Auditoria de Sistemas

Prof. Luiz Antonio Ferraro Mathias

Aula 03

Conceitos fundamentais da auditoria

Conceitos Fundamentais da Auditoria

O processo de auditoria é baseado em um conjunto de conceitos fundamentais, dentre os quais, há de se destacar:

a) Ativo: qualquer coisa que tenha valor e relevância para organização, envolvendo: documentos, sistemas informatizados, ativos de processamento de informação (equipamentos), manuais etc.;

b) Incidente: um simples ou uma série de eventos de segurança indesejados ou inesperados que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança (exemplo: vírus de computador, instalação de softwares ilegal, acessos não autorizados etc.;

c) Vulnerabilidade: fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças;

As vulnerabilidades por si só não provocam incidentes de segurança, porque são elementos passivos. Porém, quando possuem um agente causador, como ameaças, esta condição favorável causa danos ao ambiente. As vulnerabilidades podem ser:

Conceitos Fundamentais da Auditoria

Controle	Descrição
Físicas	• instalações prediais fora do padrão; • salas de datacenter mal planejadas; • falta de extintores, detectores de fumaça e outros para combate a incêndio em sala com armários • fichários estratégicos; • risco de explosões, vazamentos ou incêndio.
Naturais	• os computadores são suscetíveis a desastres naturais, como incêndios, enchentes, terremotos, tempestades, e • outros, como falta de energia, o acúmulo de poeira, o aumento de umidade e de temperatura etc.
Hardware	• falha nos recursos tecnológicos (desgaste, obsolescência, má utilização) ou erros durante a instalação.
Software	• erros na aquisição de softwares sem proteção ou na configuração podem ter como consequência, uma maior quantidade de acessos indevidos, vazamentos de informações, perda de dados ou indisponibilidade do recurso quando necessário.
Mídias	• discos, fitas, relatórios e impressos podem ser perdidos ou danificados. A radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
Comunicação	• acessos de intrusos ou perda de comunicação.
Humanas	• rotatividade de pessoal, • falta de treinamento, • compartilhamento de informações confidenciais na execução de rotinas de segurança, erros ou omissões; • ameaça de bomba, sabotagens, distúrbios civis, greves, vandalismos, roubos, destruição da propriedade ou dados, invasões ou guerras.

Conceitos Fundamentais da Auditoria

d) Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

O termo genérico para identificar quem realiza ataques em um sistema de computadores é hacker. Porém, tal generalização possui diversas ramificações, pois cada ataque apresenta um objetivo diferente. Por definição, hacker são aqueles que utilizam seus conhecimentos para invadir sistemas, sem a intenção de causar danos às vítimas, mas como um desafio às suas habilidades.

Conceitos Fundamentais da Auditoria

As mais famosas técnicas de ataques às redes corporativas são:

I. Quebra de Senha – O quebrador de senha, ou cracker, é um programa usado pelo hacker para descobrir uma senha do sistema. Uma das formas de quebra são os testes de exaustão de palavras, a decodificação criptográfica etc.;

II. Denial of Service – Também conhecido como DoS, estes ataques de negação de serviço são aborrecimentos semelhantes aos mails bomba, porém muito mais ameaçadores porque eles podem incapacitar temporariamente uma rede corporativa ou um provedor de acesso. É um ataque que consiste em sobrecarregar um servidor com uma quantidade excessiva de solicitações de serviços. Sua finalidade não é o roubo de dados, mas a indisponibilidade de serviço. Existem variantes deste ataque, como o DoS distribuído, chamado DDoS, ou seja, a tentativa de sobrecarregar o I/O de algum serviço é feita de vários locais ao mesmo tempo;

Conceitos Fundamentais da Auditoria

iii. Cavalo de troia – É um programa disfarçado que executa alguma tarefa maligna. Um exemplo, o usuário roda um jogo qualquer que foi pego na internet. O jogo instala o cavalo-de-troia, que abre uma porta TCP (*Transmission Control Protocol*) no micro para a invasão. Este software não propaga a si mesmo de um computador para outro. Há também o cavalo-de-troia dedicado a roubar senhas e outros dados.

e) Risco: probabilidade de uma ameaça explorar uma vulnerabilidade e o impacto desta ocorrência. Categorias: Baixo, médio ou Elevado. O risco pode ser interpretado como a probabilidade de uma ameaça explorar uma vulnerabilidade, multiplicado pelo impacto que será gerado.

Conceitos Fundamentais da Auditoria

Durante o processo de auditoria, é importante a verificação do nível de maturidade do processo de gerenciamento de riscos, que envolve um conjunto de práticas e atividades que incluem a identificação, análise, priorização e monitoramento de eventos que podem ter efeitos positivos ou negativos sobre as metas e objetivos estabelecidos pela organização, seja no nível estratégico, tático ou operacional.

O gerenciamento de riscos envolve:

i. Aumento da probabilidade de atingimento dos objetivos.
ii. Enfrentamento de fatores externos e internos que tornam incertos os objetivos serão alcançados.
iii. Auxílio das organizações no estabelecimento de estratégias e na tomada de decisões fundamentadas.

Conceitos Fundamentais da Auditoria

O gerenciamento de riscos envolve benefícios:

i. Aumenta a probabilidade de atingimento dos objetivos;
ii. Promove a tomada de decisões gerenciais mais assertiva;
iii. Melhora o conhecimento organizacional, a aprendizagem e a comunicação interna e externa;
iv. Aumenta a competitividade no mercado;
v. Aumenta a confiança das partes interessadas;
vi. Encoraja uma cultura de gestão proativa e a mentalidade de riscos;
vii. Promove a gestão de mudanças eficaz;

Conceitos Fundamentais da Auditoria

viii. Otimizar os recursos com foco em riscos críticos;

ix. Fornece base confiável para relatórios confidenciais;

x. Protege as operações de ameaças e incertezas;

xi. Antecipa o conhecimento de potenciais eventos, antes desconhecidos;

xii. Busca a redução de multas, penalidades, e infrações das operações;

xiii. Aumenta o desempenho e a confiabilidade dos processos;

xiv. Minimiza perdas operacionais, financeiras e de qualidade.

Conceitos Fundamentais da Auditoria

O processo de gerenciamento de riscos pode ser observado abaixo: