Introdução à Segurança da Informação

Prof. Dr. José Augusto de Sena Quaresma

Jq.quaresma12@gmail.com

Boas práticas em Segurança da Informação

Introdução

- O que são boas práticas?

Boas práticas

- Nunca compartilhar senhas;
- Sempre utilizar antivírus e mantê-lo atualizado;
- Observar se os sites acessados são confiáveis;
- Nunca abrir links ou fazer download de arquivos enviados por e-mails não confiáveis ou de remetentes desconhecidos;
- Baixar programas apenas de fornecedores oficiais;
- Fazer backup de arquivos regularmente;
- Habilitar o firewall do sistema operacional;
- Manter o sistema sempre atualizado.

Gerenciamento de senhas – Política

- As senhas devem ter, pelo menos, oito caracteres.
- Deve-se alterar as senhas com frequência e nunca as repetir.
- Observar se houve algum tipo de vazamento de dados de determinados serviços. Caso tenha ocorrido, as credenciais de acesso aos sistemas, equipamentos e demais recursos devem ser modificadas para evitar que dados sejam obtidos por indivíduos mal-intencionados.
- Para aumentar a segurança das senhas, elas devem conter letras maiúsculas e minúsculas, números e caracteres não alfanuméricos (por exemplo: @, $, #). Ou seja, não se deve utilizar apenas letras ou números.

Gerenciamento de senhas – Política

- As senhas não devem conter nomes dos usuários e nem o nome da empresa em que trabalham ou qualquer variação desse tipo.
- Não utilizar a mesma senha para todas as contas, em especial nas contas institucionais, pois, caso alguém descubra uma das senhas do usuário, não conseguirá acessar todos os serviços em que ele possui cadastro.
- Nunca informar a senha a terceiros, nem as anotar em papel ou em arquivos digitais, ou inclui-las em um processo automático de acesso ao sistema. Senhas devem ser sempre memorizadas e de uso estritamente pessoal, de modo a nunca serem compartilhadas ou acessíveis a terceiros.

Gerenciamento de senhas – Validação

Senhas	Aceita ou Não aceita	Justificativa
K03Y0@	Não aceita	Essa senha não será aceita, pois as senhas devem ter pelo menis oito caracteres.
RTGE1598	Não aceita	Essa senha não será aceita, pois não se deve utilizar apenas letras ou números.
Kut@4896	Aceita	Essa senha será aceita, pois além de letras e números ela possui o caractere @.
Jose_6523	Não aceita	Essa senha não será aceita, pois contém o nome do usuário.

Treinamentos segurança – ISO IEC 27002

- Obrigatoriedade do envolvimento da diretoria
- Envolvimento de toda a organização
- Criação de conteúdos para treinamento e conscientização de segurança
- Diversidade de treinamento
- Exercício de simulação
- Periodicidade na realização do treinamento de conscientização

Mecanismos de proteção

- Organização
  - Referem-se às restrições de comportamento de seus membros e de possíveis atacantes por meio de mecanismos como portas, fechaduras, chaves e paredes.
- Usuário
  - A política de segurança aborda restrições de funções e de fluxo, entre elas, restrições de acesso por sistemas externos e adversários, incluindo programas e acesso a dados por pessoas.

Mecanismos de proteção – Princípios

- Economia de mecanismos
  - O projeto de sistema deve ser o mais simples e pequeno possível para que possa ser facilmente analisado, testado e validado.
- Padrões a prova de falha
  - O tipo de acesso que um usuário deve ter em um sistema deve ser feito com base na permissão e não na exclusão.
- Mediação completa
  - Todos os acesso a recursos devem ser verificados pelos mecanismos de segurança.
- Separação de privilégios
  - Deve ser identificado quem pode e deve executar determinadas funções no sistema.

Mecanismos de proteção – Princípios – 2

- Privilégio mínimo
  - Defini uma permissão associada a um usuário ou grupo de usuários
- Compartilhamento mínimo
  - Minimização de compartilhamento de recursos entre diferentes programas e pessoas
- Aceitação psicológica
  - A interface do sistema deve ser projetada para que os usuários apliquem rotinas de proteção.

Política contra vírus

- Vírus é um software malicioso carregado em um computador, sem que o proprietário saiba da sua existência ou funcionalidade.
- Dividido em vários grupos

Política contra vírus – Tipos

- Vírus de arquivo
  - Infecta o sistema anexando-se ao final de um arquivo e altera o início de um programa para controlar o código. Após a execução do código do vírus, o controle retorna ao programa principal. Sua execução nem é notada. Também é chamado de vírus parasitário, porque danifica os arquivos atacados.
- Vírus de boot
  - Atinge o setor de inicialização do sistema, sendo executado durante essa etapa, antes do carregamento do sistema operacional. Esse vírus infecta outras mídias inicializáveis, como discos rígidos.
- Vírus de macro
  - É acionado quando um programa executa macro. Por exemplo, esse tipo de vírus pode estar contido em arquivos de planilha.

Política contra vírus – Tipos 2

- Código-fonte vírus
  - Procura o código-fonte e o modifica para incluir vírus e ajudar a espalhá-lo.
- Mutante
  - Vírus programado para dificultar a detecção por antivírus, pois se altera a cada execução do arquivo contaminado.
- Polimorfico
  - É uma variação do vírus mutante que tenta dificultar a ação do antivírus ao mudar sua estrutura interna ou suas técnicas de codificação
- Cavalo de Troia (trojan)
  - Trata-se de programas aparentemente inofensivos que trazem embutidos em si outro programa malicioso

Política contra vírus – Tipos 3

- Multipartite
  - Esse tipo de vírus é capaz de infectar várias partes de um sistema, incluindo o setor de inicialização, memória e arquivos. Isso dificulta a sua detecção e contenção.
- Stealth
  - É um vírus muito complicado, pois altera o código usado para detectá-lo. Portanto, a sua detecção se torna muito difícil. Por exemplo, ele pode alterar a chamada do sistema de leitura para, sempre que o usuário solicite a leitura de um código modificado por vírus, a forma do original do código ser mostrada em vez do código infectado..

Política contra vírus – Tipos 4

- Encapsulamento
  - Esse vírus tenta ignorar a detecção pelo antivírus, instalando-se na cadeia do manipulador de interrupções. Os programas de interceptação, que permanecem no fundo de um sistema operacional e capturam vírus, ficam desabilitados durante o curso de um vírus de encapsulamento. Vírus semelhantes instalam-se nos drivers de dispositivo.
- Criptografado
  - Usado para evitar a detecção por antivírus. Esse tipo de vírus existe na forma criptografada e carrega consigo um algoritmo de descriptografia. Assim, o vírus primeiro descriptografa e depois executa.

Política contra vírus – Tipos 5

- Blindado
  - É codificado para dificultar a identificação e o entendimento do antivírus. Usa uma variedade de técnicas para fazer isso, como enganar o antivírus e fazê-lo acreditar que o arquivo malicioso está em outro lugar que não seja a sua localização real. Também pode usar a compactação para complicar seu código.

Política contra vírus – Passo a passo

1

Todos os computadores conectados à rede de uma instituição devem ter um **antivírus padrão instalado**, programado para ser executado em intervalos regulares. Além disso, o software antivírus e os arquivos de definição de vírus devem ser sempre atualizados.

2

Todos os computadores devem ser configurados de forma a agendar **atualizações regulares** dos servidores antivírus centralizados dos serviços de rede.

3

Todos os arquivos de dados e programas que foram transmitidos eletronicamente para um computador de outro local, interno ou externo, devem ser **verificados** quanto à existência de vírus imediatamente após o recebimento.

4

Todos os dispositivos de armazenamento, como, por exemplo, pendrives e HDs externos, são uma fonte potencial de vírus de computador. Portanto, eles devem ser **verificados** quanto à infecção por vírus antes de usá-los em um computador ou servidor da rede.

Sistemas de Backup

- É a criação de cópias redundantes de informações. Os sistemas de backups são utilizados como cópia de segurança de arquivos e dados.
- Importante para recuperação dos dados
- Necessário ser feito testes com os backups
- Manutenção periódica dos backups

Sistemas de Backup – Tipos

- Completo
  - Faz cópias de todos dados, inclusive dos logs de transações associadas para outro conjunto de mídia, como, por exemplo, disco rígido, DVDs, CDs, pendrives.
- Incremental
  - Grava somente arquivos alterados desde o último backup, por isso é mais rápido que o backup completo e ocupa menos espaço. O último backup pode ser completo, diferencial ou incremental. No início, é feito um backup completo e nos subsequentes são copiados apenas os dados que foram alterados ou criados desde o último backup.
- Diferencial
  - É a cópia dos dados criados e modificados desde o último backup. Após realizar o primeiro backup completo, cada backup diferencial compara o conteúdo a ser copiado com o do último backup completo e copia todas as alterações realizadas. Esse tipo de backup também é chamado de backup incremental cumulativo.

Sistemas de Backup – Tipos

- Completo
  - Faz cópias de todos dados, inclusive dos logs de transações associadas para outro conjunto de mídia, como, por exemplo, disco rígido, DVDs, CDs, pendrives.
- Incremental
  - Grava somente arquivos alterados desde o último backup, por isso é mais rápido que o backup completo e ocupa menos espaço. O último backup pode ser completo, diferencial ou incremental. No início, é feito um backup completo e nos subsequentes são copiados apenas os dados que foram alterados ou criados desde o último backup.
- Diferencial
  - É a cópia dos dados criados e modificados desde o último backup. Após realizar o primeiro backup completo, cada backup diferencial compara o conteúdo a ser copiado com o do último backup completo e copia todas as alterações realizadas. Esse tipo de backup também é chamado de backup incremental cumulativo.

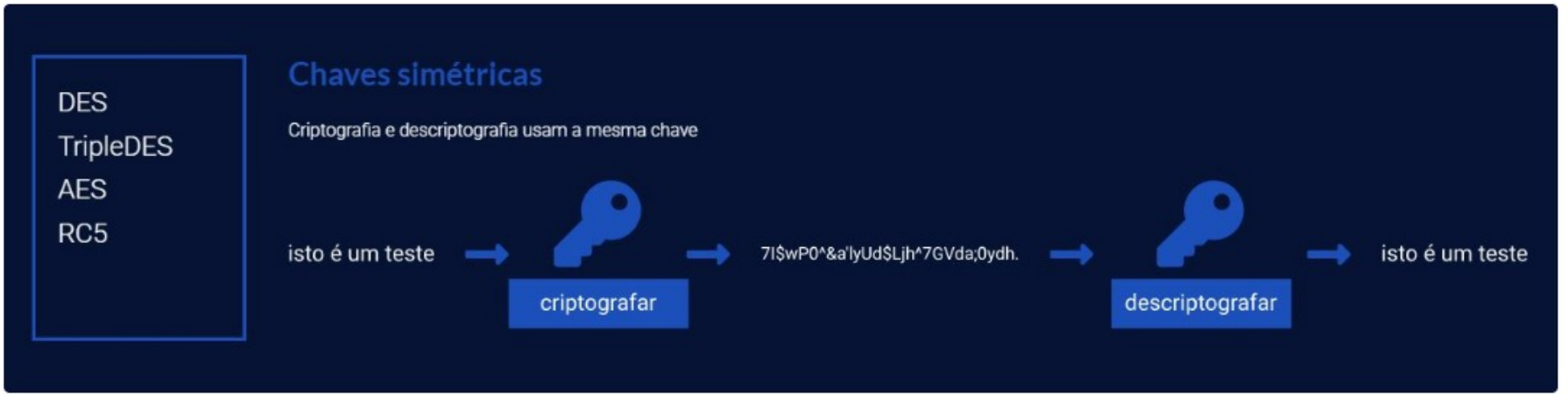
Criptografia

- Criptografia consiste no ato de codificar dados para que apenas pessoas autorizadas consigam ter acesso às informações.
- Segundo Stallings (2008), a criptografia das informações pode ser classificada em três tipos:
- Chave simétrica
- Função Hash
- Chave Assimétrica

Criptografia – Chave simétrica

- Conhecida por criptografia de chave privada ou secreta. Aqui, o receptor da informação e o remetente usam uma única chave para criptografar e descriptografar a mensagem. O tipo frequente de criptografia usada nesse método é AES (Advanced Encryption System). Alguns exemplos de tipos de criptografia de chave simétrica são: Block, Block cipher, DES (Data Encryption System), RC2, IDEA, Blowfish e Stream cipher

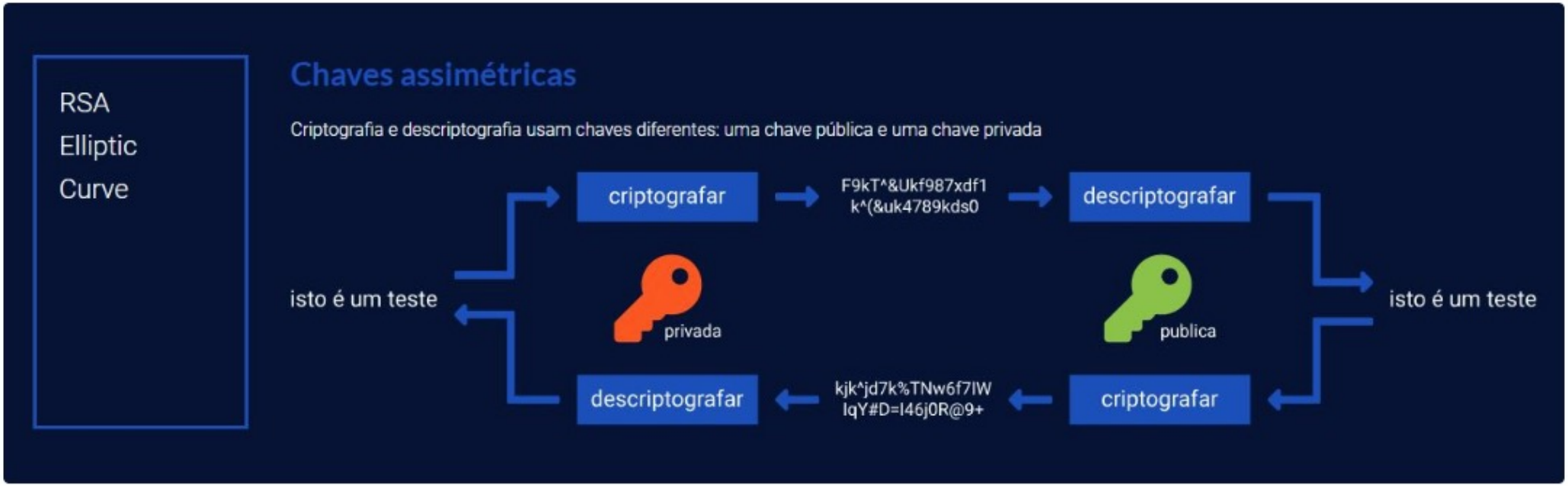
Criptografia – Chave simétrica



Criptografia – Chave assimétrica

- Denominada como criptografia de chave pública. Usando duas chaves, o remetente e o destinatário seguem os processos de criptografia e descriptografia. Uma chave privada é armazenada com cada pessoa e a chave pública é compartilhada na rede para que uma mensagem possa ser transmitida através de chaves públicas. O algoritmo mais comum de criptografia usado nesse método é o RSA. O método da chave pública é mais seguro do que o da chave privada. Alguns tipos de criptografia de chave assimétrica são: RSA, DAS, PKCs e técnicas de curva elíptica.

Criptografia – Chave assimétrica



Criptografia – Função hash

- Usa uma função matemática para criptografar irreversivelmente as informações, fornecendo uma impressão digital delas. Esse tipo de criptografia é usada, principalmente, para garantir a integridade da mensagem. Alguns exemplos de algoritmos de hash são: Message Digest 5 (MD5), RIPEMD, Whirlpool e SHA (Secure Hash Algorithm).

Criptografia – Função hash

Criptografia

Chave simétrica	Chave assimétrica	Função hash
Usa **chave única** para criptografar e descriptografar a mensagem.	Usa um **par de chaves**, em que uma chave é usada para criptografia e outra para descriptografia.	**Não requer nenhuma chave** para criptografia e descriptografia.
É **mais rápida**, porém é **menos confiável** em termos de **segurança**.	É **menos rápida**, porém é **mais confiável** em termos de **segurança**.	É **menos rápida**, porém é **mais confiável** em termos de **segurança**.
Foi introduzida para executar rapidamente os **processos criptográficos**.	Foi introduzida para **superar o problema da troca de chaves** na chave simétrica.	Foi introduzida para fornecer **mais segurança**.
Se por algum motivo a chave estiver comprometida/violada na rede, **haverá perda tanto do remetente como do receptor**.	Há **perda** apenas do **proprietário**.	Não há chave para comprometer.
É menos **complexa**.	É **mais complexa**.	Possui **média complexidade**.

Sérgio Assunção Monteiro.

Atividade

- O que são boas práticas de segurança da informação?
- Descreva uma política de segurança de senha.
- Com base na política de segurança de senha vista em sala de aula descreva 7 senhas aderentes e 7 não aderentes
- Quais as recomendações para treinamento da ISO IEC 27002?
- Identifique e defina os tipos de vírus repassados em sala de aula
- Defina um sistema de backup e seus tipos
- O que é criptografia?
- Quais os tipos de criptografia?