TI.exames Com êxito

EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

Fundamentos da Segurança da Informação com base na ISO/IEC 27002

Curso e-learning completo

Preparatório para o exame EXIN ISO 27002 Foundation

Módulo 3

Conceitos de riscos e ameaças para a segurança da informação

Este módulo cobre:

- Conceitos de riscos e ameaças para a segurança da informação
- Tipos de ameaças, danos e riscos
- Medidas para redução de riscos
- Guias para implantação de medidas de segurança

Slide 2

Ameaças e riscos

- Antes de iniciarmos a definição e implantação de medidas de segurança, nós necessitamos saber contra o quê precisamos ser protegidos. Para isso precisamos fazer análise de risco (mais tarde vamos ver algumas alternativas para isso).
- A análise de risco é utilizada para identificar os riscos que a organização enfrenta. Um risco, dano ou perda de informação é determinado pelas ameaças, ou melhor, a chance destas ameaças ocorrerem e suas consequências.
- Exemplos:
  - → A empresa pode se incendiar
  - → Um funcionário pode descobrir os salários praticados pela empresa e divulgá-los
  - → Alguém pode se passar por funcionário para obter informações
  - → Um hacker pode obter acesso aos e-mails da empresa
- Quando uma ameaça se manifesta (por exemplo: um hacker conseguir acessar informações da empresa) chamamos este fato de **incidente**. Se for uma grande falha que impeça a empresa de dar continuidade as suas atividades, nós chamamos de **desastre** (por exemplo: terremoto, inundação, etc.).
- **Quando a ameaça se materializa, o risco se efetiva**. A extensão do risco e a avaliação do gerenciamento determinam as medidas a serem tomadas para minimizar o risco e suas consequências.

Slide 3

Vulnerabilidades

Vulnerabilidades são fraquezas associadas aos ativos da organização.

Vulnerabilidade = ponto fraco

Exemplos de vulnerabilidades:

Consultores:
- Contratação inadequada
- Falta de consultores

Instalação:
- Falta de mecanismo de monitoramento
- Proteção física inadequada
- Energia elétrica instável

Banco de dados:
- Falta de backup
- Armazenamento inadequado

Slide 4

Ameaças

Os ativos estão sujeitos a muitos tipos de ameaças que exploram suas vulnerabilidades.

Ameaça = uma ocorrência, um fato

Exemplos de ameaças:

Consultores

- Ofertas da concorrência
- Doença

Instalação

- Chuva forte, raios
- Pessoas não autorizadas com acesso

Banco de dados

- Vírus

Slide 5

Probabilidade

Qual é a probabilidade de um incidente?

10%

50%

90% de chance?

Slide 6

Exercício

- Relembre o exercício realizado no módulo 2 sobre uma empresa de consultoria:

  "Considere uma empresa de consultoria na área de informática que deseja implantar o SGSI conforme a norma ISO 27001 na sua área de vendas, dentro do seguinte escopo:

  Gerenciamento do sistema de segurança da informação para vendas de treinamento, consultoria e auditoria em segurança de informação na Rua Pau Brasil, 111, São Paulo, SP, Brasil."

- Para os ativos listados no exercício do módulo 2 identifique pelo menos para 3 ativos: suas vulnerabilidades, as ameaças que podem atingí-los e a probabilidade destas ameaças ocorrerem.
- Considere cores para identificar o valor: verde, amarelo e vermelho, sendo verde o menor valor, vermelho o maior valor e amarelo o valor intermediário.

  As respostas dependem de critérios pessoais, por isso é importante que o profissional que esteja realizando a análise busque padronizar seus conceitos antes de finalizar o tratamento de riscos.

Slide 7

Resposta do exercício

Descrição	Disponib.	Integrid.	Confidencial.	Valor	Comentário	Vulnerabilidade	Ameaças	Probabilid.
Metodologia					Acarreta dano, mas o processo pode ser executado	Não há pessoal de segurança Não há critérios de contratação para o pessoal de apoio	Roubo Divulgação	
Servidor 1					Peça-chave do processo	Antivírus desatualizado Backup inadequado e patches desatualizados	Contaminação por vírus Ataque de hacker	
Servidor 2					Peça-chave do processo		Contaminação por vírus Ataque de hacker	

Slide 8

Riscos de segurança

Um risco de segurança é o potencial que uma dada ameaça irá explorar vulnerabilidades para causar perda ou dano a um ativo ou grupo de ativos.

Nem sempre TI!
Os riscos podem ser técnicos, de equipamentos, de pessoas e de procedimentos.

Exemplos...?

Slide 9

Exemplos de riscos de segurança

- Interrupção da continuidade do negócio
- Indisponibilidade da informação
- Perda da integridade dos dados
- Perda ou roubo de informação
- Perda do controle do serviço
- Perda de credibilidade e imagem
- Perda da confidencialidade de dados
- Etc.

Slide 10

Análise de risco

- O processo que trata ameaças, riscos e medidas de segurança é chamado de Gerenciamento de Risco.
- Gerenciamento de Risco é um processo contínuo no qual os riscos são identificados, examinados e reduzidos a um nível aceitável. Este processo contínuo deve ser aplicado a todos os aspectos dos processos operacionais.
- Análise de risco é uma ferramenta usada no Gerenciamento de Risco. O propósito de se realizar a análise de risco é identificar que ameaças são relevantes aos processos operacionais e identificar os riscos associados. Então um nível de segurança apropriado em conjunto com medidas de segurança apropriadas podem ser determinados, garantindo uma boa relação de custo-benefício e o método adequado.

A análise de risco tem 4 objetivos:

- Identificar ativos e seus valores
- Determinar vulnerabilidades e ameaças
- Determinar os riscos e as ameaças que podem realmente causar danos aos processos operacionais
- Determinar o equilíbrio entre custos de um incidente e custos das medidas de segurança

Slide 11

Tipos de análise de risco

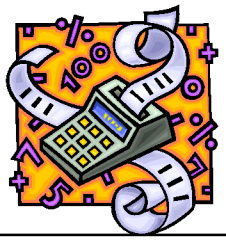
Existem 2 grupos de análise de risco: análises **quantitativas** e análises **qualitativas**.

Análise de risco quantitativa:

- Baseada no impacto do risco pretende calcular a perda financeira e a probabilidade de que uma determinada ameaça torne-se um incidente. Os valores de cada elemento dos processos operacionais é determinado. Estes valores podem ser constituídos pelos custos das medidas de segurança, como valor da propriedade incluindo itens como prédios, hardware, software, informação e impactos ao negócio.
- Deve ser feita considerando desde antes da ameaça aparecer, a efetividade e a segurança das medidas e o risco da vulnerabilidade ser explorada. Desta forma é fornecido um quadro claro do risco financeiro total e das medidas apropriadas que devem ser determinadas. O custo das medidas não deve ser maior que o valor do objeto a ser protegido do risco. Uma análise de risco puramente quantitativa é impossível.

Exemplos:

- Você é proprietário de uma seguradora e os detalhes de títulos de seus clientes foram tornados públicos devido à falha de um funcionário. Quantos clientes você irá perder devido a isso?
- Detalhes pessoais sobre uma testemunha de um caso criminal vazaram. Quantas testemunhas ainda estarão dispostas a testemunhar?
- Um empregado perdeu um pen-drive e a imprensa achou. Quão confiável ficou sua empresa aos olhos do público?



Slide 12

Análise de risco qualitativa

- Uma análise de risco qualitativa é baseada em cenários e situações. Desta forma as chance de que uma ameaça torne-se realidade é analisada com base nos sentimentos das pessoas. A análise então examina o processo operacional com o qual a ameaça se relaciona e as medidas de segurança que já tenham sido tomadas. Outras medidas podem ser tomadas, se necessário, para reduzir o risco residual a um nível aceitável.
- As análise de risco quantitativa e qualitativa têm vantagens e desvantagens. Deve-se definir para cada caso qual delas deve ser utilizada.

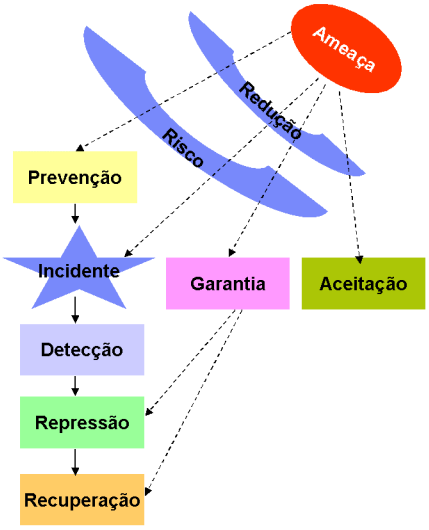
Slide 13

Medidas para reduzir o risco

- A análise de risco produz uma lista de ameaças e suas importâncias. O próximo passo é identificar para cada ameaça importante uma ou mais medidas que podem reduzí-la. As medidas podem ser de redução da chance do evento ocorrer ou da redução de suas consequências, ou a combinação dos dois.

Tipos de medidas de segurança:

1) Medidas de redução são usadas para reduzir as ameaças.
2) Medidas preventivas são usadas para prevenir incidentes.
3) Medidas de detecção são usadas para detectar incidentes.
4) Medidas repressivas são usadas para parar as consequências de um incidente.
5) Medidas corretivas são usadas para recuperação dos danos causados por um incidente.



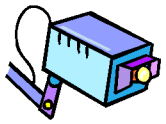
Slide 14

Tipos de medidas de segurança

Prevenção

- Prevenção impossibilita a ocorrência da ameaça ou reduz sua possibilidade. Um exemplo de prevenção é colocar informações sensíveis em um local seguro.

Detecção



- Se as consequências de um incidente não forem demasiado grandes, ou se após o incidente há tempo suficiente para minimizar os danos, então garantir que um incidente seja detectado tão rápido quanto possível e que todos sejam informados do que está ocorrendo pode ser uma boa opção. Um exemplo disso é o uso de câmeras de vigilância: só por saberem que estão sendo monitoradas as pessoas já são dissuadidas de realizar atividades impróprias.

Repressão

- Determinar que algo está ocorrendo não é suficiente, é necessário minimizar as consequências. Quando alguma coisa não vai bem e um incidente ocorre. queremos minimizar as consequências. Por exemplo, se houver um pequeno incêndio e houver um extintor à mão, este incêndio pode ser apagado por alguém. Medidas repressivas são aquelas que apagam o incêndio e também minimizam os danos causados. Fazer um backup é um exemplo de medida repressiva.

Slide 15

Tipos de medidas de segurança

Correção (Recuperação)

- Se um incidente ocorreu, há sempre algo que deve ser recuperado. A extensão dos danos vai depender das medidas repressivas tomadas. Por exemplo, se um colega fez um banco de dados e o sobrepôs acidentalmente ao banco de dados original, a extensão do dano vai depender do backup.

Garantia

- Para eventos que não têm prevenção total e para os quais as consequências não são aceitáveis, deve-se procurar métodos que reduzam as consequências. Isso é chamado mitigação. Seguro contra fogo e contra as consequências do fogo é um exemplo.

Aceitação

- Quando as medidas necessárias são conhecidas, mas decide-se aceitar o risco porque o custo para implantação da medida não é aceitável ou porque não há medidas possíveis.

Slide 16

Tipos de ameaças

Ameaças podem ser divididas em ameaças humanas e ameaças não-humanas.

- Normalmente os profissionais de segurança da informação já possuem uma lista padrão de ameaças e a usam como orientação para determinar quais são ou não relevantes. Segurança requer investimento da organização, mas não se deve gastar dinheiro com ameaças que não irão ocorrer.

Ameaças humanas

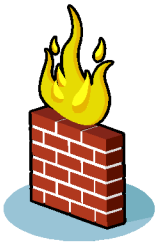
- Pessoas podem causar danos propositadamente ao sistema de informação por várias razões. Normalmente imaginamos que um hacker externo à empresa seria a pessoa a provocar estes danos. No entanto, são empregados de empresas que foram demitidos ou não foram promovidos como desejavam que na maioria das vezes destroem dados ou fornecem informação aos concorrentes.
- Não se trata apenas de informação armazenada eletronicamente, mas também de documentos físicos e até equipamentos. Engenheiros sociais usam pessoas e estas voluntariamente fornecem informações confidenciais da companhia.
- As pessoas também podem causar danos sem intenção, por exemplo pressionando acidentalmente a tecla delete ou usando um pen-drive que tem vírus e espalhando este vírus pelo sistema, ou utilizando um extintor de incêndio inadequado para apagar o fogo em um servidor.

Slide 17

Tipos de ameaças

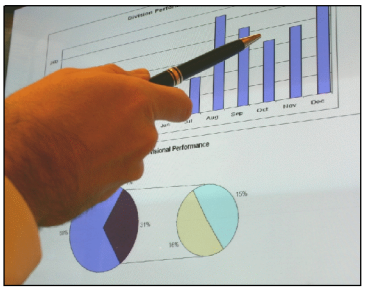
Ameaças não-humanas

- Existem ameaças que não são criadas por seres humanos. Podemos ter incêndios, inundações, raios e em países mais desafortunados terremotos, tufões e maremotos. Além dos citados ainda podemos ter desmoronamentos ou outros eventos que coloquem em risco a segurança da informação. Muitos dos danos causados vão depender da localização dos equipamentos.
- As ameaças podem ser divididas em ameaças humanas e não-humanas quando falamos em infra-estrutura básica como hardwares, softwares e bancos de dados, e transtornos no ambiente físico como prédios, instalações elétricas, documentos físicos, fornecimento de água, aquecimento, ventilação e refrigeração.



Slide 18

Tipos de danos



Os danos resultantes da manifestação das ameaças apresentadas até aqui podem ser classificados em:

- Danos diretos: roubo, furto.
- Danos indiretos: causados por uso inadequado de extintores de incêndio.

Parâmetros importantes:

- Expectativa de perda anual (ALE – Annual Loss Expectancy)
- Expectativa de perda por evento (SLE – Single Loss Expectancy)

Estratégias para lidar com os riscos (risk strategies)

- **Evitar o risco (Risk avoiding)**
  - →Medida são tomadas para eliminar a ameaça de tal forma que a ameaça não leve a um incidente.
  - →Exemplos: Não usar uma nova tecnologia que não se domina e optar por usar uma tecnologia antiga na qual o pessoal tem pleno conhecimento. Deixar de fazer a troca de versão de um software e ficar com a versão antiga para evitar os possíveis erros na nova versão

- **Aceitar o risco (Risk Bearing)**
  - →Consideramos que certos riscos são aceitos (nos arriscamos).
  - →Isto pode acontecer quando o custo da medida de segurança excede o dano.
  - →Nesta estratégia a organização vai optar por medidas de segurança repressivas.
  - →Exemplo: se houver um incêndio na sala iremos apagar o fogo com o extintor de incêndio.

- **Tornar o risco neutro (Risk neutral)**
  - →Medidas são tomadas mesmo que as ameaças já não se manifestam mais, mas se por ventura venham a se concretizar, o resultado do dano é minimizado.
  - →Nesta estratégia a organização pode optar pela combinação de medidas preventivas, detectivas e repressivas.

Guia para implantação de medidas de segurança

- **ISO 20000 -1** - Gestão de Serviços de TI
- **ISO 27001:2005** - Requisitos para um Sistema de Gestão de Segurança da Informação
- **ISO 27002:2005** - Código de Prática para Sistema de Segurança da Informação

Slide 21