1.ISO 27001:2013 - Mitigando os riscos à segurança

Controles de segurança são salvaguardas ou contramedidas técnicas ou administrativas que evitam, neutralizam ou minimizam perdas ou indisponibilidade devido a ameaças agindo sobre a sua correspondente vulnerabilidade. Controles são referenciados o tempo todo na segurança, mas são raramente definidos.

Antes de considerar o tratamento de um risco, a organização deve definir um critério para determinar se os riscos podem ou não ser aceitos. Um risco pode ser aceito se, por exemplo, for avaliado que o risco é baixo ou o custo do tratamento não é rentável para a organização. Tais decisões devem ser registradas. Uma decisão de tratamento de risco deve ser tomada para cada um dos riscos identificados após a avaliação de riscos. Possíveis controles para o tratamento do risco incluem:

1. Aplicar controles adequados para reduzir os riscos
2. Aceitar de forma consciente e objetiva os riscos, desde que satisfaçam claramente a política e os critérios de aceitação de risco da organização
3. Evitar riscos, não permitindo ações que possam causar a sua ocorrência
4. Transferir os riscos associados a outras partes, como seguradoras ou fornecedores
5. Ser selecionados e implementados para atender aos requisitos identificados por uma avaliação do risco
6. Assegurar que os riscos foram reduzidos a um nível aceitável levando em conta: requisitos e restrições da legislação; objetivos organizacionais; requisitos e restrições operacionais; o custo de implementação e operação em relação aos riscos sob o tratamento “redução” permanecendo proporcional às exigências e limitações da organização.

Os controles podem ser selecionados a partir da norma ISO 27002 ou de outros conjuntos de controle que a sua empresa use, ou novos controles podem ser projetados para atender às necessidades específicas da organização. É necessário reconhecer que alguns controles podem não ser aplicáveis a qualquer ambiente ou sistema de informação e podem não ser factíveis para todas as organizações.

Deve-se ter em mente que nenhum conjunto de controles consegue alcançar a segurança plena e que uma ação administrativa adicional deve ser implementada para monitorar, avaliar e melhorar a eficiência e a eficácia dos controles de segurança visando apoiar os objetivos da organização.

Quando uma ameaça se manifesta, tal como quando um hacker age para obter acesso à rede da empresa, nós chamamos isso de um incidente. Uma falha de energia, como os blecautes, é um grande incidente que pode ameaçar a sobrevivência da respectiva empresa de energia elétrica. Isso é chamado de desastre.

2.Contramedidas para mitigar o risco

A análise de riscos produz uma lista de ameaças e suas importâncias relativas. O passo seguinte é analisar cada ameaça grave e encontrar uma ou mais contramedidas que possam reduzir a ameaça. As contramedidas podem ser destinadas a: reduzir as chances de um evento acontecer; minimizar as consequências; uma combinação de ambas as coisas

Existem várias formas de definir um plano de segurança da informação e depende dos objetivos. Medidas de segurança devem sempre estar ligadas aos resultados da análise de riscos e baseadas nos aspectos de confiabilidade e características da informação. Isso pode ser dividido em seis categorias diferentes:

1. Contramedidas preventivas visam evitar incidentes
2. Contramedidas de redução visam diminuir a probabilidade de uma ameaça ocorrer
3. Contramedidas de detecção visam detectar incidentes
4. Contramedidas repressivas visam limitar um incidente
5. Contramedidas repressivas visam limitar um incidente
6. A aceitação do risco também é uma possibilidade. Dependendo do nível dos riscos, podemos também optar por aceitá-los. Uma empresa pode investir em seguros, pois decidiu que a chance de uma ameaça se tornar realidade é muito baixa para justificar o investimento em contramedidas caras

A prevenção torna impossível a ameaça ocorrer. Exemplos na segurança de TI podem incluir a desconexão de conexões com a Internet e conexões da rede local, visando assegurar que hackers externos não consigam obter acesso.

Em termos de segurança física, fechar as portas para prevenir que pessoas entrem no prédio é um exemplo, embora essa contramedida não seja muito prática. Existem outras medidas preventivas que são mais práticas.

O controle de alterações, no âmbito dos sistemas de gestão da qualidade (SGQ) e dos sistemas de tecnologia da informação (TI), é um processo formal usado para garantir que as alterações em um produto ou sistema são introduzidas de forma controlada e coordenada. O controle de alterações é um processo preventivo para reduzir a possibilidade de que alterações desnecessárias sejam introduzidas em um sistema sem premeditação. Isso também pode reduzir a possibilidade de introduzir falhas em um sistema ou desfazer mudanças feitas por outros usuários do software. Os objetivos de um procedimento de controle de alterações normalmente incluem interrupções mínimas aos serviços, redução de retrocessos e uso eficiente dos recursos envolvidos na implementação de mudanças.

Quando as consequências diretas de um incidente não são muito grandes, ou há tempo para minimizar o dano esperado, detecção pode ser uma opção. Certifique-se de que cada incidente possa ser detectado o mais cedo possível Apenas informar às pessoas que o uso da Internet é monitorado irá coibir a navegação imprópria na Internet de muitos funcionários. Uma ferramenta de monitoramento de Internet deve estar disponível para detectar o comportamento dos usuários, pois não há sentido em meramente fazer um anúncio preventivo sobre o monitoramento.

Quanto às atividades de monitoramento de rede do profissional de segurança dão uma indicação de que algo irregular aconteceu, uma ação tem que ser tomada. Quando algo realmente dá errado, isto é, quando um incidente ocorre, a coisa a ser feita é minimizar as consequências. Não há nenhuma vantagem em ter extintores de incêndio se ninguém tiver a iniciativa de usá-los em caso de incêndio. Medidas repressivas, tais como extinguir um incêndio, visam minimizar qualquer dano que possa ser causado. Fazer um backup também é um exemplo de medida repressiva. O backup pode ser usado para restaurar a última versão armazenada do documento, de forma que apenas uma parte do documento seja perdida.

Se um incidente ocorreu, sempre há algo que deve ser recuperado. A extensão do dano, seja ela pequena ou grande, depende das medidas repressivas que foram tomadas. Se um colega criar uma nova base de dados que sobrescreva a base de dados anterior, então a extensão do dano depende do backup. Quanto mais velho for o backup, maiores serão os danos produzidos.

Para eventos que não possam ser inteiramente prevenidos e para os quais as consequências não são aceitáveis, buscamos métodos que possam aliviar as consequências. Isso se chama mitigação. Seguro de incêndio nos protege contra as consequências financeiras de um incêndio. Armazenar uma cópia de toda informação importante em um local fora da organização todos os dias garante que, no caso de um incêndio, possamos ao menos ainda ter a informação que é insubstituível. Tais medidas não são baratas, mas geralmente são consideradas justificáveis.

Quando todos os riscos necessários e conhecidos são identificados, a gerência responsável pode decidir não realizar contramedidas de segurança. Às vezes os custos não são proporcionais ao risco apresentado e ao dano que pode resultar deste. Às vezes não há contramedida adequada para mitigar a ameaça que não o risco. A contramedida reduz os riscos.