By @kakashi_copiador

Estratégia Concursos

Aula 03

Caixa Econômica Federal (CEF) (Técnico Bancário) Passo Estratégico de Informática - 2023 (Pré-Edital)

Autor:
Thiago Rodrigues Cavalcanti

29 de Dezembro de 2022

Segurança da informação: fundamentos, conceitos e mecanismos de segurança; Segurança cibernética: Resolução CMN nº 4893, de 26 de fevereiro de 2021

Sumário

ANÁLISE ESTATÍSTICA

Inicialmente, convém destacar os percentuais de incidência de todos os assuntos previstos no nosso curso – quanto maior o percentual de cobrança de um dado assunto, maior sua importância:

Assunto	Grau de incidência em concursos similares CESGRANRIO
8 - Visão geral sobre sistemas de suporte à decisão e inteligência de negócio.	23,49%
1 - Edição de planilhas (ambientes Microsoft Office - Excel - versão O365).	20,13%
4 - Redes de computadores: Conceitos básicos, ferramentas, aplicativos e procedimentos de Internet e intranet.	14,09%
1 - Edição de textos (ambientes Microsoft Office - Word - versão O365).	9,40%
2 - Segurança da informação: fundamentos, conceitos e mecanismos de segurança; Segurança cibernética: Resolução CMN nº 4893, de 26 de fevereiro de 2021.	9,40%
3 - Conceitos de organização e de gerenciamento de informações, arquivos, pastas e programas.	7,38%
1 - Edição de apresentações (ambientes Microsoft Office - PowerPoint - versão O365).	6,71%
6 - Correio eletrônico, grupos de discussão, fóruns e wikis. 7 - Redes Sociais (Twitter, Facebook, Linkedin, WhatsApp, YouTube, Instagram e Telegram).	6,04%
5 - Navegador Web (Microsoft Edge versão 91 e Mozilla Firefox versão 78 ESR).	3,36%
9 - Conceitos de tecnologias e ferramentas multimídia, de reprodução de áudio e vídeo. 10 - Ferramentas de produtividade e trabalho a distância (Microsoft Teams, Cisco Webex, Google Hangout, Zoom, Google Drive e Skype).	0,00%

ROTEIRO DE REVISÃO E PONTOS DO ASSUNTO QUE MERECEM DESTAQUE

A ideia desta seção é apresentar um roteiro para que você realize uma revisão completa do assunto e, ao mesmo tempo, destacar aspectos do conteúdo que merecem atenção.

Para revisar e ficar bem preparado no assunto, você precisa, basicamente, seguir os passos a seguir:

Segurança da Informação

A segurança de redes é um tema muito discutido por gestores e analistas de TI. A cada ano que passa, grandes investimentos são feitos para proteger a privacidade, integridade e disponibilidade das informações. Tudo isso por causa dos crescentes ataques e sequestros de dados que atingem diversas pessoas e empresas ao redor do mundo – que duplicaram no ano de 2017, segundo pesquisa da ISOC (Internet Society).

Conceitos Básicos

Os conceitos de segurança da informação estão diretamente relacionados com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.

De acordo com a norma ISO 17799:2005, "segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio".

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos das políticas de segurança, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais. Entretanto, "muitas vezes é difícil obter o apoio da própria alta administração da organização para realizar os investimentos necessários em segurança da informação. Os custos elevados das soluções contribuem para esse cenário, mas o desconhecimento da importância do tema é provavelmente ainda o maior problema". (CAMPOS, 2007)[1]

O Decreto Nº 3.505 de 13 de junho de 2000 instituído pelo presidente da República Federativa do Brasil, define segurança da informação como:

> *Art. 2. Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:*
>
> *II – Segurança da Informação: proteção dos sistemas de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão, e a modificação desautorizada de dados ou informações, armazenados, em processamento ou em trânsito, abrangendo, inclusive, a segurança dos recursos humanos, da documentação e do material, das áreas e instalações das comunicações e computacional, assim como as destinadas a prevenir, detectar, deter e documentar eventuais ameaças a seu desenvolvimento.*

[1] CAMPOS, A. Sistema de segurança da informação: controlando os riscos. Florianópolis: Visual Books, 2ª ed, 2007.

Dessa forma, a segurança da informação é imprescindível para qualquer organização tanto do ponto de vista estratégico, quanto do tático e operacional.

Antes de falar sobre as políticas de segurança, precisamos entender que na segurança da informação existem quatro princípios básicos, definidos na norma ABNT NBR ISO/IEC 27002:2005, que fundamentam a proteção dos dados. A partir do quadro abaixo vamos citar e definir cada um destes princípios.

O dicionário Aurélio nos dá, entre os dezesseis significados de princípio, dois que se encaixam bem dentro deste contexto: 1 - Frase ou raciocínio que é base de uma arte, de uma ciência ou de uma teoria; 2 - Regras ou conhecimentos fundamentais e mais gerais. Ou seja, um princípio é uma definição sobre algo que se almeja.

Princípio		Definição
D isponibilidade	-	Princípio que garante que a informação estará sempre disponíveis.
I ntegridade	-	Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações.
C onfidencialidade	-	Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha.
A utenticidade	-	Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações.

Note que foi formado o mnemônico **DICA** para facilitar a memorização e associação das definições.

É importante notar que nos princípios sempre está presente a partícula "...idade". Por exemplo: caso a banca cite o princípio da autenticação, estará incorreto. O correto é "Princípio da Autentic**idade**".

Algumas bancas indicam o Não Repúdio como parte dos princípios de segurança da informação, porém ele só é efetivamente usado junto com o princípio da Autenticidade que garante que as informações são verídicas e por este motivo não podem ser refutadas.

N ão Repúdio (Irrefutabilidade)	-	Incapacidade de negação da autoria de uma informação. (Este princípio está ligado diretamente ao princípio da Autenticidade)

Princípios

Disponibilidade

O operacional de uma organização depende diretamente desse princípio, pois ele está relacionado ao tempo e à acessibilidade que se tem dos dados e sistemas, ou seja, se eles podem ser consultados a qualquer momento pelos colaboradores.

Praticamente todos os processos de trabalho de uma organização dependem da chegada ou busca de uma informação. Quando a informação está indisponível, os processos que dependem dela ficam impedidos de serem executados.

Integridade

Esse princípio é absolutamente crítico do ponto de vista operacional, pois valida todo o processo de comunicação em uma organização. Conforme vimos na tabela acima, é importante que os dados circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los ou comprometê-los.

Toda organização se comunica interna e externamente o tempo todo, transmitindo números, resultados, projeções, estratégias, regras, procedimentos e dados em todas as direções; e a comunicação efetiva só acontece quando o emissor e o receptor da informação a interpretam da mesma maneira.

Informação sem integridade demanda verificação, correção e retrabalho, que causa desperdício de energia, traduzido em perda de recursos, seja tempo, pessoal ou financeiro.

Confidencialidade

A norma ISO/IEC 17799 define confidencialidade como “garantir que a informação seja acessível apenas àqueles autorizados a ter acesso”. Com isso, chegamos à conclusão que a confidencialidade tem a ver com a privacidade dos dados de uma organização. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas dos sistemas organizacionais por meio de cyber ataques, espionagem, entre outras práticas.

Para que a confidencialidade seja reforçada, as organizações adotam medidas preventivas, como por exemplo a definição dos níveis de acesso as informações. Isso garante que apenas pessoas autorizadas terão acesso a dados sensíveis para a organização. Os níveis também precisam ser limitados conforme as áreas a que se relacionam (marketing, vendas, financeiro, administração, etc.).

Além de níveis de acesso para as pessoas, os dados são classificados de acordo com o potencial de impacto, caso sejam acessados por pessoas indevidas. Dessa forma as organizações criam modelos de contingencia que abrangem todas as possibilidades.

Autenticidade

Esse princípio identifica e registra as ações de envio ou edição de uma informação, realizadas pelo usuário. Toda ação é documentada, garantido a autenticidade da informação proveniente de uma fonte confiável. Acima citei que esse princípio torna a informação irrefutável, ou seja, a pessoa que cria, edita ou exclui um dado, não pode negar a sua ação.

Métodos Relacionados aos Princípios

Disponibilidade

Um exemplo de disponibilidade é o site para inscrição em um concurso. Dependendo do concurso pode acontecer de o site ficar ”fora do ar”, ferindo o princípio e causando uma indisponibilidade. Isso normalmente ocorre quando os recursos acessados estão ultrapassando o limite fornecido pelo servidor.

Integridade

Em um arquivo é utilizada uma função *hash*, que mapeia os dados de comprimento variável para dados de comprimento fixo, criando, a partir dos valores retornados, um código *hash* ou *checksum*. Os algoritmos da função *hash* mais utilizados são MD5 e SHA-1. Os códigos gerados são únicos para cada arquivo, possuem tamanho entre 20 e 256 caracteres e a partir do código gerado não é possível retornar ao arquivo, ou seja, é um processo de via única.

Confidencialidade

O uso de criptografia garante o sigilo quando a informação é confidencial. Existem dois métodos de criptografia: chaves simétricas e chaves assimétricas (com ou sem certificado digital). Além desses métodos, pode ser implantada a autenticação de dois fatores, a verificação biométrica e o uso de token.

Autenticidade

O reconhecimento de firma em um cartório é um exemplo de um método de autenticidade. Em informática o uso de certificado digital é o que garante a autenticidade.

Chave Simétrica está relacionada diretamente a uma senha única.

Chave Assimétrica está relacionada a duas chaves diferentes que são correspondentes – chave pública e chave privada. A chave pública, como o próprio no diz, qualquer pessoa possui acesso. A chave privada apenas o próprio dono tem acesso. Quando um arquivo é criptografado com a chave pública, apenas o proprietário da chave privada poderá ter acesso a informação.

Noções de vírus, worms e pragas virtuais

Uma ameaça acontece quando há uma ação sobre uma pessoa ou sobre um processo fazendo uso de uma fraqueza, causando um problema ou consequência.

A partir das ameaças podem surgir ataques. Um ataque pode ser decorrente da invasão de um sistema de segurança com intuito de tornar vulnerável os sistemas e serviços. Eles são divididos em ativo, passivo e destrutivo; o ativo modifica os dados, o passivo libera os dados e o destrutivo impede qualquer acesso aos dados. Os ataques podem ser realizados a partir da ação de um vírus ou do uso de técnicas específicas.

Malware

Malware é um termo abreviado para *malicious software* (software malicioso). Esse software é criado especificamente para obter acesso ou danificar um computador, sem o conhecimento do seu proprietário. Existem vários tipos de malware, incluindo spyware, keyloggers, vírus verdadeiros, worms ou qualquer outro tipo de código malicioso que se infiltra em um computador.

Normalmente um software é considerado malware com base na intenção de seu criador e não nas funcionalidades para as quais foi criado. Originalmente ele foi criado para experimentos e pegadinhas, mas acabou resultando em vandalismo e destruição dos computadores alvo. Atualmente, a maioria do malware é criada para a obtenção de lucros por meio de publicidade forçada (adware), roubo de informações confidenciais (spyware), propagação de spam ou pornografia infantil por e-mail (computadores zumbi) ou propagação de extorsões financeiras (ransomware).

Vírus

Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.

Para que o vírus contamine o computador, será necessário executar o programa infectado, o que por sua vez obriga o código do vírus a ser executado. Isso significa que um vírus pode permanecer inativo em seu computador, sem demonstrar nenhum sinal ou sintoma. Porém, quando o vírus contamina o computador, ele pode também contaminar outros computadores na mesma rede. Roubar senhas ou dados, registrar o uso do teclado, corromper arquivos, enviar spam aos seus contatos de e-mail e até mesmo controlar o seu computador são apenas algumas das ações irritantes e devastadoras que um vírus pode executar.

Os vírus podem se propagar através de anexos de e-mail ou mensagens de texto, downloads de arquivos da Internet e links para golpes em mídias sociais. Até mesmo os dispositivos móveis e smartphones podem ser infectados com vírus através do download de aplicativos duvidosos nesses dispositivos. Os vírus podem se esconder disfarçados como anexos de conteúdos compartilhados socialmente, como imagens humorísticas, cartões comemorativos ou arquivos de áudio e vídeo.

Existem muitos tipos de vírus e eles são classificados de acordo com a sua ação sobre o computador. Vamos entender como cada um dele funcionam.

Spyware

De forma simples e direta, é um software de espionagem, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. Normalmente entra em seu computador sem o seu conhecimento ou permissão e é executado em segundo plano.

O spyware é conhecido por capturar e transmitir informações altamente pessoais como contas bancárias online e senhas, ou informações de cartão de crédito.

As formas como o spyware captura as informações subdivide sua classificação.

Registro de toques nas teclas

Chamados de "keyloggers", esse tipo de spyware é usado para coletar senhas e rastrear comunicações em que o teclado é utilizado.

Acompanhamento das atividades

Alguns cookies de rastreamento podem, indiscutivelmente, ser considerados spyware, no sentido que eles acompanham seus movimentos online e relatam o que você visita aos publicitários, para que eles possam servir informações mais pertinentes a você.

Redução da velocidade do dispositivo

Frequentemente, o único sinal que denuncia que você está infectado com spyware será a maneira parasita com que ele rouba potência de processamento e largura de banda de Internet para comunicar o que foi roubado.

Cavalo de Tróia

O cavalo de Tróia é um malware disfarçado de software legítimo para obter acesso aos sistemas dos usuários. Uma vez ativados, os cavalos de Tróia permitem que os criminosos espionem, roubem dados confidenciais e obtenham acesso ao sistema através de uma backdoor. Ele se confunde em algumas características com o spyware. Os principais tipos de cavalo de Tróia são:

Backdoor

Com um cavalo de Tróia backdoor, usuários maliciosos controlam remotamente o computador infectado. Os cavalos de Tróia backdoor costumam ser usados para reunir um conjunto de computadores e formar uma rede zumbi, que pode ser usada para fins criminosos.

Exploit

Exploits são programas que contêm dados ou códigos que tiram proveito de uma vulnerabilidade do software de um aplicativo executado no computador.

Rootkit

Os rootkits têm como objetivo ocultar certos objetos ou atividades no sistema. Geralmente, o principal objetivo é evitar a detecção de programas maliciosos para estender o período em que os programas são executados em um computador infectado.

Trojan-Banker

Programas Trojan-Banker são criados para roubar dados de contas de sistemas de bancos on-line, pagamentos eletrônicos e cartões de débito e crédito.

Spam

O spam é o equivalente eletrônico das correspondências indesejadas enviadas pelo correio e das ligações de telemarketing. Apesar de certos de tipos de spam serem apenas publicidade indesejada, porém legítima, outros são muito piores. Eles podem incluir todo tipo de golpe, desde ofertas falsas até códigos maliciosos, criados para causar destruição na sua situação financeira ou em seu computador, pois podem ser usados para transmitir Cavalos de Tróia, vírus, worms, spywares e ataques de phishing direcionados. O spam representa aproximadamente 80% do volume de e-mails em todo o mundo.

Phishing

É basicamente um golpe on-line de falsificação. Os phishers enviam e-mails que tentam imitar mensagens de empresas financeiras legítimas ou de outras empresas e instituições que você talvez até utilize. O e-mail de phishing do spam solicitará que você acesse um site falso para reinserir o número do seu cartão de crédito ou verificar sua senha. A partir da inserção desses dados eles têm acesso a todas as informações necessárias para aplicar golpes.

Worm

Um worm é um software malicioso capaz de se autorreplicar em computadores ou por redes de computadores sem que você desconfie que sua máquina foi infectada. Como cada cópia subsequente do worm também consegue se autorreplicar, as infecções podem se disseminar muito rapidamente. Há diversos tipos de worms, sendo que muitos deles podem causar altos níveis de destruição. Eles podem explorar erros de configuração da rede (por exemplo, copiar a si mesmos em um disco totalmente acessível) ou explorar brechas na segurança do sistema operacional e dos aplicativos. Muitos worms usam mais de um método para propagar cópias pelas redes.

Ransomware

O ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é cobrado em bitcoins.

O ransomware pode se propagar de diversas formas, embora as mais comuns sejam: através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link; ou explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança.

Botnet

Botnet é uma palavra formada pelos termos robot e network que indica um grupo de computadores conectados à Internet, cada um deles rodando um ou mais bots que se comunicam com outros dispositivos, a fim de executar determinada tarefa. O termo também pode ser aplicado a uma rede de agentes de software ou bots que executam tarefas de maneira autônoma e automática. Pode se referir, ainda, a uma rede de computadores que utilizam software de computação distribuída.

Entretanto a palavra botnet geralmente é associada ao uso de software malicioso, para realizar ataques distribuídos de negação de serviço (ataque DDoS), seja mediante o envio de spam, seja permitindo que o invasor acesse o dispositivo e sua conexão, a fim de furtar dados. Esses ataques geralmente utilizam computadores infectados para atacar outros computadores sem que o usuário perceba essa ação.

Ferramentas e dispositivos de segurança

Existem várias formas para promover a proteção dos arquivos e o controle de segurança. Abaixo vamos listar algumas das mais cobradas em concursos.

Autenticação e Autorização

De acordo com o dicionário Aurélio, autenticação é o ato de autenticar, que significa "validar; reconhecer algo como verdadeiro; admitir a autenticidade, a veracidade de algo. Legitimar; reconhecer como verídico; validar de modo jurídico: o notório autenticou o documento".

Para Hutington[2], o processo de autenticação é aquele capaz de determinar se alguém é quem está dizendo ser. Tal procedimento pode ser realizado a partir de uma senha, um token, cartão ID ou uma leitura biométrica e é realizado com base em uma medida de riscos onde sistemas aplicações e informações de alto risco exigem diferentes formas de autenticação que confirmem de forma mais precisa a identidade digital do usuário enquanto aplicações de baixo risco onde a confirmação da identidade digital não é tão importante. Este conceito é normalmente referido como "autenticação forte". O autor enumera diversos tipos de autenticação tal como PKI, biométrica, senha entre outras, mas nota-se que todas elas possuem similaridades que nos permite agrupa-las nos chamados fatores de autenticação.

Fatores e Métodos de Autenticação

Os fatores de autenticação, são de forma geral classificados em três categorias distintas: **O que você tem**, **o que você é** e **o que você sabe**.

"O que você sabe" – Autenticação baseada no conhecimento

[2] Huntington, Guy. The Business of Authentication. 27-Jun-2009. disponível em <http://www.authenticationworld.com/>.

Para se autenticar é necessário saber previamente alguma informação para ser validado, a senha é o melhor exemplo deste método. Você precisa informar ela corretamente, do contrário não será autenticado, e terá o acesso barrado.

A vantagem deste método é que ele já é amplamente difundido e simples de ser utilizado. Já o grande problema é que outra pessoa pode saber ou até mesmo descobrir a sua senha, ao realizar diversas tentativas.

"O que você tem" – Autenticação baseada na propriedade

Nesta categoria você só é autenticado se você possuir algum dispositivo. Um bom exemplo deste tipo é o token, o dispositivo gera uma nova senha a cada período de tempo, desta maneira, é preciso ter o token para se autenticar. Caso outra pessoa obseve a senha enquanto você digita a senha para entrar no site bancário, em questão de minutos esta senha será trocada, e a senha observada não servirá mais.

Esta categoria já se mostra mais segura que a anterior, pois é necessário ter a posse do cartão ou do token, e caso outra pessoa consiga estes dispositivos o proprietário notaria a falta, o usuário pode solicitar um novo cartão ou token.

Mas, mesmo esta categoria apresenta alguns riscos, no caso do cartão de senhas, os criminosos criam páginas falsas de bancos que pedem todas as senhas do cartão da vítima. No caso dos tokens, existe a possibilidade da empresa que cria os tokens ter suas chaves roubadas, e com isto permite que os criminosos se passem pela vítima.

"O que você é" – Autenticação baseada na característica

Nesta categoria a autenticação é mais rigorosa, apenas a princípio apenas a própria pessoa pode ser autenticada, isto porque é utilizado a biometria, um bom exemplo deste tipo é a leitura da impressão digital.

Há também outros tipos de biometria não tão populares, como escaneamento de veias, identificação da íris, reconhecimento da voz, e outros.

Note que os métodos de autenticação que utilizam a biometria são mais seguros que os demais, mas mesmo assim não garante 100% de segurança, como já foi noticiado que pessoas utilizavam um molde de silicone da digital de outra pessoa para passar pelo leitor de impressão digital.

Autorizar

É o mecanismo responsável por garantir que apenas usuários autorizados consumam os recursos protegidos de um sistema computacional. Os recursos incluem arquivos, programas de computador, dispositivos de hardware e funcionalidades disponibilizadas por aplicações instaladas em um sistema.

Prevenção Contra Riscos e Códigos Maliciosos

Antivírus

Com a finalidade de garantir um nível de segurança, é necessário instalar um programa de antivírus. Os antivírus e anti-malwares são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador

e outros tipos de softwares nocivos ao sistema operacional. Ele funciona identificando, bloqueando e alertando ao usuário sobre a ação de um vírus em e-mails e outros arquivos. Caso algum seja encontrado, o antivírus coloca em quarentena (isola) o vírus ou o exclui completamente, antes que ele danifique o computador e os arquivos.

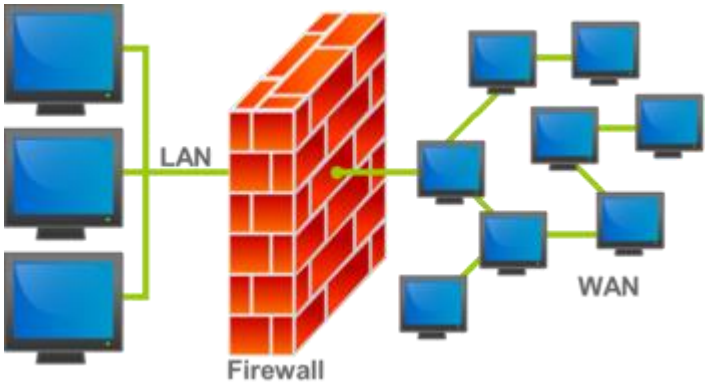
A principal diferença entre antivírus pago e antivírus gratuito é que as versões pagas oferecem proteções extras, que em sua grande maioria não disponíveis nas versões grátis.

Como exemplos de antivírus gratuitos mais conhecidos temos: AVG, Avast, Avira e Microsoft Security Essential.

Como exemplos de antivírus pagos temos: Kaspersky, BitDefender, McAfee e Norton.

Firewall

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma "parede de fogo" que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware, onde a combinação de ambos é chamada tecnicamente de "appliance".



Sua complexidade depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado. A partir das regras, o firewall pode ajudar a impedir o acesso de hackers e softwares mal-intencionados aos computadores conectados na rede.

Na sua forma mais simples de implementação, o firewall funciona como um filtro de pacotes (stateless) que pode ser configurado tanto para a rede interna, quanto para a rede externa (Internet). A outra forma de configuração é a de estado de sessão (statefull), onde o firewall analisa os pacotes e guarda o estado de cada conexão de maneira que seja possível para identificar e fazer uma previsão das respostas legítimas, de forma a impedir o tráfego de pacotes ilegítimos.

Normalmente o firewall é implementado em dispositivos que fazem a separação das redes interna e externa, tornando-se assim um roteador.

APOSTA ESTRATÉGICA

A ideia desta seção é apresentar os pontos do conteúdo que mais possuem chances de serem cobrados em prova, considerando o histórico de questões da banca em provas de nível semelhante à nossa, bem como as inovações no conteúdo, na legislação e nos entendimentos doutrinários e jurisprudenciais[3].

Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.
Para que o vírus contamine o computador, será necessário executar o programa infectado, o que por sua vez obriga o código do vírus a ser executado. Isso significa que um vírus pode permanecer inativo em seu computador, sem demonstrar nenhum sinal ou sintoma. Porém, quando o vírus contamina o computador, ele pode também contaminar outros computadores na mesma rede. Roubar senhas ou dados, registrar o uso do teclado, corromper arquivos, enviar spam aos seus contatos de e-mail e até mesmo controlar o seu computador são apenas algumas das ações irritantes e devastadoras que um vírus pode executar.
Os vírus podem se propagar através de anexos de e-mail ou mensagens de texto, downloads de arquivos da Internet e links para golpes em mídias sociais. Até mesmo os dispositivos móveis e smartphones podem ser infectados com vírus através do download de aplicativos duvidosos nesses dispositivos. Os vírus podem se esconder disfarçados como anexos de conteúdos compartilhados socialmente, como imagens humorísticas, cartões comemorativos ou arquivos de áudio e vídeo.

Spyware

De forma simples e direta, é um software de espionagem, isto é, sua função é coletar informações sobre uma ou mais atividades realizadas em um computador. Normalmente entra em seu computador sem o seu conhecimento ou permissão e é executado em segundo plano. O spyware é conhecido por

[3] Vale deixar claro que nem sempre será possível realizar uma aposta estratégica para um determinado assunto, considerando que às vezes não é viável identificar os pontos mais prováveis de serem cobrados a partir de critérios objetivos ou minimamente razoáveis.

capturar e transmitir informações altamente pessoais como contas bancárias online e senhas, ou informações de cartão de crédito. As formas como o spyware captura as informações subdivide sua classificação.

Registro de toques nas teclas - Chamados de "keyloggers", esse tipo de spyware é usado para coletar senhas e rastrear comunicações em que o teclado é utilizado.

Acompanhamento das atividades - Alguns cookies de rastreamento podem, indiscutivelmente, ser considerados spyware, no sentido que eles acompanham seus movimentos online e relatam o que você visita aos publicitários, para que eles possam servir informações mais pertinentes a você.

Redução da velocidade do dispositivo - Frequentemente, o único sinal que denuncia que você está infectado com spyware será a maneira parasita com que ele rouba potência de processamento e largura de banda de Internet para comunicar o que foi roubado.

Cavalo de Tróia

O cavalo de Tróia é um malware disfarçado de software legítimo para obter acesso aos sistemas dos usuários. Uma vez ativados, os cavalos de Tróia permitem que os criminosos espionem, roubem dados confidenciais e obtenham acesso ao sistema através de uma backdoor. Ele se confunde em algumas características com o spyware. Os principais tipos de cavalo de Tróia são:

Backdoor - Com um cavalo de Tróia backdoor, usuários maliciosos controlam remotamente o computador infectado. Os cavalos de Tróia backdoor costumam ser usados para reunir um conjunto de computadores e formar uma rede zumbi, que pode ser usada para fins criminosos.

Exploit - Exploits são programas que contêm dados ou códigos que tiram proveito de uma vulnerabilidade do software de um aplicativo executado no computador.

Rootkit - Os rootkits têm como objetivo ocultar certos objetos ou atividades no sistema. Geralmente, o principal objetivo é evitar a detecção de programas maliciosos para estender o período em que os programas são executados em um computador infectado.

Trojan-Banker - Programas Trojan-Banker são criados para roubar dados de contas de sistemas de bancos on-line, pagamentos eletrônicos e cartões de débito e crédito.

Fatores e Métodos de Autenticação
Os fatores de autenticação, são de forma geral classificados em três categorias distintas: O que você tem, o que você é e o que você sabe.

"O que você sabe" – Autenticação baseada no conhecimento
Para se autenticar é necessário saber previamente alguma informação para ser validado, a senha é o melhor exemplo deste método. Você precisa informar ela corretamente, do contrário não será autenticado, e terá o acesso barrado.

A vantagem deste método é que ele já é amplamente difundido e simples de ser utilizado. Já o grande problema é que outra pessoa pode saber ou até mesmo descobrir a sua senha, ao realizar diversas tentativas.

"O que você tem" – Autenticação baseada na propriedade
Nesta categoria você só é autenticado se você possuir algum dispositivo. Um bom exemplo deste tipo é o token, o dispositivo gera uma nova senha a cada período de tempo, desta maneira, é preciso ter o token para se autenticar. Caso outra pessoa obseve a senha enquanto você digita a senha para entrar no site bancário, em questão de minutos esta senha será trocada, e a senha observada não servirá mais.
Esta categoria já se mostra mais segura que a anterior, pois é necessário ter a posse do cartão ou do token, e caso outra pessoa consiga estes dispositivos o proprietário notaria a falta, o usuário pode solicitar um novo cartão ou token.
Mas, mesmo esta categoria apresenta alguns riscos, no caso do cartão de senhas, os criminosos criam páginas falsas de bancos que pedem todas as senhas do cartão da vítima. No caso dos tokens, existe a possibilidade da empresa que cria os tokens ter suas chaves roubadas, e com isto permite que os criminosos se passem pela vítima.

"O que você é" – Autenticação baseada na característica
Nesta categoria a autenticação é mais rigorosa, apenas a princípio apenas a própria pessoa pode ser autenticada, isto porque é utilizado a biometria, um bom exemplo deste tipo é a leitura da impressão digital.
Há também outros tipos de biometria não tão populares, como escaneamento de veias, identificação da íris, reconhecimento da voz, e outros.
Note que os métodos de autenticação que utilizam a biometria são mais seguros que os demais, mas mesmo assim não garante 100% de segurança, como já foi noticiado que pessoas utilizavam um molde de silicone da digital de outra pessoa para passar pelo leitor de impressão digital.

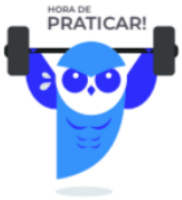
Tipo de Backup	Dados Copiados	Tempo de Backup	Tempo de Restauração	Espaço de Armazenamento
Backup Completo	Todos os dados	Lento	Rápido	Muito espaço
Backup Incremental	Apenas dados novos / modificados (arquivos e diretórios)	Rápido	Moderado	Pouco espaço
Backup Diferencial	Todos os dados desde o último backup completo	Moderado	Rápido	Moderado

Imprima o capítulo Aposta Estratégica separadamente e dedique um tempo para absolver tudo o que está destacado nessas duas páginas. Caso tenha alguma dúvida, volte ao Roteiro de Revisão e Pontos do Assunto que Merecem Destaque. Se ainda assim restar alguma dúvida, não hesite em me perguntar no fórum.

QUESTÕES ESTRATÉGICAS

Nesta seção, apresentamos e comentamos uma amostra de questões objetivas selecionadas estrategicamente: são questões com nível de dificuldade semelhante ao que você deve esperar para a sua prova e que, em conjunto, abordam os principais pontos do assunto.

A ideia, aqui, não é que você fixe o conteúdo por meio de uma bateria extensa de questões, mas que você faça uma boa revisão global do assunto a partir de, relativamente, poucas questões.



1. CESGRANRIO - Técnico Administrativo (ANP)/2016

Uma das redes da sede de uma empresa foi invadida por um software que coletou informações de vários computadores, instalou favoritos, barras de ferramentas e links indesejados nos navegadores da Web, alterou home pages padrão e fez com que fossem exibidos anúncios de pop-ups frequentemente.

Um modo de previnir invasões desse gênero é

A) instalar switches inteligentes na rede.

B) instalar antispywares nas máquinas da rede.

C) criar um algoritmo de criptografia para e-mails.

D) traduzir os endereços IPv4s para formato IPv6.

E) refazer todas as senhas de acesso aos computadores da rede.

Comentários

O enunciado da questão nos descreve problemas que são resultado da ação de um adware. Segundo o AVAST, o adware é um tipo de software maligno que bombardeia com pop-ups incessantes. Além da irritação criada, o adware pode também reunir informações pessoais, rastrear sites acessados e até mesmo registrar tudo que você digita. Portanto, a alternativa correta é a letra B.

Gabarito: alternativa B.

---

2. CESGRANRIO - Técnico Bancário (BASA)/2015

Um usuário deseja proteger seu computador, de modo a impedir que um hacker utilize portas de protocolo para invadir esse computador.

Uma forma de permitir essa proteção é através da

A) criação de um disco de restauração do sistema

B) configuração do navegador para trabalhar em modo anônimo

C) instalação de um software de firewall

D) criação de senha para e-mail

E) cópia de arquivos do sistema para uma pasta protegida

Comentários

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma "parede de fogo" que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware. Sua complexidade depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado. A partir das regras, o firewall pode ajudar a impedir o acesso de hackers e softwares mal-intencionados aos computadores conectados na rede.

Gabarito: alternativa C.

---

3. CESGRANRIO - Técnico (BR)/Administração/Controle Júnior/2015 (e mais 4 concursos)

Um grupo de torcedores, insatisfeitos com o resultado do jogo em que seu time sofreu uma goleada, planejou invadir a rede de computadores do estádio onde ocorreu a disputa para tentar alterar o placar do jogo. Os torcedores localizaram a rede, porém, entre a rede interna e a externa, encontraram uma barreira que usou tecnologia de filtragem dos pacotes que eles estavam tentando enviar.

Essa barreira de segurança de filtro dos pacotes é o

A) firewall

B) antivírus

C) antispam

D) proxy

E) PKI

Comentários

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma "parede de fogo" que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Sua complexidade depende do tamanho da rede, da política de segurança, da quantidade de **regras que controlam o fluxo de entrada e saída de informações** e do grau de segurança desejado. Ou seja, um firewall pode ser configurado como um filtro de pacotes.

Gabarito: alternativa A.

---

4. CESGRANRIO - Enfermeiro do Trabalho (BB)/2014/1

Informações importantes de uma pessoa que teve seu computador invadido foram coletadas e enviadas para terceiros. Um amigo, especialista em informática, sugere-lhe a instalação de um programa que bloqueie o acesso de outros computadores que estejam tentando se conectar a programas instalados em seu computador.

Esse tipo de programa é chamado de

A) bloqueador de pop-ups

B) antivírus

C) filtro antispam

D) filtro antiphishing

E) firewall

Comentários

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma "parede de fogo" que de acordo com regras pré-definidas decide permitir ou **bloquear tráfegos específicos**. A partir das regras, **o firewall pode ajudar a impedir o acesso de hackers e softwares mal-intencionados aos computadores conectados na rede**.

Gabarito: alternativa E.

---

5. CESGRANRIO - Técnico Científico (BASA)/Medicina do Trabalho/2014

Um dos recursos presentes no Windows, desde a versão xp, é o Windows Firewall.

Esse recurso tem o objetivo de

A) aumentar a segurança do sistema.

B) melhorar o desempenho do sistema.

C) tornar o sistema mais acessível e prático.

D) melhorar a comunicação dos usuários com a Microsoft.

E) facilitar o uso do sistema por pessoas com necessidades especiais.

Comentários

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Essa é a principal informação que você precisa ter ao se deparar com uma questão sobre firewall. Após isso, você precisa saber que o firewall pode ser tanto um software, quando um hardware e que os dois sistemas podem ser combinados.

Gabarito: alternativa A.

---

6. CESGRANRIO - Inspetor de Segurança Interna (PETROBRAS)/2011/PSP-RH-1 2011

Um computador recebe um programa mal-intencionado, que pode prejudicar seus arquivos e sua segurança.

Qual a ferramenta adequada para descobrir e remover esse programa?

A) spam

B) firewall

C) adware

D) antivírus

E) spyware

Comentários

O antivírus é um programa que tem a finalidade de garantir um nível de segurança. Os antivírus e anti-malwares são programas desenvolvidos para prevenir, detectar e eliminar vírus de computador e outros tipos de softwares nocivos ao sistema operacional. Ele funciona identificando, bloqueando e alertando ao usuário sobre a ação de um vírus em e-mails e outros arquivos. Caso algum seja encontrado, o antivírus coloca em quarentena (isola) o vírus ou o exclui completamente, antes que ele danifique o computador e os arquivos.

Gabarito: alternativa D.

QUESTIONÁRIO DE REVISÃO E APERFEIÇOAMENTO

A ideia do questionário é elevar o nível da sua compreensão no assunto e, ao mesmo tempo, proporcionar uma outra forma de revisão de pontos importantes do conteúdo, a partir de perguntas que exigem respostas subjetivas.

São questões um pouco mais desafiadoras, porque a redação de seu enunciado não ajuda na sua resolução, como ocorre nas clássicas questões objetivas.

O objetivo é que você realize uma autoexplicação mental de alguns pontos do conteúdo, para consolidar melhor o que aprendeu ;)

Além disso, as questões objetivas, em regra, abordam pontos isolados de um dado assunto. Assim, ao resolver várias questões objetivas, o candidato acaba memorizando pontos isolados do conteúdo, mas muitas vezes acaba não entendendo como esses pontos se conectam.

Assim, no questionário, buscaremos trazer também situações que ajudem você a conectar melhor os diversos pontos do conteúdo, na medida do possível.

É importante frisar que não estamos adentrando em um nível de profundidade maior que o exigido na sua prova, mas apenas permitindo que você compreenda melhor o assunto de modo a facilitar a resolução de questões objetivas típicas de concursos, ok?

Nosso compromisso é proporcionar a você uma revisão de alto nível!

Vamos ao nosso questionário:

Perguntas

1) O que é um vírus e como ele afeta um sistema?

2) Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.

3) O que é um firewall? Quais os tipos de firewall? Como eles funcionam?

4) Qual a diferença entre phising, worm e ransomware?

5) Quais os fatores e métodos de autenticação e como eles são aplicados?

Perguntas com respostas

1) O que é um vírus e como ele afeta um sistema?

Um vírus de computador é um programa ou código malicioso criado para alterar a forma como um computador funciona. Ele atua se inserindo ou se anexando a um programa ou documento legítimo, que tenha suporte para macros, a fim de executar o seu código. Durante esse processo, um vírus pode potencialmente causar efeitos inesperados ou prejudiciais, como danificar o sistema, corrompendo ou destruindo os dados.

2) Qual a definição de cada princípio da segurança da informação? Cite exemplos relacionados a cada princípio.

Disponibilidade - Princípio que garante que a informação estará sempre disponível.

Integridade - Princípio que garante que as informações serão guardadas ou enviadas em sua forma original, sem sofrer alterações.

Confidencialidade - Princípio que garante o sigilo da informação com a capacidade de controlar o acesso, assegurando que elas só serão acessadas por pessoas autorizadas. Ou seja, é a garantia que as informações só serão acessadas através de uma senha.

Autenticidade - Princípio que permite verificar a identidade de uma pessoa em um sistema, garantindo a veracidade das informações.

3) O que é um firewall? Quais os tipos de firewall? Como eles funcionam?

Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede. Traduzindo de forma literal ele é uma “parede de fogo” que de acordo com regras pré-definidas decide permitir ou bloquear tráfegos específicos. Ele pode ser tanto um software quanto um hardware, onde a combinação de ambos é chamada tecnicamente de “appliance”. Na sua forma mais simples de implementação, o firewall funciona como um filtro de pacotes (stateless) que pode ser configurado tanto para a rede interna, quanto para a rede externa (Internet). A outra forma de configuração é a de estado de sessão (statefull), onde o firewall analisa os pacotes e guarda o estado de cada conexão de maneira que seja possível para identificar e fazer uma previsão das respostas legítimas, de forma a impedir o tráfego de pacotes ilegítimos.

4) Qual a diferença entre phising, worm e ransomware?

O phishing é um golpe on-line de falsificação. Os phishers enviam e-mails que tentam imitar mensagens de empresas financeiras legítimas ou de outras empresas solicitando que o usuário acesse um site falso para reinserir o número do seu cartão de crédito ou verificar sua senha. A partir da inserção desses dados eles têm acesso a todas as informações necessárias para aplicar golpes. Um worm é um software malicioso capaz de

se autorreplicar em computadores ou por redes de computadores sem que você desconfie que sua máquina foi infectada. Eles podem explorar erros de configuração da rede (por exemplo, copiar a si mesmos em um disco totalmente acessível) ou explorar brechas na segurança do sistema operacional e dos aplicativos. O ransomware é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (ransom) para restabelecer o acesso ao usuário.

5) Quais os fatores e métodos de autenticação e como eles são aplicados?

“O que você sabe” – Autenticação baseada no conhecimento. Exemplo: senha; “O que você tem” – Autenticação baseada na propriedade. Exemplo: token, certificado digital; “O que você é” – Autenticação baseada na característica Exemplo: biometria.

...

Forte abraço e bons estudos!

"Hoje, o 'Eu não sei', se tornou o 'Eu ainda não sei'"

(Bill Gates)

Thiago Cavalcanti

Face: www.facebook.com/profthiagocavalcanti
Insta: www.instagram.com/prof.thiago.cavalcanti
YouTube: youtube.com/profthiagocavalcanti

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.