Necessidades de Segurança

Docente: AA. Covele & S. Mavie.
Maputo, 2021

Menu

- Introdução
- Segurança para fins de Negócio
- Ameaças
  - Justificativa
  - Ameaças deliberadas
  - Ameaças naturais
- Resumo.

Introdução

- Um plano de segurança de informação é garantir que os sistemas e os seus conteúdos permaneçam os mesmos.
- As organizações gastam avultadas somas de dinheiro e horas de trabalho para manter os seus sistemas de informação.

Introdução

- Se não existissem ameaças às informações e sistemas, estes recursos poderiam ser utilizados para melhorar os sistemas que suportam a informação.
- No entanto, os ataques contra sistemas de informação são uma ocorrência diária, e a necessidade de segurança da informação cresce junto com a sofisticação de tais ataques.

Introdução

- As organizações devem compreender o ambiente em que operam os sistemas de informação para que seus planos de segurança da informação possam resolver os problemas reais e potenciais.

Finalidade da Segurança

A segurança da informação desempenha **quatro funções** importantes para uma organização:

1. **Proteger a funcionalidade de uma organização**

Ambos administração geral e gestão de TI são responsáveis pela implementação da segurança da informação que protege a capacidade da organização para funcionar.

Finalidade da Segurança

1. **Proteger a funcionalidade de uma organização**

A gestão de segurança da informação tem mais a ver com a política e sua aplicação do que com a tecnologia de sua implementação.

Finalidade da Segurança

2. Garantir uma operação segura das aplicações.

- As organizações de hoje estão sob imensa pressão para adquirirem e operarem com aplicações de forma integrada, eficiente e capaz.
- As organizações modernas precisam criar um ambiente que protege estas aplicações, particularmente aquelas que são mais importantes.

Finalidade da Segurança

3. Proteção de dados que a organização colecciona e usa.

- Sem dados, uma organização perde seu registo de transações e / ou sua capacidade de satisfação aos seus clientes.
- A proteção de dados em movimento e dados em repouso são os dois aspectos críticos de segurança da informação.

Finalidade da Segurança

3. Proteção de dados que a organização coleciona e usa.

- O valor dos dados motiva os atacantes para roubar, sabotarem, ou corrompê-los.
- Um plano de segurança da informação eficaz implementado pela administração protege a integridade e valor dos dados da organização.

Finalidade da Segurança

4. Salvaguardar os activos tecnológicos da organização.

Para ter desempenho efectivo, as organizações devem contratar serviços de infra-estrutura segura apropriadas para o tamanho e o escopo da empresa.

Em geral, como a rede de uma organização cresce para acomodar necessidades de mudança, soluções de tecnologia mais robustas devem substituir os programas vigentes de segurança da organização.

Ameaças

1.Introdução.

Para tomar decisões significativas sobre a segurança da informação, os gestores devem estar esclarecidos sobre as várias ameaças ao **pessoal** da organização, às **aplicações**, aos **dados** e aos **sistemas de informação**.

No contexto da segurança da informação, uma **ameaça é um objeto, pessoa ou outra entidade que representa um perigo permanente para um ativo.**

Ameaças

1. **Introdução.**

Existe um amplo consenso de que a ameaça de fontes externas aumenta quando uma organização se conecta à Internet. O número de utilizadores da Internet continua a crescer; cerca de 26% dos 6,8 bilhões de pessoas, correspondendo a 1,7 bilhões de pessoas do mundo, têm algum tipo de acesso à Internet.

Ameaças

1. **Introdução.**

- O CSI realizou um estudo em 2009 e descobriu que 64 por cento das organizações que responderam à pesquisa sofreram infecções de malware, com apenas 14 por cento indicando a penetração do sistema por um estranho.

Ameaças

1. **Introdução.**

- As organizações relataram perdas de aproximadamente US $ 234.244 por respondente, abaixo de um máximo histórico de mais de US $ 3 milhões em 2001

Ameaças

2. **Comprometimento da propriedade intelectual.**

- Muitas organizações criam, ou apoiam o desenvolvimento de propriedade intelectual (IP) como parte de suas operações de negócios.
- A propriedade intelectual é a propriedade de ideias e controlo sobre a representação tangível ou virtual dessas ideias.
- Utilização da propriedade intelectual de outra pessoa pode ou não envolver pagamentos de royalities, mas deve sempre incluir o devido crédito à fonte.

Ameaças

2. **Comprometimento da propriedade intelectual.**

- Uma apropriação de IP sem autorização constitui ameaça a segurança de informação.
- A ferramenta mais comum de combate é uma janela de contrato de licença que geralmente aparece durante a instalação do novo software, estabelece que o utilizador leu e concorda com o contrato de licença.

Ameaças

2. **Comprometimento da propriedade intelectual.**

- Outro esforço para combater a pirataria é o processo de registo online.
- Indivíduos que instalarem softwares muitas vezes são feitas ou mesmo obrigados a registar seu software para obter apoio técnico ou o uso de todos os recursos.

Ameaças

2-14.Tabela resumo e ficha

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk drive failure without proper backup and recovery plan organizational policy or planning in place
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies