Análise de Riscos

Uma Análise de Riscos deve estar em conformidade com os objetivos e escopo de projetos que visam uma assessoria estratégica de segurança da informação e em composições estratégicas para o investimento e ações de continuidade dos negócios.

Atualmente podemos encontrar várias abordagens diferentes no que diz respeito a elaboração de uma Matriz de Risco. Baseadas em normas internacionais ou códigos de boas práticas, a avaliação de risco é vital na avaliação de segurança da informação.

Mas como fica a criação da Matriz de Risco ? Qual a melhor metodologia ?

Para responder estas perguntas é preciso ter bem esclarecido o objetivo da avaliação de risco. A partir deste ponto, podemos compor a nossa própria matriz de risco, pois a base dela são os controles que serão avaliados. Por exemplo, se estamos tratando especificamente sobre segurança da informação de uma forma geral e abrangente, os controles propostos pela norma ISO/IEC 27002 são suficientes para a avaliação. Outro exemplo é se estamos focando a continuidade e negócios, onde uma combinação de controles da ISO/IEC 27002, com SOX, DRI e NIST é mais recomendado. Uma vez estabelecidos os controles que serão avaliados, é preciso contextualizar a aplicação deles, ou seja, identificar e mapear o ambiente onde estes controles estão sendo aplicados.

Uma característica padrão de avaliação de risco e de elaboração da matriz de risco é que deve-se tratar dos seguintes temas:

Impacto: é importante avaliar o ambiente em relação aos critérios básicos de segurança da informação (**Disponibilidade, Integridade e Confidencialidade**). Nesta avaliação, é estimado o impacto baseados nestes destes critérios de cada item do ambiente avaliado.

Vulnerabilidade: ela é uma característica intrínseca de qualquer elemento que tenhamos que avaliar, pois praticamente todos os componentes do ambiente computacional possuem pontos vulneráveis.

Ameaça: cada vulnerabilidade pode ser explorada por uma ou mais ameaças, e a melhor forma de proteção é conhecer as ameaças existentes e seu potencial.

Probabilidade: saber a probabilidade de uma ameaça explorar uma vulnerabilidade é fundamental para identificar riscos. As probabilidades indicam o quão perto uma ameaça está para uma vulnerabilidade.

Risco: é uma função do Impacto x Probabilidade. Geralmente criamos uma tabela para relacionar e identificar o risco. Esta tabela segue parâmetros de criticidade específico para cada matriz de risco.

Tratamento de Risco: Podemos fazer quatro ações com os riscos

1. Mitigá-lo - através da aplicação de controles específicos;
2. Transferi-lo - através de atividades como um seguro;
3. Aceitá-lo - simplesmente tomando o conhecimento mas sem adoção de medidas de controle;
4. Evitá-lo - executando outra atividade, tomando outro caminho, não utilizando o item.

Tabela de Risco

A tabela de risco é utilizada para identificarmos o risco e, para isso, geralmente utilizamos uma combinação de cores (ou números). Neste exemplo usaremos a seguinte padronização:

Impacto de nível Alto (VERMELHO)
Resulta na perda altamente cara de recursos tangíveis ou principais. Pode significativamente violar ou impedir a operação de negócio.

Impacto de nível Médio (AMARELO)
Resulta na perda cara de recursos tangíveis, podendo prejudicar a operação de negócio.

Impacto de nível Baixo (VERDE)

Resulta na perda de algum recurso tangível, assim como afeta a operação do negócio.

Probabilidade de nível Alto (VERMELHO)
a fonte de ameaça é altamente motivada e suficientemente capaz e os controles para prevenir não são efetivos

Probabilidade de nível Médio (AMARELO)
a fonte de ameaça está motivada, é suficientemente capaz e os controles para prevenir são efetivos

Probabilidade de nível Baixo (VERDE)
a fonte de ameaça não está motivada, não é suficientemente capaz e os controles para prevenir são efetivos

A matriz de risco base relaciona as probabilidades (alta, média e baixa) com os impactos (alto, médio, baixo). Além disso, pontua os riscos seguindo a seguinte regra:

Probabilidade Alta = 1,0
Probabilidade Média = 0,5
Probabilidade Baixa = 0,1

Impacto Alto = 100
Impacto Médio = 50
Impacto Baixo = 10

Exemplo Conservador

	Imp. Baixo (10)	Imp. Médio (50)	Imp. Alto (100)
Prob. Alto (1,0)	Baixo (10)	Médio (50)	Alto (100)
Prob. Médio (0,5)	Baixo (5)	Médio (25)	Médio (50)
Prob. Baixo (0,1)	Baixo (1)	Baixo (5)	Baixo (10)

Escala de Risco: Alto (>50 a 100) Médio (>10 a 50) Baixo (1 a 10)

Exemplo Agressivo

	Imp. Baixo (10)	Imp. Médio (50)	Imp. Alto (100)
Prob. Alto (1,0)	Médio (10)	Alto (50)	Alto (100)
Prob. Médio (0,5)	Baixo (5)	Médio (25)	Alto (50)
Prob. Baixo (0,1)	Baixo (1)	Baixo (5)	Médio (10)

Escala de Risco: Alto (>45 a 100) Médio (>5 a 45) Baixo (1 a 5)

Matriz de Risco

Item	Disponibilidade	Integridade	Confidencialidade	Impacto	Vulnerabilidade	Ameaça	Probabilidade	RISCO
Roteador Internet	Alto	Médio	Baixo	Médio	Firmware antigo	DDoS	Médio	Médio
Banco de Dados	Alto	Alto	Alto	Alto	Senhas Fracas	Acesso Indevido	Baixo	Médio