Avaliação AV

avalie seus conhecimentos

Disc.: DGT0288 - INTRODUÇÃO À SEGUR
Aluno: MARIA VALÉRIA PEREIRA DA SILVA
Prof.: SAMUEL ZANFERDINI OLIVA

Período: 2023.1 EAD (GT)
Matr.: 202301346479
Turma: 9002

Lupa

VERIFICAR E ENCAMINHAR

Prezado(a) Aluno(a),

Responda a todas as questões com atenção. Somente clique no botão **FINALIZAR PROVA** ao ter certeza de que respondeu a todas as questões e que não precisará mais alterá-las.

A prova será SEM consulta. O aluno poderá fazer uso, durante a prova, de uma folha em branco, para rascunho. Nesta folha não será permitido qualquer tipo de anotação prévia, cabendo ao aplicador, nestes casos, recolher a folha de rascunho do aluno.

Valor da prova: 10 pontos.

1 ponto

1. Em relação a códigos maliciosos (malwares), analise as assertivas a seguir:

I. Vírus é uma categoria de malware que pode ser infectado através de pen drives e outros dispositivos, porém não pode ser propagado por e-mail.

II. Um worm é capaz de se propagar automaticamente em redes de computadores e não se propaga por meio da inclusão de cópias de si mesmo em outros programas.

III. Um computador denominado zumbi é aquele que pode ser controlado remotamente, sem o conhecimento do seu dono.

IV. Spyware é um programa que pode ser utilizado apenas de forma maliciosa, não sendo permitida a utilização de forma legítima.

Quais estão corretas?

(Ref.: 202306292452)

- ( ) Apenas I e II.
- (•) Apenas II e III.
- ( ) I, II, III e IV.
- ( ) Apenas III e IV.
- ( ) Apenas II, III e IV.

1 ponto

2. A notícia divulgada na imprensa e identificada por uma analista de TI como sendo um ataque de malware corretamente relatado é:

(Ref.: 202306286439)

- (●) O funcionário da empresa verificou no Gerenciador de Tarefas do Windows e o processo não estava lá. O malware fez com que o arquivo malicioso desaparecesse da listagem. Para conseguir essa invisibilidade, os rootkits normalmente grampeiam funções do Windows, podendo ser instalados como drivers.
- ( ) O funcionário teve um software, com capacidade de interceptar e registrar o que foi digitado por ele, instalado sem seu conhecimento. O backdoor enviou os dados digitados para um PC remoto controlado pelo invasor. Com isso, suas senhas de acesso aos documentos confidenciais do escritório de advocacia foram capturadas.
- ( ) Quase 1 milhão de usuários da web ficaram sem conexão na Alemanha devido a um ataque do adware Mirai. Essa versão do Mirai, ao invés de abrir os roteadores, configurando os administradores com senhas padrão, consegue infectar mais aparelhos a partir da execução de códigos remotos.
- ( ) O ransomware, conhecido como Gazer, vem sendo utilizado ativamente em ataques com o objetivo de espionar governos e diplomatas. O trojan utiliza métodos avançados para se esconder por longos períodos, facilitando o roubo de informações. A sua propagação é feita por meio de campanhas de phishing.
- ( ) Após o ataque de backdoor, o CIO recebeu um e-mail de cibercriminosos que dizia: "Invadimos seu servidor e bloqueamos seus documentos. Pague 15.000 euros em moeda virtual para recuperá-los. Mas, para provar que podemos recuperar seus arquivos, liberaremos dois documentos de sua escolha".

1 ponto

3. Um funcionário estava varrendo o chão da sala de uma empresa, na qual se encontra um servidor de domínio de rede local, quando não reparou que o cabo de rede que conecta ele ao roteador presente no outro lado da sala estava solto passando pelo chão, e então acabou por puxar o cabo com a vassoura, arrancando-o da placa de rede do servidor.

Segundo a norma ABNT NBR ISO/IEC 27002:2013, o responsável pela segurança do servidor deixou de colocar em prática o controle relacionado à:

(Ref.: 202306676387)

- ( ) Acordo de confidencialidade
- ( ) Inventário dos ativos
- ( ) Gerenciamento de senha de usuário
- ( ) Segregação de funções
- (●) Segurança do cabeamento

1 ponto

4. A cláusula do Anexo L, cuja norma ISO/IEC 27001:2013 é alinhada, que trata do estabelecimento dos resultados desejados do sistema de gestão, é:

(Ref.: 202306676385)

- ( ) Liderança
- ( ) Escopo
- ( ) Suporte
- (●) Referência normativa
- ( ) Termos e definições

1 ponto

5. Uma forma de se proteger em relação aos vírus é através do uso de programas antivírus que procuram por padrões para detectar e eliminá-los. Cada vírus tem uma estratégia para tentar evitar sua identificação. Selecione a opção que apresenta o vírus que faz o antivírus acreditar que o programa mal-intencionado está em outro lugar que não seja a sua localização real.

(Ref.: 202306628872)

- ○ Cavalo de Troia.
- ○ Mutante.
- ○ Polimórfico.
- ○ Vírus *stealth*.
- ◉ Vírus blindado.

1 ponto

6. Crime cibernético é todo crime executado on-line e inclui, por exemplo, o roubo de informações no meio virtual. Uma recomendação correta de segurança aos usuários da internet para se proteger contra a variedade de crimes cibernéticos é:

(Ref.: 202306631487)

- ○ Usar a mesma senha (composta por letras maiúsculas e minúsculas, números e símbolos) em todos os sites com conteúdo de acesso restrito, mantendo essa senha protegida em um aplicativo de gerenciamento de senhas.
- ○ Usar uma suíte de segurança para a internet com serviços como *firewall, blockwall* e antivírus, como o *LibreOffice Security Suit.*
- ◉ Gerenciar as configurações de mídias sociais para manter a maior parte das informações pessoais e privadas bloqueadas.
- ○ Proteger a rede *wireless* com senha que utiliza criptografia *Wired Equivalent Privacy* - WEP ou com uma *Virtual Protect Network* - VPN.
- ○ Manter os softwares atualizados, exceto os sistemas operacionais, pois esses já possuem mecanismos de segurança como *firewall,* antivírus e *antispyware.*

1 ponto

7. Selecione a opção que contenha os pilares de um negócio:

(Ref.: 202306617738)

- ◉ Unidades, processos e componentes de negócios e ativos.
- ○ Tecnologia da Informação, Recursos Humanos e Infraestrutura interna.
- ○ Componentes, planos de continuidade e de recuperação de desastre.
- ○ ITIL, PDCA (Plan-Do-Check-Act) e PCN (Plano de Continuidade).
- ○ Plano de Contingência, Plano de Recuperação de Desastres e Plano de Continuidade Operacional.

1 ponto

8. Sobre Firewall, Firewall Pessoal e Antivírus, são feitas as seguintes afirmações:

I. Um Firewall é um software ou hardware que verifica informações provenientes da rede/internet ou do computador e toma ações como bloquear ou liberar a passagem dessas informações.

II. Um Firewall Pessoal é um software que é executado apenas em servidores para proteger os dados do servidor contra hackers/vírus.

III. Antivírus e Firewall têm a mesma funcionalidade, diferenciando-se apenas na forma como tomam as ações. O antivírus impede o vírus de entrar no computador, bloqueando portas. Já o firewall apaga vírus que entraram, por exemplo, por pendrive.

IV. Antivírus são softwares projetados para identificar, analisar e eliminar softwares maliciosos e vírus de computador. Geralmente utilizam base de dados de definição de vírus para ajudar na identificação desses nos computadores.

Em relação a estas afirmações, assinale a alternativa correta:

(Ref.: 202306639579)

- ○ Somente a afirmação I está correta.
- ○ Somente a afirmação IV está correta.
- ○ Somente as afirmações II, III e IV estão corretas.
- ◉ Somente as afirmações I e IV estão corretas.
- ○ Somente as afirmações I, II e IV estão corretas.

1 ponto

9. Suponha que uma entidade R (remetente) deseja enviar uma mensagem m para outra entidade D (destinatário) utilizando a internet. Para se comunicarem, R e D utilizam criptografia de chave pública. R+ e R são as chaves pública e privada de R, respectivamente, e D+ e D- são as chaves pública e privada de D, respectivamente.

A partir dessa situação, avalie o que se afirma.

I - Se R utilizar D+ para criptografar m, então D poderá utilizar D- para decriptar m.

II - Se R utilizar R+ para criptografar m, então D poderá utilizar D- para decriptar m.

III - Se R utilizar R- para criptografar m, então D poderá utilizar R+ para decriptar m.

IV - Se R utilizar D- para criptografar m, então D poderá utilizar R+ para decriptar m.

Está correto apenas o que se afirma em:

(Ref.: 202306647978)

- ○ I e III.
- ◉ II e III.
- ○ III e IV.
- ○ I e IV.
- ○ II e IV.

1 ponto

10. 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.

Em sua avaliação, a estratégia utilizada por Pedro para tratar o risco é considerada:

(Ref.: 202306617760)

- ○ Aceitação do risco.
- ◉ Mitigação do risco.

- ◯ Transferência do risco.
- ◯ Especificação do risco.
- ◯ Eliminação do risco.

VERIFICAR E ENCAMINHAR

Não respondida Não gravada Gravada