Questão 1

(2019 - IF-BA - assistente em administração) A respeito dos conceitos que envolvem a segurança da informação, analise as afirmativas a seguir.

I.Os mecanismos de segurança podem ser lógicos ou físicos.
II. A perda de confidencialidade, integridade e disponibilidade é um exemplo dos eventos que comprometem a segurança da informação.
III. Assinatura digital, encriptação e firewall são exemplos de mecanismos lógicos de segurança.

Assinale:

A Se somente as afirmativas I e II estiverem corretas.

B Se somente a afirmativa II estiver correta.

C Se somente a afirmativa I estiver correta.

D Se todas as afirmativas estiverem corretas. check_circle

E Se nenhuma das afirmativas estiver correta.

check_circle

Parabéns! A alternativa D está correta.

Mecanismos ou controles de segurança podem ser lógicos e físicos. A segurança da informação é baseada em três aspectos fundamentas: confidencialidade, integridade e disponibilidade. Desse modo, a perda de qualquer um dos três aspectos já impacta na segurança. A pior situação ocorre quando perdemos os três juntos: trata-se praticamente de uma catástrofe. Por fim, os mecanismos lógicos, por definição, envolvem algoritmos.

Questão 2

(2019 - Comperve - UFRN - analista de tecnologia da informação) A segurança computacional possui uma terminologia própria. Uma padronização na utilização dessa terminologia garante o correto entendimento entre os diferentes agentes envolvidos. Em relação a isso, considere as seguintes afirmações sobre a segurança computacional.

I. A segurança física visa providenciar mecanismos para restringir o acesso às áreas críticas da organização a fim de garantir a integridade e a autenticidade dos dados.
II. Uma ameaça pode ser definida como algum evento que pode ocorrer e acarretar algum perigo a algum ativo da rede. As ameaças podem ser intencionais ou não intencionais.
III. São ameaças mais comuns às redes de computadores o acesso não autorizado, o reconhecimento (ex.: PortScan) e a negação de serviço (ex.: DoS ou DDoS).
IV. O “tripé da segurança” é formado de pessoas, processos e políticas de segurança. De nada adianta uma política do tipo se as pessoas e os processos não forem considerados.

Em relação à segurança computacional, estão corretas as afirmativas:

A III e IV.

B II e IV.

C II e III. check_circle

D I e II.

E I e III.

check_circle

Parabéns! A alternativa C está correta.

A segurança é baseada em camadas; na parte física, são definidos os controles de acesso a determinadas regiões da instituição, como cancelas, catracas e sistemas de acesso biométrico. Quando eles perdem sua finalidade, o atacante pode chegar fisicamente perto do equipamento, podendo danificar a parte física dele. Dos vários problemas que podem ser realizados, devemos destacar a possibilidade de se quebrar o equipamento (colocando em risco a integridade da informação) ou modificá-lo de forma prejudicial (colocando em risco a autenticidade da informação). Contudo, não podemos garantir esses fatores. Neste ponto, um problema é gerado, pois ainda existem outros mecanismos que podem prover, pelo menos, a autenticidade dos dados.

A ameaça é um evento que pode provocar a perda de um dos três pilares da segurança: confidencialidade, integridade e disponibilidade. Sobre as ameaças comuns às redes, os exemplos estão corretos, porém, de acordo com as últimas estatísticas, isso pode mudar a qualquer momento. Tais ameaças são comuns, pois, até o momento, não existe uma solução completa para isso.

Questão 3

(2016 - CESPE /Cebraspe - TRT - 8ª Região - analista judiciário - tecnologia da informação) Correspondem a itens capazes de oferecer controle ou proteção no âmbito da segurança física preventiva:

A As chaves públicas criptográficas.

B Os dispositivos de autenticação biométrica. check_circle

C Os sistemas de autenticação por senhas *single sign on*.

D Os certificados digitais.

E Os sistemas de Firewall.

check_circle

Parabéns! A alternativa B está correta.

A segurança física está relacionada ao acesso às dependências das instalações; a lógica, aos algoritmos que protegem os dados.

Questão 4

(2013 - FCC - TRT - 9ª Região - técnico judiciário – segurança) Convém que sejam utilizados perímetros de segurança (barreiras, como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação. Além disso, que sejam levadas em consideração e implementadas as seguintes diretrizes para perímetros de segurança física, quando apropriado:

I. Os perímetros de segurança devem ser claramente definidos, assim como a localização e capacidade de resistência de cada perímetro precisam depender dos requisitos de segurança dos ativos existentes no interior do perímetro e dos resultados da análise/avaliação de riscos.
II. Os perímetros de um edifício ou de um local que contenha instalações de processamento da informação precisam ser fisicamente sólidos (ou seja, o perímetro não deve ter brechas nem pontos onde poderia ocorrer facilmente uma invasão).
III. Deve-se implantar uma área de recepção ou outro meio para controlar o acesso físico ao local ou ao edifício. Esse acesso deve ficar restrito somente ao pessoal autorizado.
IV. Devem ser construídas barreiras físicas para impedir o acesso físico não autorizado e a contaminação do meio ambiente.

Está correto o que se afirma em:

A II, III e IV.

B I, II e III.

C II e III.

D I, II, III e IV. check_circle

E I e III.

check_circle

Parabéns! A alternativa D está correta.

As instalações físicas devem possuir seguranças justapostas de forma que a fraqueza de uma camada possa ser recoberta por outra. Essa lógica fica clara no funcionamento de guaritas, cancelas e sensores biométricos.

Questão 5

Ao projetar uma rede, é comum adotar um firewall para proteger uma rede interna. Com relação ao papel do firewall, marque a opção que apresenta uma forma correta de classificar esse ativo de TIC.

A Segurança lógica check_circle

B Segurança física

C Segurança patrimonial

D Segurança empresarial

E Nenhuma das alternativas

check_circle

Parabéns! A alternativa A está correta.

O firewall é um importante ativo de rede; desse modo, encontrá-lo em um projeto de rede torna-se imprescindível. Ele protege uma rede interna analisando e bloqueando, por meio de algoritmos proprietários de cada marca, o acesso e o transporte de dados para dentro dela. Por manipulá-los, este ativo é classificado como segurança lógica.

Questão 6

A partir da pandemia ocorrida em 2020, os sistemas de acesso evoluíram para o uso de reconhecimento facial. Muitos desses sistemas possuem slogans bem criativos, como este: “Um sistema de acesso com reconhecimento facial permite levar a sua empresa diretamente para o mundo da alta tecnologia por meio do uso desta importante ferramenta de segurança: _____”.

Marque a alternativa que apresenta o termo que completa o slogan anterior de forma mais satisfatória.

A Lógica

B Física check_circle

C Mista

D Empresarial

E Patrimonial

check_circle

Parabéns! A alternativa B está correta.

Um sistema de acesso, independentemente do tipo de chave (senha) criado, permite o bloqueio físico a determinado local. Esta chave (senha), com o passar do tempo, vem evoluindo bastante: cartões com códigos de barra, tarja magnética, digital, veias da mão e, agora, reconhecimento facial.