Introdução a segurança em sistemas de informação

Víctor Orozco, Dr. Ana Trindade Winck

Centro de Tecnologia
Universidade Federal de Santa Maria

15 de Janeiro de 2013

Objetivos da aula

- Apresentar uma visão geral da grande área de segurança da informação
- Identificar princípios básicos de segurança
- Discutir um modelo genérico de segurança de informação

Roteiro

Segurança

Segurança

- A segurança é um dos mais antigos problemas que governos, organizações comerciais e quase todas as pessoas tem de enfrentar
- Pode-se definir a segurança como a percepção de estar protegido contra riscos, perigos ou perdas.

Segurança

- Em um sentido amplio a segurança significa proteger os nossos ativos
  - Proteger os nossos sistemas contra atacantes
  - Proteger o nosso prédio contra desastres naturais
  - Proteger a nossa carteira de roubos na boate

Segurança

- Dependendo do contexto assim tem que ser as medidas de segurança
  - Ativos físicos: Computadores, carros
  - Ativos lógicos: Arquivos de dados, código fonte de aplicativos
  - Ativos humanos: Seres humanos a base de qualquer negocio

Segurança em SI

- Segurança SI = Proteger sistemas de informação e a informação mesma de acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição

Segurança em SI

- Conceito que se torna cada vez mais presente em muitos aspectos da nossa sociedade
- Embora a tecnologia nos permite ser mais produtivos, ela também carrega consigo uma série de questões de segurança
- A introdução de sistemas de informação na industria tem aumentado o problema de segurança ainda mais
- Se a informação sobre os sistemas utilizados pelos nossos empregadores ou nossos bancos fica exposta a um atacante, as consequências podem ser devastadoras

Assegurando Informação

"O único sistema realmente seguro é aquele que está desligado, dentro dum bloco de concreto com guardas armados, e mesmo assim eu tenho minhas dúvidas"[Andress 2011].

Assegurando Informação

- Quanto mais aumentamos o nível de segurança, geralmente diminui o nível de produtividade
- Devemos também considerar como o nível de segurança refere-se o valor do item que está sendo assegurado
- Podemos construir uma instalação militar cercada por cães assassinos . . . mas não faz sentido se o ativo a proteger for a lista de compras do mercado.

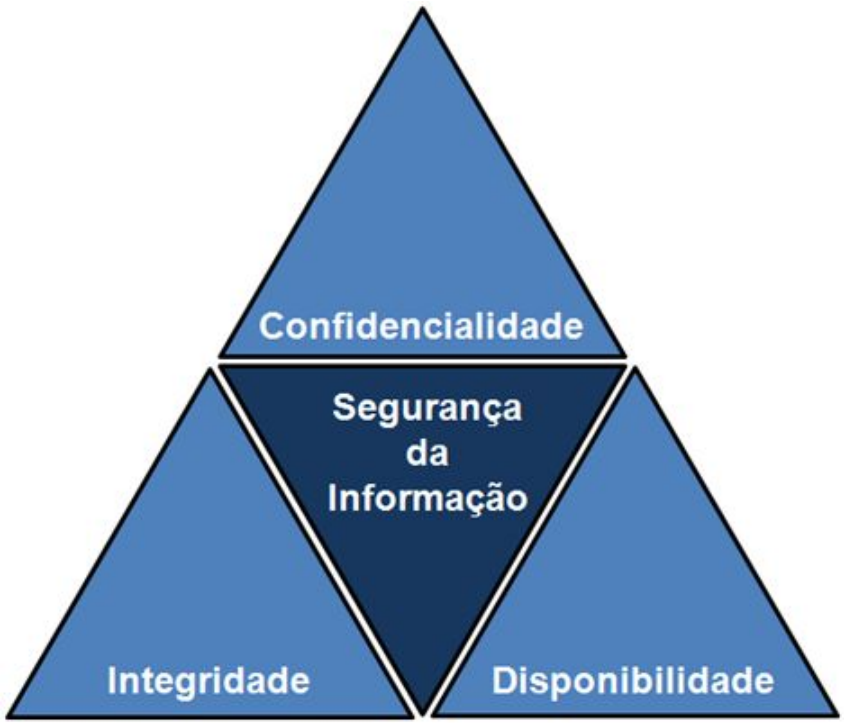
Assegurando Informação

- Definir um nível aceitável de segurança é um processo subjectivo
- Técnica generalizada: Definir uma lista dos ativos onde somos vulneráveis (sempre vai ter alguma coisa a mais)
- Alguns regulamentos tentam definir o que proteger, ou pelo menos alguns dos passos que uma organização deve tomar para ser “seguro”.

Assegurando Informação

- Como pode-se definir esse listado?
- Listando nossos ativos e verificando se eles apresentam características seguras de acordo a algum modelo estandardizado

Modelo CID


Confidencialidade
Segurança
da
Informação
Integridade
Disponibilidade

Modelo CID - Confidencialidade

Nossa capacidade de proteger nossos dados daqueles que não estão autorizados a ver eles.

Modelo CID - Confidencialidade

- Password do nosso computador
- Registo bancário
- ?

Modelo CID - Integridade

A capacidade de impedir os nossos dados sejam alteradas numa forma não autorizada ou indesejável.

Modelo CID - Integridade

- Sistema de arquivos Windows que separa e protege o acesso aos arquivos de um usuário para outro
- ?

Modelo CID - Disponibilidade

A capacidade de acessar aos dados quando precisamos deles.

Modelo CID - Disponibilidade

- Sobrecarga mal intencionada nos servidores do nosso banco
- ?

Modelo Parkeriano -2002-

Confidencialidade	Disponibilidade	Integridade	Propriedade	Autenticidade	Utilidade

Modelo Parkeriano

- Propriedade - A disponibilidade física donde a informação tem sido guardada
- Autenticidade - A atribuição adequada quanto ao proprietário ou criador dos dados em questão
- Utilidade - Quão útil são os dados e suas características para nós

Ataques

- Os sistemas de informação podem enfrentar ataques desde uma grande variedade de abordagens e ângulos
- Os ataques podem ser classificados de acordo com o tipo de ataque que ele representa, o risco que o ataque representa, e os controles podemos usar para mitigar eles
- Cada ataque pode afetar um ou mais princípios CID

Ataques


Confidencialidade
Intercepção
Integridade
Interrupção
Modificação
Fabricação
Disponibilidade
Interrupção
Modificação
Fabricação

Ataques - Intercepção

- Permitem que usuários não autorizados acessem os nossos dados, aplicações, ou ambientes, e são principalmente um ataque contra a confidencialidade (chaves de acesso).
- Exemplos: Visualização ou copia de arquivos não autorizados, espionagem em conversas, ler e-mail
- Corretamente executados, ataques de interceptação podem ser muito difíceis de detectar.

Ataques - Interrupção

- Atacam ativos visando tornar eles inutilizáveis ou indisponíveis para uso, de forma temporária ou permanente.
- Exemplos: Ataques de denegação de serviço (disponibilidade), sobrecarga aos bancos de dados (disponibilidades+integridade),
- Modificação
- Fabricação

Ataques - Modificação

- São todos aqueles que mexem na informação.
- Exemplos: Acesso não autorizado a arquivos (integridade), acesso a arquivos de configuração de serviços (integridade+disponibilidade)

Ataques - Fabricação

- Geração de dados, processos, comunicações ou outras atividades similares com um sistema de
- Exemplo: Criação de informações falsas no banco de dados (integridade ou integridade+disponibilidade)
- São considerados maioritariamente como ataques na integridade, mas dependendo da quantidade dos dados podem ser também ataques de disponibilidade

Referencias I


Andress, J. (2011).
The basics of information security understanding the fundamentals of InfoSec in theory and practice.
Syngress, Waltham, MA.