Objetivos da Segurança

Roteiros e tópicos para estudo por

Vinícius da Silveira Serafim
professor@serafim.eti.br
http://professor.serafim.eti.br

Palavras-chave: Confidencialidade, Integridade, Disponibilidade, Irrefutabilidade e Autenticidade

Objetivos da Segurança (PFLEEGER, 2006, p. 10):

- Confidencialidade
- Integridade
- Disponibilidade

Alguns autores chamam esses objetivos de *princípios* da segurança ou mesmo *atributos* da segurança. No entanto, seguiremos usando *objetivos (ou atributos)* da segurança conforme a referência citada e vamos usar princípios com outro significado mais adiante nas aulas.

Confidencialidade

Definição

Somente as partes autorizadas acessam determinado ativo. (PFLEEGER, 2006, p. 10)

Explicação

É importante compreender o significado de três palavras chave da definição: *partes, acessam* e *ativo*. Quando nos referimos à partes queremos dizer: uma pessoa, um sistema ou mesmo um servidor. O termo acessar, no caso da confidencialidade, compreende não só leitura, mas também termos como visualizar, imprimir ou simplesmente saber que um determinado ativo existe. E ativo, segundo a definição da ISO 27001:2006, é qualquer coisa que tenha valor para a organização (ex.: informações em qualquer mídia - armazenadas ou em trânsito -, equipamentos, serviços de rede, etc).

Portanto, para garantir a confidencialidade deve-se saber: quais partes podem ter quais tipos de acesso a um determinado ativo. Vamos a um exemplo:

- *Ativo*: folha de pagamento (informações armazenadas em um sistema)
- *Parte*: Setor de Recursos Humanos; *Acessos*: visualizar e alterar
- *Parte*: Financeiro; *Acessos*: visualizar
- *Parte*: TI; Acesso: nenhum

Se, no nosso exemplo, alguém da TI visualizou o salário de um ou mais funcionários, há uma quebra de segurança, mais especificamente há o comprometimento (ou quebra) da confidencialidade do ativo.

Um outro exemplo: uma determinada empresa presta serviços de monitoramento remoto de cargas em regime 24x7. No entanto, eventualmente, essa empresa paralisa suas rotinas de monitoramento em razão de manutenções a serem realizadas em seu ambiente. Neste exemplo temos:

Ativo: a informação de quando uma dessas manutenções irá ocorrer
Parte: gerente do monitoramento; *Acessos*: saber
Parte: equipe de monitoramento; *Acessos*: nenhum

Sendo assim, se uma quadrilha de ladrões de carga obtém conhecimento sobre o agendamento de uma manutenção, teremos a quebra da segurança de novo no que diz respeito ao comprometimento da confidencialidade.

Integridade

Definição

Ativos podem ser modificados somente pelas partes autorizadas ou somente de formas autorizadas. (PFLEEGER, 2006, p. 10)

Explicação

Há um outro termo que deve aqui ser melhor explanado: modificados. Modificar, na definição de integridade, inclui expressões como: escrever, mudar, apagar e criar.

O termo *integridade* é um tanto amplo e pode significar diferentes coisas em diferentes contextos. (PFLEEGER, 2006, p. 11) Por exemplo, quando dizemos que a integridade de um ativo foi preservada, podemos estar querendo dizer que o item:

- é preciso
- não foi modificado
- foi modificado somente de formas aceitáveis
- foi modificado somente por pessoas autorizadas
- foi modificado somente por programas autorizados
- é consistente
- possui significado e é utilizável

Vamos ver alguns exemplos para tornar a ideia mais clara. Partindo do exemplo dado no item *confidencialidade* (acima) sobre folha de pagamento, ao afirmarmos que as informações de salários são íntegras estamos querendo dizer que:

- os salários, ao serem alterados, permaneceram dentro dos parâmetros normais de remuneração da empresa
- os salários somente foram modificados pelo Setor de Recursos Humanos da empresa
- os salários somente foram modificados através do sistema ERP da empresa
- os salários de pessoas com os mesmos cargos e funções são similares

Um outro exemplo é quando dizemos que um HD está íntegro. Ao fazer essa afirmativa podemos estar querendo dizer:

- que os dados lidos correspondem aos dados gravados, ou seja, não há nenhuma falha no equipamento; ou
- que os dados não foram modificados a partir de um dado momento (imagine nesse caso um HD apreendido pela polícia para ser então periciado, é fundamental que os dados não tenham sofrido modificações desde a apreensão do HD).

Disponibilidade

Definição

Ativos são acessíveis às partes autorizadas nos momentos apropriados. (PFLEEGER, 2006, p. 10)

Explicação

Quantas vezes não ouvimos um atendente nos dizer que está impedido de realizar determinada operação pois o "sistema está fora do ar". Esse é um caso típico de comprometimento da disponibilidade (ou indisponibilidade) de um ativo, sendo este último o sistema e, consequentemente, as informações nele contidas.

A indisponibilidade pode ter diversas causas como, por exemplo: queda de luz, queda de um link Internet, falhas em discos rígidos, ataques de negação de serviço (DoS ou Denial-of-Service). Esses últimos serão estudados mais adiante em nossa cadeira.

Apenas para dar um exemplo, uma forma bem comum de causar um DoS em um sistema é provocar o bloqueio de contas por número de tentativas erradas de login. Talvez manualmente seja trabalhoso para o atacante, mas imagine esse ataque implementado através de um programa?

A disponibilidade é o objetivo da segurança mais visível para clientes e empresários. Uma quebra de confidencialidade, muitas vezes, não é percebida até que o atacante faça uso do ativo a que obteve acesso. E mesmo quando o faz, de acordo com as particularidades das suas ações, muitas vezes não é detectado. A detecção de um comprometimento da integridade, assim como a quebra da confidencialidade, só é percebida quando os seus efeitos se fazem patentes afetando, por exemplo, o funcionamento de um sistema.

Uma forma bastante comum de se garantir algum nível de disponibilidade é através do uso de recursos redundantes. Por exemplo:

- Uso de dois links Internet ao invés de apenas um
- Uso de geradores de energia
- HDs em RAID 5

Objetivos “adicionais”

Outros dois objetivos, irrefutabilidade e autenticidade, devem ser também considerados. Embora Pfleeger não os liste como objetivos da segurança, diversos outros autores o fazem.

Além disso, a autenticidade é um objetivo que acaba por permear todos os outros.

Irrefutabilidade (ou não-repúdio)

Definição

As partes envolvidas em uma transação são capazes de provar, posteriormente, o que aconteceu. (ANDERSON, 2008, p. 343)

Explicação

A irrefutabilidade, ou não-repúdio, é um objetivo bastante desejado em, por exemplo, sistemas bancários. Imagine um cliente (malicioso) de um banco que realiza um saque em um caixa eletrônico. Mais tarde ele volta ao banco e alega que não fez o referido saque, ou seja, refuta (ou repudia) a operação. O objetivo do cliente é fazer com que a transação seja desfeita, fazendo com que o banco corrija o problema realizando um crédito em sua conta no valor do saque. Se tudo der certo, o cliente atinge seu objetivo: ficar com o dinheiro sacado sem que sua conta seja debitada (fraude bancária).

Situações similares, onde uma das partes refuta a transação, podem ser facilmente imaginadas:

- envio de e-mails
- alteração de um salário em um sistema
- navegação em sites pornográficos na empresa
- etc

Autenticidade

Definição

É um processo em que se estabelece a validade:

- de uma mensagem, de uma transação; ou
- de um indivíduo, de uma identidade ou de um atributo de uma parte (PFLEEGER, 2006, p. 619)

Essa definição será aprofundada ao tratarmos de criptografia e também na aula 9 (Identidade e Autenticação).

Explicação

Assim como a integridade, a autenticidade pode ter diversos significados de acordo com o contexto em que é empregada. A autenticidade de uma identidade (ID), por exemplo, significa que uma determinada identidade é válida. Em termos mais práticos, uma carteira de identidade contém além dos dados da pessoa, uma série de mecanismos que visam impedir a falsificação desse documento, permitindo que alguém com conhecimento desses mecanismos possa verificar a autenticidade do documento.

O documento em si é simplesmente uma identidade porém, sendo esta autêntica, e havendo nela alguma informação que permita correlacioná-la fisicamente a uma pessoa específica (ex: foto, assinatura ou digital), é possível então autenticar um indivíduo.

Ainda considerando o exemplo da identidade, é possível autenticarmos um ou mais atributos como, por exemplo: idade e nome dos pais.

No caso de uma mensagem autêntica, queremos dizer que a mesma não foi alterada por uma parte não autorizada. Isso, até certo ponto, pode causar confusão com o papel da integridade. E, de fato, há razão para isso: quando afirmamos que para garantir a integridade temos que garantir que o ativo foi modificado somente por pessoas autorizadas. Como saber se a pessoa que o modificou foi autorizada? A resposta é identificação e autenticação, assunto da aula 9.

Os cinco objetivos

Os cinco objetivos estudados de forma alguma existem por si só. De acordo com o contexto em que são aplicados eles se sobrepõem (algumas vezes causando discussões sobre os seus significados), se complementam (confidencialidade implica algum nível de autenticidade, por exemplo) e em outros contextos entram em choque.

Esse último caso pode parecer estranho, mas é perfeitamente possível. Não será mais fácil garantir a confidencialidade das informações se elas forem armazenadas em um sistema completamente off-line e que está trancado numa sala segura? Porém, como fica a disponibilidade dessas informações? Será que uma empresa ou organização com pontos de presença pelo mundo, podem se dar ao luxo de utilizar tal sistema?

A resposta pode ser tanto “não” (talvez a primeira que você pensou ao ler a pergunta) quanto “sim”. O que vai de fato determiná-la é qual o valor relativo entre confidencialidade e disponibilidade para que a empresa (ou organização) realize seus objetivos de negócio.

Embora esse valor relativo possa variar bastante de acordo com o contexto, em geral, o valor da disponibilidade faz com que a resposta seja “não”.

Nunca analise isoladamente os objetivos de segurança de um ativo, lembre-se que todos se relacionam de algum modo e que uma visão limitada, sem considerar as implicações entre os objetivos, pode levar à quebra da sua segurança.

Bibliografia

ANDERSON, R. J. Security Engineering: A Guide to Building Dependable Distributed Systems. 2a edição. Wiley, 14 de abril de 2008. 1080 pág.

PFLEEGER, C. P. Security in Computing. 4a edição. Prentice Hall, 23 de outubro de 2006. 880 pág.

A última versão desde documento sempre será disponibilizada no site
http://professor.serafim.eti.br