GESTÃO DE SEGURANÇA DA INFORMAÇÃO

ESTRATÉGIAS DE PROTEÇÃO

Olá!

Nesta aula, você irá:

Conhecer as principais estratégias de proteção aplicadas nas organizações através da implementação de:

1. Proteção em camadas.

2. do estudo das melhores práticas:

•Cuidados com senhas.

•Educação dos usuários.

•Controle de acesso.

•Uso eficaz de antivirus e antispywares.

•Backups (cópia de segurança).

•Plano de continuidade de negócios.

•Criptografia e certificação digital.

Segundo (Guimarães, Oliveira & Lins) é necessário que se compreenda que nenhum componente único poderá garantir um sistema de segurança adequado para uma rede corporativa e que possa defendê-la com perfeição contra ataques. Existem várias estratégias de proteção que podem ser utilizadas. Uma destas estratégias é a implementação de um modelo de proteção em camadas. Este modelo tem como objetivo dificultar invasões que comprometam a integridade, a autenticidade e o sigilo das informações que trafegam em uma rede IP, definindo componentes com base nas necessidades específicas de cada empresa.

Segundo Northcutt, podemos pensar na segurança de rede como uma cebola. Quando descascamos a camada mais externa, muitas camadas permanecem por baixo.

Este modelo, também conhecido como Defesa em profundidade (Defense in Depth), refere-se à aplicação de defesas distintas, de controles complementares para no caso de uma falha ou violação de um ativo, existam outros controles e não torne o sistema como um todo vulnerável e restrito a somente um único controle.

Para que possamos implementar o modelo de defesa em profundidade torna-se necessário a segmentação inteligente dos ativos da organização de forma que seja possível a aplicação de controles adequados. É preciso estabelecer o perímetro de segurança. Segundo Sêmola, a teoria do perímetro esta associado a compartimentalização de espaços físicos e lógicos e ao papel de alerta e mecanismos de resistência distribuído por áreas, a fim de permitir que tentativas de acesso indevido e invasão gerem sinais de alerta e encontrem

resistências que propiciará tempo para que as medidas contingenciais sejam tomadas antes da ação avançar ainda mais em direção do alvo.

Perímetro de segurança e seus componentes

Cada rede que compões a topologia da organização precisa ser classificada em um dos três tipos de redes:

Redes Confiáveis

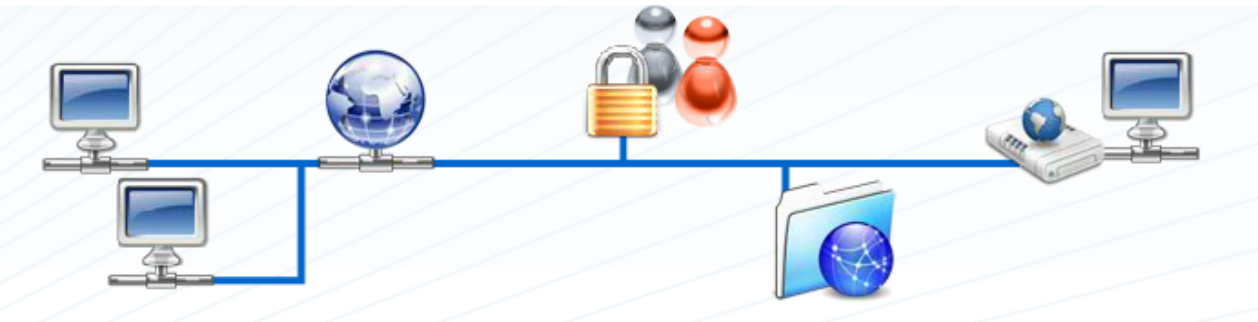
Localizadas no perímetro de segurança da rede, portanto necessitam de proteção

Redes Não Confiáveis

Estão fora do perímetro de segurança, possuem portanto não controle da administração ou das políticas de segurança.

Redes Desconhecidas

São as redes desconhecidas, pois não é possível informar, de modo explícito, se a rede é confiável ou não confiável



As redes corporativas podem conter vários perímetros dentro de um perímetro de segurança. É necessário que a organização estabeleça as redes que serão protegidas, defina o conjunto de perímetros de rede e os mecanismos que exercerão a proteção de cada perímetro. Em geral, são encontrados dois tipos de perímetros de rede:

Perímetro exterior

Representa o ponto de separação entre os recursos que estão sob controle e os recursos que não estão sob controle.

Perímetro interior

Recurso particular que se pretende proteger.

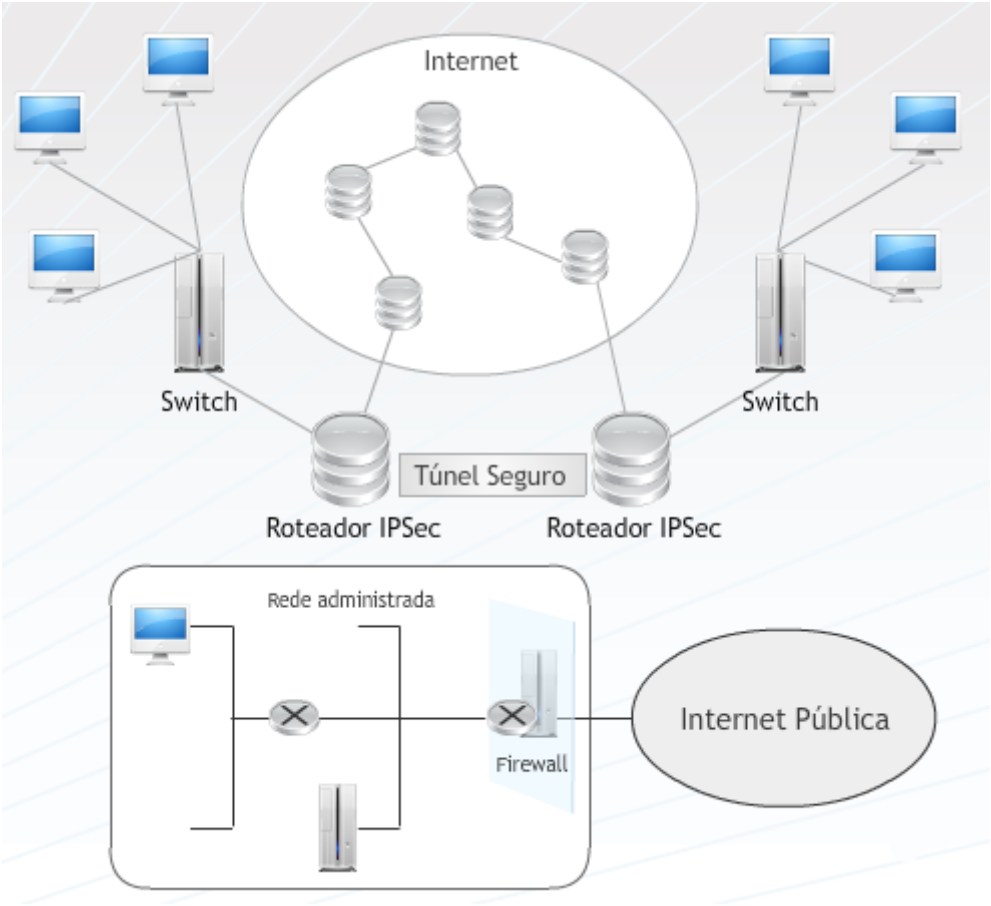
Roteador de borda

É o roteador do perímetro exterior, ou seja, é o último roteador que se pode controlar antes da rede não-confiável. Em uma corporação que acessa a Internet, todo o tráfego de rede que possui origem ou destino à internet passa por este roteador. Funciona como a primeira e última linha de defesa de uma rede através da filtragem de pacotes iniciais e final.

Firewall

Isola a rede interna da organização da área pública da Internet, permitindo que alguns pacotes passem e outros não, prevenindo:

- Ataques de negação de serviço:
- Modificações e acessos ilegais aos dados internos
- Permite apenas acesso autorizado à rede interna



Os firewall podem ser divididos em:

Filtros de Pacotes: A filtragem de pacotes é um dos principais mecanismos que, mediante regras definidas pelo administrador, permite ou não a passagem de datagramas IP em uma rede. Podem ser implentados pelos roteadores ou através de software de firewall como por exemplo, o Iptables, presente nas distribuições Linux.

Se observamos sob o ponto de vista da proteção em camadas, a utilização de filtros de pacotes é a primeira camada de fora para dentro e a última de dentro para fora.

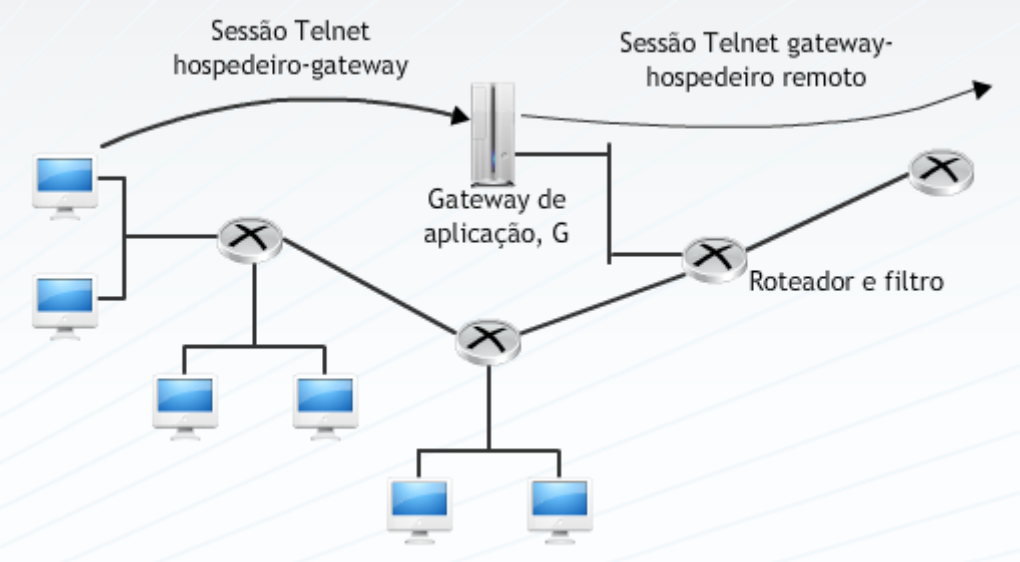
Como funciona?

A rede interna é conectada à Internet através de um roteador com firewall implementado (filtro de pacotes). O roteador filtra os pacotes e a decisão de enviar ou descartar os pacotes baseia-se em:

- Endereço IP de origem, endereço IP de destino
- Número de portas TCP/UDP de origem e de destino
- Tipo de mensagem ICMP
- Bits TCP SYN e ACK

Firewall com estado: Monitoram as conexões em uma tabela de estado, na qual armazena o seu banco de regras, bloqueando todo o tráfego que não esteja em sua tabela de conexões estabelecidas. Este banco de regras determina o IP e a porta de origem e de destino que são permitidos para estabelecer conexões.

Firewall Proxy: Permite executar a conexão ou não a serviços em uma rede modo indireto. Possui todas as características e funcionalidades de um firewall com estado, porém impede que os hosts internos e externos se comuniquem diretamente.



Sistema de Detector de Intrusos (IDS)

Tem como principal objetivo reconhecer um comportamento ou uma ação intrusiva, através da análise das informações disponíveis em um sistema de computação ou rede. Caso detecte alguma anomalia suspeita ou ilegal, gera uma notificação para alertar o administrador da rede e / ou automaticamente disparar contra-medidas. Para realizar a detecção várias tecnologias podem ser utilizadas: análise estatística, inferência, inteligência artificial, data mining, redes neurais e diversas outras. Podem ser classificados em relação a:

Sua forma de monitoração (origem dos dados)

Sensores de host (Host Based IDS -HIDS)

São instalados em servidores para alertar e identificar ataques e tentativas de acesso indevido à própria máquina, Observam as ações realizadas no sistema operacional, ações dos serviços e o comportamneto da pilha TCP/IP, protegendo apenas o sistema host em que reside. É empregado no caso em que a segurança está focada em informações contidas em um servidor;

Sensores de rede (Network Based IDS- NIDS)

São instalados em máquinas responsáveis por identificar ataques direcionados a toda a rede, monitorando o conteúdo dos pacotes de rede e seus detalhes como informações de cabeçalhos e protocolos. Observam o tráfgo da rede, o formato do pacote de todos os pacotes que trafegam na rede.

Quanto aos mecanismos (algoritmos) de detecção utilizados

Quanto à Origem dos Dados

Existem basicamente dois tipos de implementação de ferramentas IDS:

Detecção por assinatura

Os dados coletados são comparados com uma base de registros de ataques conhecidos (assinaturas). Por exemplo, o sistema pode vasculhar os pacotes de rede procurando seqüências de bytes que caracterizem um ataque de buffer overflow contra o servidor WWW Apache;

Detecção por anomalia

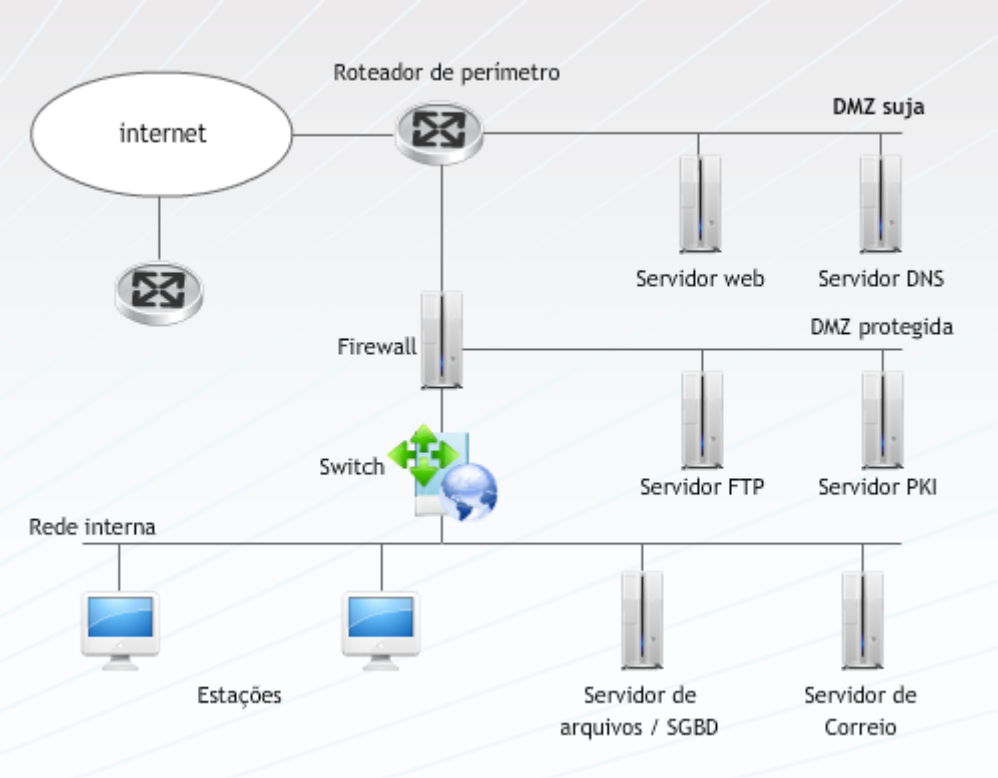
Os dados coletados são comparados com registros históricos da atividade considerada normal do sistema. Desvios da normalidade são sinalizados como ameaças.

Detecção hibrida

O mecanismo de análise combina as duas abordagens anteriores, buscando detectar ataques conhecidos e comportamentos anormais.

Zona Desmilitarizada (DMZ)

São pequenas redes que geralmente contém serviços públicos que são conectados diretamente ao firewall ou a outro dispositivo de filtragem e que recebem a proteção deste dispositivo. Muitos autores apresentam o conceito de DMZ suja e DMZ protegida ou também conhecida por screened subnets. Em uma DMZ suja os servidores estariam conectados diretamente na interface do roteador sem a proteção do firewall enquanto que uma DMZ protegida ou screened subnets está protegida por um firewall ou outro dispositivo de filtragem, hospedando normalmente serviços públicos, como DNS e correio eletrônico por exemplo.



Cuidados com senhas

Segundo a cartilha de sergurança para internet, produzida pelo CERT, a senha utilizada pelos usuários tanto para acessar a Internet quanto aos sistemas computacionais da organização é utilizada no processo de verificação da identidade do usuário, assegurando que este é realmente quem diz ser, ou seja, é utilizada no processo de autenticação. Caso uma outra pessoa tem acesso a senha de algum usuário da rede poderá utilizá-la para se passar por alguém da empresa.

Portanto, é muito importante a conscientização de todos os usuários da organização quanto a utilização e proteção das senhas, pois é de responsabilidade de cada usuário da organização.

Saiba mais

Clique aqui para ver mais informações sobre este assunto

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/10GSI_doc01.pdf

Educação dos usuários

Para que a implementação da política de segurança seja efetiva deve ser claramente comunicada às pessoas de uma organização. Segundo a norma ISO/IEC 27001 no item que trata sobre Conscientização, educação e treinamento em segurança da informação:

A organização deve assegurar que os usuários e demais envolvidos no SGSI estejam cientes das ameaças e das preocupações de segurança da informação e equipados para apoiar a aplicação da política de segurança da organização durante a execução normal do seu trabalho.

Devem ser treinados nos procedimentos de segurança e no uso correto das instalações de processamento da informação, de forma a minimizar possíveis riscos de segurança.

Saiba mais

Clique aqui para ver mais informações sobre este assunto

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/10GSI_doc02.pdf

A comunicação é outro ponto importante a ser observardo na elaboração de uma campanha de conscientização. A comunicação acontece quando duas pessoas têm o mesmo interesse ou os interesses são comuns e consequentemente a mensagem flui.

Pode ser ser classificada como:

Comunicação não-verbal: simbólica e sonora

Comunicação oral: código que expressam sensações e sentimentos

Comunicação escrita: Representação gráfica como os desenhos e escrita propriamente dita

O que é um programa de conscientização de segurança em TI ?

É um conjunto de atividades e materiais associados, planejados para promover e manter uma situação em uma organização onde os funcionários tenham um alto nível de consciência sobre segurança

Um programa de conscientização de segurança é portanto um processo contínuo que visa mudar o modo como pessoas pensam e agem. Um bem sucedido programa de conscientização de segurança de TI deve mudar o modo como o usuário de sistema pensa e age, de forma que a segurança de TI torne-se parte das atividades de negócios da empresa.

Principais itens tratados por um programa de conscientização de segurança:

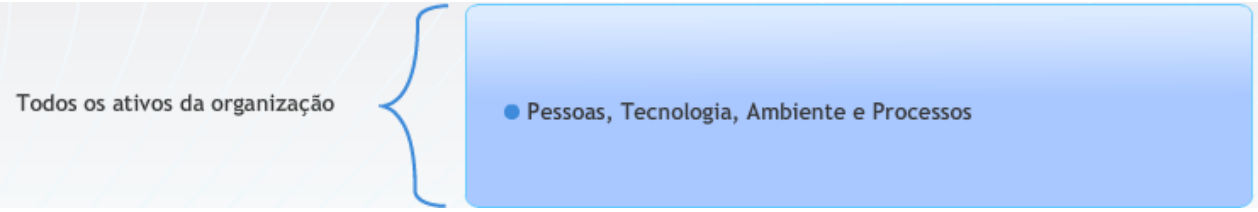
- O quê significa segurança da informação para a organização
- Que as informações guardadas nos computadores são um recurso importante e valioso
- Como aplicar as ações de segurança em seu ambiente de trabalho
- Que os funcionários também são responsáveis pela segurança da informação
- A política de segurança, padronização dos sistemas e princípios da empresa

Fique ligado

Um programa de conscientização pode variar de organização para organização ou até mesmo de negócio para negócio. A organização é considerada tendo um ambiente de segurança positivo quando os funcionários agem instintivamente e são pró-ativos de um modo que promova boas práticas de segurança de TI.

Controle de acessos

O que deve ser controlado em uma organização?



E por que devemos controlar?

Para limitar os impactos causados os ativos de informação.

Para reduzir as vulnerabilidades.

Saiba mais

Clique aqui para ver mais informações sobre este assunto

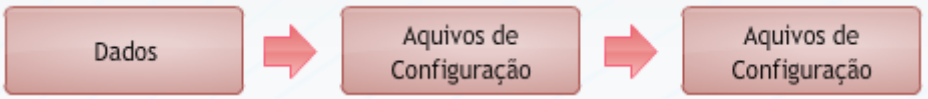
http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/10GSI_doc03.pdf

Backups (cópia de segurança)

Os Backups ou cópias de seguranças são itens muitos importantes na administração de sistemas devendo fazer parte da rotina de operação dos sistemas da organização, através de uma política pré-determinada.

Sempre que possível devem ser realizados da mais automatizada possível, de modo a reduzir o impacto sobre o trabalho dos administradores e operadores de sistemas.

Devem fazer parte da lista de itens de backup:



Você sabia?

Sem as cópias de segurança (Backup), muitos dados seriam simplesmente irrecuperáveis caso fossem perdidos devido a uma falha acidental ou a uma invasão

Alguns cuidados devem ser tomados em relação ao local onde são guardados os backups:

- O acesso ao local deve ser restrito, para evitar que pessoas não autorizadas roubem ou destruam os backups;
- O local deve ser protegido contra agentes nocivos naturais (poeira, calor, umidade);
- Se possível, é aconselhável que o local seja também `a prova de fogo.

Você sabia?

Sem as cópias de segurança (Backup), muitos dados seriam simplesmente irrecuperáveis caso fossem perdidos devido a uma falha acidental ou a uma invasão

Tome nota

- Os backups devem ser verificados logo após a sua geração e, posteriormente, em intervalos regulares. Isto possibilita a descoberta de defeitos em dispositivos e meios de armazenamento e pode evitar que dados sejam perdidos por problemas com backups que não podem ser restaurados.
- Algumas organizações providenciam meios para armazenar backups fora das suas instalações, como em cofres de bancos, por exemplo. Essa é uma boa maneira de garantir a disponibilidade dos backups em caso de problemas nas instalações . Entretanto, isso pode comprometer a confidencialidade e integridade desses backups.

Plano de continuidade de negócios

Tem como objetivo garantir a continuidade de processo e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos do desastre, conforme já estudado na aula 9.

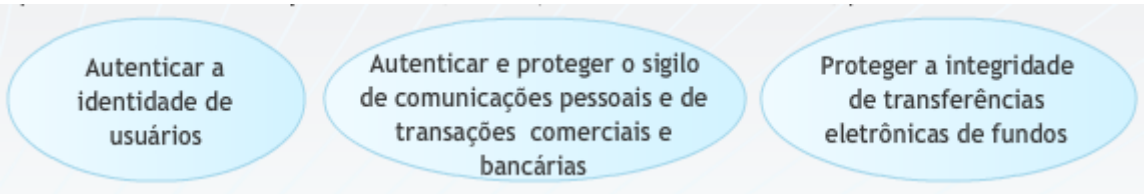
Seja qual for o objeto da contigência – uma aplicação, um processo de negócio, um ambiente físico e, até mesmo uma equipe de funcionários, a emrpesa deverá selecionar a estratégia de contingência que melhor conduza o objeto a operar sob um nível de risco controlado.

Estratégias de Contigência

Warm-site	Aplicada a objetos que aceitam urna maior tolerância a falhas que na hot-site, podendo se sujeitar a indisponibilidade por mais tempo, até o retorno operacional da atividade
Realocação de operação	Deslocamento da atividade atingida pelo evento que provocou a quebra de segurança para outro ambiente físico, equipamento ou link, pertencentes a mesma empresa. Esta estratégia somente é possível se existir recursos sobressalentes ou com "folga" para serem alocados em situação de crise.
Bureau serviço	Considera a possibilidade de transferir a operacionalização da atividade atingida para um ambiente terceirizado fora do ambiente da empresa.Por requerer um tempo maior de tolerância para sua reativação operacional está restrita a algumas poucas situações. O fato das informações serem manipuladas por terceiros e em ambiente fora do controle da organização, requer atenção na adoção de procedimentos, critérios e mecanismos de controle que garantam as condições de segurança adequadas À relevância e criticidade da atividade cintingenciada.
Acordo de reciprocidade	Acordo formal com empresas que possuem características físicas, tecnológicas ou humanas semelhantes e que estejam também dispostas a possuir um alternativa de continuidade operacional.Estabelecem em conjunto as situações de contingências e definem os procedimentos de compartilhamento de recursos para alocar a atividade na outra empresa. Desta forma ambas obtêm redundância.
Cold-site	Propõe uma alternativa de contigência a partir de um ambiente com os recursos mínimos de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto aplicado em ambientes com tolerância ainda maior de indisponibilidade.
Hot-site	Propõe uma alternativa de contigência a partir de um ambiente com os recursos mínimos de infra-estrutura e telecomunicações, desprovido de recursos de processamento de dados. Portanto aplicado em ambientes com tolerância ainda maior de indisponibilidade

Criptografia

A eficiência e eficácia dos serviços de segurança em ambientes de redes, como a privacidade, autencidade, integridade, não repúdio e controle de acesso, está diretamente relaciona às técnicas de criptografia utilizadas. A criptografia é a ciência e arte de escrever mensagens em forma cifrada ou em código. È parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para:



Como funciona a criptografia?

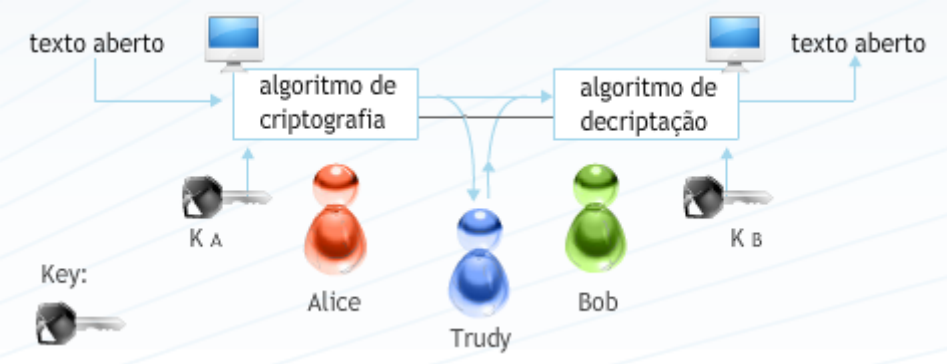
Podemos descrever o processo de criptografia como:

O emissor no caso Alice, gera uma mensagem original chamada de texto simples ou texto puro. Para enviar a mensagem alice utiliza uma chave e um algoritmo de cifragem e gera um texto cifrado que é transmitido para um receptor. Ao chegar ao receptor, no caso BOB, este texto passa pelo processo inverso, chamado de decifragem, resultando no texto simples original. A mensagem deverá ser incompreensível para quem não tem autorização para lê-la, no caso Trudy, pois não possui a chave para decifrar a mensagem a emissão.

Saiba mais

Clique aqui

http://estaciodocente.webaula.com.br/cursos/gsgisi/docs/10GSI_doc04.pdf



Classificação dos sistemas de criptografia

A criptografia pode ser genericamente classificada em três diferentes dimensões:

Quanto aos tipos de cifras utilizadas

Todos os algoritmos de cifragem são baseados em dois tipos de categorias de operações:

Tipos de operações utilizadas na transformação do texto simples para o cifrado

Cifras de substituição

Cada elemento do texto simples (bit, letra, grupo de bits ou letras) é substituído por um outro elemento correspondente, sendo sempre o mesmo elemento

Cifras de Transposição

Os elementos do texto simples são reordenados(embaralhados).

Classificação **quanto à simetria das chaves utilizadas**

A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens. Os métodos criptográficos são subdivididos em duas categorias, de acordo com o tipo de chave utilizada:

A criptografia simétrica ou de chave única, quando o emissor e receptor utilizam a mesma chave;

A criptografia assimétrica ou de chave pública, quando o emissor e receptor utilizam chaves diferentes.

Quanto à simetria das chaves utilizadas

A chave é uma sequência de caracteres, que pode conter letras, dígitos e símbolos (como uma senha), e que é convertida em um número, utilizado pelos métodos de criptografia para codificar e decodificar mensagens. Os métodos criptográficos são subdivididos em duas categorias, de acordo com o tipo de chave utilizada:

Modo Electronic Code Book (ECO)

O texto simples é dividido em blocos de 64 ou 128 bits.

Modo de Encadeamento de blocos de Cifra

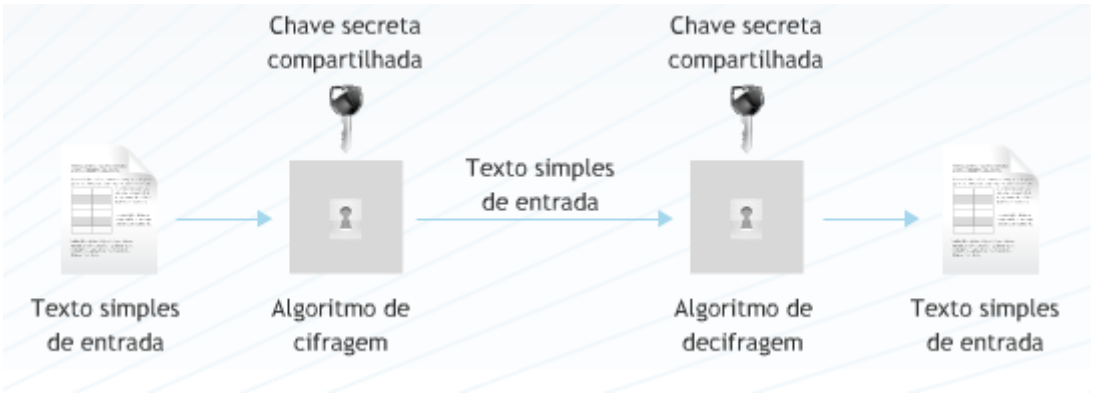
Muito semelhante ao modo ECB, porém, o bloco de texto simples é submetido a uma operação xOR com o bloco de texto cifrado anterior antes de ser codificado.

Modo de feedback de Cifra

É semelhante ao modo de bloco de cifra, porém, realiza a cifragem byte a byte.

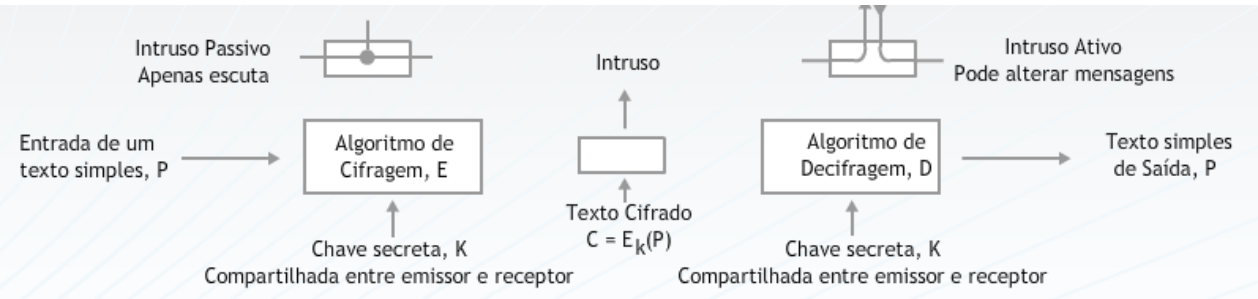
Modo de Cifra de Fluxo

Neste modo o texto simples é submetido a uma operação XOR com uma sequência de blocos chamada de fluxo de chaves.



Criptografia de chave simétrica ou privada

A criptografia de chave única utiliza a mesma chave tanto para a codificar quanto para decodificar mensagens sendo conhecida por ambos os lados do processo. Apesar deste método ser bastante eficiente em relação ao tempo de processamento, ou seja, o tempo gasto para codificar e decodificar mensagens, tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas.



Algoritmos simétricos e tamanhos de chave:

- Data Encryption Standard(DES) – 64 bits
- Triple Data Encrypption Standard(3DES) – utiliza duas chaves de 64 bits;
- Advanced Encryption Standard(AES) – 128 bits ate 256 bits.
- International Data Encryption Algorithm (IDEA) – 448 bits.
- Twofish – 128, 192, 256 bits.

- Serpent – 128,192 ou 256 bits.

Criptografia de Chave Assimétrica ou pública

Os algoritmos assimétricos utilizam-se de duas chaves diferentes, uma em cada extremidade do processo. As duas chaves são associadas através de um relacionamento matemático, pertencendo a apenas um participante, que as utilizará para se comunicar com todos os outros de modo seguro.

Essas duas chaves são geradas de tal maneira que a partir de uma delas não é possível calcular a outra a um custo computacional viável, possibilitando a divulgação de uma delas, denominada chave pública, sem colocar em risco o segredo da outra, denominada chave secreta ou privada Uma das chaves será utilizada para codificar e outra para decodificar mensagens. Neste método cada pessoa ou entidade mantém duas chaves:

Uma pública, que pode ser divulgada livremente

Uma privada, que deve ser mantida em segredo pelo seu dono.

Como funciona?

Alice e Bob desejam trocar mensagens secretas. Que passos devem executar?

1)A chave pública de Alice e o seu algoritmo de cifragem (EA) tornam-se públicos, assim como os de BOB(EB) .

2)Tanto Alice quanto BOB mantêm suas chaves secretas, DA e DB respectivamente.

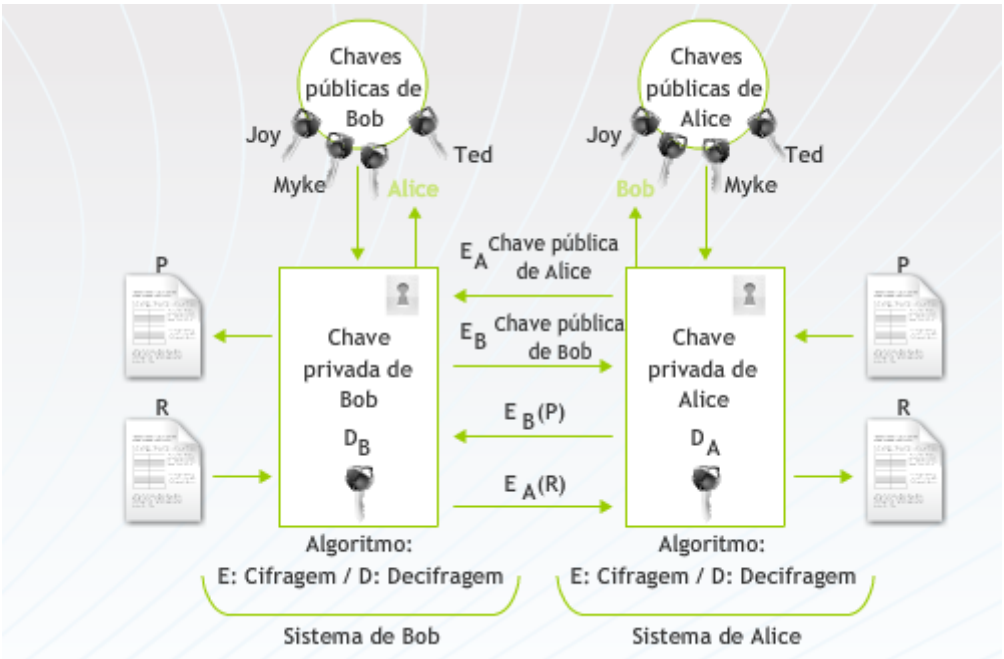
3)Alice então gera e envia uma mensagem (P) para BOB, utilizando a chave pública de BOB (EB(P)).

4)Bob descriptografa a mensagem enviada por Alice com a sua chave secreta (DB);

5) caso BOB deseje responder a Alice, deverá utilizar a chave pública de Alice EA) para criptografar a mensagem.

Um exemplo de algoritmo assimétrico e tamanho de chave:

Rivest, Shamir e Adlerman(RSA) – 512, 768, 1024 ou 2048 bits.



Você sabia?

Se o emissor utilizara chave privada para cifrar uma mensagem no lugar da chave pública, qualquer pessoa poderá cifrá-la, uma vez que a pública é de conhecimento de todos, o que garantirá apenas a autenticidade da mensagem.

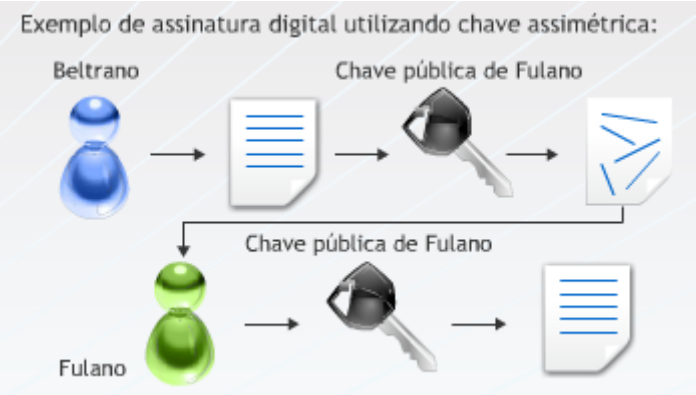
Assinatura digital

A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada. Assinatura digital tenta resolver o problema de autencidade de documentos digitais. Tem como objetivos garantir:

Que o receptor da mensagem possa verificar e certificar a identidade alegada pelo transmissor

Que o transmissor não possa repudiar o conteúdo da mensagem, portegendo o receptor da mensagem

Que o receptor não possa forjar ele mesmo a mensagem. Esta característica pode proteger o transmissor de possíveis tentativas de fraudes



Você sabia?

A assinatura digital faz uso da criptografia assimétrica, utilizando um par de chaves, uma privada e outra pública. A chave privada serve para assinar o documento, enquanto que a pública serve para verificar a assinatura. Porém pode-se utilizar a chave simétrica também.

Na assinatura digital com chave simétrica existe uma autoridade central na qual todas as entidades confiam e que possue o conhecimentos de todas as chaves secretas dessas entidades. Somente a entidade comunicante e a entidade centralizadora conhecem a chave secreta

Certificação Digital

O certificado digital é um arquivo assinado eletronicamente por um entidade confiável chamada Autoridade Certificadora (CA). Um certificado tem como objetivo um dos objetivos associar a chave pública a uma pessoa física ou jurídica, servindo como um mecanismo para a divulgação da chave pública. A autoridade Certifcadora verifica a identidade do sujeito e emite o certificado digital.

Os certificados digitais não são secretos ou protegidos, qualquer entidade que conheça a chave pública da CA pode examinar o conteúdo e confirmar a autenticidade de um certificado emitido por essa Autoridade, uma vez quea CA assina os certificados com a sua chave pública. Informações presentes nos certificados:

- Chave pública do usuário;
- Número de série do certificado;
- Nome da CA que emitiu o certificado;
- A assinatura digital da CA;
- O período de vaidade do certificado;

O ICP, ou Infra-estrutura de Chaves Públicas, é a sigla no Brasil para PKI - Public Key Infrastructure -, um conjunto de técnicas, práticas e procedimentos elaborado para suportar um sistema criptográfico com base em certificados digitais.

Foi criado em julho de 2001, pelo Comitê Gestor da ICP-Brasil responsável por estabelece a política, os critérios e as normas para licenciamento de Autoridades Certificadoras (AC), Autoridades de Registro (AR) e demais prestadores de serviços de suporte em todos os níveis da cadeia de certificação, credenciando as respectivas empresas na emissão de certificados no meio digital brasileiro. Para saber mais sobre o ICP Brasil, sua legislação, como obter um certificado e quais os já emitidos, consulte o site: http://www.gov.br/twiki/bin/iview/Main/WebHome

Você sabia?

O padrão mais utilizado para a produção de certificados digitais é o X.509, formulado pelo International Telecommunication Union, Telecounication Standardization Sector (ITU-T).

CONCLUSÃO

Nesta aula, você:

- Conheceu as principais estratégias de proteção aplicadas nas organizações.
- Compreendemos como se dá a implementação da proteção em camadas e
- Conhecemos as melhores práticas implementadas pelas organizações através do estudo de: Cuidados com senhas; Educação dos usuários; Controle de acesso; Uso eficaz de antivirus e antispyware; Backups (cópia de segurança); Plano de continuidade de negócios; Criptografia e certificação digital.