MUST UNIVERSITY
FLORIDA - USA

Mitigando os Riscos à Segurança da Informação (parte 2)

Mitigando os Riscos à Segurança da Informação (parte 2)

Conteúdo organizado por **Dallas Morais de Almeida** em 2022 do livro ***Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002***, publicado em 2018 por Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H.

Objetivos de Aprendizagem

- Conhecer as características das contramedidas de controle dos riscos à segurança da informação
- Entender as aplicações das contramedidas no controle dos riscos à segurança da informação

Introdução

Estabelecer e aplicar um plano de controle de riscos à segurança da informação, demanda a avaliação dos riscos e ameaças e o desenvolvimento de contramedidas que serão aplicadas para tratar cada tipo de risco que tem a possibilidade de ocorrer na empresa.

Essas contramedidas tem características e aplicações específicas, porém não são excludentes entre si, ou seja, elas podem ser desenvolvidas e executadas em conjunto num modelo de interdependência e fortalecimento. Isso significa que em alguns casos a utilização de uma contramedida só terá efeito se a outra também estiver sendo executada, mas em outros casos a utilização de uma contramedida irá fortalecer ou potencializar a aplicação de outra.

Esses aspectos devem ser avaliados e decididos no momento em que se está estabelecendo o plano de controle dos riscos à segurança da informação que é baseado nas análises de riscos e potenciais ameaças que foram previamente estabelecidos.

Entender as características e especificidades de cada contramedida é essencial para que o plano de controle dos riscos contemple contramedidas eficazes e que realmente garantam um tratamento adequado dos riscos à segurança da informação.

Contramedidas de Prevenção

As contramedidas de prevenção têm o objetivo de impossibilitar a ação de um agente ameaçador. Nesse sentido, a organização dispõe de diversas atitudes que buscam impedir o avanço de uma ameaça. Essas atitudes podem no contexto material ou digital, depende dos recursos que a empresa dispõe e da probabilidade de ocorrência.

Exemplos de contramedidas de prevenção:

- Reforçar as trancas dos locais onde as informações sensíveis são armazenadas.
- Adicionar monitoramento por câmeras.
- Desconexão de processos estratégicos da internet.

Contramedidas de Detecção

Contramedidas de detecção diz respeito a ações que permitem à organização identificar de forma ágil a ocorrência de um incidente. Normalmente essas contramedidas são aplicadas quando as consequências do incidente não são muito grandes.

Exemplos de contramedidas de detecção:

- Ferramentas de fiscalização do uso da internet permitem a identificação do usuário que possivelmente acessou um site não autorizado.
- O monitoramento por câmeras de segurança permite a identificação de possíveis invasores.

Contramedidas de Repressão

Contramedidas de repressão são aquelas desenvolvidas depois que um incidente aconteceu. O objetivo principal dessas contramedidas é o de minimizar ao máximo o dano proveniente de uma falha no processo de segurança da informação. Medidas de repressão precisam ser dinâmicas e ágeis, pois só são aplicadas depois que a ameaça conseguiu explorar uma vulnerabilidade e quanto maior for o tempo de resposta a um incidente, maiores serão os danos e perdas.

Exemplos de contramedidas de repressão:

- Bloqueio de acesso de um usuário que conecta um *pen drive* não autorizado na rede.
- *Backups* automáticos garantem a preservação mesmo que parcial de informações que foram deletadas do sistema.

Contramedidas de Restauração

As contramedidas de restauração são utilizadas com o objetivo de recuperar aquilo que foi perdido depois da ocorrência de um incidente. O potencial das medidas de correção depende da efetividade das medidas de repressão, ou seja, quanto mais eficaz for a ação de repressão ao dano mais fácil será recuperar o que sofreu o dano.

Exemplos de contramedidas de restauração:

- Utilização de geradores de energia em caso de interrupção do fornecimento.
- Revistar alguém que furtou um HD externo com informações sigilosas.

Contramedidas de Seguro

As contramedidas de seguro são acionadas em casos onde o incidente não pode ser plenamente prevenido, porém os riscos não são aceitos. Nesse sentido, contramedidas de seguro são aquelas que tem o objetivo de mitigar (diminuir) as consequências de uma possível ocorrência.

Exemplos de contramedidas de seguro:

- Contratar um seguro contra incêndio.
- Manter uma cópia das informações estratégicas em outro lugar fora das dependências da empresa.

Aceitação

O plano de segurança da informação a ser desenvolvido por uma empresa naturalmente implica na tomada de decisões importantes que irão impactar todo o funcionamento da organização. Sendo assim, essas decisões precisam ser bem avaliadas e aplicadas, pois as consequências de decisões ruins podem ser desastrosas.

As decisões tomadas num plano de segurança da informação precisam acontecer após a identificação e avaliação de todos os possíveis riscos. Os responsáveis pelo tratamento de cada um desses riscos devem responder a seguinte pergunta: "Como iremos tratar esse risco"? As contramedidas mencionadas acima apresentam ações que objetivam combater diretamente um potencial risco, porém existe a possibilidade de simplesmente aceitar o risco.

Pode parecer estranho, porém, existem situações em que é melhor para a empresa aceitar a condição de risco do que adotar contramedidas para combatê-lo. Isso normalmente acontece quando os custos de se adotar uma contramedida é muito alto quando comparado com a probabilidade de ocorrência e o possível dano causado.

É importante, porém frisar que nesses casos, a aceitação do risco ocorre de forma consciente e somente após sua análise. Isso significa que a empresa não está ignorando ou deixando de estudar e examinar o risco, pelo contrário, a decisão de se aceitar o risco se baseia nos resultados da análise de riscos.

Em Resumo

Gerenciar riscos é uma tarefa fundamental para se garantir a sobrevivência e posicionamento de uma organização no mercado. Isso se dá pelo fato de que as informações organizacionais se caracterizam como um ativo de grande potencial e se esses dados caírem em mãos erradas podem causar enormes prejuízos a empresa.

Sendo assim, desenvolver ações de prevenção e tratamento de riscos deve estar sempre no radar dos gestores, pois as ameaças à segurança podem vir de muitos lugares. Os processos de tratamento dos riscos devem ser dinâmicos e apresentar contramedidas claras, objetivas e totalmente alinhadas aos objetivos organizacionais.

Essas contramedidas devem ser adotadas e aplicadas somente após os resultados das análises de riscos para que o custo de implementação seja equilibrado e não cause desfalques. As contramedidas aos riscos têm o propósito de mitigá-los ao máximo e garantir que a informação se mantenha íntegra nos processos organizacionais.

Aceitar riscos também pode ser uma decisão de controle, porém só deve ser tomada depois que os ricos foram devidamente avaliados e seus possíveis impactos mensurados.

Na ponta da língua

Referências Bibliográficas

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2018). *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. Brasport.

LIVRO DE REFERÊNCIA:

Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H.

Brasport, 2018.

Imagens: Shutterstock

MUST UNIVERSITY
FLORIDA - USA