1)

A segurança da informação envolve a proteção da confidencialidade, integridade e disponibilidade da informação, e para isso é necessário tratar de todos os ativos e componentes dos sistemas que suportam a informação.

Quais dos ataques a seguir podem comprometer, respectivamente, a (i) confidencialidade, (ii) integridade e (iii) disponibilidade?

**Alternativas:**

* a)

*SYN Flooding*, ataque do homem do meio, força bruta

* b)

Ataque do homem do meio, DoS, força bruta

* c)

DoS, ataque do homem do meio, força bruta

* d)

Ataque do homem do meio, vírus, *SYN Flooding*

Alternativa assinalada

* e)

Vírus, ataque do homem do meio, força bruta

2)

Ataques de negação de serviço distribuídos (DDoS) de rede se baseiam na geração de grande quantidade de tráfego, e estudos indicam que 85% dos ataques estiveram abaixo de 500 Mbps, o que é considerado um valor baixo, mas ainda suficiente para interromper recursos mal protegidos conectados à Web. O Mirai, um dos principais ataques já vistos na internet, teve origem em 18.705 endereços IP associados a dispositivos infectados, e atingiu 654 Gbps, em uma campanha que durou quase 10 dias. A maioria dos ataques, no entanto, possuem duração mais curta, com cerca de 88% dos ataques cessando em no máximo uma hora.

O DDoS afeta qual princípio básico da segurança, e qual processo da segurança pode identificar este tipo de ataque? Indique a alternativa correta.

**Alternativas:**

* a)

Disponibilidade e proteção

* b)

Disponibilidade e detecção

Alternativa assinalada

* c)

Disponibilidade e resposta

* d)

Confidencialidade e proteção

* e)

Confidencialidade e resposta

3)

Babuk é mais um ransonware que está agindo na internet. Segundo um relatório que analisou o Babuk, “Como esta é a primeira detecção desse malware em circulação, não é surpreendente que Babuk não esteja ofuscado. No geral, é um ransomware bastante padronizado, que utiliza algumas das novas técnicas que conhecemos, como criptografia multi-threading, bem como abusa do gerenciador de reinicialização do Windows, semelhante ao Conti e REvil”. Ainda segundo o relatório, “para o esquema de criptografia, o Babuk usa sua própria implementação de hashing SHA256, criptografia ChaCha8 e geração de chave Diffie – Hellman (ECDH) de curva elíptica e algoritmo de troca para proteger suas chaves e criptografar arquivos. Como muitos ransomware que vieram antes, ele também tem a capacidade de espalhar sua criptografia por meio da enumeração dos recursos de rede disponíveis”.

O ransonware é um tipo de malware que afeta qual princípio básico da segurança da informação, e como você pode se proteger?

**Alternativas:**

* a)

Confidencialidade, com proteção por backup.

* b)

Integridade, com proteção por backup.

* c)

Disponibilidade, com proteção por backup.

Alternativa assinalada

* d)

Confidencialidade, com proteção por firewall.

* e)

Disponibilidade, com proteção por firewall.

4)

Malwares podem infectar navegadores de internet. Um deles, conhecido como Adrozek, modifica uma DLL específica no navegador de destino e altera as suas configurações para inserir anúncios adicionais não autorizados em páginas da web, além de, muitas vezes, anúncios legítimos de mecanismos de buscas. Os invasores ganham por meio de programas de publicidade afiliados, que pagam pela quantidade de tráfego direcionado a páginas patrocinadas.

Outra possibilidade é o envio do usuário para uma página falsa, onde ele pode entregar dados pessoais e credenciais de acesso. Este tipo de ataque em que o usuário é enviado para uma página falsa indica problemas com qual princípio básico de segurança? E quando há a entrega de dados pessoais e credenciais de acesso? Assinale a alternativa relacionada com estes dois pontos (i) página falsa e (ii) entrega de dados.

**Alternativas:**

* a)

Integridade e confidencialidade

Alternativa assinalada

* b)

Integridade e disponibilidade

* c)

Confidencialidade e confidencialidade

* d)

Integridade e integridade

* e)

Confidencialidade e disponibilidade

5)

Um sistema criptográfico é composto pelo algoritmo criptográfico e pelas chaves criptográficas. A fraqueza ou vulnerabilidade pode existir no algoritmo, na implementação do algoritmo ou na chave criptográfica. Um incidente de segurança recente fez com que chaves criptográficas utilizadas pelo governo americano fossem comprometidas.

Qual controle de segurança deve tratar de situações com essa relacionada ao comprometimento de chaves criptográficas?

**Alternativas:**

* a)

Gestão de chaves criptográficas

Alternativa assinalada

* b)

Criptografia de chave pública

* c)

Hash criptográfico

* d)

Firewall

* e)

Backup