1. Requisitos de segurança de sistemas de informação

Desde o primeiro momento em que a empresa considera comprar e desenvolver um sistema de informação, é recomendável que a segurança faça parte do projeto. A principal razão para isso é que adicionar segurança ao sistema de informação em uma fase posterior normalmente é mais caro do que fazer isso no projeto inicial. Projetar sistemas de informação seguros não é fácil, uma vez que eles normalmente são compostos por sistemas operacionais, infraestruturas, processos operacionais, produtos pré-fabricados, serviços e aplicações. O projeto e a implementação dos sistemas de informação que apoiam os processos operacionais podem ser fatores decisivos na forma como a segurança é implementada.

Adicionar segurança, em uma fase posterior, a um dos elementos de um sistema de informação pode ter efeitos negativos em outras partes. Para evitar tais problemas ao máximo, os requisitos de segurança precisam ser acordados e documentados antes que os sistemas de informação sejam desenvolvidos e/ou implementados. Como sistemas de informação são compostos por muitos elementos inter-relacionados e dependentes, é consideravelmente mais barato implementar, testar e manter medidas de segurança durante a fase de concepção do que durante, ou após, a implementação.

Quando requisitos de segurança são documentados durante a análise de riscos e a especificação dos requisitos para o projeto, eles são justificados, acordados e documentados como parte do "caso de negócio" completo feito para um sistema de informação.

1.1 Serviços para comércio eletrônico

Quando uma empresa decide estabelecer uma loja on-line, ela passa a enfrentar riscos novos, bem diferentes dos que enfrentava quando ela usava a Internet apenas para buscar informações. Serviços de comércio eletrônico e seu uso devem ser efetivamente protegidos. A confidencialidade e a integridade das transações de compra, das informações de pagamento incluindo detalhes do cartão de crédito, detalhes do endereço do destinatário e recibos de confirmação devem ser garantidas, e os clientes têm que se sentir confiantes de que nenhum estranho pode ter acesso a tudo isso. As informações das transações on-line devem ser protegidas para evitar transferências incompletas, roteamento incorreto, mudanças não autorizadas, publicações não autorizadas, cópias não autorizadas ou exibições de mensagens.

1.2 Informações publicamente disponíveis

A informação da empresa que é apresentada ao mundo inteiro em uma página da Internet é pública, mas ainda deve ser correta e incapaz de ser manipulada. Informações erradas causarão danos à reputação da organização. Seria extremamente irritante se você verificasse o website de uma empresa em busca de detalhes bancários para pagar uma conta e depois descobrisse que estavam incorretos e que o dinheiro foi depositado em outro lugar. Também é importante que um programa de computador que tenha sido disponibilizado atenda aos requisitos de segurança e do usuário.

2. Segurança nos processos de desenvolvimento e suporte

Os gerentes responsáveis pelas aplicações também são responsáveis pela segurança do ambiente de projeto no qual as aplicações são desenvolvidas, bem como pelo ambiente em que as aplicações são suportadas. Eles também determinam se as mudanças propostas podem comprometer a segurança. Por exemplo, eles precisam determinar se o desenvolvedor do sistema possui medidas de segurança que obedeçam aos requisitos da própria organização. A garantia sobre essas medidas de segurança pode, por exemplo, ser obtida através da auditoria do desenvolvedor do sistema por meio de terceiros.

3. Projeto de sistemas de informação seguros

Muitos sistemas da informação não foram projetados para serem seguros. A segurança que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por gestões e procedimentos apropriados. Identificar quais controles devem ser aplicados requer um planejamento cuidadoso e atenção aos detalhes. A gestão de segurança da informação requer, no mínimo, a participação de todos os funcionários da organização. Também pode exigir envolvimento de acionistas, fornecedores, terceiros, clientes ou outras partes externas. Também pode ser necessário aconselhamento especializado de outras organizações.

A gestão da segurança da informação da informação estabelece a base para um programa de segurança abrangente, a fim de garantir a proteção dos ativos de informação da organização. Hoje, as organizações estão altamente interligadas através da Internet. Praticamente nenhuma organização pode alegar ter sistemas de computadores isolados. Às vezes, uma organização faz uma rigorosa separação entre a Internet e a rede corporativa. Mesmo assim, muitas vezes uma ou mais conexões à Internet são estabelecidas. Isso se faz necessário para compreender os riscos para a empresa e como lidar com esses riscos. O gestor de riscos tem que compreender os objetivos do negócio e deve saber como mitigar tais riscos, de forma que a empresa consiga implementar contramedidas de segurança sem que isso seja um fardo para ela.

A segurança da informação engloba os controles administrativos, técnicos e físicos necessários para proteger a confidencialidade, integridade e disponibilidade dos aviso de informação. Os controles se manifestam através da implementação de políticas, procedimentos, padrões e diretrizes.

4.Teste e aceitação de sistemas

A fim de garantir que as mudanças não sejam implementadas de forma descontrolada, também é recomendado estabelecer vários ambientes físicos para desenvolvimento, teste, aceitação e produção dos sistemas de informação. Deve haver procedimentos para a movimentação do software de um ambiente para o outro. A opção de manter ambientes separados não é sempre frequentemente combinados.

Para a fase de desenvolvimento, aplicam-se requisitos de segurança específicos. No ambiente de desenvolvimento, desenvolvedores podem criar novos softwares ou trabalhar em mudanças nos softwares existentes. É muito importante criar versões.

O ambiente de testes se destina a determinar se o desenvolvimento atende aos requisitos gerais e, mais especificamente, aos requisitos de segurança. É no ambiente de aceitação que usuários finais podem verificar se o produto atende às suas especificações. Após a aceitação, um sistema pode então ser colocado em produção seguindo os procedimentos estabelecidos. Durante a transição do software existente para o novo software, sempre deve haver um plano de restauração, para que, em caso de um problema grave, seja possível reverter para a versão antiga. O ambiente de produção é destinado a ser usado para o software de produção, e esse é o ambiente em que os usuários finais normalmente trabalham.

5.Proteção dos dados de teste

É importante que equipamentos e dados de teste do programa sejam cuidadosamente escolhidos, protegidos e gerenciados. Dados reais, que podem conter informações sensíveis, como detalhes pessoais, não devem ser usados para teste. Sistemas de teste devem utilizar apenas dados fictícios. Há inúmeros exemplos na vida real nos quais o uso de dados reais para testar um sistema levou a situações indesejadas.