1)

Em 2011, em uma operação conhecida como “Operation Cupcake”, a MI6 - agência britânica de inteligência – atacou uma revista online da Al-Qaeda. A revista continha instruções para a construção de bombas, que foram substituídas por receitas de bolo.

Este incidente de segurança envolvendo a MI6 e a Al-Qaeda envolve qual princípio de segurança da informação?

**Alternativas:**

* a)

Apenas confidencialidade

* b)

Apenas integridade

Alternativa assinalada

* c)

Apenas disponibilidade

* d)

Nenhuma

* e)

Confidencialidade e integridade

2)

Segundo o Índice Global de Ameaças da Check Point Research, uma das principais vulnerabilidades exploradas em setembro de 2020 foi o *OpenSSL TLS DTLS Heartbeat Information Disclosure*, também conhecido como Heartbleed. Este vulnerabilidade foi descoberta em 2014 no OpenSSL, e possibilita a interceptação de comunicações seguras e roubo de informações confidenciais, como credenciais de acesso, senhas, dados pessoais e até mesmo chaves de decodificação.

A exploração do Heartbleed possibilita o roubo de informações confidenciais. Qual princípio de segurança da informação está relacionado com esta ameaça?

**Alternativas:**

* a)

Confidencialidade

Alternativa assinalada

* b)

Integridade

* c)

Disponibilidade

* d)

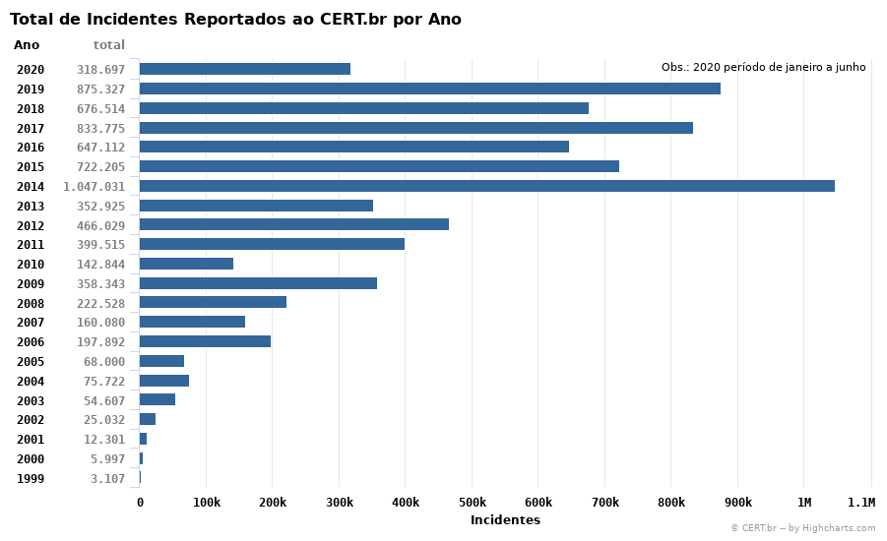
Nenhum destes princípios

* e)

Vulnerabilidade

3)

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, e o gráfico abaixo indica o número de incidentes reportados no decorrer dos anos.



Incidentes de segurança devem ser evitados. Qual das alternativas a seguir MELHOR representa o papel do especialista em segurança da informação para EVITAR os incidentes de segurança?

**Alternativas:**

* a)

Avaliar e tratar os riscos de segurança da informação

Alternativa assinalada

* b)

Tornar tudo confidencial

* c)

Implantar firewall

* d)

Utilizar senhas

* e)

Eliminar os exploits

4)

Segundo o Índice Global de Ameaças da Check Point Research, uma das principais vulneralidades exploradas em setembro de 2020 foi o OpenSSL TLS DTLS Heartbeat Information Disclosure, também conhecido como Heartbleed. Este vulnerabilidade foi descoberta em 2014 no OpenSSL, e possibilita a interceptação de comunicações seguras e roubo de informações confidenciais, como credenciais de acesso, senhas, dados pessoais e até mesmo chaves de decodificação.

O que o caso do Heartbeat está representando, com relação aos elementos do risco?

**Alternativas:**

* a)

OpenSSL é uma vulnerabilidade que pode ser atacada

* b)

OpenSSL é um *exploit* que pode ser usado em ataques

* c)

Heartbleed é um *exploit* que pode ser usado em ataques

* d)

Heartbleed é uma vulnerabilidade do OpenSSL

Alternativa assinalada

* e)

Heartbleed é um *exploit* do OpenSSL