Conceitos e Gerenciamento de Risco

Segurança e Auditoria de Sistemas

Curso de Sistemas de Informação - Uniube

Prof. Luciano Lopes

A Relativização da Segurança

O entendimento da segurança ou daquilo que representa um ambiente seguro é bastante relativo.

Gerenciamento de Riscos: Ativos

Definição de tudo que tem valor para o negócio. Estes elementos serão os ativos de informação.

Exemplos de Ativos

- **banco de dados de um ERP**
- **computadores e outros dispositivos de *hardware***
- ***softwares***

Exemplos de Ativos

- relatórios impressos
- colaboradores
- a marca da empresa ou de um de seus produtos ou serviços

Vulnerabilidades

Pontos fracos em processos, na gestão ou na tecnologia que podem ser explorados para comprometer a segurança da informação

Ex.: *software*, *hardware*, procedimento ou falha humana que possam ser explorados.

Vulnerabilidades

- **Sistemas operacionais desatualizados**

- **Redes sem fio abertas**

- **Serviços mal configurados em servidores**

- **Falhas de código**

- **Falhas de segurança física (falta de controles em portas, fechaduras, etc.)**

- **Portas abertas em sistemas operacionais ou *firewalls***

Ameaças

- acontecimentos provocados ou acidentais que podem trazer prejuízo para a organização.

- perigo potencial associado com a exploração de uma vulnerabilidade

- ocorre quando algo, ou alguém, identifica uma vulnerabilidade e a usa contra um alvo.

Ex.: incêndios, furtos, vírus de computador, *hackers*

Ameaças

Agente de ameaça é o nome que se dá àquele tira vantagem de uma vulnerabilidade

Ex.: funcionário ingênuo repassando informações confidenciais; invasor acessando uma porta de um servidor aberta acidentalmente em um *firewall*; enchente, etc.

Riscos

São a possibilidade de um agente de ameaça explorar uma vulnerabilidade.

Riscos

Ex.: quanto mais portas abertas existirem em um *firewall*, maior será a possibilidade de um invasor utilizar uma delas para um acesso não-autorizado.

Riscos

Ex.: se os usuários não são conscientizados sobre segurança da informação, maior será a possibilidade de um usuário desavisado ou inocente cometer um erro que pode significar um incidente de segurança.

Riscos

Riscos vinculam as vulnerabilidades, ameaças, e possibilidade de exploração que resultam no impacto do negócio

Riscos

Quanto <u>mais vulnerabilidades</u> existirem, maiores serão os <u>riscos</u> de prejuízo para o negócio

Exposição

Ocorrência quando um ativo de informação é exposto a possíveis perdas.

Uma vulnerabilidade expõe uma empresa (ou pessoa) a possíveis danos.

Exposição

Ex.: quando o gerenciamento de senhas é falho e as regras sobre o uso de senhas não são aplicadas, a empresa está exposta ao risco de ter as senhas de seus colaboradores capturadas e utilizadas de forma não autorizada.

Controle

Controles (ou contramedidas) são ações tomadas para mitigar riscos potenciais. Podem ser configurações de sistemas, dispositivos de *hardware* ou procedimentos que eliminem vulnerabilidades ou reduzam a possibilidade de um agente de ameaça explorar vulnerabilidades.

Controle

Ex.: gerenciamento de senhas, *firewalls*, guardas armados, mecanismos de controle de acesso e criptografia.

Medidas de proteção

Proteção ADMINISTRATIVA: regras que devem ser cumpridas por colaboradores e terceiros que utilizem os recursos computacionais da organização

Medidas de proteção

Proteção LÓGICA: fatores associados a recursos tecnológicos como *firewalls*, *software* antivírus e direitos que os usuários da rede tem nos sistemas

Medidas de proteção

Proteção FISICA: fatores como barreiras de proteção, muros, portas, grades e cadeados

Gestão de Riscos

É o planejamento das atividades que nortearão a forma com que a organização suportará as ameaças e os riscos

Gestão de Riscos

Etapas

Análise

Avaliação

Tratamento

Aceitação

Comunicação

Análise de Riscos

É o levantamento dos riscos possíveis, identificando, com o critério da organização, aqueles que representam maior probabilidade de prejuízos para o ambiente ou maior impacto para o negócio

Avaliação de Riscos

É o processo de tomada de decisões para cada risco analisado. Nesta etapa, opta-se por tratar ou aceitar cada risco

Tratamento de Riscos

Este processo resulta em tomar medidas para mitigar - ou eliminar, quando possível - os riscos identificados na fase da análise

Aceitação de Riscos

É o que se deve fazer quando não é possível tratar o risco.

Ex.: quando o custo para o tratamento do risco é mais elevado do que o valor do ativo de informação a ser protegido

Comunicação de Riscos

É o processo de esclarecer e atribuir responsabilidades sobre o tratamento dos riscos avaliados para todos os colaboradores da empresa