Aula 3

Segurança em Sistemas de Informação

Prof. Douglas Eduardo Basso

1

Conversa Inicial

2

Conversa Inicial

- Nesta aula, vamos abordar temas relacionados às políticas de segurança da informação, seus elementos e definições, o tratamento de dados, vamos ver em detalhes a lei LGPD, abordaremos também a segurança de infraestrutura, sistemas e redes. O objetivo da aula é ter uma visão geral de como podemos montar uma boa política de segurança além dos elementos que fazem parte de toda a estrutura de segurança de informação de uma organização

3

Política de segurança da informação

4

Política de segurança da informação

- A política de segurança é um guia que apresenta e estabelece uma série de princípios, valores, requisitos, diretrizes, premissas, compromissos, orientações e responsabilidades sobre o que pode ser realizado para que seja possível alcançar um bom padrão de proteção das informações

5

- Existem três tipos de políticas de segurança:
  - Estratégia: faz a definição de todos os planos e diretrizes
  - Tática: faz a definição de toda a padronização (normas)
  - Operacional: faz a definição dos procedimentos de todos os processos

6

- Uma política de segurança eficiente é dividida em três camadas:

7

- Regulatória – política referente às necessidades legais impostas à empresa
- Consultiva – política opcional, isto é, não é obrigatória. Este tipo de política indica quais ações devem ser realizadas e como isso deve acontecer para que determinada atividade seja efetuava
- Informativa – especifica o que é desejado dos funcionários, porém, não descreve as consequências para o descumprimento das normas estabelecidas. Este tipo de política contém apenas informações adicionais

8

Elementos da política de segurança

- Alguns elementos devem fazer parte da PSI, entre eles podemos considerar:
- Utilização
- Integridade
- Disponibilidade
- Autenticidade
- Confidencialidade

9

Definições de política de segurança

- A norma ISO 17799 está subdivida em 12 pontos, enumerados a seguir:
- 1. Objetivo
- 2. Termos e definições
- 3. Política de segurança
- 4. Segurança organizacional
- 5. Classificação e controle dos ativos de informação

10

- 6. Segurança de recursos humanos
- 7. Segurança física e do ambiente
- 8. Gerenciamento das operações e comunicações
- 9. Controle de acessos
- 10. Desenvolvimento e manutenção de sistemas de informação
- 11. Gestão de continuidade de negócios
- 12. Conformidade

11

Tratamento de dados

- Depois de uma boa revisão da política de segurança é preciso inserir nesse documento uma área relacionada ao tratamento de dados pessoais. Esse tratamento de dados deve ser revisado e todos devem estar cientes, existe uma nova legislação que se aplica ao tratamento de dados

12

Lei Geral de Proteção de Dados

- No dia 14 de agosto de 2018, foi promulgada a Lei n. 13.709, intitulada Lei Geral de Proteção de Dados Pessoais (LGPD), que altera a Lei n. 12.965, de 23 de abril de 2014, o Marco Civil da Internet. Essa lei é dividida em dez capítulos

13

Segurança da infraestrutura

14

Segurança de infraestrutura

- A segurança da infraestrutura tem a responsabilidade de proteger todos os dados e informações armazenados em sistemas de informação, essa segurança não pode incluir apenas softwares, equipamentos de tecnologia, a segurança é algo muito mais complexo e deve ter uma abrangência bem maior, se faz necessário pensar na segurança física e lógica de todos os recursos presentes na organização

15

- Dentre os principais elementos que fazem parte e compõem uma infraestrutura de tecnologia, podemos elencar alguns:
- Computadores, notebooks, servidores de rede
- Sistemas operacionais (Windows, Linux, Android, MacOS, entre outros)
- Impressoras, copiadoras, scanners

16

- Softwares e aplicativos diversos
- Equipamentos de redes de computadores (*switches*, *firewalls*, roteadores)
- Servidores de internet (serviços na nuvem)
- Unidades de armazenamento (*storages*)
- Equipamentos multimídia (câmeras, microfones, videoconferência)
- Sistemas gerenciadores de banco de dados

17

Controles físicos

- Os controles físicos são uma série de medidas que devem ser aplicadas para respeitar a segurança, garantir que um produto não seja algo de roubo, furto, espionagem, sabotagem ou outro tipo de dano

18

- Dentre os controles físicos, podemos elencar os principais que devem ser levados em consideração:
  - Proteção e gerência dos equipamentos
  - Controles de acesso
  - Localização geográfica
  - Infraestrutura de *datacenter*

19

Controles lógicos

- Os controles lógicos estão relacionados à segurança de softwares, programas, aplicativos, banco de dados, servidores, computadores, sistemas de informação, redes de computadores e visa garantir o acesso autorizado aos recursos de tecnologia

20

- Dentre os controles lógicos, podemos elencar os principais que devem ser levados em consideração, esses temas serão vistos de maneira mais detalhada nas próximas aulas:
  - Controle de acesso
  - Combate a invasões e ataques
  - *Firewalls*
  - Filtros de conteúdos e aplicações

21

- Sistemas de detecção de intrusão
- Antivírus
- Criptografia
- Assinatura digital
- Certificado digital
- Rede privada virtual

22

Segurança de recursos humanos

- A maioria dos problemas de segurança da informação tem relação com colaboradores internos, podem ser causados de maneira acidental ou intencional por funcionários sem treinamento e formação adequada, falta de vivência ou experiência na função, negligência, ou até mesmo insatisfação com a organização

23

Segurança de redes

24

Segurança de redes

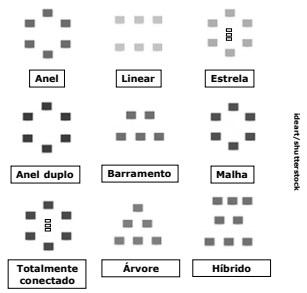
- As redes de computadores se multiplicaram e os sistemas operacionais estão ficando cada dia mais rápidos, mas, com todo esse crescimento, as mesmas redes e sistemas começaram a sofrer ataques e invasões. Informações armazenadas pelas organizações passaram a ser violadas e dados confidenciais, principalmente de clientes, foram expostos

25

Conceito de redes

- Uma rede consiste em dois ou mais computadores ligados entre si, esses computadores compartilham dados, entre outros recursos, como impressoras, servidores e a comunicação de modo geral

26



27

- Em relação aos meios de transmissão temos:
  - Redes de cabeamento coaxial
  - Redes de cabeamento de fibras ópticas
  - Redes de cabeamento de cobre com pares trançados
  - Redes sem fios que utilizam sinais infravermelhos, micro-ondas e rádio

28

Tipos de servidores

- Servidores de arquivos: armazenam e compartilham informações
- Servidores de impressão: fazem toda a gerência das filas de impressão e comunicação com impressoras
- Servidores de mensagens: fazem o gerenciamento das mensagens, e-mails, contatos, listas de distribuição e mensagens

29

- Servidores de aplicação: hospedam os sistemas e aplicativos das organizações, páginas web, entre outros
- Servidores de comunicação: fazem o controle de acesso, encaminham requisições, filtro de conteúdo, roteamento, entre outras funções

30

Controles de redes

- As redes atuam utilizando elementos de hardware e software, deve haver um alinhamento no gerenciamento ao acesso e no impedimento à instalação de diferentes ameaças na rede. São um conjunto de camadas de defesa interligadas desde a borda da rede para permitir acesso somente a usuários autorizados, e bloquear aqueles que têm potencial para executar ações indevidas, até as redes e dispositivos internos utilizados dentro da empresa

31

Serviços de redes

- A segurança de redes tem a responsabilidade de controlar a largura de banda, coordenar a instalação de aplicativos, evitar que dispositivos conectados por usuários causem algum dano à rede, fiscalizar os usuários dos sistemas, colocar em prática políticas de segurança

32

33

Segurança de software

- O software é parte fundamental da tecnologia da informação e de sistemas convencionais, tais como sistemas de transporte, militares, da área médica, financeiros, entre outros. Diversos estudos apontam que cerca de 90% das vulnerabilidades estão em software

34

Processos de desenvolvimento de software

- Os processos de desenvolvimento de software referem-se ao conjunto de atividades que cobre todo o ciclo que envolve desde a concepção de ideias até a descontinuação do software. Esse ciclo está estruturado em cinco processos fundamentais:

35

- Processo de aquisição
- Processo de fornecimento
- Processo de desenvolvimento
- Processo de operação
- Processo de manutenção

36

Princípios para segurança de software

- O conhecimento de alguns princípios e fundamentos básicos de segurança de softwares pode ajudar na implementação da segurança, entre esses princípios, podemos elencar alguns (esses temas serão discutidos em detalhes nas próximas aulas):

37

- Segurança por padrão
- Menor privilégio
- Defesa em profundidade
- Controles de acesso
- Proteção de dados sensíveis
- Garantias de integridade
- Tolerância a falhas
- Auditorias

38

Boas práticas no desenvolvimento de software

- Dentre algumas boas práticas relacionadas ao desenvolvimento de software, podemos destacar algumas:
  - Gerenciamento de código fonte
  - Realização de testes
  - Correção de erros
  - Integração contínua
  - Documentação do software
  - Padrões de códigos seguros

39

Segurança de dados

40

Banco de dados

- Um banco de dados é um conjunto de informações relacionadas entre si, armazenadas de maneira estruturada e, de preferência, com o mínimo de redundância possível

41

Ciclo de vida de dados

- Entender e documentar o ciclo de dados na sua empresa é vital para o desenvolvimento do processo de adequação. É acompanhar e entender tudo o que acontece com os dados desde a criação ou o recebimento até a sua exclusão. O ciclo de vida dos dados envolve a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação etc.

42

Ashalatha/shutterstock

43

Classificações e mapeamento de dados

- **A classificação e mapeamento de dados auxiliam na operação e manutenção das principais características da informação, algumas normas como a ISO 27002 recomendam que os dados de informações de uma organização sejam classificados e mapeados, seguindo alguns critérios:**

44

- **Confidencialidade**
- **Disponibilidade**
- **Integridade**
- **Autenticidade**
- **Outros fatores**

45

Segurança de dados

- **Uma das etapas mais difíceis e complexas da segurança de dados é fazer o mapa de onde estão todos os dados da organização, com o advento da internet, da computação em nuvem e da computação distribuída de maneira geral, fica praticamente impossível para os gestores de tecnologia fazer esse controle**

46

- **Existem alguns softwares que podem ajudar dentro desse cenário:**
  - **Na descoberta dos dados (*Data Discovery*), disponibilidade**
  - **Nos controles de prevenção de perda de dados (*Data Loss Prevention*)**
  - **Na classificação de dados (*Data Classification*)**

47

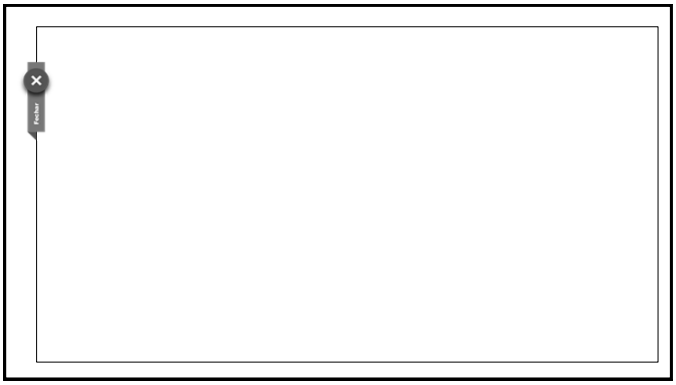
Recursos de segurança de dados

- **A segurança de informações armazenadas em banco de dados utiliza alguns recursos que podem ser utilizados para diminuir as probabilidades de ocorrência de incidentes de segurança:**

48

- **Acesso de administração**
- **Segurança local e física**
- **Blindagem de servidores**
- **Criptografia**
- **Auditoria e gerência de eventos**
- **Cópias de segurança**

49



50