1.Avaliando riscos de segurança - Gerenciamento de Riscos Segundo a ISO 27005

Gerenciamento de riscos é o processo de planejar, organizar, conduzir e controlar as atividades de uma organização visando minimizar os efeitos do risco sobre o capital e o lucro de uma organização.

Riscos podem surgir de vários lugares e maneiras. Diversos padrões de gerenciamento de riscos foram desenvolvidos, incluindo os do PMI (Project Management Institute), NIST (National Institute of Science and Technology) e padrões ISO. As estratégias de risco podem incluir transferir o risco para outra parte, evitar o risco, reduzir o efeito negativo do risco e aceitar algumas ou todas as consequências de um risco em particular.

Gerenciamento de riscos é um processo contínuo que se aplica a todos os aspectos dos processos operacionais. Em grandes organizações, a tarefa de monitorar esse processo é conduzida por um especialista em segurança da informação, tal como um encarregado de segurança da informação (ISO) ou um chefe de segurança da informação (CISO), que é designado especialmente para essa função é responsável pelo mais alto nível de gestão. São requisitos de segurança da informação:

1. A avaliação dos riscos à organização, levando em conta a estratégia e os objetivos globais de negócio da organização. Por meio de uma avaliação do risco, as ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o potencial impacto é estimado

2. Os requisitos legais determinados por estatutos, regulamentos e contratos que uma organização, seus parceiros comerciais, contratantes e provedores de serviço têm que satisfazer, e seu ambiente sociocultural

3. O conjunto de princípios, objetivos e requisitos de negócio para o manuseio, processamento, armazenamento, comunicação e arquivamento da informação que uma organização desenvolveu para apoiar suas operações.

Os recursos empregados na implementação de controles precisam ser equilibrados de acordo com os prejuízos de negócios que podem resultar de problemas de segurança na ausência de tais controles. O resultado da avaliação do risco irá ajudar a guiar e a determinar as ações de gestão adequadas e as prioridades para gerir os riscos.

2.Avaliação do Risco

Uma avaliação do risco da segurança da informação é conduzida nas primeiras etapas do projeto para identificar os controles necessários, enquanto a segurança da informação é parte de todas as fases da metodologia de projeto aplicada.

Em um mundo ideal, a segurança da informação é parte das operações diárias. Todos os funcionários estão cientes da segurança e reconhecem as falhas de segurança.

A segurança da informação é implementada em todos os sistemas e um alto nível de maturidade é alcançado.

Avaliações de risco devem identificar, quantificar e priorizar os riscos segundo critérios de aceitação do risco e objetivos que são relevantes para a organização. Os resultados devem guiar e determinar as prioridades e ações de gerência adequadas para gerir os riscos de segurança da informação e implementar os controles selecionados para proteger contra esses riscos.

A avaliação do risco deve incluir uma abordagem sistemática para estimar a magnitude dos riscos e o processo de comparar o risco estimado em relação a um critério a fim de determinar a importância do risco.

As avaliações de risco também devem ser analisadas periodicamente para tratar de mudanças nos requisitos de segurança e nas situações de risco.

A avaliação do risco da segurança da informação deve ter um âmbito claramente definido, a fim de ser eficaz, e deve incluir as relações com as avaliações de risco de outras áreas, se for o caso. O âmbito de uma avaliação do risco pode ser toda a organização, partes da organização, um sistema de informação individual, componentes específicos do sistema ou serviços onde isso for viável, realista e útil.

3.Abordagem Sobre a Análise de Riscos Segundo a ISO 27005

O objetivo de realizar uma análise de riscos é esclarecer quais ameaças são relevantes para os processos operacionais e identificar os riscos associados. O nível de segurança apropriado, juntamente com as medidas de segurança associadas, pode então ser determinado.

Uma análise de riscos é usada para garantir que as medidas de segurança sejam implementadas de forma economicamente eficiente e oportuna, fornecendo, com isso, uma resposta eficaz às ameaças.

Segurança como um estado ou condição é a resistência a danos. De uma perspectiva objetiva, é o verdadeiro grau de resistência a danos de uma estrutura. Isso significa que o grau de resistência a danos pode variar dia após dia.

A segurança como forma de proteção é feita de estruturas e processos que fornecem ou melhoram a sensação de segurança como condição. O ISECOM (Institute for Security and Open Methodologies) define segurança como “uma forma de proteção onde é criada uma separação entre os ativos e a ameaça”. Para ser seguro, ou o ativo é fisicamente removido da ameaça, ou a ameaça é fisicamente removida do ativo.

Uma análise de riscos ajuda a empresa a avaliar corretamente os riscos e a estabelecer medidas de segurança corretas e equilibradas. A administração também pode identificar os custos que estão envolvidos na adoção das medidas adequadas. Uma análise de riscos possui quatro objetivos principais:

1. Identificar os ativos e seus valores

2. Determinar os ativos e seus valores

3. Determinar o risco de as ameaças se tornarem realidade e interromperem os processos operacionais

4. Estabelecer um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança

Parte da análise de risco é uma avaliação de custo/benefício. Os custos anuais associados às medidas de segurança são comparados com as potenciais perdas que ocorreriam se as ameaças se tornassem realidade.

4.Análise Quantitativa do Risco

Uma análise quantitativa do risco tem como objetivo calcular, com base no impacto do risco, o nível de prejuízo financeiro e a probabilidade de uma ameaça se tornar um incidente. O valor de cada elemento em todos os processos operacionais é determinado. Esses valores podem ser compostos pelo custo das medidas de segurança, bem como pelo valor do próprio estabelecimento, incluindo itens como edifícios, hardware, software, informações e impacto dos negócios. Desta forma, é fornecida uma imagem clara do risco financeiro total e as medidas adequadas podem então ser determinadas.

Uma análise de riscos puramente quantitativa é praticamente impossível. Ela tenta atribuir valores a todos os aspectos, mas isso nem sempre é possível.

5.Análise Qualitativa do Risco

Outra abordagem da análise de risco é qualitativa, e aqui números e valores monetários não são atribuídos a componentes e perdas. Ao invés disso, os métodos qualitativos caminham através de diferentes cenários de possibilidades de risco e classificam a gravidade das ameaças e a validade das possíveis contramedidas. As técnicas de análise qualitativa que podem ser utilizadas incluem bom senso, melhores práticas, intuição e experiência. Exemplos destas técnicas são: grupos de discussão, pesquisas, questionários, listas de verificações, reuniões entre duas pessoas e entrevistas.

Quando uma equipe realiza uma análise de riscos, ela reúne pessoal com experiência e conhecimento das ameaças sobre avaliação. Este grupo é apresentado a um cenário que descreve as ameaças e as potenciais perdas, e cada membro então responde com sua intuição e experiência sobre a probabilidade da ameaça e a extensão do dano que pode resultar.

6.SLE, ALE, EF e ARO:

Expectativa de perda singular (SLE) é uma quantidade atribuída a um único evento, que representa a perda potencial da empresa se uma ameaça específica ocorresse: $valor\ do\ ativo\ *\ fator\ de\ exposição\ -\ EF\ =\ SLE$. O fator de exposição (EF) representa a percentagem de perda que uma ameaça ocorrida pode ter sobre certo ativo.

Expectativa de perda anual (ALE) é um valor desdobrado de suposição caso aconteça algum incidente. $ALE\ =\ SLE\ *\ ARO$.

A taxa de ocorrência anual (ARO) é o valor que representa a frequência estimada de ocorrência de uma ameaça específica dentro de um período de um ano. A faixa pode variar entre 0,0 (nunca) e 1,0 (ao menos uma vez ao ano) até valores maiores do que 1 (várias vezes ao ano).