processos e tecnologias para desenvolvimento de software seguro.
   - Práticas: Treinamento de pessoal, definição de políticas de segurança, configuração de ferramentas de segurança.
2. *Protect the Software (PS) - Proteja o Software*
   - Objetivo: Proteger todos os componentes do software contra adulteração e acesso não autorizado.
   - Práticas: Uso de ferramentas de análise estática e dinâmica, implementação de controles de segurança, proteção de dados sensíveis.
3. *Produce Well-Secured Software (PW) - Produza um software seguro*
   - Objetivo: Produzir software bem protegido com mínimas vulnerabilidades.
   - Práticas: Revisão de código, testes de segurança, integração contínua e entrega contínua (CI/CD).
4. *Respond to Vulnerabilities (RV) - Responda às vulnerabilidades*
   - Objetivo: Identificar vulnerabilidades residuais e responder adequadamente para prevenir futuras ocorrências.
   - Práticas: Monitoramento contínuo, resposta a incidentes, atualização e manutenção de software.

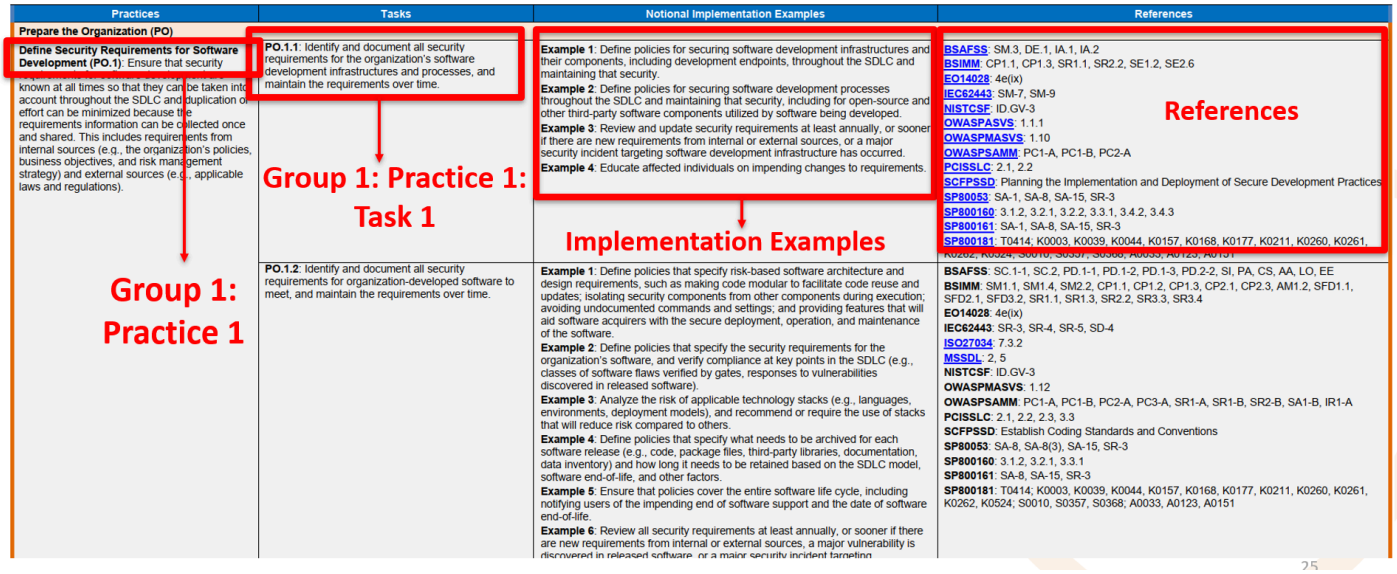


Conforme já vimos, há diversas práticas distribuídas em cada área. Ainda, dentro de cada área, a norma estrutura as práticas em:

1. Prática: Uma frase curta resumindo Objetivos, Formas de alcançá-los, Papéis e Responsabilidades
2. Tarefas: Descrever as ações necessárias para cumprir a prática
3. Exemplos de Implementação: Descreve como implementar as tarefas com todas as possibilidades
4. Referências: Referências e links para documentação relacionada aos exemplos de implementação listados



A imagem a seguir nos dá um exemplo desse processo:



Tentando destacar alguns benefícios do SSDF, podemos citar:

- Redução de Vulnerabilidades: Seguindo as práticas do SSDF, os desenvolvedores podem reduzir significativamente o número de vulnerabilidades em software.
- Mitigação de Impacto: As práticas ajudam a mitigar o impacto de vulnerabilidades não detectadas ou não tratadas.
- Comunicação Melhorada: O SSDF fornece uma linguagem comum para descrever práticas de desenvolvimento seguro, facilitando a comunicação entre desenvolvedores e compradores de software.
- Redução de custos: Identificar e corrigir vulnerabilidades no início do ciclo de desenvolvimento é mais barato do que lidar com as consequências de um ataque após o lançamento do software.
- Melhoria da Qualidade do Software: O SSDF promove a criação de software mais robusto e confiável, reduzindo o número de falhas e vulnerabilidades.
- Proteção da Reputação: Softwares seguros protegem a reputação da organização, evitando incidentes de segurança que podem prejudicar a confiança dos clientes.

- Conformidade com Regulamentações: O SSDF ajuda as organizações a cumprir os requisitos de conformidade, como a Lei Geral de Proteção de Dados (LGPD).

Considerando ainda as boas práticas de utilização de esteiras de desenvolvimento, ele pode ser integrado com Modelos de Ciclo de Vida de Desenvolvimento de Software (SDLC), isto é, o SSDF pode ser integrado a qualquer modelo de SDLC, como Agile, DevOps, Waterfall, etc. Isso garante que práticas de segurança sejam incorporadas em todas as fases do desenvolvimento.

Bom, mergulhando um pouco mais, portanto, vamos conhecer as principais atividades de cada um dos grupos:

Grupo 1: Preparar a Organização (PO)

O primeiro grupo de práticas (Grupo 1) no NIST SSDF é conhecido como POs, que se refere a pessoas, processos e ferramentas, e foca na capacidade organizacional de produzir software seguro. Há cinco práticas no Grupo 1, de PO.1 a PO.5, conforme segue:

1. PO.1: Definir Requisitos de Segurança para o Desenvolvimento de Software

PO.1 considera as necessidades de segurança ao longo de todo o ciclo de vida do desenvolvimento de software (SDLC). Inclui fatores internos, como as políticas da organização, metas de negócios e estratégias de gerenciamento de riscos, assim como quaisquer fatores externos, como leis e regulamentos relevantes. Ao seguir o PO.1, as equipes de desenvolvimento podem minimizar a duplicação de esforços, pois as informações sobre os requisitos podem ser coletadas uma única vez e compartilhadas.

PO.2: Implementar Papéis e Responsabilidades

PO.2 foca na definição dos papéis necessários, revisão, manutenção e atualização periódica dos papéis definidos. Fornece diretrizes sobre o treinamento de pessoal baseado em papéis, para garantir que todos os envolvidos no SDLC estejam prontos para desempenhar suas funções e responsabilidades.

PO.3: Implementar Cadeias de Ferramentas de Suporte

PO.3 se destina ao uso de cadeias de ferramentas e ferramentas automatizadas em diferentes níveis, como em toda a organização ou específicas de um projeto, e aborda uma parte particular do SDLC. O principal objetivo é reduzir o esforço humano e os erros humanos, ao mesmo tempo em que melhora a precisão, reprodutibilidade, usabilidade e abrangência das práticas de segurança ao longo do SDLC.

PO.4: Definir e Usar Critérios para Verificações de Segurança de Software

A segurança do software deve ser verificada durante o desenvolvimento, e os desenvolvedores de software devem definir e usar critérios para verificar a segurança do software, a fim de garantir que ele atenda às expectativas da organização. O PO.4 foca em fornecer diretrizes para verificações de segurança de software.

PO.5: Implementar e Manter Ambientes Seguros para o Desenvolvimento de Software

O PO.5 garante que todos os componentes dos ambientes para o desenvolvimento de software (ambientes de construção, desenvolvimento, teste e distribuição) estejam fortemente protegidos contra ameaças internas e externas. Ele mitiga o risco de comprometimento do ambiente de desenvolvimento, aderindo a melhores práticas, como o princípio do menor privilégio.

2. Grupo 2: Proteger o Software (PS)

O segundo grupo de práticas (Grupo 2) no NIST SSDF é conhecido como PSs, que foca na integridade do software e em garantir que os produtos sejam feitos de forma segura em todas as etapas do processo de desenvolvimento de software. Há três práticas no Grupo 2, de PS.1 a PS.3, conforme segue:

PS.1: Proteger Todas as Formas de Código Contra Acesso Não Autorizado e Manipulação

PS.1 foca na proteção do código-fonte contra alterações não autorizadas, que podem ser acidentais ou intencionais, com o objetivo de prevenir furtos e reduzir ao mínimo as vulnerabilidades no software. O PS.1 recomenda ter avisos como "não destinado a ser acessível publicamente" para código privado ou proprietário.

PS.2: Fornecer um Mecanismo para Verificar a Integridade da Liberação de Software

PS.2 visa apoiar os adquirentes de software (por exemplo, o Governo Federal) a verificar a autenticidade e a integridade do software que compram. Ele garante que o software esteja livre de quaisquer modificações não autorizadas ou manipulações.

PS.3: Arquivar e Proteger Cada Liberação de Software

PS.3 foca na preservação das liberações de software para ajudar a identificar, analisar e eliminar vulnerabilidades descobertas no software após a liberação.

3. Grupo 3: Produzir Software Bem Protegido (PW)

O terceiro grupo de práticas (Grupo 3) no NIST SSDF é conhecido como PWs, que se concentra em projetar, escrever e testar software seguro. Inclui técnicas relacionadas a revisão de código, revisão de design e seleção de componentes. Além disso, fornece orientações sobre a manutenção da cadeia de ferramentas. Há nove práticas no Grupo 3, de PW.1 a PW.9, conforme segue:

PW.1: Projetar Software para Atender aos Requisitos de Segurança e Mitigar Riscos de Segurança

Abordar os requisitos de segurança e riscos durante o design do software (seguro por design) é fundamental para melhorar a segurança do software e também ajuda a aumentar a eficiência do desenvolvimento. O PW.1 visa identificar e avaliar os requisitos de segurança para o software. Ele determina quais riscos de segurança o software provavelmente enfrentará durante a operação e como o design e a arquitetura do software devem mitigar esses riscos. Além disso, fornece justificativa para quaisquer casos em que a análise baseada em riscos indique que os requisitos de segurança devem ser relaxados ou dispensados.

PW.2: Revisar o Design do Software para Verificar a Conformidade com os Requisitos de Segurança e Informações de Risco

PW.2 garante que o software atenda aos requisitos de segurança e aborde adequadamente as informações de risco identificadas. Ele cria uma lista de materiais de software para ajudar a auditar cada componente incluído quanto às informações de risco.

PW.3: Verificar se o Software de Terceiros Está em Conformidade com os Requisitos de Segurança

As tarefas do PW.3 foram transferidas para o PO.1 e PW.4.

PW.4: Reutilizar Software Existente e Bem Protegido Sempre que Viável, em vez de Duplicar Funcionalidades

PW.4 tem como objetivo reduzir o custo de desenvolvimento de software, aumentar a velocidade de desenvolvimento e diminuir a probabilidade de introduzir vulnerabilidades de segurança adicionais no software, reutilizando seus módulos e serviços de software que já passaram por avaliações de segurança. Minimizar exposições é importante para software que implementa funcionalidades de segurança, como módulos e protocolos criptográficos.

PW.5: Criar Código-Fonte Adotando Práticas de Codificação Segura

PW.5 foca em diminuir o número de vulnerabilidades de segurança no software e reduzir custos, minimizando vulnerabilidades introduzidas durante a criação do código-fonte que atendem ou excedem os critérios de severidade de vulnerabilidade definidos pela organização, aderindo às Práticas de Codificação Segura.

PW.6: Configure a Compilação, o Interpretador e os Processos de Construção para Melhorar a Segurança dos Executáveis

PW.6 foca em diminuir o número de vulnerabilidades de segurança nos compiladores e interpretadores e reduzir custos ao eliminar vulnerabilidades antes da fase de testes.

PW.7: Revisar e Analisar Código Legível por Humanos para Identificar Vulnerabilidades e Verificar Conformidade com os Requisitos de Segurança

PW.7 busca identificar vulnerabilidades em códigos legíveis por humanos para que as equipes de desenvolvimento possam corrigi-las antes de lançar o software, a fim de prevenir explorações. Código legível por humanos inclui código-fonte, scripts e qualquer outra forma que uma organização considere legível por humanos. PW.7 incentiva o uso de métodos automatizados, que reduzem o esforço e os recursos necessários para detectar vulnerabilidades.

PW.8: Testar Código Executável para Identificar Vulnerabilidades e Verificar Conformidade com os Requisitos de Segurança

PW.8 busca identificar vulnerabilidades em códigos executáveis para que os desenvolvedores possam corrigi-las antes de lançar o software, a fim de prevenir explorações. Código executável inclui binários, bytecode executado diretamente e código-fonte, além de qualquer outra forma que uma organização considere executável.

PW.9: Configurar Software para Ter Configurações Seguras por Padrão

PW.9 foca em melhorar a segurança do software no momento da instalação para reduzir a probabilidade de que o software seja implantado com configurações de segurança fracas, colocando-o em maior risco de comprometimento.

4. Grupo 4: Responder às Vulnerabilidades (RV)

O quarto grupo de práticas (Grupo 4) no NIST SSDF é conhecido como RVs, e foca em responder às vulnerabilidades, incluindo mitigar, reduzir o impacto e recuperar. Existem três práticas no Grupo 4, de RV.1 a RV.3, conforme descrito a seguir:

RV.1: Identificar e Confirmar Vulnerabilidades de Forma Contínua

RV.1 destaca a importância de identificar continuamente as vulnerabilidades de forma rápida e abordá-las de acordo com o nível de risco. Isso garante um prazo mais curto para a remediação, ao mesmo tempo em que reduz a janela de oportunidade para potenciais ataques.

RV.2: Avaliar, Priorizar e Remediar Vulnerabilidades

RV.2 assegura que as organizações remediem as vulnerabilidades de software de acordo com o nível de risco, para reduzir a janela de oportunidade para os atacantes.

RV.3: Analisar Vulnerabilidades para Identificar suas Causas Raiz

RV.3 visa reduzir a frequência de vulnerabilidades no futuro, refinando iterativamente o processo de desenvolvimento de software. Isso ajudará a organização a prevenir que a mesma exposição ocorra novamente e a ajustar o processo de gerenciamento de vulnerabilidades.

Ainda, o NIST traz algumas práticas transversais recomendadas a serem observadas:

- Treinamento em Codificação Segura: Desenvolvedores devem receber treinamento sobre práticas de codificação segura, incluindo como evitar vulnerabilidades comuns, como injeção de SQL, cross-site scripting (XSS) e estouro de buffer.
- Revisão de Código: Revisões de código devem ser realizadas para identificar potenciais vulnerabilidades e garantir a conformidade com os padrões de codificação segura. Ferramentas de análise estática podem auxiliar nesse processo.
- Testes de Segurança: Diferentes tipos de testes de segurança, como testes de penetração, testes de fuzzing e testes de unidade de segurança, devem ser realizados para identificar e corrigir vulnerabilidades.
- Gerenciamento de Dependências: As dependências de software devem ser gerenciadas cuidadosamente para garantir que estejam atualizadas e livres de vulnerabilidades conhecidas.
- Análise de Arquitetura: A arquitetura do software deve ser analisada para identificar potenciais riscos de segurança e garantir que os controles de segurança adequados sejam implementados.
- Proteção de Dados: Dados sensíveis devem ser protegidos usando técnicas como criptografia e controle de acesso.
- Monitoramento de Segurança: O software deve ser monitorado continuamente para detectar atividades suspeitas e responder a incidentes de segurança.

Questões Comentadas - Desenvolvimento Seguro de Aplicações - CESPE

1. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

Comentários:

Conforme vimos, a segurança e controle dos formatos de senhas permitidas pelos usuários faz parte de um processo seguro de uma aplicação. Mencionamos ainda que na prática, utiliza-se oito caracteres como uma quantidade segura, entretanto, algumas aplicações e examinadores consideram seis como uma quantidade suficiente.

Gabarito: C

---

2. (CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

A modelagem de ameaças se dá na fase de DESIGN. Lembremos os principais aspectos considerados nessa fase:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

---

3. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

---

4. (CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

É uma das definições apresentadas para o CLASP, complementada por suas VISÕES do software, conforme vimos em nossa teoria.

Gabarito: C

QUESTÕES COMENTADAS - DESENVOLVIMENTO SEGURO DE APLICAÇÕES - FCC

1. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

Comentários:

Conforme vimos, a segurança e controle dos formatos de senhas permitidas pelos usuários faz parte de um processo seguro de uma aplicação. Mencionamos ainda que na prática, utiliza-se oito caracteres como uma quantidade segura, entretanto, algumas aplicações e examinadores consideram seis como uma quantidade suficiente.

Gabarito: C

---

2. (CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

A modelagem de ameaças se dá na fase de DESIGN. Lembremos os principais aspectos considerados nessa fase:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

---

3. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

---

4. (CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

É uma das definições apresentadas para o CLASP, complementada por suas VISÕES do software, conforme vimos em nossa teoria.

Gabarito: C

QUESTÕES COMENTADAS - DESENVOLVIMENTO SEGURO DE APLICAÇÕES - CESPE

1. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

Comentários:

Conforme vimos, a segurança e controle dos formatos de senhas permitidas pelos usuários faz parte de um processo seguro de uma aplicação. Mencionamos ainda que na prática, utiliza-se oito caracteres como uma quantidade segura, entretanto, algumas aplicações e examinadores consideram seis como uma quantidade suficiente.

Gabarito: C

---

2. (CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

A modelagem de ameaças se dá na fase de DESIGN. Lembremos os principais aspectos considerados nessa fase:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

---

3. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

---

4. (CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

É uma das definições apresentadas para o CLASP, complementada por suas VISÕES do software, conforme vimos em nossa teoria.

Gabarito: C

QUESTÕES COMENTADAS - DESENVOLVIMENTO SEGURO DE APLICAÇÕES - FCC

1. (CESPE – CNJ/Técnico Judiciário – Programação de Sistemas/2013) Para aumentar a segurança de um programa, deve-se evitar o uso de senhas consideradas frágeis, como o próprio nome e identificador de usuário, sendo recomendada a criação de senhas consideradas fortes, ou seja, aquelas que incluem, em sua composição, letras (maiúsculas e minúsculas), números e símbolos embaralhados, totalizando, preferencialmente, mais de seis caracteres.

Comentários:

Conforme vimos, a segurança e controle dos formatos de senhas permitidas pelos usuários faz parte de um processo seguro de uma aplicação. Mencionamos ainda que na prática, utiliza-se oito caracteres como uma quantidade segura, entretanto, algumas aplicações e examinadores consideram seis como uma quantidade suficiente.

Gabarito: C

---

2. (CESPE – TCE-PA/Auditor de Controle Externo – Informática/2016) Na metodologia de desenvolvimento seguro de software SDL (Security Development Lifecycle), a modelagem de ameaças é realizada na fase de requisitos.

Comentários:

A modelagem de ameaças se dá na fase de DESIGN. Lembremos os principais aspectos considerados nessa fase:

- Definir as diretivas de design e arquitetura de segurança;
- Documentar os elementos da superfície de ataque do software;
- Realizar a modelagem de ameaças;
- Definir critérios de fornecimento complementar.

Gabarito: E

---

3. (CESPE – CNJ/Analista Judiciário – Análise de Sistemas/2013) O SDL é um processo de desenvolvimento de software seguro, que envolve a adição de produtos e atividades, como o desenvolvimento de modelos de ameaças.

Comentários:

Essa é a definição básica do processo contemplado pelo SDL.

Gabarito: C

---

4. (CESPE – Polícia Federal/Perito Criminal Federal – Cargo 3/2013) O CLASP (Comprehensive, Lightweight Application Security Process) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Comentários:

É uma das definições apresentadas para o CLASP, complementada por suas VISÕES do software, conforme vimos em nossa teoria.

Gabarito: C

SAST (Static Application Security Testing)

Avançando na nossa discussão a respeito da criação de softwares seguros, vamos conversar um pouco a respeito de ferramentas de testes que podem ser utilizadas para tais finalidades.

O primeiro agrupamento deste tipo de solução é conhecido como SAST, ou em sua tradução literal, "aplicação estática para teste de segurança".

Quando nos remetemos ao conceito de estático, imediatamente vinculamos o código gerado para as aplicações e softwares em geral. Essas ferramentas de análise também são conhecidas como "Ferramentas de análise de Código Fonte".

Então até aqui não temos muito segredo. O seu propósito é avaliar o código fonte e as diversas versões compiladas para buscar identificar brechas de segurança.

A utilização dessas ferramentas na fase de implementação e codificação reduz drasticamente o risco de se propagar um código de produto que possua falhas de implementação. Então, pensando no ciclo de vida de desenvolvimento, utilizá-las de maneira contínua ao longo das fases tende a evitar possíveis retrabalhos futuros, resolvendo o problema diretamente com os desenvolvedores envolvidos.

Podemos considerar como VANTAGENS desse tipo de ferramenta:

a) Pode ser executado sucessivamente em versões de software ou agrupamento destes, de maneira repetitiva e baixo custo;
b) Pode ser utilizado para verificar aspectos de segurança na parcela de código considerada sensível e, por vezes, altamente confidencial, como capacidades de buffer (prevendo estouro de buffers da aplicação), bem como outras regras de banco de dados, por exemplo;
c) Resultados são ótimos para os desenvolvedores considerando ainda a fase de desenvolvimento. É capaz de apontar exatamente o ponto de falha ou vulnerabilidade (linha de código ou seção do código), cabendo ao desenvolvedor corrigir de maneira precisa e objetiva.

Como DESVANTAGENS, podemos considerar:

a) Possui capacidade limitada de identificação de falhas, uma vez que os principais ataques são feitos sobre falhas no contexto de funcionamento da solução (aspectos dinâmicos). Desse modo, acabam por atuar sobre uma pequena parcela de todo o rol de vulnerabilidades possíveis;
b) Gera bastante falso-positivo. (Alerta de falha, porém, na prática, não é uma falha);
c) Não abrange falhas de segurança referentes a configurações do software, uma vez que extrapolam simplesmente o código-fonte;
d) Dificuldade em lidar com versões não compiláveis ou ainda, com as diversas bibliotecas utilizadas para desenvolvimento do software;

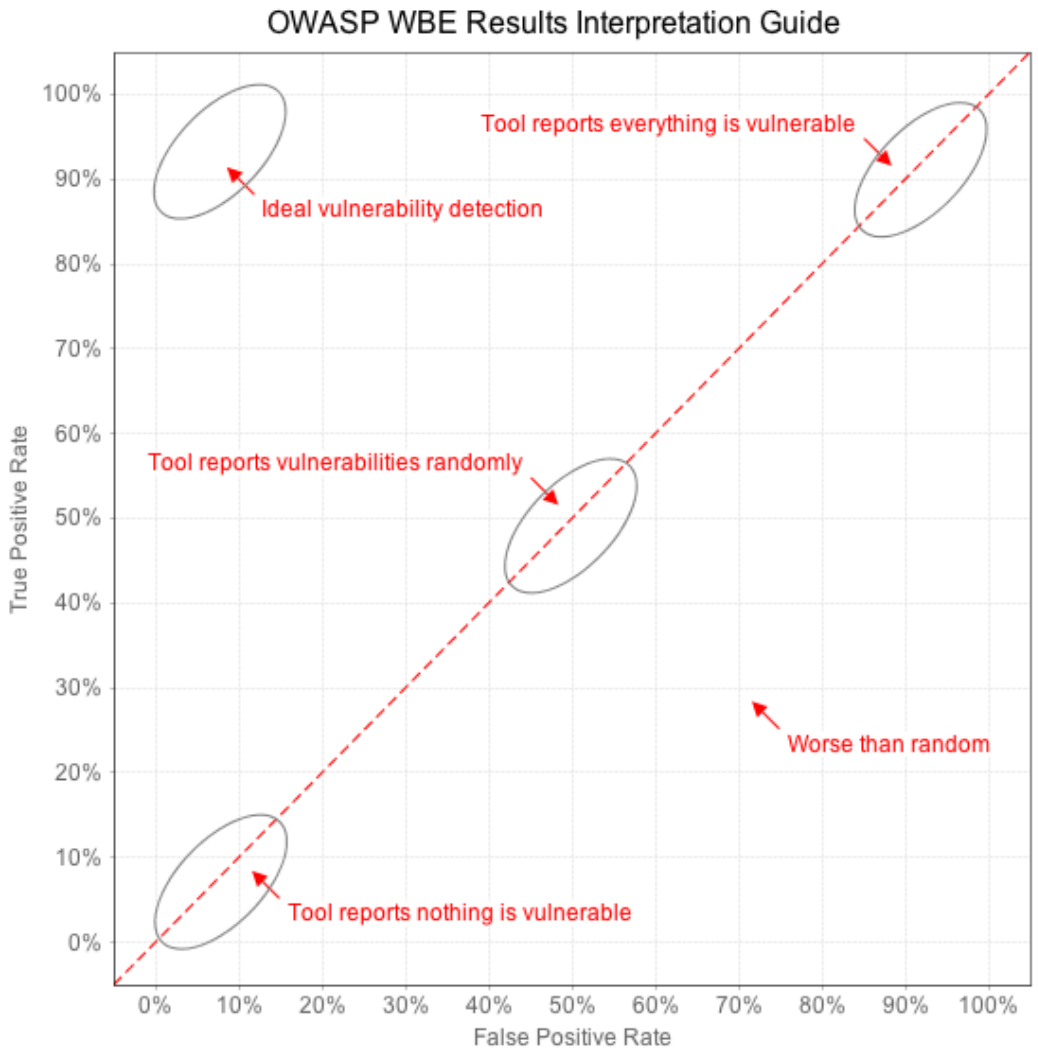
Todos esses aspectos são definidos diretamente pela OWASP (Open Application Security Project). Trata-se de uma comunidade aberta dedicada a permitir que as organizações concebem,

desenvolvam, adquiram, operem e mantenham aplicativos confiáveis, fornecendo conhecimento para aprendizado e compartilhamento contínuo.

Um ponto de observação a ser considerado diz respeito aos critérios a serem considerados na escolha de uma ferramenta do tipo SAST:

1) Deve ser aderente à linguagem de desenvolvimento utilizada;
2) Quais os principais tipos de vulnerabilidades que a ferramenta é capaz de detectar;
3) Qual o nível de acurácia e precisão dos resultados? Quais as taxas de falsos positivos/falsos negativos registrados?
4) Possui consolidado adequado às diversas bibliotecas e frameworks utilizados?
5) Depende de versões completas e compiladas para processamento?
6) Suporta análise do código binário e código fonte?
7) Quão complexo é seu processo de configuração e ajuste para análise?
8) Possui suporte a implementação de regras de automatização e análise contínua?
9) Custos de licença envolvidos;

A imagem abaixo nos dá uma perspectiva de comparação quando se considera a performance em termos de resultados das diversas ferramentas:



DAST (Dynamic Application Security Testing)

Dando continuidade à nossa discussão, quando falamos de ferramentas dinâmicas, basicamente consideramos o software em operação, ou seja, em funcionamento com as diversas operações e interações que são geradas.

Esse tipo de teste é amplamente utilizado para fins de verificação de compliance de segurança e padrões internacionais da indústria, bem como para geração de releases e evoluções do software após seu lançamento.

Pode ser chamado também de TESTE DE COMPORTAMENTO. Ou seja, a falha pode não estar relacionada diretamente ao código fonte, mas são comportamentos gerados durante sua utilização. Assim, a partir de um comportamento que gere risco, deve-se fazer o processo reverso para buscar mapear uma forma de evitar o devido comportamento.

Um outro viés que se constrói com esse tipo de ferramenta é o teste de penetração. Assim, utiliza-se de diversas ferramentas com características e capacidades diferentes de maneira complementar para avaliar as vulnerabilidades comportamentais do software.

Podemos elencar como VANTAGENS:

a) Geralmente é rápido em termos de análise e possui custo reduzido;
b) Geralmente exige um conhecimento técnico menor quando comparado com as ferramentas SAST;
c) Testa os códigos que já estão expostos e em produção;

Como DESVANTAGENS:

a) Atuação tardia no processo do Ciclo de Vida de Desenvolvimento;
b) Testa apenas o impacto na abordagem frontal e direta da aplicação;

Na prática, o que se busca é a utilização conjugada das aplicações de teste que possuem os dois recursos.

IAST (Interactive Application Security Testing)

Trata-se de uma abordagem de teste de segurança de software que ocorre durante o ciclo de desenvolvimento de um aplicativo. Ao contrário de outras técnicas de teste de segurança, o IAST se integra diretamente ao código do aplicativo e monitora sua execução em busca de vulnerabilidades em tempo real.

O IAST combina elementos de SAST (Static Application Security Testing) e DAST (Dynamic Application Security Testing). Ele examina o código-fonte em busca de problemas potenciais e simula ataques reais em tempo de execução para identificar vulnerabilidades que podem não ser detectadas apenas durante a análise estática.

Essa abordagem ajuda as equipes de desenvolvimento a identificar e corrigir vulnerabilidades de segurança de maneira mais eficaz e precoce no processo de desenvolvimento. Isso ocorre porque o IAST fornece informações detalhadas sobre onde as vulnerabilidades foram encontradas e como elas podem ser exploradas.

Há ainda algumas classificações derivadas do IAST como PASSIVO e ATIVO. Basicamente o PASSIVO faz referência de quando o IAST é incorporado às ferramentas SAST. Ele permite que esses scanners confirmem alguns dos falsos positivos, compilando e testando o código. Portanto, a taxa de falsos positivos é reduzida.

As ferramentas passivas do IAST geralmente pesquisam vulnerabilidades em partes de código atualmente analisadas pela parte estática da solução. Isso significa que o aplicativo inteiro não é compilado e testado como um todo, o que pode causar a perda de certas vulnerabilidades.

Já o IAST ativo é quando os DAST's incorporam os IAST's em sua função. O seu foco é na identificação da origem dos problemas para facilitar a interação e reação dos desenvolvedores. Estas acabam por fornecer resultados mais precisos e reduzem o número de falsos positivos.

No caso de linguagens como PHP, uma ferramenta IAST ativa pode realmente identificar a linha exata de código que causa a vulnerabilidade. No caso de linguagens pré-compiladas, ele pode identificar o problema no código de bytes, o que acelera sua localização no código-fonte.

Quero fechar esse bloco trazendo um compilado de práticas e benefícios que são informados por fabricantes diversos deste produto. Faço isso pois, infelizmente, as bancas têm se valido desse recurso para cobrar em prova, uma vez que não há referências bibliográficas e teóricas para esses assuntos mais atuais.

Análise durante a Execução: Ao contrário das ferramentas estáticas que analisam o código-fonte ou das ferramentas dinâmicas que simulam ataques, as ferramentas IAST examinam a aplicação em tempo de execução. Isso permite a detecção de vulnerabilidades reais à medida que a aplicação interage com dados, APIs e usuários reais.

1. Inteligência Contextual: As ferramentas IAST têm a capacidade de entender o contexto da aplicação em execução. Elas podem entender os fluxos de dados, como os dados são manipulados, e como eles fluem através das diferentes camadas da aplicação. Isso ajuda a identificar vulnerabilidades relacionadas ao fluxo de dados e contexto específico.
2. Mínima Falsa Positividade: Uma das vantagens das ferramentas IAST é a redução de falsos positivos. Como elas examinam a aplicação em tempo de execução, podem determinar com mais precisão se uma vulnerabilidade é explorável ou se é apenas um cenário teórico.
3. Cobertura Profunda: Ferramentas IAST podem fornecer uma cobertura de testes mais profunda, pois interagem diretamente com a aplicação em execução. Elas podem examinar as interações entre componentes e partes da aplicação que podem ser difíceis de analisar com outras abordagens.
4. Integração com o Ciclo de Desenvolvimento: As ferramentas IAST podem ser integradas ao processo de desenvolvimento, permitindo que as vulnerabilidades sejam identificadas e corrigidas durante o desenvolvimento, em vez de apenas no final do ciclo.
5. Baixo Impacto no Desempenho: Em comparação com algumas abordagens dinâmicas, as ferramentas IAST geralmente têm um impacto menor no desempenho da aplicação, já que operam em segundo plano e coletam informações enquanto a aplicação é executada.
6. Detecção em Tempo Real: As vulnerabilidades são identificadas em tempo real, à medida que a aplicação é usada, permitindo a correção imediata e a mitigação de riscos.
7. Suporte a Diferentes Tecnologias: Boas ferramentas IAST têm suporte para uma ampla gama de tecnologias, linguagens de programação e estruturas de desenvolvimento, o que as torna versáteis para uso em diferentes tipos de aplicações.
8. Aprendizado Contínuo: Algumas ferramentas IAST podem aprender com os padrões de comportamento da aplicação, melhorando sua capacidade de identificar anomalias e vulnerabilidades à medida que a aplicação evolui.
9. Integração com Ferramentas de Gerenciamento de Vulnerabilidades: As descobertas das ferramentas IAST podem ser integradas em sistemas de gerenciamento de vulnerabilidades para rastreamento e correção eficientes.

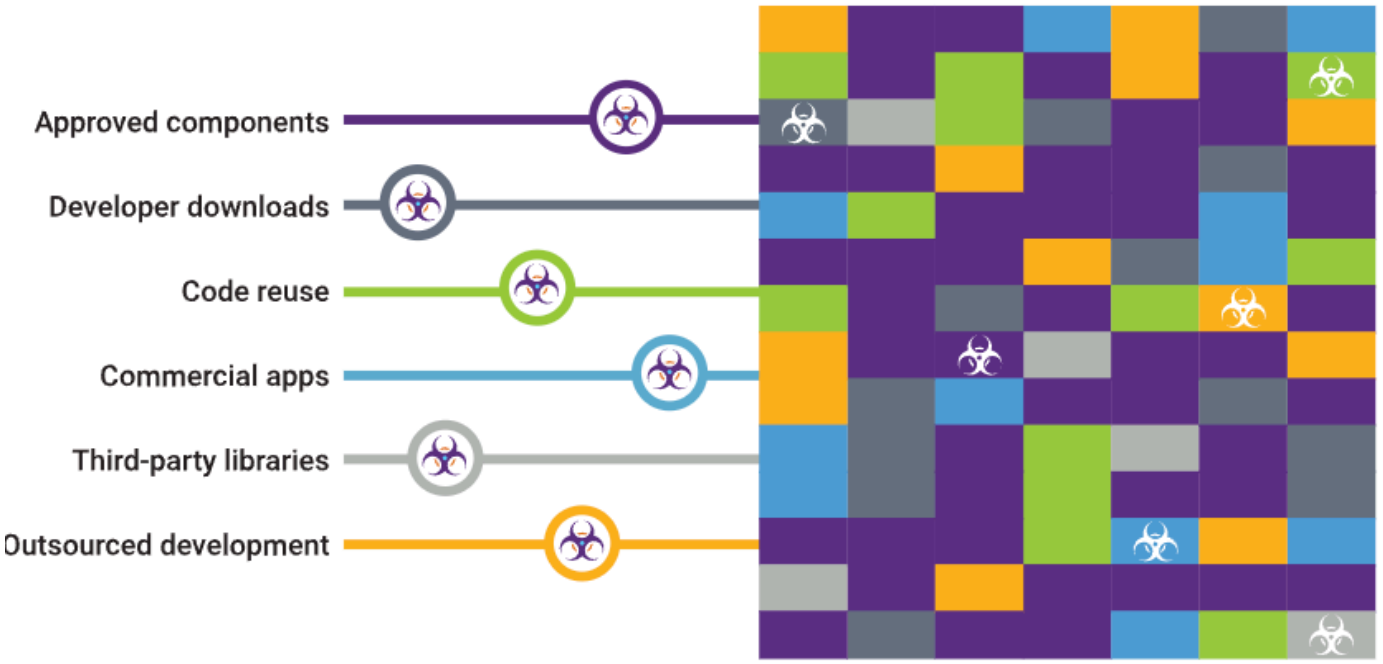
SCA (Software composition analysis)

O SCA (Software Composite Analysis) é uma técnica utilizada para analisar a composição de softwares. Ele examina o código-fonte, bibliotecas e componentes para identificar vulnerabilidades, problemas de licenciamento e dependências. Geralmente, esse processo é manual, o que onera sobremaneira as equipes, e acaba por não fornecer uma visão completa e

robusta, prejudicando a segurança, celeridade e confiabilidade nos processos de deploy de aplicações.

Lembremos que o contexto moderno de aplicações mais complexas e com maior nível de dependências e integrações, em contextos de nuvem e multi-cloud, por exemplo, reforçam essa problemática. Tudo isso associado a esteiras produtivas de DEVOPS, ou melhor dizendo, DEVSECOPS.

Uma imagem para nossa reflexão do desafio:



O SCA, geralmente é dividido nas seguintes etapas em seu processamento:

1. Escaneamento: O software escaneia o código-fonte e as bibliotecas utilizadas no projeto.

2. Identificação: Ele identifica todas as dependências e componentes de terceiros.

3. Análise: O SCA analisa esses componentes para verificar a existência de vulnerabilidades conhecidas, questões de conformidade de licenciamento e outros riscos de segurança.

4. Relatório: Ele gera relatórios detalhados com as vulnerabilidades encontradas, sugerindo correções ou atualizações necessárias.

O objetivo é garantir que o software seja seguro e conforme as licenças de uso, ajudando a evitar problemas legais e de segurança.

Em termos de capacidades de detecção e recursos associados, há um desafio por envolver múltiplos fabricantes em diferentes categorias de oferta. Mas trago aqui uma lista de possibilidades a serem ofertadas no âmbito de um SCA:

- Varredura multifatorial: com varredura de dependência, binária e assinatura, tem-se abordagens de varredura multifacetada do mercado, com capacidades de identificar código aberto que oferta dependência singulares. Isso inclui dependências encontradas em código-fonte, imagens de contêiner, binários, firmware e código gerado por IA .
- Base de dados Proprietárias - KnowledgeBase: Aqui temos um dos principais valores e capacidades das ferramentas de mercado, ao considerar os seus repositórios mais abrangentes do que os setores de informações de código aberto, licença e segurança, alcançando muito além das informações padrão encontradas em feeds gratuitos como o NVD.
- Alertas e Avisos pró-ativos : Esses avisos oferecem notificações de segurança priorizadas e selecionadas. Basicamente busca-se antecipar informações qualificadas quando comparadas às publicações oficiais e abertas das principais fontes públicas.Sabemos que um dos principais desafios da segurança é a antecipação e prevenção.
- Identificação de licença: Rastreamento de licenças de código aberto, ajudando os usuários a evitar violações de licença que podem resultar em litígios dispendiosos ou comprometer a propriedade intelectual.
- Configurações de política: possibilidades de customização da configuração de política tornando-a mais personalizável e detalhada, permitindo a simplificação das atividades de segurança.
- Inserções nas esteiras de CI/CD: Necessidade de se integrar às cadeias de ferramentas SDLC e CI/CD existentes , minimizando o atrito e ajudando a manter a velocidade de desenvolvimento.
- Software Bills of Materials (SBOMs): Simplificação do gerenciamento de SBOM, com a capacidade de importação de SBOMs de terceiros com o objetivo de mapear automaticamente dependências para componentes conhecidos e criar novos componentes para dependências personalizadas ou comerciais. Também possui a capacidade de exportar SBOMs em diferentes formatos para diferentes necessidades.

Ainda, trazendo uma visão dos desafios nesse gerenciamento de riscos na cadeia de fornecimento de software, podemos citar:

- Dependências indiretas: as dependências de um aplicativo podem ter suas próprias dependências. Essas cadeias podem atingir vários níveis de profundidade, dificultando a visibilidade total.
- Identificação de Dependências: Diferentes linguagens de programação e ecossistemas lidam com dependências de maneira diferente. As soluções SCA devem compreender todas as maneiras pelas quais o código-fonte aberto pode ser importado para um aplicativo.
- Gerenciamento de vulnerabilidade: Novas vulnerabilidades são descobertas a cada dia e as fontes de gerenciamento de vulnerabilidade nem sempre estão atualizadas. Como resultado, o SCA pode perder vulnerabilidade e as equipes de desenvolvimento podem ter dificuldades para acompanhar o backlog.

- Complexidade de Implantação: Implementação complexa e trabalhosa que pode levar meses até ficar totalmente operacional
- Diferentes formatos e estruturas de base de dados: Cada produto usa seu próprio banco de dados proprietário de componentes OSS que podem variar drasticamente em termos de tamanho e cobertura
- Limitação de base de dados públicas: Limitar os dados de vulnerabilidade apenas aos relatórios sobre vulnerabilidades oficialmente reportadas no NVD (o que pode ocorrer meses após a vulnerabilidade ter sido descoberta originalmente)
- Falta de ação e orientação: Falta de orientação automatizada sobre as ações a tomar com base nos relatórios e dados da SCA e falta de orientação sobre os requisitos legais das licenças OSS que são detectadas

O SCA (Software Composite Analysis) pode ser aplicado tanto a códigos open source quanto a códigos proprietários. Ele analisa qualquer tipo de código-fonte e seus componentes, independentemente da licença, para identificar vulnerabilidades, problemas de conformidade e dependências. O foco é garantir a segurança e a conformidade do software, seja ele open source ou proprietário.

Importante lembrar que tanto o SCA, SAST, DAST e IAST são todas tecnologias usadas para garantir a segurança e a qualidade do software, mas elas se focam em aspectos diferentes.

Então, enquanto o SCA foca na análise de componentes de terceiros, SAST e DAST focam no código próprio e na execução do software, respectivamente.

Apenas para termos no radar a respeito de algumas das principais ferramentas de Software Composition Analysis (SCA) disponíveis hoje, pois, muitas das vezes, as bancas extraem conceitos e informações diretamente dos sites desses fabricantes:

1. Black Duck: Oferecida pela Synopsys, é conhecida por sua capacidade de analisar componentes open source e gerenciar vulnerabilidades e licenças.

2. Snyk: Foca na segurança de código open source, ajudando a identificar e corrigir vulnerabilidades em bibliotecas de terceiros.

3. WhiteSource: Fornece soluções para gerenciamento de vulnerabilidades e conformidade de licenciamento em componentes open source.

4. FOSSA: É uma ferramenta que automatiza a descoberta de componentes open source, gerenciando licenças e detectando vulnerabilidades.

5. Jfrog Xray: Parte do ecossistema Jfrog, Xray oferece análise profunda de artefatos para detectar vulnerabilidades e problemas de licenciamento.

6. Sonatype Nexus Lifecycle: Ajuda a monitorar e gerenciar a segurança de componentes open source ao longo do ciclo de vida do software.

Mergulhando um pouco mais na dinâmica de funcionamento do SCA, temos que eles inspecionam gerenciadores de pacotes, arquivos manifestos, código-fonte, arquivos binários, imagens de contêiner e muito mais. O código-fonte aberto identificado é compilado em uma Lista de Materiais (Bill of Materials - BOM), que é então comparada com uma variedade de bancos de dados, incluindo o National Vulnerability Database (NVD). Basicamente um banco de dados com CVE's e vulnerabilidades conhecidas mantida pelo Governo Americano.

Além disso, cada uma dessas ferramentas também possuem suas bases próprias com inteligências específicas geradas e outros regimes de parceria para cruzamento de dados e troca de informações.

OWASP TOP 10 - Riscos de Segurança de Aplicações WEB

Pessoal, para iniciar nossa conversa sobre o assunto, não tem como fugirmos da definição do próprio site sobre o assunto, vejamos:

> O OWASP Top 10 é um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web. Ele representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos da web.
>
> Reconhecido globalmente pelos desenvolvedores como o primeiro passo para uma codificação mais segura.
>
> As empresas devem adotar este documento e iniciar o processo de garantir que suas aplicações web minimizem esses riscos. Usar o OWASP Top 10 talvez seja o primeiro passo mais eficaz para mudar a cultura de desenvolvimento de software em sua organização para uma que produza um código mais seguro.

O OWASP Top 10 é baseado, essencialmente, em submissões de dados de empresas especializadas na área da segurança aplicacional e em inquéritos realizados a profissionais individuais do setor. Estes dados refletem as vulnerabilidades identificadas em centenas de organizações, aplicações e APIs reais. Os tópicos do Top 10 são selecionados e ordenados de acordo com a sua prevalência, combinada com uma estimativa ponderada do potencial de abuso, detecção e impacto.

O principal objetivo do OWASP Top 10 é o de educar programadores, desenhadores e arquitetos de aplicações, bem como gestores e as próprias organizações sobre as consequências dos problemas de segurança mais comuns e mais importantes no contexto das aplicações web. O Top 10 oferece não só técnicas básicas para proteção nestas áreas problemáticas e de elevado risco, mas também direções sobre onde encontrar informação adicional sobre estes assuntos.

CESPE / CEBRASPE - 2022 - TCE-RJ - Analista de Controle Externo

Classificação de Risco para o Top 10 é uma metodologia baseada na OWASP Risk Rating Methodology e consiste em estimar, para cada categoria do Top 10, o risco peculiar que cada falha introduz em uma aplicação web típica e, posteriormente, ordenar o Top 10 de acordo com as falhas que tipicamente introduzem o risco mais significativo para uma aplicação.

Comentários:

Típica questão conceito pessoal, que aborda a metodologia de classificação de riscos da própria OWASP para se chegar à referida classificação.

Esse é um exemplo para o TOP 1 da lista:

CWEs mapeados - 34

Taxa de incidência máxima – 55,97%

Taxa média de incidência – 3,81%

Exploração média ponderada – 6,92

Impacto médio ponderado – 5,93

Cobertura máxima – 94,55%

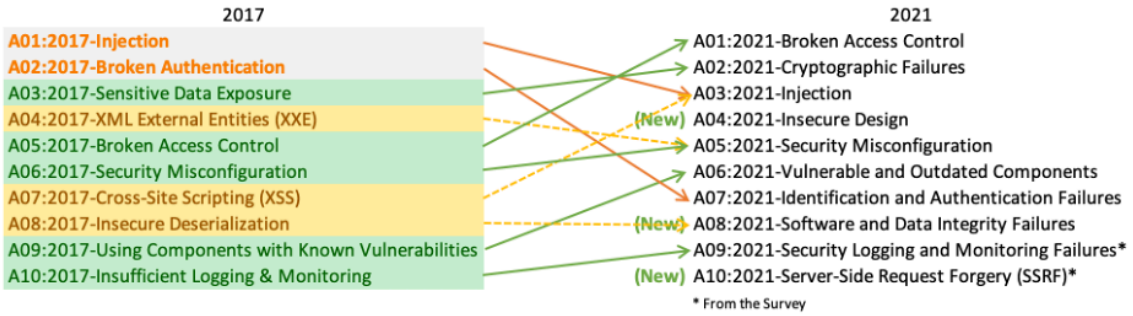
Cobertura média – 47,72%

Total de Ocorrências – 318,487

Total de CVEs – 19,13

Gabarito: C

Nesse sentido, temos a classificação direta e objetiva da lista, trazendo inclusive o histórico de evolução e mudança das classificações.



Nesse contexto, é importante verificar as evoluções da análise, pois é justamente onde as bancas gostam de tentar trabalhar com o candidato. Três categorias anteriores deixaram de existir, e foram incorporadas em estruturas mais genéricas, então é um ponto que a banca pode querer explorar, ao referenciá-los, pois estavam em 2017, a saber:

A04:2017 - XML External Entities (XXE)

A07:2017 - Cross-Site Scripting (XSS)

A08:2017 -Insecure Deserialization

Ainda, importante ter no radar o surgimento de três novas categorias nesse processo, a saber:

A04:2021 - Security Misconfiguration

A08:2021 - Software and Data Integrity Failures

A10:2021 - Server-Side Request Forgery (SSRF)

Bom pessoal, avançando, infelizmente, não temos para onde correr agora a não ser percorrer todos os itens das 10 categorias previstas no OWASP. As bancas estão cobrando itens específicos dentro de cada controle, conforme veremos a seguir.

Basicamente, cada categoria apresenta uma visão geral da vulnerabilidade, com uma descrição associada, e contramedidas/prevenções que devem ser aplicadas ou realizadas. Por fim, tem-se exemplos práticos com cenários específicos para cada um. Não passaremos pelos exemplos, nos atendo até as medidas de prevenção. Desta feita, vamos avançar...

A01:2021 - Quebra de Controle de Acesso

1. Descrição

- Restrição de ações com base em suas permissões
- Falhas nesse processo levam a divulgação, modificação ou destruição não autorizadas da informação

2. Vulnerabilidades

I. Violação do princípio de privilégio mínimo ou negação por padrão, onde o acesso deve ser concedido apenas para recursos, funções ou usuários específicos, mas está disponível para qualquer pessoa.
II. Ignorando as verificações de controle de acesso modificando a URL (alteração de parâmetro ou navegação forçada), o estado interno do aplicativo ou a página HTML, ou usando uma ferramenta de ataque modificando solicitações de API.
III. Permitir a visualização ou edição da conta de outra pessoa, fornecendo seu identificador exclusivo (referências de objetos diretos inseguros)
IV. Acessando API com controles de acesso ausentes para POST, PUT e DELETE.
V. Elevação de privilégio. Atuar como usuário sem estar conectado ou atuar como administrador quando estiver conectado como usuário.
VI. Manipulação de metadados, como reproduzir ou adulterar um token de controle de acesso JSON Web Token (JWT), ou um cookie ou campo oculto manipulado para elevar privilégios ou abusar da invalidação de JWT.
VII. A configuração incorreta do Cross-Origin Resource Sharing - CORS - permite o acesso à API de origens não autorizadas/não confiáveis.
VIII. Força a navegação em páginas autenticadas como usuário não autenticado ou em páginas privilegiadas como usuário padrão.

Pessoal, então o que tenho a acrescentar aqui é sempre no horizonte de quebra de autenticação e utilização indevida desses acessos para interação com domínios não autorizados ou restritos. Tenham isso em mente no que tange às vulnerabilidades geradas dentro desta categoria.

3. Prevenção

I. Exceto para recursos públicos, negar por padrão.

II. Implemente mecanismos de controle de acesso uma vez e reutilize-os em todo o aplicativo, inclusive minimizando o uso do Cross-Origin Resource Sharing (CORS).
III. Os controles de acesso do modelo devem impor a propriedade do registro em vez de aceitar que o usuário possa criar, ler, atualizar ou excluir qualquer registro.
IV. Os requisitos exclusivos de limite de negócios do aplicativo devem ser impostos por modelos de domínio.
V. Desative a listagem de diretórios do servidor web e certifique-se de que os metadados do arquivo (por exemplo, .git) e os arquivos de backup não estejam presentes nas raízes da web.
VI. Registre falhas de controle de acesso, alerte os administradores quando apropriado (por exemplo, falhas repetidas).
VII. Taxa de limite de acesso à API e ao controlador para minimizar os danos das ferramentas de ataque automatizadas.
VIII. Os identificadores de sessão com estado devem ser invalidados no servidor após o logout. Os tokens JWT sem estado devem ser de curta duração para que a janela de oportunidade para um invasor seja minimizada. Para JWTs de vida mais longa, é altamente recomendável seguir os padrões OAuth para revogar o acesso.

Meu destaque aqui vai sempre para exceções... Então tem-se um princípio de Arquitetura Zero-Trust aqui, ao se negar por padrão, exceto aqueles recursos públicos. Chamo sua atenção para isso.

FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

A falha ou quebra de controle de acesso ("Broken Access Control") é um risco de segurança crítico para aplicações Web.

Para prevenir essa vulnerabilidade, o OWASP recomenda que

A a listagem de diretórios do servidor web seja desativada.

B os tokens JWT stateless sejam de longa duração.

C as sessões stateful sejam mantidas no servidor após o logout.

D evite reutilizar os mecanismos de controle de acesso.

E utilize APIs sem taxa limite de requisições.

Comentários:

Exatamente conforme o item V previsto na prevenção:

V. Desative a listagem de diretórios do servidor web e certifique-se de que os metadados do arquivo (por exemplo, .git) e os arquivos de backup não estejam presentes nas raízes da web.

Gabarito: A

FGV - 2022 - TJ-DFT - Analista Judiciário - Análise de Sistemas

PedidosSemEstresse é uma aplicação Web destinada a digitalizar o processo de pedidos de serviços de um órgão da administração pública. A interface de PedidosSemEstresse utilizada pelos usuários faz chamadas a uma API RESTful e não utiliza facilidades de login único (single sign-on – SSO). Recentemente, o usuário interno João utilizou suas próprias credenciais com privilégios somente de execução de métodos GET para explorar vulnerabilidades e teve acesso direto a API RESTful. Assim, João fez chamadas a métodos POST com sucesso.

Com base no OWASP Top Ten, a vulnerabilidade explorada por João é da categoria:

A Injection;

B Broken Access Control;

C Software and Data Integrity Failures;

D Vulnerable and Outdated Components;

E Identification and Authentication Failures

Comentários:

Vejam que estamos na mesma linha da questão anterior, onde há uma falha de autorização, uma vez que um usuário, que tinha permissão somente para determinada ação, consegue realizar outra ação.

Gabarito: B

A02:2021 - Falhas criptográficas

1. Descrição

- Falhas relacionadas à criptografia ou falta dela
- Exposição de dados sensíveis ou confidenciais
- Necessidade de determinação de segurança de dados em trânsito ou repouso
- Destaques a dados privados suscetíveis a regulações próprias

Meu destaque pessoal fica por conta do fortalecimento e necessidade de uso da criptografia, tanto para dados em repousou, como em trânsito. Veremos mais alguns detalhes a seguir, que merecem também sua atenção.

2. Vulnerabilidades

I. Algum dado é transmitido em texto simples? Isso diz respeito a protocolos como HTTP, SMTP, FTP também usando atualizações TLS como STARTTLS. O tráfego externo da Internet é perigoso. Verifique todo o tráfego interno, por exemplo, entre balanceadores de carga, servidores web ou sistemas back-end.

II. Algum algoritmo ou protocolo criptográfico antigo ou fraco é usado por padrão ou em código mais antigo?
III. As chaves criptográficas padrão estão em uso, as chaves criptográficas fracas são geradas ou reutilizadas ou o gerenciamento ou rotação de chaves está ausente? As chaves criptográficas são verificadas nos repositórios de código-fonte?
IV. A criptografia não é aplicada. Por exemplo, há alguma diretiva de segurança de cabeçalhos HTTP (navegador) ou cabeçalhos ausentes?
V. O certificado do servidor recebido e a cadeia de confiança estão devidamente validados?
VI. Os vetores de inicialização são ignorados, reutilizados ou não gerados suficientemente seguros para o modo de operação criptográfico? Está em uso um modo de operação inseguro, como o BCE? A criptografia é usada quando a criptografia autenticada é mais apropriada?
VII. As senhas estão sendo usadas como chaves criptográficas na ausência de uma função de derivação de chave de base de senha?
VIII. A aleatoriedade é usada para fins criptográficos que não foram projetados para atender aos requisitos criptográficos? Mesmo que a função correta seja escolhida, ela precisa ser propagada pelo desenvolvedor e, caso contrário, o desenvolvedor sobrescreveu a funcionalidade de propagação forte incorporada a ela com uma semente que não possui entropia/imprevisibilidade suficiente?
IX. As funções de hash obsoletas, como MD5 ou SHA1, estão em uso ou as funções de hash não criptográficas são usadas quando as funções de hash criptográficas são necessárias?
X. Estão em uso métodos de preenchimento criptográfico obsoletos, como PKCS número 1 v1.5?
XI. As mensagens de erro criptográficas ou informações de canal lateral podem ser exploradas, por exemplo, na forma de ataques oracle de preenchimento?

Pessoal, então o que tenho a acrescentar aqui é sempre no horizonte de quebra de autenticação e utilização indevida desses acessos para interação com domínios não autorizados ou restritos. Tenham isso em mentes no que tange às vulnerabilidades geradas dentro desta categoria.

3. Prevenção

I. Classifique os dados processados, armazenados ou transmitidos por um aplicativo. Identifique quais dados são confidenciais de acordo com as leis de privacidade, requisitos regulatórios ou necessidades de negócios.
II. Não armazene dados confidenciais desnecessariamente. Descarte-o o mais rápido possível ou use tokenização compatível com PCI DSS ou até mesmo truncamento. Os dados que não são retidos não podem ser roubados.
III. Certifique-se de criptografar todos os dados confidenciais em repouso.
IV. Garantir que algoritmos, protocolos e chaves padrão atualizados e fortes estejam em vigor; use o gerenciamento de chaves adequado.
V. Criptografe todos os dados em trânsito com protocolos seguros, como TLS com cifras de sigilo de encaminhamento (FS), priorização de cifras pelo servidor e parâmetros seguros. Imponha a criptografia usando diretivas como HTTP Strict Transport Security (HSTS).
VI. Desabilite o armazenamento em cache para respostas que contenham dados confidenciais.
VII. Aplique os controles de segurança necessários de acordo com a classificação dos dados.
VIII. Não use protocolos legados, como FTP e SMTP, para transportar dados confidenciais.

IX. Armazene senhas usando funções de hashing adaptáveis e salgadas fortes com um fator de trabalho (fator de atraso), como Argon2, scrypt, bcrypt ou PBKDF2.
X. Os vetores de inicialização devem ser escolhidos de acordo com o modo de operação. Para muitos modos, isso significa usar um CSPRNG (gerador de números pseudo-aleatórios criptograficamente seguro). Para modos que exigem um nonce, o vetor de inicialização (IV) não precisa de um CSPRNG. Em todos os casos, o IV nunca deve ser usado duas vezes para uma chave fixa.
XI. Sempre use criptografia autenticada em vez de apenas criptografia.
XII. As chaves devem ser geradas criptograficamente aleatoriamente e armazenadas na memória como arrays de bytes. Se uma senha for usada, ela deverá ser convertida em uma chave por meio de uma função de derivação de chave de base de senha apropriada.
XIII. Certifique-se de que a aleatoriedade criptográfica seja usada quando apropriado e que não tenha sido propagada de maneira previsível ou com baixa entropia. A maioria das APIs modernas não exige que o desenvolvedor semeie o CSPRNG para obter segurança.
XIV. Evite funções criptográficas obsoletas e esquemas de preenchimento, como MD5, SHA1, PKCS número 1 v1.5 .
XV. Verifique de forma independente a eficácia da configuração e configurações.

Vejamos uma questão sobre o assunto:

CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

Comentários:

Exatamente pessoal. Típica questão que demonstra que não temos para onde correr, a não ser passar por todas as medidas e prevenções do OWASP. Este item está previsto na prevenção de nº 6 do Controle A02:2021 - Falhas Criptográficas.

Gabarito: C

CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

Comentários:

Novamente, vejam que quando é para colocar a assertiva como CORRETA, a banca pega exatamente o texto apresentado.

Gabarito: C

A03:2021 - Injeção

1. Descrição

- Congrega diversas técnicas de ataque, incluindo XSS e CSRF, por exemplo, além dos clássicos SQL Injection
- A revisão constante dos códigos e scripts é fundamental para tentar identificar as vulnerabilidades
- Pode-se utilizar ferramentas como SAST, DAST e IAST

Pessoal, para este item, é importante vocês terem em mente que houve uma agragação de tipos de ataques que possuem como premissa básica o ato de injeção de código ou scripts. Dito isso, tivemos os ataques de XSS e CSRF em conjunto com o "famoso" SQL Injection. Em que pese tenham característica semelhantes de entrada, os impactos e consequência, bem como cada ataque é derivado posteriormente à injeção, é diferente, inclusive no que tange à sua finalidade.

Ainda, merece destacar a importância do uso de ferramentas automatizadas que buscam avaliar a qualidade do código em torno dos aspectos de segurança. Nesse quesito, tem-se o SAST (que olha código estático, basicamente, seu código fonte), o DAST (que foca nas funcionalidades do sistema, simulando a ótica do usuário), e o IAST (que traz uma perspectiva das interações do código e produto).

2. Vulnerabilidades

I. Os dados fornecidos pelo usuário não são validados, filtrados ou higienizados pelo aplicativo.
II. Consultas dinâmicas ou chamadas não parametrizadas sem escape sensível ao contexto são usadas diretamente no interpretador.
III. Dados hostis são usados em parâmetros de pesquisa de mapeamento relacional de objeto (ORM) para extrair registros confidenciais adicionais.
IV. Dados hostis são usados diretamente ou concatenados. O SQL ou comando contém a estrutura e os dados maliciosos em consultas dinâmicas, comandos ou procedimentos armazenados.

Importante termos em mente, como principal característica, as vulnerabilidades associadas à entrada de dados diretamente nas páginas, por parte de áreas dinâmica e chamadas diversas ao código por parte do usuário.

3. Prevenção

I. Manter os dados separados de comandos e consultas
II. A opção preferencial é usar uma API segura, que evite totalmente o uso do interpretador, forneça uma interface parametrizada ou migre para Object Relational Mapping Tools (ORMs).
    i. Nota: Mesmo quando parametrizados, os procedimentos armazenados ainda podem introduzir injeção de SQL se PL/SQL ou T-SQL concatenando consultas e dados ou executar dados hostis com EXECUTE IMMEDIATE ou exec().
III. Use validação de entrada positiva do lado do servidor. Essa não é uma defesa completa, pois muitos aplicativos exigem caracteres especiais, como áreas de texto ou APIs para aplicativos móveis.

IV. Para quaisquer consultas dinâmicas residuais, escape caracteres especiais usando a sintaxe de escape específica para esse interpretador.
    i. Nota: Estruturas SQL, como nomes de tabelas, nomes de colunas e assim por diante, não podem ser escapadas e, portanto, os nomes de estrutura fornecidos pelo usuário são perigosos. Este é um problema comum em software de redação de relatórios.
V. Use LIMIT e outros controles SQL nas consultas para evitar a divulgação em massa de registros em caso de injeção de SQL.

Aqui, o que imaginamos a banca realizando, é justamente permutar itens de vulnerabilidades e prevenção do injection com outras categorias. Então é importante ficarem atentos a essa dinâmica.

FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De modo a prevenir falhas de injeção de dados maliciosos, recomenda-se não usar, para o transporte de dados confidenciais, protocolos legados, como FTP e SMTP.

Comentários:

Pessoal, a descrição em tela se refere a recomendações de prevenção da categoria de FALHAS CRIPTOGRÁFICAS e não de INJEÇÃO DE DADOS. Vejam justamente a dinâmica que comentei com vocês sobre troca de características.

Gabarito: E

A04:2021 - Design inseguro

1. Descrição

- Trata-se de uma nova categoria.
- Foca nos aspectos voltados a problemas de arquitetura e design (desenho) do produto
- Possui foco na pré codificação, isto é, antes do código ser desenvolvido
- Pode-se ter problemas de ausência de controles ou este ser ineficaz durante o período de design
- Deve-se fortalecer as ações associadas ao proecsso de coleta de requisitos e ao Ciclo de Desenvolvimento Seguro

Um design seguro ainda pode ter defeitos de implementação levando a vulnerabilidades que podem ser exploradas. Um design inseguro não pode ser corrigido por uma implementação perfeita, pois, por definição, os controles de segurança necessários nunca foram criados para se defender contra ataques específicos.

Por este motivo pessoal, é de suma importância ter um processo bem definido e desenhado na construção de uma solução, incorporando, ainda antes do desenvolvimento, essas questões e segurança. Importante lembrar como se fosse a fundação de uma casa. Se ela sair com problema,

a casa sempre terá problemas estruturais independentemente do que faça por cima, ou seja, da qualidade do código que será desenvolvido.

2. Prevenção

I. Estabeleça e use um ciclo de vida de desenvolvimento seguro com profissionais da AppSec para ajudar a avaliar e projetar controles relacionados à segurança e privacidade
II. Estabeleça e use uma biblioteca de padrões de projeto seguros ou componentes prontos para uso de estradas pavimentadas
III. Use a modelagem de ameaças para autenticação crítica, controle de acesso, lógica de negócios e fluxos de chaves
IV. Integre linguagem e controles de segurança em histórias de usuários
V. Integre verificações de plausibilidade em cada camada do seu aplicativo (do front-end ao back-end)
VI. Escreva testes de unidade e integração para validar se todos os fluxos críticos são resistentes ao modelo de ameaça. Compile casos de uso e casos de uso indevido para cada camada de seu aplicativo.
VII. Segregar camadas de camadas no sistema e nas camadas de rede, dependendo das necessidades de exposição e proteção
VIII. Separe os locatários de forma robusta por design em todas as camadas

FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De acordo com a OWASP TOP 10 2021, para o risco design inseguro, são medidas de prevenção para o desenvolvimento seguro o uso da modelagem de ameaças para autenticações críticas, controle de acesso e lógica de negócios.

Comentários:

Exatamente na linha do que conversamos pessoal.

Gabarito: C

A05:2021 - Configuração incorreta de segurança

1. Descrição

Envolve a configuração de ambientes e servidores, bem como ausências de baselines seguras e ferramentas de compliance.

Importante reforçar o conceito de baseline, que trata justamente daquela configuração de referência que poderá ser incorporada e espelhada, com todas as diretrizes e padrões de segurança já conhecidos e mapeados.

2. Vulnerabilidades

I. Falta de proteção de segurança apropriada em qualquer parte da pilha de aplicativos ou permissões configuradas incorretamente em serviços de nuvem.

II. Recursos desnecessários são ativados ou instalados (por exemplo, portas, serviços, páginas, contas ou privilégios desnecessários).
III. As contas padrão e suas senhas ainda estão habilitadas e inalteradas.
IV. O tratamento de erros revela rastreamentos de pilha ou outras mensagens de erro excessivamente informativas aos usuários.
V. Para sistemas atualizados, os recursos de segurança mais recentes são desabilitados ou não configurados com segurança.
VI. As configurações de segurança nos servidores de aplicativos, estruturas de aplicativos (por exemplo, Struts, Spring, ASP.NET), bibliotecas, bancos de dados etc., não são definidas para valores seguros.
VII. O servidor não envia cabeçalhos ou diretivas de segurança ou eles não estão configurados para valores seguros.
VIII. O software está desatualizado ou vulnerável (consulte A06:2021-Componentes vulneráveis e desatualizados). Importante termos em mente, como principal característica, as vulnerabilidades associadas a entrada de dados diretamente nas páginas, por parte de áreas dinâmica e chamadas diversas ao código por parte do usuário.

3. Prevenção

I. Um processo de proteção repetível torna rápido e fácil a implantação de outro ambiente devidamente bloqueado. Os ambientes de desenvolvimento, controle de qualidade e produção devem ser configurados de forma idêntica, com credenciais diferentes usadas em cada ambiente. Esse processo deve ser automatizado para minimizar o esforço necessário para configurar um novo ambiente seguro.
II. Uma plataforma mínima sem recursos, componentes, documentação e amostras desnecessários. Remova ou não instale recursos e estruturas não utilizados.
III. Uma tarefa para revisar e atualizar as configurações apropriadas para todas as notas de segurança, atualizações e patches como parte do processo de gerenciamento de patches (consulte A06:2021-Componentes vulneráveis e desatualizados). Revise as permissões de armazenamento em nuvem (por exemplo, permissões de bucket do S3).
IV. Uma arquitetura de aplicativo segmentada fornece separação eficaz e segura entre componentes ou locatários, com segmentação, conteinerização ou grupos de segurança de nuvem (ACLs).
V. Envio de diretivas de segurança para clientes, por exemplo, Cabeçalhos de Segurança.
VI. Um processo automatizado para verificar a eficácia das configurações e ajustes em todos os ambientes.

CESPE / CEBRASPE - 2021 - SEFAZ-CE - Auditor Fiscal de Tecnologia da Informação da Receita Estadual

A inadequada configuração de segurança, um dos riscos da OWASP Top 10, pode ocorrer em qualquer nível de serviço de uma aplicação; em razão disso, o uso de scanners e testes automatizados é ineficaz na tarefa de detectar falhas de configuração.

Comentários:

Estamos falando do tipo de Controle A05 - Security Misconfiguration. Então, a primeira parte da questão está correta, pois, de fato, pode ocorrer em qualquer nível de serviço. Agora o erro está

na segunda parte, ao afirmar que o uso de scanners e testes são ineficazes. Muito pelo contrário, esses testes ajudam, e muito nesse processo.

Gabarito: E

A06:2021 - Componentes Vulneráveis e Desatualizados

1. Descrição

Basicamente essa família está associada ao processo de inventário de software. A partir de então, conhecendo-se o parque, é possível entender possíveis vulnerabilidades, bem como ações de mitigação.

Uma das referências é a utilização das atualizações automáticas. Entretanto, nem sempre atualizar é simples, e pode gerar quebras na aplicação utilizada, exigindo retrabalho por parte dos atores.

2. Vulnerabilidades

I. Se você não conhece as versões de todos os componentes que usa (tanto do lado do cliente quanto do lado do servidor). Isso inclui componentes que você usa diretamente, bem como dependências aninhadas.
II. Se o software for vulnerável, sem suporte ou desatualizado. Isso inclui o sistema operacional, servidor de aplicativos/web, sistema de gerenciamento de banco de dados (DBMS), aplicativos, APIs e todos os componentes, ambientes de tempo de execução e bibliotecas.
III. Se você não verificar vulnerabilidades regularmente e assinar boletins de segurança relacionados aos componentes que usa.
IV. Se você não corrigir ou atualizar a plataforma, estruturas e dependências subjacentes de maneira oportuna e baseada em risco. Isso geralmente acontece em ambientes em que a correção é uma tarefa mensal ou trimestral sob controle de alterações, deixando as organizações abertas a dias ou meses de exposição desnecessária a vulnerabilidades corrigidas.
V. Se os desenvolvedores de software não testarem a compatibilidade de bibliotecas atualizadas, atualizadas ou corrigidas.
VI. Se você não proteger as configurações dos componentes (consulte A05:2021-Configuração incorreta de segurança).

3. Prevenção

I. Remova dependências não utilizadas, recursos, componentes, arquivos e documentação desnecessários.
II. Faça um inventário contínuo das versões de componentes do lado do cliente e do lado do servidor (por exemplo, estruturas, bibliotecas) e suas dependências usando ferramentas como versões, verificação de dependência OWASP, retire.js etc. Monitore continuamente fontes como Vulnerabilidade e exposições comuns (CVE) e National Vulnerability Database (NVD) para vulnerabilidades nos componentes. Use ferramentas de análise de composição de software para automatizar o processo. Assine alertas por e-mail para vulnerabilidades de segurança relacionadas aos componentes que você usa.

III. Obtenha apenas componentes de fontes oficiais em links seguros. Prefira pacotes assinados para reduzir a chance de incluir um componente mal-intencionado modificado (consulte A08:2021-Falhas de integridade de software e dados).
IV. Monitore bibliotecas e componentes que não são mantidos ou não criam patches de segurança para versões mais antigas. Se a aplicação de patches não for possível, considere a implantação de um patch virtual para monitorar, detectar ou proteger contra o problema descoberto.

A07:2021 - Falhas de Identificação e Autenticação

1. Descrição

Na versão de 2017, aparecia como Quebra de Autenticação. Importante, desde já, diferenciar do grupo A01, pois lá naquela categoria, estávamos falando de autorização. Já nesse item, estamos focados no processo de identificação e autenticação.

Não há dúvidas quanto à importância e necessidade de se identificar, autenticar e gerenciar as sessões desses usuários com vistas a proteger contra ataques de personificação ou falsificação de identidade.

2. Vulnerabilidades

I. Permite ataques automatizados, como preenchimento de credenciais, em que o invasor possui uma lista de nomes de usuários e senhas válidos.
II. Permite força bruta ou outros ataques automatizados.
III. Permitir senhas padrão, fracas ou conhecidas, como "Password1" ou "admin/admin".
IV. Usa recuperação de credenciais fraca ou ineficaz e processos de esquecimento de senha, como "respostas baseadas em conhecimento", que não podem ser seguras.
V. Usa armazenamentos de dados de senhas de texto simples, criptografados ou com hash fraco (consulte A02:2021-Falhas de criptografia).
VI. Não tem autenticação multifator ou é ineficaz.
VII. Expõe o identificador de sessão na URL.
VIII. Reutilize o identificador de sessão após o login bem-sucedido.
IX. Não invalida corretamente os IDs de sessão. Sessões de usuário ou tokens de autenticação (principalmente tokens de logon único (SSO)) não são invalidados corretamente durante o logout ou um período de inatividade.

Já falamos bastante sobre estes aspectos ao longo da nossa aula. Sem dúvida, a utilização de uma estrutura de autenticação robusta no lado corporativo, é fundamental. Entretanto, aqui entram itens relativos aos controles de usuários, pois as senhas destes podem ser violadas e gerar dano à organização.

Por isso, os itens relativos à política de senhas e procedimentos de renovação é fundamental.

3. Prevenção

I. Sempre que possível, implemente a autenticação multifator para evitar ataques automatizados de preenchimento de credenciais, força bruta e reutilização de credenciais roubadas.
II. Não envie ou implante com credenciais padrão, principalmente para usuários administradores.
III. Implemente verificações de senhas fracas, como testar senhas novas ou alteradas na lista das 10.000 piores senhas.
IV. Alinhe as políticas de comprimento, complexidade e rotação de senha com as diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) 800-63b na seção 5.1.1 para Segredos Memorizados ou outras políticas de senha modernas baseadas em evidências.
V. Garanta que os caminhos de registro, recuperação de credenciais e API sejam protegidos contra ataques de enumeração de conta usando as mesmas mensagens para todos os resultados.
VI. Limite ou retarde cada vez mais as tentativas de login com falha, mas tome cuidado para não criar um cenário de negação de serviço. Registre todas as falhas e alerte os administradores quando forem detectados preenchimento de credenciais, força bruta ou outros ataques.
VII. Use um gerenciador de sessão integrado, seguro e do lado do servidor que gera um novo ID de sessão aleatório com alta entropia após o login. O identificador de sessão não deve estar no URL, ser armazenado com segurança e invalidado após o logout, inatividade e tempos limites absolutos.

FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Comentários:

Certo pessoal. Ambos são viáveis, e não são as únicas hipóteses.

Gabarito: C

A08:2021 - Falhas de integridade de software e dados

1. Descrição

Mais uma nova categoria no OWASP. Basicamente, este item está associado ao processo de deploy ou disponibilização em produção, alcançando as esteiras de Integração Contínua e Entrega contínua, quando não há verificações de integridades no processo.

Deve-se estar atento aos códigos e à infraestrutura quando ambos não protegem contra violações de integridade do código.

Um exemplo disso é quando um aplicativo depende de plugins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs). Um pipeline de CI/CD inseguro pode introduzir o potencial de acesso não autorizado, código malicioso ou comprometimento do sistema.

2. Prevenção

I. Use assinaturas digitais ou mecanismos semelhantes para verificar se o software ou os dados são da fonte esperada e não foram alterados.
II. Garanta que bibliotecas e dependências, como npm ou Maven, estejam consumindo repositórios confiáveis. Se você tiver um perfil de risco mais alto, considere hospedar um repositório interno em boas condições que seja verificado.
III. Certifique-se de que uma ferramenta de segurança da cadeia de suprimentos de software, como OWASP Dependency Check ou OWASP CycloneDX, seja usada para verificar se os componentes não contêm vulnerabilidades conhecidas
IV. Certifique-se de que haja um processo de revisão para alterações de código e configuração para minimizar a chance de que código ou configuração mal-intencionados possam ser introduzidos em seu pipeline de software.
V. Certifique-se de que seu pipeline de CI/CD tenha segregação, configuração e controle de acesso adequados para garantir a integridade do código que flui pelos processos de compilação e implantação.
VI. Certifique-se de que os dados serializados não assinados ou não criptografados não sejam enviados para clientes não confiáveis sem alguma forma de verificação de integridade ou assinatura digital para detectar adulteração ou repetição dos dados serializados

A09:2021 - Falhas de registro e monitoramento de segurança

1. Descrição

Aqui temos o foco na detecção, escalação e resposta às violações ativas. Quando não há registro e monitoramento, as violações não podem ser detectadas, tratadas e conhecidas de forma eficiente.

2. Vulnerabilidades

I. Eventos auditáveis, como logins, logins com falha e transações de alto valor, não são registrados.
II. Avisos e erros geram mensagens de log inexistentes, inadequadas ou pouco claras.
III. Os logs de aplicativos e APIs não são monitorados quanto a atividades suspeitas.
IV. Os logs são armazenados apenas localmente.
V. Limites de alerta apropriados e processos de escalação de resposta não estão em vigor ou não são eficazes.
VI. Testes de penetração e varreduras por ferramentas de teste de segurança de aplicativos dinâmicos (DAST) (como OWASP ZAP) não acionam alertas.

Neste item, temos um apelo muito forte às práticas de registros e logs da ISO 27002.

3. Prevenção

I. Garanta que todas as falhas de login, controle de acesso e validação de entrada do lado do servidor possam ser registradas com contexto de usuário suficiente para identificar contas suspeitas ou maliciosas e mantidas por tempo suficiente para permitir análises forenses atrasadas.
II. Certifique-se de que os logs sejam gerados em um formato que as soluções de gerenciamento de log possam consumir facilmente.
III. Certifique-se de que os dados de log sejam codificados corretamente para evitar injeções ou ataques nos sistemas de log ou monitoramento.
IV. Garanta que as transações de alto valor tenham uma trilha de auditoria com controles de integridade para evitar adulteração ou exclusão, como tabelas de banco de dados somente anexadas ou similares.
V. As equipes de DevSecOps devem estabelecer monitoramento e alertas eficazes para que atividades suspeitas sejam detectadas e respondidas rapidamente.
VI. Estabeleça ou adote um plano de resposta e recuperação de incidentes, como o Instituto Nacional de Padrões e Tecnologia (NIST) 800-61r2 ou posterior.

A10:2021 - Falsificação de solicitação do lado do servidor (SSRF)

1. Descrição

Aqui, temos uma categoria nova também na lista, que traz um ataque diferenciado no sentido de que o servidor WEB envolvido na condição de vítima, nada mais é do que um vetor para um outro ataque. Já comentamos sobre isso.

Assim, de forma resumida, temos que são criadas requisições no lado do servidor para URL's ou serviços de terceiros indevidamente

Um dos destaques dessa categoria é a possibilidade de conseguir burlar firewalls internos na rede.

2. Prevenção

Da camada de rede

I. Segmente a funcionalidade de acesso remoto a recursos em redes separadas para reduzir o impacto do SSRF
II. Aplique políticas de firewall “negar por padrão” ou regras de controle de acesso à rede para bloquear todo o tráfego de intranet, exceto o essencial.
III. Dicas:
   ~ Estabeleça uma propriedade e um ciclo de vida para regras de firewall baseadas em aplicativos.
   ~ Registre todos os fluxos de rede aceitos e bloqueados em firewalls (consulte A09:2021-Registro de segurança e falhas de monitoramento).

Da camada de aplicação:

I. Higienize e valide todos os dados de entrada fornecidos pelo cliente
II. Aplique o esquema de URL, a porta e o destino com uma lista de permissões positiva
III. Não envie respostas brutas aos clientes
IV. Desabilitar redirecionamentos HTTP
V. Esteja ciente da consistência do URL para evitar ataques como religação de DNS e condições de corrida "tempo de verificação, tempo de uso" (TOCTOU)
VI. Não reduza o SSRF por meio do uso de uma lista de negação ou expressão regular. Os invasores têm listas de carga útil, ferramentas e habilidades para contornar as listas de negação.
VII. Não implante outros serviços relevantes de segurança em sistemas frontais (por exemplo, OpenID). Controle o tráfego local nesses sistemas (por exemplo, localhost)
VIII. Para frontends com grupos de usuários dedicados e gerenciáveis, use criptografia de rede (por exemplo, VPNs) em sistemas independentes para considerar necessidades de proteção muito altas

Percebam que muito mais do que tratar as regras padrões de entradas positivas, tal qual fora feito na categoria de injeção, tem-se ainda procedimentos para colocar uma regra relativo ao usuário, na perspectiva de identificação e autorização.

FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Ao analisar uma aplicação web, um auditor verificou que ela estava vulnerável a um ataque conhecido como SSRF, uma das vulnerabilidades Top Ten 2021 do OWASP.

Caso um invasor consiga explorar tal vulnerabilidade, ele poderá

A) ler os conteúdos dos cookies que um navegador armazenou relativos a um dado domínio.

B) executar scripts no navegador da vítima, podendo inclusive realizar um sequestro de sessão do usuário.

C) injetar dados maliciosos no banco de dados da aplicação.

D) realizar requisições não autorizadas a outras localidades por meio do lado servidor dessa aplicação web vulnerável.

E) realizar uma desfiguração em qualquer página da aplicação web vulnerável.

Comentários:

Com taxa de incidência relativamente baixa, as vulnerabilidades da família Server-Side Request Forgery (SSRF), ou Falsificação de Solicitação no Lado do Servidor ocorrem sempre que uma aplicação busca um recurso remoto, sem validar a URL fornecida pelo usuário.

Gabarito: D

À luz das 10 categorias, vamos ver algumas questões adicionais:

FGV – Auditor de Controle Externo – Tecnologia da Informação (TCE-TO)/2022

A aplicação Web SiCONTA viabiliza a recuperação de credenciais de acesso por meio da conferência de respostas previamente cadastradas pelo usuário a questionamentos realizados a ele no processo de criação da credencial.

Considerando a metodologia Open Web Application Security Project (OWASP), a aplicação Web SiCONTA possui uma vulnerabilidade classificada na categoria:

a) Broken Access Control; ¬

b) Insecure Identification;

c) Security Misconfiguration;

d) Insecure Design and Implementation;

e) Identification and Authentication Failures.

Comentários:

Pessoal, questão bem tranquila né? Veja que a vulnerabilidade está associada ao processo de autenticação e identificação do usuário. Muito cuidado pois, o controle de acesso, trata-se de autorização e será a próxima fase do acesso ao serviço.

Reforço, a questão narra um problema associado ao usuário e senha, ou seja, ainda não se chegou na etapa de autorização, mas tão somente identificação e autenticação.

Muita atenção nesses detalhes.

Gabarito: E

CESPE / CEBRASPE Órgão: SERPRO Prova: CESPE / CEBRASPE - 2021 - SERPRO - Analista - Especialização: Desenvolvimento de Sistemas

Quanto aos riscos de segurança derivados da exposição de dados sensíveis contidos na lista OWASP Top 10, é recomendável que o tráfego de dados confidenciais seja criptografado e que

o seu armazenamento interno seja feito sem criptografia, de modo a viabilizar as funções de auditoria dos sistemas.

Comentários:

Pessoal, não há essa segregação do uso de criptografia, conforme a questão apresenta. Deve-se usar em toda a rede, na medida do possível, pois nunca se sabe onde o ataque pode ocorrer ou invasor possa estar.

Gabarito: E

CESPE / CEBRASPE - 2020 - Ministério da Economia - Tecnologia da Informação - Segurança da Informação e Proteção de Dados

O guia de testes do OWASP enumera verificações para cerca de setenta vulnerabilidades, agrupadas em classes, como a de gerenciamento de sessões, que trata de erros na implementação das regras de negócio.

Comentários:

Não há mais a categoria de gerenciamento de sessões.

Gabarito: E

QUESTÕES COMENTADAS - OWASP TOP 10 - CESPE

1. CESPE / CEBRASPE - 2022 - TCE-RJ - Analista de Controle Externo

Classificação de Risco para o Top 10 é uma metodologia baseada na OWASP Risk Rating Methodology e consiste em estimar, para cada categoria do Top 10, o risco peculiar que cada falha introduz em uma aplicação web típica e, posteriormente, ordenar o Top 10 de acordo com as falhas que tipicamente introduzem o risco mais significativo para uma aplicação.

Comentários:

Típica questão conceito pessoal, que aborda a metodologia de classificação de riscos da própria OWASP para se chegar à referida classificação.

Esse é um exemplo para o TOP 1 da lista:

CWEs mapeados - 34

Taxa de incidência máxima – 55,97%

Taxa média de incidência – 3,81%

Exploração média ponderada – 6,92

Impacto médio ponderado – 5,93

Cobertura máxima – 94,55%

Cobertura média – 47,72%

Total de Ocorrências – 318,487

Total de CVEs – 19,13

Gabarito: C

2. CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

Comentários:

Exatamente pessoal. Típica questão que demonstra que não temos para onde correr, a não ser passar por todas as medidas e prevenções do OWASP. Este item está previsto na prevenção de nº 6 do Controle A02:2021 - Falhas Criptográficas.

Gabarito: C

3. CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

Comentários:

Novamente, vejam que quando é para colocar a assertiva como CORRETA, a banca pega exatamente o texto apresentado.

Gabarito: C

4. CESPE / CEBRASPE - 2021 - SEFAZ-CE - Auditor Fiscal de Tecnologia da Informação da Receita Estadual

A inadequada configuração de segurança, um dos riscos da OWASP Top 10, pode ocorrer em qualquer nível de serviço de uma aplicação; em razão disso, o uso de scanners e testes automatizados é ineficaz na tarefa de detectar falhas de configuração.

Comentários:

Estamos falando do tipo de Controle A05 - Security Misconfiguration. Então, a primeira parte da questão está correta, pois, de fato, pode ocorrer em qualquer nível de serviço. Agora o erro está na segunda parte, ao afirmar que o uso de scanners e testes são ineficazes. Muito pelo contrário, esses testes ajudam, e muito nesse processo.

Gabarito: E

5. CESPE / CEBRASPE Órgão: SERPRO Prova: CESPE / CEBRASPE - 2021 - SERPRO - Analista - Especialização: Desenvolvimento de Sistemas

Quanto aos riscos de segurança derivados da exposição de dados sensíveis contidos na lista OWASP Top 10, é recomendável que o tráfego de dados confidenciais seja criptografado e que o seu armazenamento interno seja feito sem criptografia, de modo a viabilizar as funções de auditoria dos sistemas.

Comentários:

Pessoal, não há essa segregação do uso de criptografia, conforme a questão apresenta. Deve-se usar em toda a rede, na medida do possível, pois nunca se sabe onde o ataque pode ocorrer ou invasor possa estar.

Gabarito: E

6. CESPE / CEBRASPE - 2020 - Ministério da Economia - Tecnologia da Informação - Segurança da Informação e Proteção de Dados

O guia de testes do OWASP enumera verificações para cerca de setenta vulnerabilidades, agrupadas em classes, como a de gerenciamento de sessões, que trata de erros na implementação das regras de negócio.

Comentários:

Não há mais a categoria de gerenciamento de sessões.

Gabarito: E

Questões Comentadas - OWASP TOP 10 - FGV

1. (FGV - AJ (TJ RN)/TJ RN/Apoio Especializado/Análise de Sistemas/2023)

O COLABORA é um sistema que apoia atividades da gestão de recursos humanos de uma empresa e, por isso, mantém alguns dados sensíveis sobre pessoas. O COLABORA faz uso do módulo pgcrypto do PostgreSQL para criptografar colunas que armazenam os dados sensíveis.

Com base no OWASP Top Tem, a solução de criptografia adotada pelo COLABORA apresenta uma vulnerabilidade categorizada como:

a) A01:2021 – Data Exposure;

b) A02:2021 – Cryptographic Failures;

c) A03:2021 – Broken or Risky Crypto Algorithm;

d) A05:2021 – Security Misconfiguration;

e) A08:2021 – Software and Data Integrity Failures.

Comentários:

Estamos observando um recurso associado aos aspectos de criptografia aplicada a banco de dados, e que se a criptografia falhar, podemos ter problemas. Vejam um exemplo do próprio OWASP:

Cenário #1 : Um aplicativo criptografa números de cartão de crédito em um banco de dados usando criptografia automática de banco de dados. No entanto, esses dados são automaticamente descriptografados quando recuperados, permitindo que uma falha de injeção de SQL recupere números de cartão de crédito em texto não criptografado.

Gabarito: B

2. FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

A falha ou quebra de controle de acesso ("Broken Access Control") é um risco de segurança crítico para aplicações Web.

Para prevenir essa vulnerabilidade, o OWASP recomenda que

A a listagem de diretórios do servidor web seja desativada.

B os tokens JWT stateless sejam de longa duração.

C as sessões stateful sejam mantidas no servidor após o logout.

D evite reutilizar os mecanismos de controle de acesso.

E utilize APIs sem taxa limite de requisições.

Comentários:

Exatamente conforme o item V previsto na prevenção:

V. Desative a listagem de diretórios do servidor web e certifique-se de que os metadados do arquivo (por exemplo, .git) e os arquivos de backup não estejam presentes nas raízes da web.

Gabarito: A

3. FGV - 2022 - TJ-DFT - Analista Judiciário - Análise de Sistemas

PedidosSemEstresse é uma aplicação Web destinada a digitalizar o processo de pedidos de serviços de um órgão da administração pública. A interface de PedidosSemEstresse utilizada pelos usuários faz chamadas a uma API RESTful e não utiliza facilidades de login único (single sign-on – SSO). Recentemente, o usuário interno João utilizou suas próprias credenciais com privilégios somente de execução de métodos GET para explorar vulnerabilidades e teve acesso direto a API RESTful. Assim, João fez chamadas a métodos POST com sucesso.

Com base no OWASP Top Ten, a vulnerabilidade explorada por João é da categoria:

A Injection;

B Broken Access Control;

C Software and Data Integrity Failures;

D Vulnerable and Outdated Components;

E Identification and Authentication Failures

Comentários:

Vejam que estamos na mesma linha da questão anterior, onde há uma falha de autorização, uma vez que um usuário, que tinha permissão somente para determinada ação, consegue realizar outra ação.

Gabarito: B

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De modo a prevenir falhas de injeção de dados maliciosos, recomenda-se não usar, para o transporte de dados confidenciais, protocolos legados, como FTP e SMTP.

Comentários:

Pessoal, a descrição em tela se refere a recomendações de prevenção da categoria de FALHAS CRIPTOGRÁFICAS e não de INJEÇÃO DE DADOS. Vejam justamente a dinâmica que comentei com vocês sobre troca de características.

Gabarito: E

5. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De acordo com a OWASP TOP 10 2021, para o risco design inseguro, são medidas de prevenção para o desenvolvimento seguro o uso da modelagem de ameaças para autenticações críticas, controle de acesso e lógica de negócios.

Comentários:

Exatamente na linha do que conversamos pessoal.

Gabarito: C

6. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Comentários:

Certo pessoal. Ambos são viáveis, e não são as únicas hipóteses.

Gabarito: C

7. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Ao analisar uma aplicação web, um auditor verificou que ela estava vulnerável a um ataque conhecido como SSRF, uma das vulnerabilidades Top Ten 2021 do OWASP.

Caso um invasor consiga explorar tal vulnerabilidade, ele poderá

A) ler os conteúdos dos cookies que um navegador armazenou relativos a um dado domínio.

B) executar scripts no navegador da vítima, podendo inclusive realizar um sequestro de sessão do usuário.

C) injetar dados maliciosos no banco de dados da aplicação.

D) realizar requisições não autorizadas a outras localidades por meio do lado servidor dessa aplicação web vulnerável.

E) realizar uma desfiguração em qualquer página da aplicação web vulnerável.

Comentários:

Com taxa de incidência relativamente baixa, as vulnerabilidades da família Server-Side Request Forgery (SSRF), ou Falsificação de Solicitação no Lado do Servidor ocorrem sempre que uma aplicação busca um recurso remoto, sem validar a URL fornecida pelo usuário.

Gabarito: D

8. FGV – Auditor de Controle Externo – Tecnologia da Informação (TCE-TO)/2022

A aplicação Web SiCONTA viabiliza a recuperação de credenciais de acesso por meio da conferência de respostas previamente cadastradas pelo usuário a questionamentos realizados a ele no processo de criação da credencial.

Considerando a metodologia Open Web Application Security Project (OWASP), a aplicação Web SiCONTA possui uma vulnerabilidade classificada na categoria:

a) Broken Access Control; ¬

b) Insecure Identification;

c) Security Misconfiguration;

d) Insecure Design and Implementation;

e) Identification and Authentication Failures.

Comentários:

Pessoal, questão bem tranquila né? Veja que a vulnerabilidade está associada ao processo de autenticação e identificação do usuário. Muito cuidado pois, o controle de acesso, trata-se de autorização e será a próxima fase do acesso ao serviço.

Reforço, a questão narra um problema associado ao usuário e senha, ou seja, ainda não se chegou na etapa de autorização, mas tão somente identificação e autenticação.

Muita atenção nesses detalhes.

Gabarito: E

QUESTÕES COMENTADAS - OWASP TOP 10 - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

O OWASP Top 10 2021 elenca os problemas de segurança mais comuns e mais importantes no contexto das aplicações web. O problema de segurança que ocupa a primeira posição é:

a) Falha criptográfica.

b) Injeção.

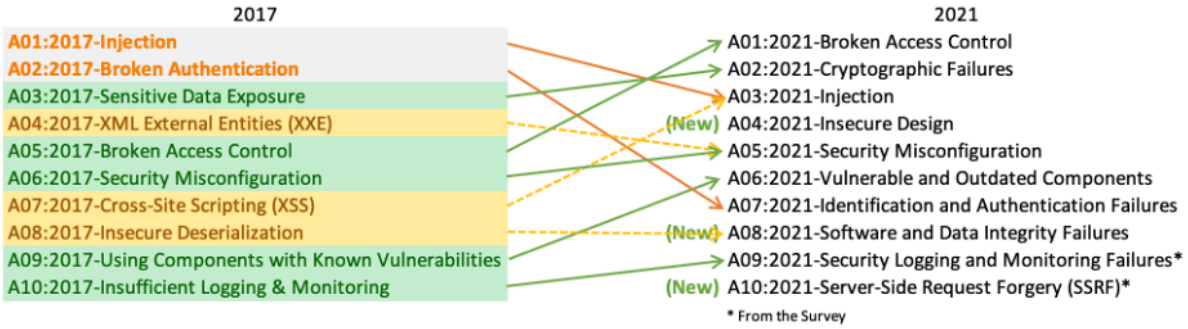
c) Quebra de controle de acesso.

d) Design inseguro.

e) Server-Side Request Forgery.

Comentários:

Mais uma típica questão decoreba da FCC.



Gabarito: C

Lista de Questões - OWASP TOP 10 - CESPE

1. CESPE / CEBRASPE - 2022 - TCE-RJ - Analista de Controle Externo

Classificação de Risco para o Top 10 é uma metodologia baseada na OWASP Risk Rating Methodology e consiste em estimar, para cada categoria do Top 10, o risco peculiar que cada falha introduz em uma aplicação web típica e, posteriormente, ordenar o Top 10 de acordo com as falhas que tipicamente introduzem o risco mais significativo para uma aplicação.

2. CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

3. CESPE / CEBRASPE - 2022 - BANRISUL - Desenvolvimento de Sistemas

No que se refere a falhas de criptografia, recomenda-se desabilitar o cache para respostas que contenham dados sensíveis.

4. CESPE / CEBRASPE - 2021 - SEFAZ-CE - Auditor Fiscal de Tecnologia da Informação da Receita Estadual

A inadequada configuração de segurança, um dos riscos da OWASP Top 10, pode ocorrer em qualquer nível de serviço de uma aplicação; em razão disso, o uso de scanners e testes automatizados é ineficaz na tarefa de detectar falhas de configuração.

5. CESPE / CEBRASPE Órgão: SERPRO Prova: CESPE / CEBRASPE - 2021 - SERPRO - Analista - Especialização: Desenvolvimento de Sistemas

Quanto aos riscos de segurança derivados da exposição de dados sensíveis contidos na lista OWASP Top 10, é recomendável que o tráfego de dados confidenciais seja criptografado e que o seu armazenamento interno seja feito sem criptografia, de modo a viabilizar as funções de auditoria dos sistemas.

6. CESPE / CEBRASPE - 2020 - Ministério da Economia - Tecnologia da Informação - Segurança da Informação e Proteção de Dados

O guia de testes do OWASP enumera verificações para cerca de setenta vulnerabilidades, agrupadas em classes, como a de gerenciamento de sessões, que trata de erros na implementação das regras de negócio.

GABARITO

GABARITO

1. C
2. C
3. C
4. E
5. E
6. E

Lista de Questões - OWASP TOP 10 - FGV

1. (FGV - AJ (TJ RN)/TJ RN/Apoio Especializado/Análise de Sistemas/2023)

O COLABORA é um sistema que apoia atividades da gestão de recursos humanos de uma empresa e, por isso, mantém alguns dados sensíveis sobre pessoas. O COLABORA faz uso do módulo pgcrypto do PostgreSQL para criptografar colunas que armazenam os dados sensíveis.

Com base no OWASP Top Tem, a solução de criptografia adotada pelo COLABORA apresenta uma vulnerabilidade categorizada como:

a) A01:2021 – Data Exposure;

b) A02:2021 – Cryptographic Failures;

c) A03:2021 – Broken or Risky Crypto Algorithm;

d) A05:2021 – Security Misconfiguration;

e) A08:2021 – Software and Data Integrity Failures.

2. FGV - 2022 - TRT - 13ª Região (PB) - Técnico Judiciário - Tecnologia da Informação

A falha ou quebra de controle de acesso ("Broken Access Control") é um risco de segurança crítico para aplicações Web.

Para prevenir essa vulnerabilidade, o OWASP recomenda que

A a listagem de diretórios do servidor web seja desativada.

B os tokens JWT stateless sejam de longa duração.

C as sessões stateful sejam mantidas no servidor após o logout.

D evite reutilizar os mecanismos de controle de acesso.

E utilize APIs sem taxa limite de requisições.

3. FGV - 2022 - TJ-DFT - Analista Judiciário - Análise de Sistemas

PedidosSemEstresse é uma aplicação Web destinada a digitalizar o processo de pedidos de serviços de um órgão da administração pública. A interface de PedidosSemEstresse utilizada pelos usuários faz chamadas a uma API RESTful e não utiliza facilidades de login único (single sign-on – SSO). Recentemente, o usuário interno João utilizou suas próprias credenciais com privilégios somente de execução de métodos GET para explorar vulnerabilidades e teve acesso direto a API RESTful. Assim, João fez chamadas a métodos POST com sucesso.

Com base no OWASP Top Ten, a vulnerabilidade explorada por João é da categoria:

A Injection;

B Broken Access Control;

C Software and Data Integrity Failures;

D Vulnerable and Outdated Components;

E Identification and Authentication Failures

4. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De modo a prevenir falhas de injeção de dados maliciosos, recomenda-se não usar, para o transporte de dados confidenciais, protocolos legados, como FTP e SMTP.

5. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

De acordo com a OWASP TOP 10 2021, para o risco design inseguro, são medidas de prevenção para o desenvolvimento seguro o uso da modelagem de ameaças para autenticações críticas, controle de acesso e lógica de negócios.

6. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

7. FGV - 2022 - SEFAZ-AM - Analista de Tecnologia da Informação da Fazenda Estadual

Ao analisar uma aplicação web, um auditor verificou que ela estava vulnerável a um ataque conhecido como SSRF, uma das vulnerabilidades Top Ten 2021 do OWASP.

Caso um invasor consiga explorar tal vulnerabilidade, ele poderá

A) ler os conteúdos dos cookies que um navegador armazenou relativos a um dado domínio.

B) executar scripts no navegador da vítima, podendo inclusive realizar um sequestro de sessão do usuário.

C) injetar dados maliciosos no banco de dados da aplicação.

D) realizar requisições não autorizadas a outras localidades por meio do lado servidor dessa aplicação web vulnerável.

E) realizar uma desfiguração em qualquer página da aplicação web vulnerável.

8. FGV – Auditor de Controle Externo – Tecnologia da Informação (TCE-TO)/2022

A aplicação Web SiCONTA viabiliza a recuperação de credenciais de acesso por meio da conferência de respostas previamente cadastradas pelo usuário a questionamentos realizados a ele no processo de criação da credencial.

Considerando a metodologia Open Web Application Security Project (OWASP), a aplicação Web SiCONTA possui uma vulnerabilidade classificada na categoria:

a) Broken Access Control; ¬

b) Insecure Identification;

c) Security Misconfiguration;

d) Insecure Design and Implementation;

e) Identification and Authentication Failures.

GABARITO

GABARITO

1. B
2. A
3. B
4. E
5. C
6. C
7. D
8. E

Lista de Questões - OWASP TOP 10 - FCC

1. (FCC - Ana (COPERGÁS)/COPERGÁS/Sistemas/2023)

O OWASP Top 10 2021 elenca os problemas de segurança mais comuns e mais importantes no contexto das aplicações web. O problema de segurança que ocupa a primeira posição é:

a) Falha criptográfica.

b) Injeção.

c) Quebra de controle de acesso.

d) Design inseguro.

e) Server-Side Request Forgery.

GABARITO

1. C

ESSA LEI TODO MUNDO CONHECE:
PIRATARIA É CRIME.

Mas é sempre bom revisar o porquê e como você pode ser prejudicado com essa prática.

1. 

Professor investe seu tempo para elaborar os cursos e o site os coloca à venda.

2. 

Pirata divulga ilicitamente (grupos de rateio), utilizando-se do anonimato, nomes falsos ou laranjas (geralmente o pirata se anuncia como formador de "grupos solidários" de rateio que não visam lucro).

3. 

Pirata cria alunos fake praticando falsidade ideológica, comprando cursos do site em nome de pessoas aleatórias (usando nome, CPF, endereço e telefone de terceiros sem autorização).

4. 

Pirata compra, muitas vezes, clonando cartões de crédito (por vezes o sistema anti-fraude não consegue identificar o golpe a tempo).

5. 

Pirata fere os Termos de Uso, adultera as aulas e retira a identificação dos arquivos PDF (justamente porque a atividade é ilegal e ele não quer que seus fakes sejam identificados).

6. 

Pirata revende as aulas protegidas por direitos autorais, praticando concorrência desleal e em flagrante desrespeito à Lei de Direitos Autorais (Lei 9.610/98).

7. 

Concurseiro(a) desinformado participa de rateio, achando que nada disso está acontecendo e esperando se tornar servidor público para exigir o cumprimento das leis.

8. 

O professor que elaborou o curso não ganha nada, o site não recebe nada, e a pessoa que praticou todos os ilícitos anteriores (pirata) fica com o lucro.

Deixando de lado esse mar de sujeira, aproveitamos para agradecer a todos que adquirem os cursos honestamente e permitem que o site continue existindo.