Faculdade de Engenharia

Departamento de Engenharia Electrotécnica

Curso de Engenharia Informática

Primeira avaliação Escrita de Criptografia e Segurança de Dados

Data: 2017-04-21 |Semestre: 1| Turma: 4º Ano de Engenharia Informática Regime: Laboral | Duração: 120 Minutos

1. Complete a tabela abaixo como no exemplo (Não se deve repetir o mesmo problema) [3.5v]

	Problema	**Áreas de InfoSec**	**Tipo de Estratégia**	**Acção**
0	**Ataques terroristas**	**Defesa contra catástrofe**	**Sobrevivência**	**Backups**
1	Falhas temporárias de conectividade	Defesa contra faltas ou falhas do sistema	Redundância	Duplicação de provedores, Uso de Linhas de conexão alternativas
2	Inundação	Defesa contra catástrofe	Sobrevivência	Replicação de sistemas Replicação de Hadware (ex. RAID)
3	Perda por roubo de equipamentos computacionais	Defesa contra catástrofe	Sobrevivência	Backups, Replicação de Sistemas (ex. Servidor)
4	Queda no fornecimento de energia eléctrica	Defesa contra faltas ou falhas do sistema	Redundância	Uso de Gerador/Bateria
5	Bloqueio de aplicações/SOs;	Defesa contra faltas ou falhas do sistema	Sobrevivência	Uso de Sistemas transaccionais
6	Acesso a informação;	Defesa contra acções ilícitas	Defesa	Uso de criptografia, uso de ferramentas sploit para detectar e diminuir as vulnerabilidades de um sistema
7	Alteração de informação;	Defesa contra acções ilícitas	Defesa	Uso de criptografia
8	Utilização exagerada/abusiva de recursos computacionais;	Defesa contra acções ilícitas	Defesa	Uso de IDS para detectar a utilização indevida de recursos
9	Impedimento de prestação de serviços	Defesa contra acções ilícitas	Defesa	Uso de IDS para detectar e contrariar/anular ataques

2. Descreva a segurança física e lógica, identificando pelo menos três tecnologias de defesa usáveis para cada tipo de segurança. [3.0v].

Resposta:

Segurança Física – é a protecção existente ou por outras as barreiras que limitam o acesso directo ou contacto com a informação ou com a infra-estrutura onde a informação é suportada. A segurança física impede que os mal-intencionados tenham acesso físico aos activos pessoais ou organizacionais. Podemos ter como tecnologias: sensores, dispositivos electrónicos, Câmaras de vigilância, biometria, etc.

Segurança Lógica – é a protecção através de implantação de barreiras lógicas que limitam o acesso a informação que esta em ambiente controlado, por exemplo: restrição de acesso a uma base de dados com login e senha pode ser considerado segurança lógica. Podemos ter como tecnologias: Firewalls, antivírus, Sistemas criptográficos, backup, etc.

3. Identifique e descreva as categorias dos mecanismos de autenticação de usuários. [3.0v].

Autenticação - é o processo de verificar ou de testar se uma identidade proclamada é valida. A autenticação requer que o sujeito forneça factos como:

Algo que o sujeito sabe – que consiste em sequência de caracteres que o sujeito memorizou e que pode reproduzir em teclado quando solicitado. Ex: senha, pin, etc.

Algo que o sujeito tem – consistindo num dispositivo que o sujeito possui e deve ter em sua posse no momento de autenticação. Ex: smartcard, unidade USB, etc.

Algo que o sujeito é – consistindo em características físicas do sujeito ou parte delas. Ex: facto biométrico.

4. Liste pelo menos quatro métodos comuns de ataques baseados em rede. [2.0v]

Ataques baseados em rede são: Força bruta, dicionário, DoS, DoS distribuído, DoS distribuído de forma reflectiva, spoofing, botnets, sniffing do protocolo, spamming, man-in-the-middle, exploração da vulnerabilidade e saturação de dispositivos ou recursos.

5. Identifique e descreva as técnicas de gestão de risco. [3.0v]

Na posse do relatório sobre possível risco e custos justificados de contramedidas, assim como recomendações identificadas, os gestores podem optar por:

Mitigar o risco – Consiste em reduzir ou eliminar as vulnerabilidades, ameaças e o impacto do risco.

Transferir o risco – Assegurar ou passar a gestão para terceiros (outsourcing) de alguns processos em risco.

Evitar o risco - Evitar exercer algumas acções que causa risco.

Aceitar o risco – quando o risco reduzido ao nível de ser aceite ou assumido. O seu impacto é aceitável pelos gestores.

6. Compare IDS's baseados em conhecimento com IDS's baseados em comportamento e apresente duas vantagens e duas desvantagens para cada tipo. [2.5v]

IDS baseado em conhecimento, também conhecido por detecção baseada em assinatura ou ainda detecção baseada em padrão, utiliza uma base de dados de assinaturas cujo conteúdo tenta fazer corresponder com os eventos monitorados.

Vantagens: só detecta métodos de ataque conhecidos; não emite muitas alertas falsas

Desvantagens: não detecta novos métodos de ataque e requer actualização constante.

IDS baseado em comportamento, também conhecido por detecção estatística de intrusão ou ainda detecção heurística de intrusão, aprende e regista as actividades normais e eventos do sistema constituindo um padrão para comparação com futuras actividades ou eventos. Assim, quando ele detecta um comportamento desconhecido, considera que um ataque está ocorrendo e reage de acordo com as configurações ou respostas do administrador do sistema.

Vantagens: detecta métodos de ataque novos e antigos e mantém-se sempre actualizado

Desvantagens: emite falsos alarmes e pode bloquear actividades autorizadas não conhecidas.

7. Liste as 6 principais etapas (incluindo as fórmulas) de análise quantitativa de risco. [3.0v]

1. Inventário dos activos e atribuir um valor AV
2. Para cada activo produzir uma lista de ameaças. Para cada ameaça calcular o factor de exposição (EF) e expectativa de perda única (SLE).
3. Avaliar as ameaças para calcular a probabilidade de cada ameaça ocorrer dentro de um ano, isto é, a taxa anual de ocorrência (ARO).
4. Determinar o potencial de perda anual por cada ameaça, calculando a expectativa de perda anual(ALE).
5. Identificar as contramedidas para cada ameaça, e calcular as mudanças para cada ARO e ALE baseando –se na contramedida aplicada.
6. Fazer análise de custo/beneficio para cada contramedida por ameaça e por activo. Seleccionar a proposta mais apropriada por cada ameaça.

FORMULÁS: SLE = AV * EF. ARO = # / yr. ALE = SLE * ARO. Custo/beneficio = (ALE1 – ALE2) – ACS;

Onde: **SLE** = Single Loss Expectancy (Expectativa de perda única); **AV** = Asset value (valor do activo); **EF** = Exposure factor (Factor de exposição); **ARO** = Annualized rate of occurrence (Taxa anual de ocorrência); **ALE** = Annualized Loss Expectancy (Expectativa de Perda anual); **ACS** = Anual cost of safeguard (Custo anual do sistema de segurança).

Bom trabalho!