TI.exames Com êxito

EDUCAÇÃO E TREINAMENTO
PARA ALAVANCAR A SUA CARREIRA

Fundamentos da Segurança da Informação com base na ISO/IEC 27002

Curso e-learning completo

Preparatório para o exame EXIN ISO 27002 Foundation

Módulo 6

Medidas técnicas

Este módulo cobre:

- Gestão de acesso lógico
- Requisitos de segurança para sistemas da informação
- Criptografia, política de criptografia, tipos de sistemas de criptografia
- Segurança de arquivos de sistemas
- Vazamento de informações

Slide 2

Medidas técnicas

Uma análise de risco sugere medidas físicas, técnicas e organizacionais. Muitas das medidas físicas também incluem aspectos técnicos. Neste módulo nós vamos tratar das medidas apenas de natureza técnica. Vamos examinar a segurança da infra-estrutura de TI e a proteção de dados contra acesso indesejado por meio de controle de acesso e criptografia.

Sistemas de informação não são necessariamente computadorizados, mas nos tempos atuais há um crescimento exponencial neste sentido. Por isso neste módulo vamos tratar de medidas de segurança técnicas que podem ser tomadas na área de TI.

Gestão de acesso lógico

A gestão de acesso lógico é utilizada para permitir acesso à informação digital e a serviços de informação por pessoas autorizadas e impedir o acesso das que não são autorizadas. O dono dos dados (usualmente o gerente) é quem autoriza o acesso. Essa autorização pode ser automática ou liberada por meio de uma aplicação ou sistema pelo gerente.

Controle de acesso discricionário (DAC)

Neste caso a decisão de conceder acesso à informação permanece com um usuário individual. Um exemplo é você dar acesso ao seu diretório pessoal para outra pessoa. Outro exemplo é enviar informação para pessoas que não tem acesso a ela. Esse sistema é uma forma flexível de controle de acesso, mas é difícil de auditar e controlar.

Slide 3

Medidas técnicas
Gestão de acesso lógico

Controle de acesso mandatório (MAC)

Neste caso o controle de acesso é centralizado, definindo quais pessoas e sistemas têm acesso a quais sistemas de informação.

Concessão de acesso

Na concessão de acesso fazemos distinção entre as palavras identificação, autenticação e autorização. Identificação é o primeiro passo na concessão de acesso. Na identificação a pessoa ou sistema apresenta um token (uma chave, por exemplo), nome de usuário ou senha. O sistema então determina se o token é autêntico e para que recurso o acesso pode ser concedido. Quando a autenticidade é determinada a autorização pode ser concedida.

Guardas de segurança em pontos de acesso

Em adição ao controle de acesso é importante monitorar quem tem acesso para o quê, e se esta autorização está sendo ultrapassada ou não. Um exemplo são as áreas de um aeroporto onde é necessário garantir que as pessoas não tenham acesso a áreas não autorizadas. Essa guarda de acesso em certas áreas pode ocorrer por várias razões, como para reduzir riscos ou por razões regulamentares. Isso mostra que concessão de acesso não é apenas uma questão técnica, mas também é uma questão organizacional.

Slide 4

Requisitos de segurança para sistemas da informação

Desde o momento que uma empresa considera comprar e desenvolver sistemas da informação é necessário que a segurança faça parte do projeto.

Sistemas da informação compreendem sistemas operacionais, infraestrutura, processos operacionais, produtos de prateleira, serviços e aplicações que devem ser desenvolvidos para os usuários. O projeto e implementação de sistemas da informação que suportam processos operacionais podem ser um fator decisivo no estabelecimento da segurança.

Requisitos de segurança necessitam ser agrupados e documentados antes de um sistema da informação ser desenvolvido e/ou implementado.

Quando requisitos de segurança são documentados durante a análise de risco e especificação de requisitos para o projeto, eles são justificados, agrupados e documentados como parte do estudo do negócio para um sistema da informação.

É consideravelmente mais barato implementar e manter medidas de segurança durante a fase do projeto do que durante ou depois da implementação.

Quando um produto é adquirido, um teste formal e um processo de compras devem ser seguidos. O contrato com o fornecedor deve estabelecer os requisitos de segurança a que o produto deve atender. Se a funcionalidade do produto em termos de segurança não atinge os requisitos, então o risco resultante e as medidas de segurança associadas devem ser reconsiderados, tanto quanto a decisão de comprar ou não o produto.

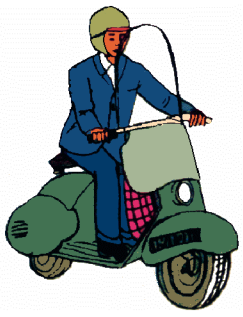
Slide 5

Processamento correto das aplicações

Aplicações (softwares, programas de computados) devem funcionar como pretendido. Um programa que causa erros e permite que dados sejam perdidos é um grande risco, pois pessoas sem autorização podem mudar ou misturar informações.

Sistemas de aplicações e aplicações que foram desenvolvidas para os usuários devem incorporar as medidas cabíveis de gestão. Tais medidas de gestão compreendem a validação dos dados de entrada, do processamento interno e dos dados de saída. Isso é importante para que se possa verificar se os dados são corretos.

De forma a simplificar os dados de entrada, listas de terminologia são definidas. Estas listas, que são construídas dentro de softwares e bases de dados, podem prevenir o uso de mais de uma palavra para o mesmo termo. Exemplo: um policial observa um acidente e registra no sistema: *pedestre na calçada foi atingido por uma motocicleta*. No dia seguinte outro policial observa um acidente na mesma localização e registra: *uma pessoa na rua foi atingida por uma scooter*. Se a base de dados for examinada posteriormente para um estudo de perigos no trânsito, este estudo fica difícil de ser realizado. O sistema deve forçar o usuário a usar uma palavra específica.

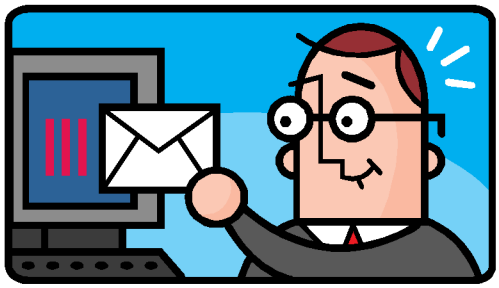


Slide 6

Validação dos dados de entrada e de saída

Dados que entram nas aplicações devem ser validados de forma a garantir sua acuracidade (ou exatidão). Transações de negócio e dados definidos podem ser automaticamente verificados. Considere, por exemplo, um campo de entrada para um código postal, o qual tem um formato pré-determinado. Pode-se utilizar o mesmo sistema para preços, limites de crédito, taxas de câmbio, etc.

Validação é uma ferramenta importante para proteger contra erros realizados por usuários.



Criptografia

O termo criptografia vem da Grécia e é uma combinação da palavra “kryptós”, que significa escondido, com “gráfo” que significa escrita. Exemplos de criptografia são tão antigos quanto Roma. A criptografia era utilizada pelos romanos para enviar mensagens militares. Mesmo que a mensagem caísse nas mãos de inimigos, eles não seriam capazes de entender o conteúdo. Pesquisas sobre algoritmos para criptografia não foram realizadas apenas para desenvolver algoritmos, a fim de criptografar mensagens: foram realizadas também para quebrar o algoritmo de mensagens enviadas pelos inimigos. A análise de criptografia se desenvolveu muito durante a segunda guerra mundial.

Política da criptografia

Criptografia é uma medida que uma organização pode tomar no caso de necessidade, como por exemplo com informação confidencial. O uso de criptografia deve ser cuidadosamente considerado e definido em uma política documentada.

Este documento deve conter o seguinte:

- → O que a organização usa para criptografar
- → Que tipo de criptografia a organização usa e em quais aplicações
- → Chaves de gestão e controle
- → Backup
- → Controle

Criptografia
Gestão de chaves

A gestão de chaves é uma parte importante da política de uso de técnicas de criptografia. Chaves de criptografia devem ser protegidas contra alteração, perda ou destruição.

Chaves pessoais e secretas devem ser protegidas de divulgação não autorizada. Equipamentos usados para geração, armazenamento e arquivamento de chaves devem ser fisicamente protegidos. Parte da gestão de chaves é o registro de pares de chave: qual par foi emitido, para quem e quando, até quando a chave será válida e o que deve ser feito se a chave for comprometida.

É um grande risco usar a mesma chave em vários equipamentos dentro da organização. Se estas chaves se tornam conhecidas fora da organização então o equipamento (usualmente notebooks) terá que ter novas chaves. Esta operação deve ser muito rápida e certamente vai custar caro.

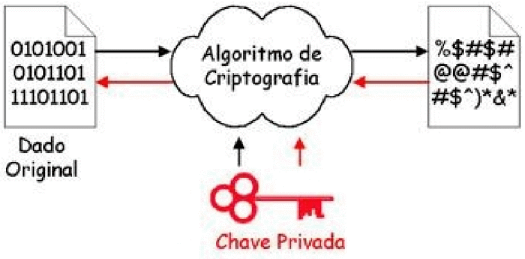
Tipos de sistemas de criptografia

De forma a se ter um sistema de criptografia, tanto o remetente quanto o recebedor devem ter o algoritmo. A característica de um bom sistema de criptografia é que o algoritmo em si é público. Existem 3 formas de algoritmos de criptografia: simétricos, assimétricos e criptografia de mão única.

Simétricos

A característica deste sistema está em um algoritmo e em uma chave que o remetente compartilha com recebedor. Na prática:

Se x=+5 então “A” torna-se “F”. Cada pessoa que conhecer a chave será capaz de decodificar as mensagens usando -5 ao longo do alfabeto. A força do sistema está na capacidade de ambos, remetente e recebedor, manterem segredo da chave secreta.



Fonte: Ilustração retirada do site da USP

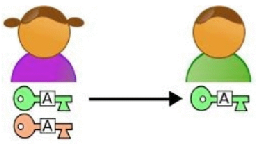
Tipos de sistemas de criptografia

Assimétricos

A criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. A chave pública é distribuída livremente para todos os correspondentes via e-mail ou outras formas, enquanto a chave privada deve ser conhecida apenas pelo seu dono.

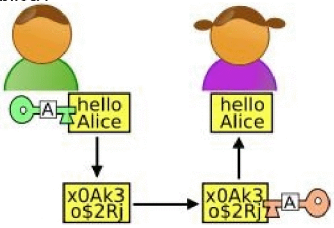
Num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente.

Os algoritmos de chave pública podem ser utilizados para autenticidade e confidencialidade. Para confidencialidade, a chave pública é usada para cifrar mensagens, com isso apenas o dono da chave privada pode decifrá-la. Para autenticidade, a chave privada é usada para cifrar mensagens, com isso garante-se que apenas o dono da chave privada poderia ter cifrado a mensagem que foi decifrada com a 'chave pública'.



Passo 1: Alice envia sua chave pública para Bob
A chave verde representa a chave pública, a chave rosa representa a chave privada.

Fonte: Wikipedia



Passo 2: Bob cifra a mensagem com a chave pública de Alice e envia para Alice, que recebe e decifra o texto utilizando sua chave privada

Slide 11

Assinatura digital

Assinaturas digitais são criadas para uso da criptografia assimétrica. A assinatura digital é um método para confirmar se a informação digital que foi produzida e enviada veio de alguém que é quem diz ser, e pode ser comparada com a assinatura em papel. Uma assinatura digital geralmente consiste de dois algoritmos: um que confirma que a informação não foi alterada por outras partes e outra que confirma a identidade da pessoa que assinou a informação.

Na Europa a assinatura digital equivale à assinatura em papel e a sua autenticidade pode ser confirmada por meio de um certificado digital elaborado por meios seguros.

Slide 12

Infraestrutura da chave pública (Public Key Infrastructure – PKI)

Criptografia assimétrica também é conhecida como criptografia por chave pública. Não é uma infraestrutura de chave pública pois em relação a esta infraestrutura muito mais está envolvido. A característica da infraestrutura de chave pública está em acordos, procedimentos e estrutura organizacional: isso provê garantias em relação a quais pessoas ou sistemas pertencem a uma chave pública específica. A infraestrutura de chave pública é normalmente gerenciada por uma autoridade independente. A Vecozo é uma organização holandesa que tem este papel: ela garante a troca de informações confidenciais na área de prestação de serviços médicos.

Exemplo: um médico deseja fazer uma declaração sobre o tratamento de uma paciente para a empresa de seguro, que tem um contrato com uma autoridade de certificação (CA – Certification Autority). O médico solicita o certificado para a CA, que é responsável por confirmar se o médico é quem afirma ser (requisitando seus diplomas e assinatura, por exemplo). É dado acesso ao médico para entrar no website e fazer upload de seus diplomas. Se o médico quer fazer uma declaração, quando ele entra no website, o certificado em seu computador é verificado e o nome de usuário e senha relacionados ao certificado são solicitados. Após a confirmação de autenticidade é permitido acesso para que ele entre com os arquivos de suas declarações, e estas são assinadas como sendo originalmente dele. O médico também pode verificar se um determinado paciente é beneficiário de determinada assistência médica.

Criptografia de mão única (One way encryption)

Esta forma de criptografia é também chamada de função por partes e pode ser comparada a uma mistura de tintas porque depois que duas cores são misturadas, elas formam uma outra cor e não podem mais ser separadas.

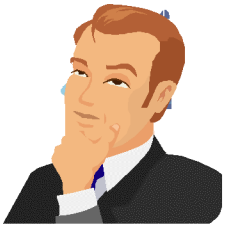
Esse tipo de algoritmo é usado principalmente para determinar se determinada data foi alterada: a mensagem é convertida em um valor numérico, e usando um algoritmo o recebedor pode verificar se a mensagem tem uma parte correta do valor. Se as duas partes combinam, a mensagem pode ser recuperada. Partes também podem ser usadas para confirmar que duas mensagens (passwords, por exemplo) são as mesmas.

Quando um password é estabelecido, o sistema faz uma divisão e armazena uma parte – não armazena o password completa. Desta forma, uma pessoa que tenha um alto nível de acesso não pode ver o password completa de determinada pessoa. Mais tarde, quando a pessoa apresenta o password para autenticação, o sistema pega uma parte dela e compara com a parte que está armazenada. Se as partes combinam, a pessoa deve ter entrado com o password correta. Esta técnica é usada para checar a integridade das mensagens, mas não garante confidencialidade.

Segurança de arquivos de sistema

Gestão de acesso para códigos-fonte de programas

Arquivos de sistema ficam no coração do sistema de informática de uma organização. Se o código-fonte destes arquivos cai nas mãos de alguém com intenções maliciosas, é possível para esta pessoa obter acesso a informações confidenciais. Estes arquivos devem ser tratados, portanto, com o máximo cuidado. Acesso a código-fonte de um programa deve ser restrito a quem realmente precisa acessá-lo.



Segurança de dados de teste

É importante que equipamentos e programas de dados de teste sejam cuidadosamente escolhidos, protegidos e mantidos. Dados reais que possam conter informações sensíveis não devem ser utilizados para teste. Testes de sistema devem usar apenas dados fictícios.

Segurança em desenvolvimento e em processos de suporte

Gestores responsáveis por aplicativos são responsáveis por segurança no ambiente de projeto no qual as aplicações são desenvolvidas, e, por segurança, no ambiente no qual as aplicações rodam. Eles também devem determinar se mudanças propostas põe esta segurança em perigo.

Vazamento de informações

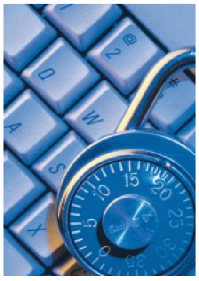
É possível que uma informação vaze por diversos canais de informação não oficiais de uma organização. Canais secretos de informação são canais que não têm a intenção de processar a informação mas que podem existir nas redes de relacionamento. É possível que o fornecedor de um programa customizado deixe um acesso secreto de forma a realizar manutenções na aplicação sem informar o comprador de tal fato. Quando uma aplicação customizada é usada para processar informações altamente confidenciais, uma empresa independente pode inspecionar o código-fonte da aplicação para garantir que tais canais não existam.

Desenvolvimento de programa por terceiros

É importante que programas desenvolvidos por terceiros sejam supervisionados e controlados pela organização. Quem fica como dono do código fonte? Se possível o cliente deve ter os direitos autorais. A qualidade e a precisão do trabalho que está sendo realizado podem ser determinadas por certificação de uma terceira parte.

Estudo de caso

Um banco de tamanho médio tem planos de expandir seu ambiente de TI. Foi decidido que a TI precisa que seus equipamentos sejam atualizados. Está se pensando em alugar os equipamentos e utilizar um fornecedor que tenha uma boa estrutura de suporte. O programa atual utilizado não está adequado e eles pretendem desenvolver um novo programa. Esse desenvolvimento será terceirizado.



É importante que o novo sistema garanta que somente informações corretas sejam dados de entrada, e as entradas devem ter vários controles dependendo do montante envolvido: se for grande deve ser checado por mais de uma pessoa.

Pergunta-se:

Você deve estabelecer um estudo sobre segurança para a nova rede que será adquirida. Como você faria a autorização de acesso?

Resposta do estudo de caso

Possível resposta

1) A gestão de acesso deverá ser feita pelo gerente de TI por meio de uma aplicação no sistema. O controle deverá ser centralizado e o gerente vai definir que função tem acesso a que informação/aplicativo/sistema. O acesso deverá já estar definido para cada descrição de cargo.
2) Na concessão de acesso teremos um processo abrangendo identificação, autenticação e autorização. O usuário entra com login e senha para acessar o sistema, e para aplicações sensíveis deve entrar com um token que e o sistema deve determinar se é autêntico.
3) Os códigos-fonte de programas serão criptografados e o acesso a esses códigos só será permitido de maneira controlada aos profissionais que atuam no desenvolvimento de software. Os direitos autorais dos códigos-fonte devem ser de propriedade da organização.
4) O aplicativo para gestão de acesso será desenvolvido por uma empresa terceirizada e um profissional interno vai ser responsável por supervisionar e controlar o projeto.