Atividade ENADE da Aula 07

Luan Brito Sousa Calazans 6°sem - segurança ofensiva

Q01

Um ataque cibernético pode ocorrer quando invasores exploram vulnerabilidades em aplicações web mal configuradas, obtendo acesso não autorizado a dados sensíveis da organização. Esse tipo de ocorrência se relaciona ao OWASP Top 10, conjunto de vulnerabilidades mais críticas em aplicações web, e pode gerar impactos diretos à confidencialidade, integridade e disponibilidade das informações.

I. A exploração de falhas em aplicações web, como injeção de código e falhas de autenticação, é frequentemente utilizada por atacantes para comprometer dados sensíveis das organizações.

PORQUE

II. O OWASP Top 10 constitui uma metodologia de pentest que descreve as fases operacionais de um teste de invasão, desde o reconhecimento até a pós-exploração.

A respeito dessas asserções, assinale a opção correta:

(C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

Q02

Para avaliar a real exposição a riscos, organizações precisam determinar o valor que seus dados possuem para o negócio. Essa avaliação é fundamental tanto para definir medidas de segurança quanto para apoiar decisões como a contratação de seguros. O valor do dado, nesse contexto, está relacionado a fatores como sua utilização nos processos de negócio, sua indispensabilidade, seu conteúdo e o grau de recuperação

em caso de perda.

Qual fator não é importante para determinar o valor do dado para uma organização?

(E) As exigências legais e regulatórias relacionadas à guarda e ao uso do dado.

Q03

Um atacante obtém acesso de leitura a um servidor web de um e−commerce e consegue visualizar um arquivo (/exports/cc_dump.csv) contendo números de cartões de crédito. Os registros de log indicam apenas requisições de leitura; o serviço permaneceu disponível e o hash do arquivo não se alterou após o acesso. A organização está sujeita a requisitos de proteção de dados e a normas setoriais.

Considerando a tríade CIA e propriedades correlatas, qual princípio da segurança da informação foi predominantemente violado no incidente descrito?

(D) Confidencialidade.

Q04

Em um corredor de acesso livre dentro de uma empresa, encontra-se instalada uma impressora de rede multifuncional, utilizada por diversos setores. O equipamento não possui controle de autenticação, permitindo que qualquer colaborador ou visitante imprima, copie ou digitalize documentos sem registro de uso. Em auditoria, constatou-se que contratos e relatórios confidenciais foram esquecidos na bandeja da impressora, ficando expostos a pessoas não autorizadas.

Considerando o cenário descrito, discorra sobre os riscos de

segurança da informação associados à situação, identificando:

1. Quais princípios da tríade CIA (Confidencialidade, Integridade, Disponibilidade) são afetados;
2. Quais vulnerabilidades e falhas de controles podem ser observadas;
3. Que medidas técnicas e administrativas poderiam ser implementadas para mitigar esses riscos.

1. Princípios da tríade CIA afetados:

- Confidencialidade: É o mais comprometido, já que documentos confidenciais (contratos, relatórios) ficam expostos na bandeja de saída, permitindo acesso não autorizado. A falta de autenticação também possibilita que qualquer pessoa imprima, copie ou digitalize dados sensíveis.

- Integridade: Pode ser indiretamente afetada se usuários não autorizados modificarem configurações da impressora ou manipularem documentos durante processos de digitalização/cópia.

- Disponibilidade: Embora não seja o foco, o uso indiscriminado por pessoas não autorizadas pode sobrecarregar o equipamento, afetando sua disponibilidade para usuários legítimos.

2. Vulnerabilidades e falhas de controles:

- Falhas técnicas: Ausência de autenticação, falta de criptografia na transmissão de dados e armazenamento temporário não protegido na impressora.

- Falhas administrativas: Políticas inadequadas de uso, falta de treinamento para colaboradores sobre manuseio de documentos confidenciais e ausência de registro de atividades (logging).

- Falhas físicas: Localização em área de livre acesso e bandeja de saída exposta, sem controle visual ou restrição.

3. Medidas técnicas e administrativas

Técnicas:

- Implementar autenticação individual e impressão segura.
- Criar logs e auditoria de uso da impressora.
- Posicionar impressora em local controlado.

Administrativas:

- Treinar colaboradores sobre confidencialidade e recolhimento imediato de documentos.
- Estabelecer políticas de impressão segura e monitoramento físico.

Q05

Uma análise de riscos em segurança da informação busca levantar os ativos de uma organização, identificar vulnerabilidades e ameaças, estimar impactos potenciais e orientar a tomada de decisão quanto a medidas de segurança. Apesar disso, alguns elementos frequentemente confundidos não são objetivos diretos da análise de riscos, mas de etapas posteriores da gestão de riscos.

Avalie as seguintes afirmações sobre os objetivos de uma análise de riscos:

I. Identificar os ativos e seus valores é um objetivo essencial da análise de riscos.

II. Implementar contramedidas faz parte dos objetivos centrais da análise de riscos.

III. Determinar vulnerabilidades e ameaças relevantes é um dos objetivos da análise de riscos.

IV. Elaborar e aplicar um plano de continuidade de negócios

detalhado é objetivo direto da análise de riscos.

É correto apenas o que se afirma em:

(C) I e III

Q06

Um escritório de administração conduz uma análise de riscos em seus processos internos para avaliar a confiabilidade das informações. Durante a avaliação, foram mapeados cenários em que falhas de configuração em sistemas, somadas a eventos externos como ataques direcionados, poderiam gerar impactos significativos na continuidade do negócio. Nesse contexto, torna-se necessário distinguir conceitos fundamentais como ameaça, vulnerabilidade

e risco, os quais frequentemente são confundidos no âmbito da gestão da segurança da informação.

I. Uma ameaça é compreendida como um possível evento ou ação que pode explorar
vulnerabilidades de um sistema, causando impacto negativo na confiabilidade, integridade ou disponibilidade da informação.

PORQUE

II. O risco corresponde exclusivamente à presença de vulnerabilidades técnicas em sistemas computacionais, independentemente da probabilidade de exploração
ou do impacto causado ao negócio.

A respeito dessas asserções, assinale a opção correta:

(C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

Q07

Uma empresa de serviços financeiros está conduzindo um processo de análise e gerenciamento de riscos em seus sistemas de TI. Durante esse processo, os gestores precisam não apenas identificar ativos e ameaças, mas também avaliar impactos, probabilidades e, sobretudo, implementar medidas para reduzir os riscos a níveis aceitáveis para o negócio. O gerenciamento de riscos, portanto, deve ser compreendido como um ciclo contínuo que vai além da simples análise, envolvendo tratamento, monitoramento e tomada de decisão estratégica.

Analise as seguintes afirmações sobre os propósitos do gerenciamento de riscos em segurança da informação:

I. Determinar a probabilidade de ocorrência de certos riscos associados aos ativos críticos.

II. Determinar os danos potenciais que incidentes de segurança podem causar à organização.

III. Esboçar e classificar as ameaças às quais os recursos de TI estão expostos.

IV. Implementar medidas e controles para reduzir os riscos a níveis aceitáveis ao negócio.

É correto apenas o que se afirma em:

(E) I, II, III e IV

Q08

Uma pequena empresa de tecnologia iniciou suas atividades com apenas um colaborador, mas após alguns anos expandiu para 20 funcionários e passou a lidar com um volume crescente de dados críticos. O gestor percebeu que já não era mais possível manter o controle de riscos de forma intuitiva e, por recomendação de um consultor, optou por iniciar um

processo de análise qualitativa de riscos. Esse tipo de análise é frequentemente utilizado em empresas em crescimento, por fornecer uma visão inicial das ameaças mais relevantes de forma acessível, sem demandar dados estatísticos detalhados.

I. A análise qualitativa de riscos busca a classificação de ameaças e vulnerabilidades usando como subterfúgio cenários e percepções, permitindo ao tomador de decisão priorizar riscos de forma subjetiva, mas prática.

PORQUE

II. A análise qualitativa de riscos utiliza cálculos estatísticos precisos e dados quantitativos para mensurar o impacto no capital da empresa visando o montante exato de cada risco identificado.

A respeito dessas asserções, assinale a opção correta:

(C) A asserção I é uma proposição verdadeira, e a II é uma proposição falsa.

Q09

Em uma filial da empresa XPTO ocorreu um incêndio de grandes proporções. O corpo de bombeiros conseguiu conter as chamas antes que todo o prédio fosse comprometido, mas parte significativa dos servidores e documentos físicos foi perdida. As fitas de backup armazenadas em uma sala adjacente também foram danificadas pelo calor. Além disso, relatórios apontaram que alguns danos adicionais foram causados pela água e pelos produtos químicos utilizados pelos extintores durante o combate ao fogo. No relatório final, a equipe de segurança da informação precisou distinguir entre danos diretos
e danos indiretos decorrentes do incidente.

Qual dos seguintes exemplos corresponde a um **dano indireto**
causado pelo incêndio na filial da empresa XPTO?

(E) Danos estruturais adicionais provocados pela água e produtos químicos utilizados no combate ao incêndio.

Q10

Você é proprietário da empresa de entregas rápidas SpeeDelivery, que cresceu rapidamente devido ao aumento do comércio eletrônico. Para manter a competitividade, a empresa adotou uma política de análise e gestão de riscos em seus sistemas de TI e na logística de transporte. Durante uma reunião estratégica, foram discutidas as três principais respostas possíveis a riscos: aceitar, evitar e neutralizar (mitigar). Cada decisão deve estar alinhada ao apetite de risco da organização e ao impacto financeiro e operacional associado a cada ameaça.

I. A decisão de **aceitar um risco** ocorre quando o custo da contramedida supera o impacto potencial do incidente, sendo a empresa capaz de lidar com esse impacto caso ele ocorra.

PORQUE

II. A decisão de **evitar um risco** implica na substituição ou abandono da atividade de negócio que origina o risco, e a decisão de **neutralizar (mitigar)** corresponde à aplicação de controles que reduzem a probabilidade ou o impacto do risco a níveis aceitáveis.

A respeito dessas asserções, assinale a opção correta:

(B) As asserções I e II são proposições verdadeiras, mas a II não é uma justificativa correta da I.