FACULDADE PITÁGORAS

PRONATEC

DISCIPLINA: SEGURANÇA DA INFORMAÇÃO

Prof. Msc. Carlos José Giudice dos Santos

Conteúdo Programático

Unidade 03
Princípios da Segurança da Informação

- Princípio da integridade da informação
- Princípio da confidencialidade da informação
- Princípio da disponibilidade da informação
- Políticas de segurança

Princípio da Integridade da Informação [1]

O primeiro dos três princípios da segurança da informação que estudaremos é a integridade. Este princípio vai garantir que a informação não será alterada de forma não autorizada. Portanto, é íntegra, mas com um detalhe a ser considerado: íntegra não significa exata. Ou seja, com uma informação podemos ter integridade, mas não exatidão. Por outro lado, não podemos ter exatidão sem integridade.

O controle da integridade deve proteger a informação de ameaças involuntárias ou intencionais, controlando os direitos de acesso, bloqueando os acessos indevidos de pessoas não autorizadas.

Princípio da Integridade da Informação [2]

Para considerarmos uma informação íntegra, ela não pode ter sido alterada de forma indevida ou não autorizada. Por exemplo, o valor de seu salário bruto no sistema de folha de pagamento com valor diferente e menor do que o do mês passado.

Neste caso, ele pode ter sido alterado por erro de operação (manutenção indevida de dados) ou por um funcionário mal-intencionado que modificou os valores nos bancos de dados da empresa.

A integridade da informação é fundamental para os negócios da empresa e para a comunicação interna ou com outras empresas.

Princípio da Integridade da Informação [3]

Quem recebe uma informação necessita ter a segurança de que a informação recebida, lida ou ouvida é exatamente a mesma que foi colocada à sua disposição por quem a emitiu para esta finalidade.

Ser íntegra significa estar em seu estado original, sem ter sofrido qualquer alteração por alguém não autorizado. Se uma informação sofre alterações em sua versão original, ela perde sua integridade, levando a erros e fraudes, prejudicando a comunicação e os processos de decisão de uma empresa como um todo. Isto não significa que uma informação original não possa ser alterada, mas que qualquer alteração só pode ser feita por pessoa autorizada, ou seja, com direito de acesso e alteração de uma informação.

Princípio da Integridade da Informação [4]

A perda de integridade ocorre quando uma informação é corrompida, falsificada, indevidamente alterada, ou excluída. Por exemplo, você acessa seu banco pela internet e seu saldo aparece zerado, sem que tenha ocorrido nenhuma movimentação da conta, ou simplesmente sua conta desapareceu e você recebe uma mensagem de que a conta não existe ou é inválida. Isso seria um caso de perda de integridade.

Uma informação poderá ser alterada de várias formas, tanto em seu conteúdo quanto no ambiente que lhe oferece suporte, isto é, o ambiente onde se encontra armazenada.

Princípio da Integridade da Informação [5]

Desta forma, a perda de integridade de uma informação poderá ocorrer sob três formas:

- Alterações do conteúdo dos dados;
- Quando forem realizadas inclusões, alterações ou exclusões de parte de seu conteúdo;
- Alterações no ambiente que oferece suporte ou armazena a informação.

Isto acontece quando são realizadas alterações na estrutura física e/ou lógica onde a informação está armazenada, seja nos sistemas e programas que apresentam a informação, seja nas estruturas de bancos de dados que armazenam estes dados.

Princípio da Integridade da Informação [6]

Para garantirmos a integridade das informações temos de assegurar que apenas as pessoas ou sistemas autorizados possam fazer alterações na forma e no conteúdo de uma informação ou que alterações causadas por acidentes ou defeitos de tecnologia não aconteçam também no ambiente de hardware (computadores, servidores, meios magnéticos de armazenagem) e comunicações (redes) no qual ela é armazenada e pela qual transita.

Em síntese, integridade significa que nos dados originais nada foi acrescentado, retirado ou modificado.

Princípio da Integridade da Informação [7]

A integridade de informações também diz respeito ao nível de confiança das informações do banco de dados, ou seja, a credibilidade e a lógica das informações.

Regras de restrição de integridade configuram um banco de dados a ser alimentado por informações com características lógicas específicas, validadas antes do seu armazenamento, diminuindo a probabilidade de falta de integridade no banco de dados. Estes aspectos são tratados no projeto e modelagem de dados em um processo de desenvolvimento de sistema de informações.

Princípio da Integridade da Informação [8]

Para revermos o que é a quebra de integridade, citamos:

- Um funcionário que modifica o valor do seu salário sem autorização no sistema de RH;
- Um vírus modifica arquivos em um computador;
- Hackers modificam um site.

Estes são alguns exemplos simples de quebra de integridade de informação.

Temos de considerar que hardware, software e os mecanismos de comunicação devem trabalhar de forma conjunta para manter e processar dados corretamente, assim como mover os dados para os destinos previstos, sem nenhuma alteração não prevista.

Princípio da Integridade da Informação [9]

Como princípio, os sistemas operacionais de computadores e as redes devem ser protegidos contra interferências e contaminações do ambiente exterior.

Para assegurar que atacantes externos ou erros cometidos por usuários não comprometam a integridade dos sistemas ou dados, todos os ambientes computacionais devem fornecer mecanismos de controle de segurança.

Os usuários geralmente afetam um sistema ou a integridade de seus dados por engano e não intencionalmente, embora usuários internos de uma empresa também possam realizar atos mal-intencionados.

Princípio da Integridade da Informação [10]

Programas de sistemas devem fornecer mecanismos que verifiquem os valores de entrada, se os mesmos são válidos e razoáveis. Isto é parte das obrigações dos programadores e analista de sistemas em relação à integridade da informação.

Os bancos de dados devem deixar apenas que indivíduos autorizados possam modificar dados, e os dados em trânsito devem ser protegidos por criptografia ou outros mecanismos que garantam o não acesso, ou modificação, deles sem autorização.

Princípio da Confidencialidade da Informação [1]

Nem todas as informações são sigilosas, ainda que sejam informações importantes, consideradas críticas. Algumas informações ou dados necessitam de confidencialidade ou sigilo, entre elas:

1. dados pessoais (por exemplo, número de telefone, endereço, CPF e RG, senha de acesso a bancos ou outros sites comerciais);
2. dados de cartões de crédito (por exemplo, número do cartão, código de segurança, senha);
3. dados de fornecedores ou de clientes de uma empresa;
4. dados de políticas financeiras de uma organização, ou de uma pessoa, como seu saldo bancário; e
5. dados de marketing ou política de preços de uma empresa, ou dados de rendimentos pessoais etc.

Princípio da Confidencialidade da Informação [2]

A perda desta confidencialidade provoca custos e prejuízos a empresas e pessoas, como perdas de clientes e fornecedores, perda de vendas e faturamento, perdas na imagem pública de uma empresa ou pessoa.

O princípio de manutenção da confidencialidade deve ser dirigido para o direito das pessoas e empresas e na classificação dos dados e informações.

O princípio da confidencialidade da informação tem como objetivo garantir que apenas a pessoa certa tenha acesso à informação devida para ela, ou seja, informação correta para a pessoa correta.

Princípio da Confidencialidade da Informação [3]

Ampliando nossos conceitos podemos afirmar que as informações trocadas entre pessoas e empresas normalmente não deverão ser do conhecimento de todos que fazem parte de uma empresa.

Muitas das informações geradas por algumas pessoas se destinam a um grupo específico de pessoas em uma empresa ou de sua rede de amigos e, muitas vezes, a uma única pessoa. Isso significa que esses dados deverão ser acessados e conhecidos apenas por um grupo limitado de pessoas, que deve ser definido pela pessoa ou, no caso de uma empresa, por um responsável pelas informações.

Princípio da Confidencialidade da Informação [4]

As informações devem possuir um grau de confidencialidade para cada uma, que deverá ser mantido para impedir que as pessoas não autorizadas tenham acesso a ela.

A classificação do grau de confidencialidade depende do tipo de organização, ou seja, cada organização pode estabelecer a sua própria classificação. Por exemplo, no Parlamento Europeu existem os seguintes graus de confidencialidade:

1) Público; 2) Reservado; 3) Confidencial;

4) Secreto; 5) Ultra-secreto

Engenharia Social [1]

A Engenharia Social é uma ciência que estuda o modo como a humanidade se comporta sob o ponto de vista procedimentos lógicos (ao contrário das ciências humanas, que possuem um viés subjetivo).

Assim, é possível prever (com razoável grau de certeza), que atitudes uma grande massa de pessoas pode tomar frente a alguns fatos que lhe são impostos.

A Engenharia Social também é um meio pelo qual induzimos as pessoas a fazer o que queremos (por exemplo, nos dar informações).

Engenharia Social [2]

A Engenharia Social existe há muito tempo, muito antes do advento das tecnologias digitais. O filme "Prenda-me se for capaz" mostra um caso típico de um falsário que abusou da Engenharia Social para obter o que queria: dinheiro e aventuras.

O advento das tecnologias da informação e da comunicação potencializou os métodos e técnicas utilizadas na Engenharia Social.

Simplificando, engenharia social é a arte de enganar outra pessoa para obter o compartilhamento de informações confidenciais, colocando-se como uma pessoa autorizada a acessar essas informações.

Engenharia Social [3]

Alguns usuários podem intencionalmente ou acidentalmente revelar informações sigilosas por não criptografá-las antes de enviá-las a outras pessoas. Eles podem, ainda, ser vítimas de um ataque de engenharia social, que se caracteriza pelo compartilhamento de segredos comerciais de uma empresa, pela falta dos cuidados necessários na proteção de informações confidenciais quando estas são processadas por sistemas, ou pelo envio de mensagens de sistemas via e-mails automáticos.

A confidencialidade pode ser fornecida por vários meios, por exemplo:

Engenharia Social [4]

- Por meio da criptografia de dados armazenados e/ou transmitidos durante o tráfego em rede;
- Por meio de um rigoroso controle de acesso aos dados;
- Por meio de uma rigorosa classificação de dados sigilosos (graus de confidencialidade);
- Por meio de treinamento de pessoal nas empresas, sobre quais são os procedimentos adequados para se tratar determinado tipo de informação.

Engenharia Social [5]

Quando falamos em tráfego de rede, queremos dizer que ter confidencialidade na comunicação é ter a segurança de que aquilo que foi enviado a alguém ou registrado em algum lugar (um e-mail, por exemplo) só será acessado ou lido por quem tiver autorização para tal.

Um outro exemplo: Pensemos no caso de um cartão de crédito. O número do cartão só deverá ser conhecido por seu proprietário e pela loja onde é usado no momento da compra. Se esse número for descoberto por alguém mal-intencionado, como nos casos noticiados sobre crimes da internet, o prejuízo causado pela perda desta confidencialidade poderá ser muito alto.

Engenharia Social [6]

Esse número poderá ser usado por alguém para fazer compras na internet ou em qualquer estabelecimento que receba pagamentos com cartão de crédito, trazendo prejuízos financeiros e uma grande dor de cabeça para o proprietário do cartão, além de afetar a imagem da empresa que recebeu pagamento com estes cartões.

Este exemplo mostra perda de confidencialidade e uma grave falha em segurança da informação.

Manter a confidencialidade é um dos fatos mais determinantes para a segurança e uma das tarefas mais difíceis de implementar, pois envolverá todos os elementos que compõem a comunicação de informações, da origem até o destino.

Engenharia Social [7]

Além disso, como já vimos no exemplo do Parlamento Europeu, as informações têm diferentes graus de confidencialidade, normalmente associados a seus valores sociais ou empresariais.

Quanto maior for o grau de confidencialidade de uma informação, maior será o nível de segurança necessário na estrutura tecnológica e humana que participar destes processos: utilização, acesso, trânsito e armazenamento das informações.

Graus de Confidencialidade [1]

As informações geradas pelas pessoas tanto no ambiente pessoal quanto em uma empresa têm uma finalidade específica e destinam-se a um indivíduo ou grupo de indivíduos dentro da empresa.

Portanto, é necessário a existência de uma classificação com relação à sua confidencialidade. É o que chamamos de grau de sigilo, isto é, a graduação atribuída a cada tipo de informação com base no grupo de usuários que possuem as permissões de acesso a esta mesma informação.

O grau de confidencialidade é um dos componentes mais importantes no processo de classificação da informação.

Graus de Confidencialidade [2]

Os graus de confidencialidade variam de organização para organização, mas normalmente as informações possuem os seguintes tipos de classificação quanto à confidencialidade:

» Confidencial.

» Restrito.

» Sigiloso.

» Público.

Neste caso, a classificação "Confidencial" representa o maior grau de confidencialidade, enquanto a classificação "Público" representa o menor grau (nenhuma confidencialidade).

Graus de Confidencialidade [3]

Dizem que o único computador totalmente seguro é aquele desligado da tomada. A arte da engenharia social concentra-se no elo mais fraco da corrente da segurança de computadores: os seres humanos. Logo o acesso à informação, mesmo aquelas com nível de classificação de confidencialidade mais alto, pode ser obtido por meio de pessoas ou ingênuas ou mal-intencionadas.

Como um ataque da chamada "engenharia social" pode revelar muitas informações?

Como tornar um sistema de computadores mais seguro?

Graus de Confidencialidade [4]

A resposta é a educação (treinamento) e difusão da classificação da informação, explicando aos funcionários e pessoas ligadas direta ou indiretamente a um determinado sistema a importância de uma política de segurança e confidencialidade. Assim evitar-se-á o ataque de pessoas que poderão tentar manipulá-los para ganhar acesso a informações privadas.

Podemos dizer e afirmar que este é um excelente começo para tornar segura a sua rede ou sistema de informações.

Vamos ver um exemplo de grau de confidencialidade:

Graus de Confidencialidade [5]

No Brasil, documentos oficiais do governo podiam ter sigilo eterno. A partir da publicação da Lei 4.553 em 2002, foi estabelecido 4 graus de sigilo:

1. **Ultrassecreto**: informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do país, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não-autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado. Prazo máximo: 30 anos, prorrogáveis, a critério do Poder Executivo.

Graus de Confidencialidade [6]

2. **Secreto**: informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicos, cujo conhecimento não-autorizado possa acarretar dano grave à segurança da sociedade e do Estado. Prazo máximo: 20 anos.

3. **Confidencial**: informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não-autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado. Prazo máximo: 10 anos.

Graus de Confidencialidade [7]

4. **Reservado**: informações cuja revelação não-autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos. Prazo máximo: 5 anos.

Para fins de avaliação deste curso, os graus de confidencialidade (geralmente utilizados em empresas) são:

1. Confidencial;
2. Restrito;
3. Sigiloso.

Princípio da Disponibilidade da Informação [1]

Toda e qualquer informação deve estar disponível sempre que for necessário. Deriva deste princípio a ideia de que devemos ter "a informação certa, na hora certa para a pessoa certa", o que une os três princípios da segurança da informação.

Os recursos tecnológicos da informação devem ser mantidos sempre em bom funcionamento e devem ser capazes de ser recuperados de forma rápida e completa, em casos de desastres naturais ou acidentais.

Quando crackers atacam um servidor de modo a tirá-lo do ar, o objetivo principal destes criminosos é tornar a informação deste servidor indisponível.

Princípio da Disponibilidade da Informação [2]

A disponibilidade da informação se refere a toda estrutura física e tecnológica necessária para permitir o acesso, o tráfego e o armazenamento das informações e dados.

Por exemplo, se durante uma reunião de diretoria de uma empresa os serviços de banco de dados falham, e com isso impede que seja tomada uma determinada decisão em pauta, estaremos com uma quebra de disponibilidade também.

Outro exemplo: se durante uma compra em um supermercado, o sistema dos caixas trava, temos uma quebra de disponibilidade, nesse caso, crítica, porque impede o faturamento de mercadorias.

Princípio da Disponibilidade da Informação [3]

Se você acessa seu banco pela internet para saber seu saldo antes de emitir um cheque, por exemplo, e o site de seu banco está fora do ar, ou sobrecarregado e não responde, isto também caracteriza uma indisponibilidade de informação. Ou seja, a quebra do princípio que estamos discutindo.

Para proteger a disponibilidade da informação, é necessário saber quem são seus usuários e organizar e definir, para cada caso, as formas de disponibilização da informação. Em outras palavras, quem tem acesso e uso para quando for necessário.

Princípio da Disponibilidade da Informação [4]

A disponibilidade da informação é sempre considerada com base no valor que esta informação tem e no impacto da indisponibilidade dela. Sites de internet, em particular, têm a necessidade de garantir de maneira ininterrupta o acesso e a disponibilidade de informações e recursos.

Podemos considerar então a existência da preocupação com a proteção da informação na internet, pois o avanço tecnológico traz consigo o surgimento de novos métodos de ataques de crackers atrelado a uma maior vulnerabilidade de sistemas que não se atualizam no mesmo ritmo.

Princípio da Disponibilidade da Informação [5]

Logo, manter disponibilidade é um princípio, porém é mais um ponto da segurança que deve ser sempre considerado.

É necessário que haja sempre controle sobre pontos específicos de falhas que devem estar em vigor, caso as medidas necessárias de backup tenham de ser tomadas. Outrossim, mecanismos de redundância de dados (bancos de dados espelhados) devem estar no local quando necessário.

Desta forma, os efeitos negativos de componentes ambientais que geram indisponibilidade de informação poderão ser evitados.

Princípio da Disponibilidade da Informação [6]

Por exemplo, um servidor de banco de dados parar por falha de hardware, como queima do equipamento por sobrecarga elétrica, deixaria indisponíveis todas as suas informações.

Uma medida de segurança seria o backup frequente dos bancos de dados para recuperação em outro equipamento, ou então a existência de um equipamento sobressalente, em que estariam duplicadas todas as informações. Este equipamento redundante substituiria automaticamente o equipamento queimado ou interrompido.

Princípio da Disponibilidade da Informação [7]

A disponibilidade de informações pode ser afetada por falha de hardware ou por falha de software, por isso a importância de backups para permitir a recuperação e a continuidade da disponibilização das informações.

Observe que as questões ambientais como calor, frio, umidade, eletricidade estática, bem como a contaminação por vírus ou ataques, também podem afetar a disponibilidade de um sistema de informações.

Então o princípio da disponibilidade deve impedir a interrupção dos serviços e manter a produtividade com sistemas de informação.

Vulnerabilidades [1]

As vulnerabilidades são os pontos que, ao serem explorados por pessoas mal-intencionadas, afetam a confidencialidade, a disponibilidade e a integridade das informações de um indivíduo ou empresa.

Um dos primeiros passos para a implementação da segurança é rastrear e eliminar os pontos vulneráveis de um ambiente de tecnologia da informação.

Muitas vezes as palavras ameaça, vulnerabilidade, exposição e risco são usadas para representar a mesma coisa, apesar de terem diferentes significados e relações entre si.

Vulnerabilidades [2]

É importante compreender a definição de cada uma delas, mas o mais importante é que você compreenda a associação de uma às outras.

Vulnerabilidade é algo que pode acontecer devido a um software, hardware ou falha de um processo que pode fornecer a um atacante uma porta aberta que ele está à procura, para entrar em um computador ou rede e ter acesso não autorizado aos recursos dentro deste ambiente.

Uma **ameaça** é qualquer perigo potencial para a manutenção dos princípios da segurança da informação.

Vulnerabilidades [3]

Um agente de ameaça pode ser, por exemplo, um intruso que venha a acessar uma rede por meio de uma porta no firewall, um determinado processo de sistemas acessando de forma que viole as políticas de segurança, ou um furacão (tempestade) destruindo uma instalação de um centro de processamento de dados, ou um empregado que venha a cometer um erro não intencional que poderia expor informações confidenciais.

A **exposição** é o fato de as informações e sistemas de tecnologia da informação serem expostos a perdas a partir de um agente de ameaça interna ou externa.

Vulnerabilidades [4]

Uma vulnerabilidade pode causar danos e perdas a uma organização, se exposta a possíveis danos por esta exposição.

Por exemplo, se o gerenciamento de senhas é frouxo e as regras de senha não são aplicadas ou não existem, a empresa pode ter suas senhas de usuários expostas, capturadas e utilizadas de forma distinta de seu titular, com finalidades destrutivas ou de violação de confidencialidade.

É muito normal em empresas existirem regras para as senhas de acesso a rede e banco de dados com no mínimo oito caracteres, sendo obrigatório que um deles seja numérico.

Vulnerabilidades [5]

Além disso, as senhas não podem conter nome, sobrenome ou data de nascimento, e o usuário é obrigado a trocá-las com uma frequência determinada.

Hoje, até mesmo alguns bancos solicitam que seus clientes troquem de senha com frequência. Do contrário, informam, por exemplo, que a senha não é trocada há mais de seis meses.

Na prática, alguém do RH utiliza uma senha simples para usuário. Outra pessoa mal-intencionada pode copiá-la a fim de ter acesso aos salários de outros funcionários, mesmo que seja somente para consulta.

Vulnerabilidades [6]

Contramedida, ou salvaguarda, é o que atenua um risco potencial. Uma medida preventiva é uma configuração de software, hardware ou um procedimento que elimina uma vulnerabilidade dos sistemas ou reduz o risco de um agente de ameaça de ser capaz de explorar uma vulnerabilidade.

Contramedida pode ser um forte gerenciamento de senhas (uma espécie de guarda de segurança para controle de acesso) assim como mecanismos de controle dentro de um sistema operacional, a implementação de um sistema básico entrada/saída (BIOS), senhas e treinamento de conscientização de segurança.

Políticas de Segurança [1]

O que é uma política de segurança?

Em síntese, é um programa de segurança que busca garantir os três princípios da segurança da informação:

1) Integridade;

2) Confidencialidade;

3) Disponibilidade.

Na política de segurança de uma empresa, a gestão estabelece como um programa de segurança será criado e as metas deste programa, atribuindo as responsabilidades, demonstrando o valor estratégico e tático da segurança e descrevendo como a aplicação desta política deve ser realizada.

Políticas de Segurança [2]

Políticas devem abordar questões específicas de segurança que a administração vier a determinar que precisam de explicação mais detalhada e mais atenção, para termos certeza de que é uma estrutura de procedimentos bem abrangente e construída para que todos os funcionários da empresa entendam que devem respeitá-las.

As empresas podem optar, por exemplo, por uma política de segurança de e-mail. Nela descreverão o que a administração pode ou não fazer com mensagens de e-mail dos funcionários, como os funcionários podem ou não usar as funcionalidades de e-mail de forma diferente, assim como as questões de privacidade específicas dos endereços.

Políticas de Segurança [3]

Uma política específica de sistemas deve apresentar as decisões da administração que estão mais próximas dos computadores atuais, redes, aplicativos e dados.

Este tipo de política deve fornecer uma lista de softwares aprovados que podem ser instalados em estações de trabalho individuais. Deve, ainda, descrever como as bases de dados serão protegidas (regras de autorizações de acesso aos dados), como os computadores podem ser bloqueados e como ferramentas tipo firewall, sistemas de detecção de intrusão e scanners devem ser utilizados na empresa.

Políticas de Segurança [4]

As políticas são escritas como uma visão geral e com objetivo de dar conta de muitos assuntos, mas muito detalhamento é necessário para desenvolver as formas e métodos que precisam acontecer para realmente apoiar e efetivar esta política.

A política de segurança prevê as bases da garantia de segurança de informação, tais como os procedimentos e seus componentes, assim como as implementações e mecanismos tecnológicos que serão usados para preencher um quadro de especificações desta política, criar um programa de segurança total e garantir uma infraestrutura segura.

Políticas de Segurança [5]

Uma política compõe-se de quatro grandes conjuntos de elementos, quais sejam:

1. Normas.
2. Linhas recomendadas (baselines).
3. Diretrizes.
4. Procedimentos.

Normas de Segurança

As normas especificam como produtos de hardware e software devem ser utilizados.

Estas normas podem ser, por exemplo, um padrão da empresa que exige que todos os funcionários tenham e usem seus crachás de identificação na empresa, com os dados sobre a sua pessoa, em todos os momentos. Ou então que indivíduos desconhecidos fora dos quadros funcionais da empresa devem ser questionados sempre sobre a sua identidade e seu propósito (por que estão ali) ou, ainda, que todas as informações confidenciais devam ser criptografadas.

Linhas Recomendadas (baselines)

As linhas recomendadas têm como objetivo prover o nível mínimo de segurança necessário para toda a empresa.

Na maioria das vezes, as linhas de base são implementações de segurança de uma única plataforma necessárias para fornecer o nível desejado de proteção e segurança da informação. Por exemplo, uma empresa pode exigir que todas as suas estações de trabalho tenham ao menos um nível de segurança, chamado C2.

O nível de segurança da linha de base seria C2, e a linha de base, o apoio aos procedimentos que forneçam instruções passo a passo sobre como o sistema operacional e os componentes dessa estação de trabalho têm de ser instalados para atingir esse nível de segurança específico. Isto é o conceito de linha de base, ou baseline.

Diretrizes [1]

Diretrizes são ações de recomendação ou guias operacionais para os usuários, que devem ser utilizados quando uma norma específica não se aplica, ou não existe uma norma específica para uma determinada situação de utilização dos recursos de TI da empresa.

Elas lidam com as metodologias de segurança de computadores e de seus softwares.

Sempre existem áreas de atuação não muito claras para um usuário, em que acontecem situações que nunca haviam sido definidas, ou ações não previstas. Portanto, algumas orientações podem ser utilizadas como referência nestes momentos.

Diretrizes [2]

Considerando que as normas são atividades obrigatórias específicas, as diretrizes são orientações gerais que fornecem a flexibilidade necessária para as circunstâncias imprevistas.

Uma política pode determinar que o acesso a dados confidenciais deve sempre ser auditado, ou seja, deve existir um registro completo deste acesso.

Por exemplo, caso um usuário se depare com um incidente de segurança (por exemplo, um acesso não autorizado a dados confidenciais), a diretriz vai informar como ele deve proceder nesses casos (quem avisar e como relatar, por exemplo).

Procedimentos [1]

Procedimentos são as ações detalhadas, passo a passo, para a realização de uma determinada tarefa.

Estes passos podem ser aplicados por usuários, pela equipe de TI, pelo pessoal operacional, pelos membros da equipe de segurança e por quem mais precise instalar ou configurar um componente de um computador.

Muitas empresas escrevem e têm procedimentos sobre a forma como os sistemas operacionais devem ser instalados, como mecanismos de segurança devem ser configurados, como configurar uma lista de controle de acessos, como criar novas contas de usuário, como atribuir privilégios, como registrar e fazer auditoria, procedimentos para destruição de materiais, relatórios de incidentes etc.

Procedimentos [2]

Procedimentos são o nível mais baixo da cadeia de uma política de segurança, porque eles estão mais próximos dos computadores e fornecem instruções detalhadas para problemas de configuração e instalação de software e hardware.

Normas, diretrizes e linhas básicas (baselines) tem finalidades específicas e públicos diferentes. Por exemplo, um documento que descreve como estar em conformidade com uma regulamentação específica pode ser repassado para a equipe de gestão. Enquanto isso, um procedimento detalhado sobre como proteger adequadamente um sistema operacional específico é dirigido a um membro da equipe de TI.

Procedimentos [3]

Cada um desse elementos (normas, baselines, diretrizes e procedimentos) podem e devem ser independentes e realizado de natureza modular, para facilitar a distribuição, compreensão e atualização adequadas, quando se fizer necessário.

Os documentos devem expor a forma como as políticas, normas e diretrizes serão realmente implementadas em um ambiente operacional.

A implementação de políticas de segurança e os itens que a apoiam deve receber o devido cuidado da empresa e de sua equipe de gestão. Nesse caso, o detalhamento é muito importante.

Procedimentos [4]

Deve ser informado, de maneira clara, aos funcionários da empresa, o que se espera deles e as consequências do não cumprimento dos elementos das políticas de segurança, destacando a responsabilidade de cada um.

Se uma empresa demite um funcionário porque ele estava baixando material pornográfico no computador de trabalho, o empregado pode levar a empresa à justiça e ganhar, caso consiga provar que ele não foi devidamente informado sobre o que era considerado de uso aceitável e inaceitável de propriedade da empresa e quais seriam as consequências.

Procedimentos [5]

Por incrível que pareça, os elementos da política de segurança estudados, devem deixar claro nas normas e linhas de base quais são as restrições, e devem ser obrigatoriamente divulgados para assegurar que funcionários respeitarão a política de segurança da informação da empresa.

Normas para proteção de computadores [1]

Os usuários comuns devem proteger os seus computadores contra ameaças potenciais. Para esta proteção ser efetiva, dez regras simples devem ser seguidas.

Muitas pessoas já conhecem todas ou pelo menos parte destas regras, mas deixam de seguir por diversos motivos, que vão da preguiça até a confiança excessiva na sorte.

As dez regras básicas para proteger o seu computador são as seguintes:

1. Utilizar um sistema operacional confiável

Isto significa utilizar um SO original. Não se deve baixar SO's de sites não oficiais, porque a chance de você estar baixando um SO modificado por um cracker é muito grande.

Baixar um SO de um site de hackers, por exemplo, é quase uma garantia de problemas futuros, porque com certeza, ninguém vai disponibilizar um SO desbloqueado (por exemplo, Windows 7) por caridade. Um SO baixado de sites não oficiais quase sempre contém algum tipo de manipulação para facilitar uma invasão futura em seu computador.

2. Atualizar sempre o seu sistema operacional

Não existem softwares perfeitos. Diariamente são descobertas falhas em SO's por hackers e que podem ser exploradas por crackers.

Não adianta nada você usar um sistema operacional confiável (original) e não atualizá-lo com frequência para corrigir as falhas descobertas pela comunidade hacker.

Assim, atualizar sempre o seu SO é um complemento de segurança em relação ao primeiro passo, que é utilizar um SO confiável.

3. Criar contas de usuários específicas

Suponha que você já utiliza um SO confiável e o atualiza com frequência, mas não tenha cadastrado uma senha para usar o seu computador. Caso você tenha feito isso, você utiliza seu SO com privilégios de administrador, e no caso de um cracker conseguir invadir o seu computador, ele terá os mesmos privilégios que você.

Assim, além de cadastrar uma senha, você deve criar contas específicas, como por exemplo, uma conta de convidado (ou **guest**). A conta de administrador deve ser usada apenas por você. Caso alguém peça seu computador emprestado, a conta de convidado vai restringir aquilo que a pessoa pode fazer em seu computador, protegendo informações vitais do sistema e até as suas informações pessoais. Para que isto aconteça é necessário configurar a conta de convidado, especificando aquilo que ele pode ou não fazer.

4. Utilizar um programa antivírus

Utilizar um antivírus hoje é praticamente obrigatório. São muitas as opções disponíveis de antivírus, e as melhores são geralmente pagas.

Existem opções gratuitas de antivírus, e alguns usuários costumam utilizar dois programas antivírus gratuitos ao mesmo tempo, para que um programa complemente a proteção contra falhas do outro.

A melhor opção é usar um antivírus pago, mas diante da impossibilidade, é melhor usar um (ou dois) programas gratuitos do que nenhum.

5. Utilizar um programa de firewall

Firewall é um programa que monitora as portas de seu computador, deixando sair ou entrar através da rede, apenas os pacotes autorizados.

Os próprios SO's hoje já possuem um firewall, mas esta proteção pode ser complementada com aplicativos específicos, que podem ser pagos ou gratuitos.

Os melhores programas antivírus pagos geralmente incluem também a proteção de um firewall.

6. Utilizar um programa anti-spyware

Spywares são programas de espionagem, que visam capturar informações de seu computador.

Muitos programas antivírus já incluem uma proteção contra spywares, mas com o tempo e a crescente sofisticação deste tipo de programa, esses programas antivírus, especialmente os gratuitos, acabaram perdendo a eficiência de proteção contra este tipo de ameaça.

Entretanto, os antivírus pagos geralmente ainda continuam fornecendo uma proteção eficiente contra os spywares.

7. Utilizar um navegador seguro

Navegadores seguros são aqueles que permitem configurar ou personalizar níveis de proteção, além de avisar ou bloquear sites potencialmente perigosos.

Navegadores como como o Internet Explorer, Firefox, Chrome ou o Safari estão entre os mais seguros. Alguns programas antivírus complementam a segurança do navegador, instalando complementos de segurança, tais como uma camada adicional de criptografia ou o recurso de Sandbox (que cria uma área separada para fazer testes de programas da Internet sem contato direto com o seu SO).

8. Fazer backup com frequência

Todo mundo sabe da importância de se ter uma cópia de segurança dos seus principais arquivos, mas geralmente as pessoas só passam a se preocupar mais seriamente com isso no dia em que perdem suas informações mais preciosas.

Existem programas que fazem backup, mas na prática, muitas vezes não é necessário utilizá-los, exceto no caso de empresas, que além de usar programas específicos, geralmente possuem uma política própria para guardar e proteger as suas informações.

9. Utilizar senhas seguras

A grande maioria das pessoas utilizam senhas fáceis de serem quebradas, utilizando palavras com nomes de parentes, de namorados, de animais de estimação, datas de nascimento, números de telefones e outras informações óbvias e fáceis de serem conseguidas por engenharia social.

Criar senhas seguras, com uma quantidade mínima de caracteres, utilizando letras maiúsculas e minúsculas, números e símbolos especiais é essencial para garantir a confidencialidade de suas informações.

10. Criar uma política de e-mails

O e-mail é hoje a forma mais comum de se receber um ataque de crackers. Hoje o simples fato de se abrir um e-mail que contenha uma imagem já é suficiente para permitir uma invasão em seu computador.

Nunca se deve abrir um e-mail de uma pessoa ou empresa desconhecida, por mais tentador que o e-mail possa parecer. Além disso, nunca se deve clicar em um anexo, seja de que tipo for, exceto se for vídeos ou imagens de uma pessoa em que você confia.

Jamais se deve enviar informações pessoais via e-mail. Empresas jamais vão pedir este tipo de informação por e-mail. Quando pedem, não é por e-mail, mas em um formulário utilizando uma conexão segura (criptografada).