Boas práticas em segurança da informação

Apresentação das boas práticas em segurança da informação, suas principais características e formas de implementação, além dos seus impactos no ambiente profissional.

Prof.º Sérgio Assunção Monteiro

Propósito

Compreender o que são boas práticas em segurança da informação e a importância de sua aplicação no cotidiano organizacional.

Objetivos

- Reconhecer as boas práticas em segurança da informação referentes ao gerenciamento de senhas, treinamento e mecanismos de proteção.
- Identificar os recursos protegidos pelos sistemas de controle de acesso e os aspectos relacionados à política de vírus e ao gerenciamento de backups.
- Identificar os tipos de criptografia de dados e os itens presentes em um certificado digital.

Introdução

Veja as notícias a seguir:

Em um ataque, ex-funcionária da Amazon comprometeu dados de 100 milhões de pessoas
Em julho de 2019, o banco de dados do CapitalOne, instituição financeira americana, foi hackeado. Os dados de mais de 100 milhões de norte-americanos e 6 milhões de canadenses foram afetados. Segundo o banco, uma ex-funcionária da Amazon acessou os dados de pessoas que entraram com pedido de cartão de crédito entre 2005 e 2019 (Época Negócios).

Hackers sequestram dados de cidades americanas
Diversos municípios dos Estados Unidos foram vítimas de ataques de ransomware em 2019. O maior deles foi Baltimore, que teve todo o sistema de informática da cidade travado. Funcionários públicos ficaram sem e-mail, o pagamento a servidores públicos foi adiado e a compra e venda de imóveis na cidade foi paralisada (Época Negócios).

Prosegur fecha site no Brasil por 24 horas após ransomware
A Prosegur, empresa espanhola de segurança e transporte de dinheiro, foi atingida pelo malware RYUK, que trancou todos os seus arquivos no mundo (Época Negócios).

É provável que você já tenha se deparado com notícias como essas, que mostram ataques de hackers a instituições, expondo dados e informações sigilosas. Todas elas estão relacionadas a um fator primordial nos dias atuais, que é tão imerso em redes de internet, dados em nuvem, aplicativos, redes socais etc. Estamos falando da **Segurança da Informação**, que pode ser entendida como: um conjunto de medidas que visa garantir a confidencialidade, a integridade e a disponibilidade das informações de uma organização ou de um usuário.

Não basta às empresas investirem em segurança da informação, é primordial que os usuários que possuem acesso aos diferentes sistemas de uma empresa tenham atitudes que contribuam para evitar o acesso de dados indevidamente. Vamos conhecer as boas práticas em segurança da informação que uma empresa deve implementar no seu cotidiano.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Vamos começar!

A importância das boas práticas em segurança da informação

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Primeiros passos

Vamos refletir sobre algumas situações do dia a dia?

Pense nos seguintes cenários:

1. Você está se organizando para sair de férias em seu trabalho e realiza todas as tarefas necessárias de modo que nada fique pendente. No entanto, você sabe que poderão ocorrer imprevistos e sua equipe pode precisar de informações que estão disponíveis apenas no seu computador.

2. Você recebeu um e-mail de um remetente desconhecido com um anexo executável.

3. Você precisa realizar uma compra. Pesquisa na internet as lojas que vendem o produto e em quais estão os melhores preços.

4. Um colega de trabalho pediu para abrir em seu computador um arquivo que estava no pendrive dele.

5. Você precisa baixar um programa no computador do trabalho.

Diante dessas situações, o que você faz?

Observe, a seguir, as ações que ajudam a garantir a segurança da informação:

- 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

> **Conteúdo interativo**
>
> Acesse a versão digital para assistir ao vídeo.

O ponto de partida de qualquer sistema de segurança é garantir o acesso a dados, equipamentos, demais sistemas e ambientes físicos e eletrônicos aos indivíduos autorizados. A essa característica dá-se o nome de **autenticidade** e a forma mais simples de oferecê-la é por meio do login e da senha de acesso.

Deve-se dar atenção particular à senha, mais especificamente ao **gerenciamento das senhas**, visto que, com o login e a senha, um usuário pode ter acesso a equipamentos, sistemas e demais recursos de uma companhia, como, por exemplo, instituições de ensino, comerciais, governamentais ou religiosas.

Além da óbvia preocupação de garantir segredo sobre a senha, também é necessário preocupar-se com o grau de dificuldade ao elaborá-la. Senhas fáceis – como datas de aniversários de familiares ou placas de carro – são alvo de pessoas mal-intencionadas, já existindo muitos ataques a senhas baseados na exploração de informações pessoais. As senhas com sequências do tipo “123” também devem ser evitadas. De acordo com Shay *et al.* (2010), para criar uma senha segura é recomendável que os colaboradores observem as seguintes instruções:

> **Shay**
>
> Richard Shay é o pesquisador principal do Laboratório Lincoln no programa HECTOR, que tem como objetivo construir aplicativos seguros utilizando técnicas avançadas de criptografia. Laboratório Lincoln – Instituto de Tecnologia de Massachusetts.

- 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.
- 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.

Diante dessas recomendações, vamos a um exemplo prático:

Imagine que você trabalhe no setor de Tecnologia da Informação (TI) de uma empresa e, juntamente com os demais funcionários, definiu os critérios para a criação das senhas de acesso aos sistemas com base nas instruções vistas anteriormente. De acordo com essas instruções, observe no quadro a seguir as senhas que não serão válidas e inválidas e os respectivos esclarecimentos:

Senhas	Aceita ou Não aceita	Justificativa
K03Y0@	Não aceita	Essa senha não será aceita, pois as senhas devem ter pelo menos 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.

Senhas aceitas e não aceitas de acordo com as recomendações de segurança da informação.

As recomendações que vimos são muito importantes para garantir que as **senhas** realmente atuem como um **mecanismo de segurança** para acesso dos indivíduos aos sistemas. Trata-se de recomendações simples que demandam disciplina e conscientização de todos os envolvidos no processo: tanto os responsáveis pelas políticas de criação e controle das senhas quanto os usuários que as utilizam para acessar os sistemas.

Treinamento

Não importa o quão abrangentes sejam as defesas de segurança de uma organização e nem quanto foi investido em produtos de segurança eletrônica, essas defesas podem ser quebradas com um único e-mail de phishing. Você pode estar se perguntando:

1

O que é phishing?

É um tipo de fraude, que se dá por meios eletrônicos, utilizada por indivíduos mal-intencionados.

É aplicada, principalmente, para roubar senhas de banco e outras informações pessoais, causando prejuízos materiais e morais, uma vez que os criminosos podem fazer compras e saques se passando pela vítima.

2Como ocorre?

Pode ocorrer por meio de websites ou e-mails falsos, muito parecidos com os de uma empresa com imagem consolidada no mercado de modo a atrair as vítimas.

Os sites ou e-mails com phishing oferecem promoções para o usuário muito atrativas como: “Parabéns, você ganhou nossa promoção especial desse mês! Para receber seu prêmio, basta clicar no link e fornecer o que é solicitado.”

Ou, ainda, solicitam que façam uma atualização dos dados bancários para evitar o cancelamento da conta, por exemplo.

Perceba que, se um e-mail contendo um ataque de phishing chegar a um usuário que não possua um entendimento básico de segurança e ele responder à mensagem, um **malware** poderá ser instalado, ou o invasor poderá, ainda, acessar a rede por meio da análise do endereço de IP do usuário, causando um dano ainda maior para outros usuários.

Malware

É a abreviação de "software malicioso" (em inglês) e se refere a um tipo de programa de computador desenvolvido para infectar o computador de um usuário legítimo e prejudicá-lo de diversas formas.Kaspersky

Atenção

O risco desse tipo de ataque levou muitas organizações a desenvolverem um programa de conscientização sobre segurança. Ao ensinar a todos os colaboradores as melhores práticas de segurança cibernética – da diretoria aos funcionários –, a postura de segurança pode ser bastante aprimorada e a vulnerabilidade a ataques de phishing e outros ataques cibernéticos pode ser bem reduzida.

No entanto, simplesmente fornecer aos funcionários uma sessão de treinamento quando eles ingressam na empresa não é suficiente, tampouco tentar disseminar a segurança cibernética com apenas uma sessão anual de reciclagem. Não se espera que os funcionários mantenham o conhecimento por um longo período, a menos que sejam fornecidas sessões frequentes de atualização. Além disso, os cibercriminosos estão constantemente desenvolvendo novas estratégias para enganar os usuários. Os **programas de treinamento** devem estar contextualizados com o intuito de refletir a **realidade dos tipos de ataques**.

A **ISO/IEC 27002 - Código de Prática para a Gestão de Segurança da Informação**, norma da **Associação Brasileira de Normas Técnicas (ABNT)**, trata de todos os aspectos necessários para garantir que as melhores práticas sejam aplicadas para a segurança da informação. Essa norma tem como objetivo dar suporte para a implantação, manutenção e melhoria contínua dos controles de segurança da informação, padronizando diretrizes e procedimentos para auxiliar na sua gestão. A norma ISO 27002 possui 133 controles, divididos em 11 seções (que abrangem a segurança da informação em todos os seus aspectos, tratando de ferramentas, processos e pessoas):

Política da Segurança da Informação
Prover orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.

Organizando a Segurança da Informação
Estrutura de gerenciamento para iniciar e controlar a implementação da segurança da informação na organização.

Gestão de Ativos
Alcançar e manter a proteção adequada dos ativos da organização.

Segurança em Recursos Humanos
Assegurar que os funcionários, fornecedores e terceiros entendam suas responsabilidades e estejam de acordo com os seus papéis, além de reduzir o risco de furto, roubo, fraude ou mau uso de recursos.

Segurança Física e do Ambiente
Prevenir acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

Gestão das Operações e Comunicações
Garantir a operação segura e correta dos recursos de processamento da informação.

Controle de Acesso
Controlar o acesso à informação com base nos requisitos de negócio e segurança da informação.

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
Garantir que a segurança seja parte integrante de sistemas da informação.

Gestão de Incidentes de Segurança da Informação
Assegurar que fragilidades e eventos de segurança da informação associados aos sistemas de informação sejam comunicados, permitindo a tomada de ação em tempo hábil.

Gestão da Continuidade do Negócio
Não permitir a interrupção das atividades dos negócios e proteger os processos críticos contra efeito de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil.

Conformidade
Adequar os requisitos de segurança para não permitir a violação de regulamentações ou leis estabelecidas, além de obrigações contratuais.

Com o objetivo de apoiar as **organizações** a **desenvolverem um programa eficaz de treinamento** em conscientização de segurança, são sugeridas as seguintes recomendações baseadas na **ISO/IEC 27002**:

Obrigatoriedade do envolvimento da diretoria

Todos os funcionários de uma organização são responsáveis por sua segurança, portanto, precisam estar comprometidos com as políticas de proteção dos dados. Dada a importância estratégica para a organização, espera-se que a diretoria entenda que a sua responsabilidade é maior do que a dos demais funcionários, pois tem direitos de acesso a dados e sistemas que, se caírem nas mãos de pessoas mal-intencionadas, podem causar grandes prejuízos.

Se a diretoria não se interessar ativamente pela segurança e não perceber a importância do elemento humano nisso, é improvável que sejam fornecidos recursos suficientes e suporte adequado. O envolvimento de executivos na segurança cibernética também pode facilitar a criação de uma cultura de segurança na organização, estimulando a colaboração dos funcionários.

Envolvimento de toda a organização

É muito provável que a responsabilidade de desenvolver e implementar um programa de conscientização de segurança seja de uma única área. Essa atividade, porém, não pode ser feita sem o apoio dos demais setores. Os líderes dos diferentes departamentos podem ajudar a garantir que o programa de treinamento de conscientização sobre segurança receba a prioridade que merece.

Para ajudar o departamento de TI (Tecnologia da Informação), os membros de outros departamentos podem ser treinados e colaborar com o fornecimento de suporte ou nos esforços de treinamento. Departamentos, como o de marketing, podem desenvolver conteúdo para boletins e outros materiais de treinamento. O departamento de RH (Recursos Humanos) pode ajudar com a definição de políticas e procedimentos.

Criação de conteúdo para treinamento e conscientização de segurança

Fala-se, cada vez mais, sobre a segurança da informação. Com o passar do tempo, os dados tornaram-se mais valorizados devido ao avanço das pesquisas em áreas como a de ciências de dados, por exemplo. Então, não é complicado encontrar cursos sobre esse assunto, que podem ser adaptados para a realidade das empresas, gerando, provavelmente, menor custo de produção interna de material de treinamento.

Diversidade de treinamento

O treinamento efetivo é um importante instrumento para criar uma cultura de segurança da informação dentro da organização. Nesse sentido, deve-se perceber que as pessoas respondem de maneira distinta aos diferentes métodos de treinamento. Alguns aprendem melhor com treinamento em sala de aula, outros podem precisar de treinamento individual e há aqueles que serão mais beneficiados com seminários periódicos de treinamento.

O programa de treinamento, portanto, deve incluir uma ampla variedade de métodos tendo em vista os diferentes estilos de aprendizado. Quanto mais envolvente for o programa, maior será a retenção de conhecimento. Com a divulgação de material informativo por e-mail, jogos e questionários, haverá grandes melhorias na conscientização sobre segurança entre os funcionários.

Exercícios de simulação

A divulgação de conhecimento é uma etapa muito importante do treinamento. Por isso, é necessário garantir a capacitação dos funcionários para que eles possam aplicar os conhecimentos adquiridos a situações de seu cotidiano. A única maneira de determinar a eficácia do programa de treinamento é por meio de simulações de ataques.

Exercícios de simulação de phishing e de outros cenários de ataque devem ser realizados em todas as etapas de treinamento. Com a aplicação desses exercícios, é possível medir a eficácia dos assuntos que foram tratados no programa de treinamento e fornecer o feedback necessário para identificar os pontos fracos e tomar medidas para a melhoria do treinamento.

Periodicidade na realização do treinamento de conscientização de segurança

O treinamento de conscientização de segurança deve ser feito periodicamente. Ao longo do ano, os funcionários devem estar envolvidos em diferentes atividades que os ajudem a fixar conhecimento, identificar pontos de melhoria e, principalmente, aplicar as boas práticas adquiridas ao seu cotidiano. O objetivo deve ser garantir que os problemas de segurança estejam sempre atualizados e contextualizados na realidade da organização.

O treinamento é um importante instrumento para fortalecer o corpo funcional com o conhecimento necessário para evitar armadilhas que exponham a segurança da organização.

A importância do treinamento na segurança da informação

Para saber um pouco mais sobre a importância do treinamento como medida para a segurança da informação, assista ao vídeo a seguir.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Espera-se que os conhecimentos adquiridos nos treinamentos sejam traduzidos em ações diárias que priorizem o uso racional dos recursos com o objetivo de proteger os sistemas, os dados e os ambientes. Estamos falando dos mecanismos de proteção que serão abordados a seguir.

Mecanismos de Proteção

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Trata-se do **conjunto de ações e recursos** que visa a **proteger um sistema ou uma organização**. Esses mecanismos são definidos considerando o ponto de vista da organização e dos sistemas. Vejamos:

Do ponto de vista da organização

Referem-se às restrições de comportamento de seus membros e de possíveis atacantes por meio de mecanismos como **portas, fechaduras, chaves** e **paredes**.

Do ponto de vista dos sistemas

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.

A seguir estão alguns exemplos de princípios que se aplicam aos mecanismos de proteção:

1

Economia de mecanismo (objetividade do mecanismo)

O projeto de um sistema deve ser o mais simples e pequeno possível para que possa ser facilmente analisado, testado e validado.

Esse princípio se aplica a qualquer aspecto de um sistema, mas merece ênfase nos mecanismos de proteção, pois erros de processos e de implementação resultam em caminhos de acesso indesejados, ou seja, não serão notados durante o uso normal, uma vez que tentativas para fazer acessos inadequados não fazem parte do uso normal de um projeto.

2

Padrões à prova de falhas

O tipo de acesso que um usuário deve ter em um sistema deve ser feito com base na permissão e não na exclusão. Esse princípio significa que o padrão é a falta de acesso e o esquema de proteção identifica as condições sob as quais o acesso é permitido. Portanto, trata-se de um equívoco tentar identificar as condições sob as quais o acesso a um sistema deve ser recusado. Um projeto conservador deve ser baseado em argumentos sobre os motivos em que os objetos devem estar acessíveis e não por que não deveriam.

Por exemplo, o servidor Apache ou Servidor HTTP Apache é o mais bem-sucedido servidor web livre que existe. Ele possui um arquivo de configuração chamado de **.htaccess**. A omissão de um parâmetro de uma chamada do sistema do controle de acesso no **.htacess** do Apache deve resultar em menos permissão.

3

Mediação completa

Todos os acessos a recursos, tanto diretos quanto indiretos, devem ser verificados pelos mecanismos de segurança. Eles devem ser organizados de forma a ser impossível contorná-los. Esse princípio, quando aplicado sistematicamente, é o principal fundamento do sistema de proteção.

Ele dá uma visão geral do controle de acesso que, além da operação normal, inclui o início, a recuperação, o desligamento e a manutenção. Isso implica o desenvolvimento de um método para identificar a fonte de cada solicitação. Se ocorrer uma mudança de acesso, esses resultados deverão ser atualizados no sistema.

4

Projeto aberto

Os mecanismos de segurança não devem depender da ignorância de possíveis invasores, mas da posse de chaves criptográficas ou de senhas, que garantem mais proteção para os sistemas. Essa dissociação permite que os mecanismos sejam examinados por muitos revisores sem a preocupação de que a própria revisão comprometa o que deve ser protegido. Além disso, qualquer usuário cético pode se convencer de que o sistema que ele está prestes a usar é adequado para seu objetivo. Por fim, não é realista tentar manter o sigilo de qualquer sistema que receba ampla distribuição.

5

Separação de privilégios

Segundo Saltzer e Schroeder (1975), um mecanismo de proteção que requer duas chaves para desbloqueá-lo é mais robusto e flexível do que aquele que permite o acesso ao apresentador de apenas uma única chave. A relevância dessa observação para os sistemas de computador foi apontada por Roger Needham (1935-2003). O motivo é que, uma vez bloqueado o mecanismo, as duas chaves podem ser separadas fisicamente, e diferentes programas, organizações ou indivíduos são responsáveis por elas. Assim, nenhum acidente, engano ou quebra de confiança é suficiente para comprometer as informações protegidas.

Esse princípio é frequentemente usado em cofres de bancos. Também está em ação no sistema de defesa que dispara uma arma nuclear apenas se duas pessoas diferentes derem o comando correto. Em um sistema de computador, chaves separadas se aplicam a qualquer situação em que duas ou mais condições sejam atendidas antes que o acesso seja permitido. Por exemplo, sistemas que fornecem tipos de dados protegidos extensíveis ao usuário geralmente dependem da separação de privilégios para sua implementação.

6

Privilégio mínimo

Um privilégio define uma permissão individual associada a um nome autorizado, habilitando-o a acessar ou modificar um recurso do sistema. Os privilégios também podem ser concedidos a grupos de usuários. Por exemplo, o gerenciamento de privilégios em um banco de dados é feito por meio da execução do comando GRANT no **SQL**, sigla inglesa para *Structured Query Language*, ou seja, linguagem de consulta estruturada. O SQL é a linguagem mais usada para fazer pesquisas em bancos de dados relacionais.

O princípio de privilégio mínimo diz que todos os programas e todos os usuários do sistema devem operar usando o menor conjunto de privilégios necessário para concluir o trabalho. Portanto, esse princípio limita os danos que podem resultar de um acidente ou erro. Desse modo, se for necessário investigar o uso indevido de um privilégio, o número de programas que deve ser auditado é reduzido.

7

Compartilhamento mínimo

Diz respeito à minimização de recursos compartilhados entre diferentes programas, pois, se um programa pode corromper um recurso compartilhado, então ele pode corromper outros programas que dependem dele.

Por exemplo, caso uma funcionalidade do sistema operacional possa ser implementada, como chamada ao núcleo (system call), ou como função de biblioteca, deve-se preferir a última forma, já que envolve menos compartilhamento.

8Aceitação psicológica

É essencial que a interface de um sistema seja projetada para facilitar o uso, para que os usuários apliquem rotineira e automaticamente os mecanismos de proteção.

Além disso, à medida que o usuário associe o sistema aos mecanismos que ele deve usar, os erros serão minimizados. Por exemplo, alguns sistemas obrigam o usuário a cadastrar senhas muito complicadas que eles esquecem ou anotam, gerando uma vulnerabilidade para o sistema.

Verificando o Aprendizado

Questão 1

Um funcionário de uma organização resolveu adotar o número de sua matrícula como senha. Marque a alternativa que apresenta a postura que deve ser adotada pela empresa para evitar essa situação:

A

A organização deve sugerir um padrão de senhas.

B

A organização não deve fazer nada, pois a responsabilidade pela senha é do funcionário.

C

A organização deve implementar um sistema que verifique se a senha atende a determinados pré-requisitos.

D

A organização deve obrigar que os funcionários mudem suas senhas periodicamente.

E

Criar mais de uma matrícula para cada um dos funcionários.

A alternativa C está correta.

O responsável pelo cadastro das senhas pode implementar um programa para evitar algumas situações, como inclusão de nomes, números de matrícula e números sequenciais, por exemplo.

Questão 2

Selecione a opção que apresenta algumas das recomendações de treinamento em conscientização de segurança que podem ser implementadas nas organizações:

A

Escolher indivíduos específicos para treinar.

B

A responsabilidade pela segurança da informação é apenas dos funcionários, portanto a organização não deve fazer nada.

C

A responsabilidade pela segurança da informação é apenas da diretoria, portanto a organização não deve fazer nada.

D

Desenvolver treinamentos e exercícios de simulação.

E

Selecionar funcionários para treinamentos mediante técnicas de amostragem.

A alternativa D está correta.

Algumas recomendações de treinamento são:

- Envolvimento da diretoria;
- Esforço por parte de toda a organização;
- Criação de conteúdo de treinamento de conscientização de segurança;
- Diversidade de treinamento;
- Exercícios de simulação;
- Constância no treinamento de conscientização de segurança.

Vamos começar!

A importância do controle de acesso, antivírus e backup

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Controle de acesso

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Imagine que uma empresa decida adquirir serviços de computação em nuvem e precise determinar os níveis de acesso dos usuários aos recursos contratados.

> Como realizar esse procedimento?

Por meio do controle de acesso, que é uma maneira de **limitar a abordagem** a um sistema ou a recursos físicos ou virtuais. Na computação, o controle de acesso é um modo pelo qual os **usuários recebem acesso** e certos privilégios a **sistemas, recursos** ou **informações**.

Nos sistemas de controle de acesso, os usuários devem apresentar **credenciais** antes de obter o acesso. Essas credenciais podem ser de várias formas como, por exemplo, físicas, biométricas, senhas, portas eletrônicas. Existem **três tipos de sistemas de controle de acesso**:

Controle de Acesso Discricionário ou *Discretionary Access Control* (DAC)

Nesse método, o administrador do sistema, dos dados ou de recursos protegidos define as políticas de quem tem permissão de acesso, ou seja, o sistema responsabiliza o proprietário da empresa por decidir quais pessoas são permitidas em um local específico, física ou digitalmente.

O DAC é menos restritivo em comparação aos outros sistemas, pois permite, essencialmente, um controle completo individual sobre quaisquer objetos que se possua, bem como sobre os programas associados a esses objetos. A desvantagem do controle de acesso discricionário é o fato de fornecer ao usuário final o controle completo para definir configurações de nível de segurança para outros usuários. Além disso, as permissões concedidas ao usuário final são herdadas em outros programas usados, o que pode levar à execução de malware, ainda que o usuário final não esteja ciente disso.

Controle de Acesso Obrigatório ou *Mandatory Access Control* (MAC)

De acordo com Red Hat (2020), uma empresa líder mundial no fornecimento de soluções de software open source, incluindo tecnologias de alto desempenho em Linux, esse mecanismo de segurança restringe o nível de controle dos usuários (sujeitos) sobre os objetos que eles criam. Diferentemente da implementação do DAC, em que os usuários têm controle total sobre seus próprios arquivos, diretórios etc., o MAC acrescenta rótulos ou categorias adicionais a todos os objetos do sistema de arquivos. Usuários e processos devem ter acesso apropriado a essas categorias antes de interagir com os objetos.

Para entender melhor, o **sujeito** é normalmente um processo ou thread enquanto **objetos** são construções, como arquivos, diretórios, portas TCP/UDP, segmentos de memória compartilhada, dispositivos de entrada e saída. Sujeitos e objetos possuem um conjunto de atributos de segurança. Sempre que um sujeito tenta acessar um objeto, uma regra de autorização imposta pelo kernel do sistema operacional examina esses atributos de segurança e decide se o acesso pode ocorrer.

Controle de Acesso Baseado em Função ou *Role-Based Access Control* (RBAC)

Concede acesso com base em funções de negócios definidas e não na identidade do usuário. A meta é fornecer aos usuários somente o acesso a dados considerados necessários para exercer sua função nas organizações. Esse método é baseado em uma combinação de atribuições de funções, autorizações e permissões.

Quando se trata da proteção dos recursos computacionais, os itens que devem ser contemplados são: **aplicativos e arquivos de dados**, além de **utilitários** e o **sistema operacional** das máquinas tanto dos usuários como da rede institucional.

> Você sabe os motivos pelos quais esses recursos devem ser protegidos?

Entenda no exemplo a seguir:

Exemplo

Júlia trabalha em uma pequena empresa de investimentos que ainda não possui uma política de controle de acessos bem definida, o que resultou no acesso de uma pessoa mal-intencionada aos dados e sistemas da empresa.A empresa possui um aplicativo para que o usuário possa acompanhar os seus investimentos. Com o acesso indevido, o comportamento do aplicativo foi alterado e os comandos que os usuários davam não eram executados.O banco de dados da empresa foi completamente apagado.E os arquivos de log foram apagados, o que dificultou a rastreabilidade das ações que foram realizadas pelo hacker.

Percebeu o quanto é prejudicial para uma empresa ter aplicativos, arquivos de dados e sistema operacional desprotegidos?

Por isso, vamos conhecer a importância da proteção de cada recurso.

1

Aplicativos

Caso um usuário não autorizado tenha acesso ao código-fonte dos aplicativos, ele poderá alterar o comportamento esperado do programa. Alguns exemplos desse tipo de fraude podem ocorrer em transações financeiras, em que o aplicativo é modificado para beneficiar o fraudador.

2

Arquivos de dados

As bases de dados, os arquivos ou as transações só podem ser alterados ou excluídos por usuários credenciados. Ainda assim, é muito importante que sejam implementados recursos de rastreabilidade para saber quem realizou cada operação no sistema.

3

Utilitários e sistema operacional

O acesso a utilitários deve ser restrito. Essas ferramentas são utilizadas para desenvolver e dar manutenção aos aplicativos e para configurar o sistema operacional. Caso um atacante tenha acesso a essas ferramentas e não haja mecanismos de proteção, comprometerá a segurança de todos os aplicativos, arquivos e sistema operacional.

4

Arquivos de senha

Os arquivos que armazenam as senhas precisam de um esquema de proteção adequado. Na ausência dessa proteção, uma pessoa não autorizada pode causar danos ao sistema.

5 Arquivos de log

São usados como mecanismos de rastreabilidade das ações realizadas pelos usuários nos sistemas. Portanto, é uma fonte de informação importante para auditorias futuras. Nos arquivos de log estão os registros de quem acessou os recursos computacionais, quando isso foi feito e que tipo de operações foram realizadas. Uma pessoa mal-intencionada pode tentar acessar o sistema, apagar ou alterar dados, acessar aplicativos, alterar a configuração do sistema operacional para facilitar futuras invasões e, posteriormente, alterar os arquivos de log para que suas ações não possam ser identificadas, fazendo com que o administrador do sistema não perceba a invasão.

Podemos dizer, então, que os objetivos dos controles de acesso são garantir:

1. O acesso aos recursos apenas por usuários autorizados.
2. A correspondência entre os recursos necessários e as atividades dos usuários.
3. O monitoramento e a restrição do acesso a recursos críticos.
4. Execução de transações compatíveis com as funções e responsabilidades dos usuários.

Controles de acesso

Para saber um pouco mais sobre os controles de acesso, assista ao vídeo a seguir.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Diante de tudo o que vimos, podemos definir o controle de acesso em termos de:

1

Funções de identificação e autenticação de usuários.

2

Alocação, gerência e monitoramento de privilégios.

3

Limitação, monitoramento e desabilitação de acessos.

4

Prevenção de acessos não autorizados.

Em relação à **identificação e autenticação** dos usuários nos sistemas, essas ações são feitas durante o **logon**. Esse processo permite conceder acesso aos dados e aplicativos em um sistema computacional e envolve a entrada de um ID (identificação do usuário), normalmente chamado de login, e uma **senha** (autenticação do usuário).

> A identificação define para o sistema quem é o usuário, e a senha é um autenticador, ou seja, é o modo como o sistema verifica que o usuário é realmente quem ele diz ser.

Devido à importância de entrar no sistema, o procedimento de logon deve divulgar o mínimo de informações que possam ser utilizadas por um invasor para conseguir identificar um usuário legítimo.

Nesse sentido, um procedimento de logon eficiente deve:

1. Informar que o **sistema** só deve ser **acessado por pessoas autorizadas**.
2. **Não apresentar informações sobre o sistema** até que o processo de logon esteja completamente concluído.
3. Não fornecer, durante o processo de logon, **mensagens de ajuda** que possam auxiliar um usuário não autorizado a acessar o sistema.
4. **Validar os dados de entrada** só **após a conclusão do processo de logon**. O sistema não deve indicar qual parte do dado de entrada está correta ou incorreta, como, por exemplo, ID ou senha, caso ocorra algum erro.
5. **Limitar a quantidade de tentativas** de logon sem sucesso, como, por exemplo, um máximo de três tentativas.
6. **Guardar as tentativas de acesso inválidas** para futura verificação.
7. **Forçar um tempo de espera antes de permitir novas tentativas** de entrada no sistema ou **rejeitar qualquer tentativa posterior de acesso** sem autorização específica.
8. **Terminar as conexões** com o sistema.
9. **Limitar o tempo para o procedimento de logon**. Se demorar, o sistema deverá encerrar o procedimento.
10. Quando o procedimento de logon no sistema finalizar corretamente, mostrar as seguintes informações: **data e hora** do último logon com sucesso; **detalhes de qualquer tentativa de logon sem sucesso**, desde o último procedimento realizado com sucesso.

A identificação do usuário deve ser única e pode ser composta por um código de caracteres (que é o caso mais comum, chamado de login), ou cartão inteligente (*Smart Card*), por exemplo. Desse modo, é possível fazer um controle das ações praticadas pelos usuários por meio dos logs. Após a identificação do usuário por meio do login, deve-se proceder à sua autenticação, isto é, o sistema deve confirmar se o usuário é realmente quem ele diz ser.

Vamos a um exemplo prático:

Imagine que você esteja programando as mensagens que aparecerão para o usuário durante o processo de logon. De acordo com as orientações que vimos, observe as mensagens que devem ou não aparecer ao usuário:

Senhas	Válida ou inválida	Justificativa
A sua senha está incorreta.	Inválida	Essa mensagem não deve aparecer para o usuário, pois o sistema não deve indicar qual parte do dado de entrada está correta ou incorreta, como, por exemplo, ID ou senha, caso ocorra algum erro.
Seus dados de logon estão incorretos. Você tem mais duas tentativas.	Válida	Essa mensagem pode aparecer para o usuário, pois o sistema deve limitar a quantidade de tentativas de logon sem sucesso, como, por exemplo, um máximo de três tentativas.
Este sistema pode ser acessado por qualquer pessoa.	Inválida	Essa mensagem não deve aparecer para o usuário. Ao contrário, o sistema deve informar que o sistema só deve ser acessado por pessoas autorizadas.

Sérgio Assunção Monteiro.

Política contra vírus

Um **vírus de computador** é um **programa** carregado em qualquer computador — incluindo computadores pessoais e servidores — sem que o proprietário tenha o conhecimento da sua existência, sendo executado contra a sua vontade. Além disso, é um programa malicioso que faz cópia de si mesmo e infecta o computador e os arquivos.

Atualmente, os vírus se dividem em várias categorias e cada uma apresenta diferentes objetivos e formas de ataques. A seguir, são apresentados alguns dos principais tipos de vírus de computador (**GEEKS FOR GEEKS**, 2020):

Geeks for Geeks

Portal de Ciência da Computação que disponibiliza artigos e textos sobre tecnologia, que é direcionado para geeks, gíria inglesa que nomeia pessoas excêntricas, fãs de tecnologia, eletrônicos, games, jogos de tabuleiros, histórias em quadrinhos, filmes, séries e livros. GeeksforGeeks.

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, uma série de comandos e instruções que são agrupados como um único comando para realizar uma tarefa automaticamente, bastante utilizadas em documentos do Word e planilhas do Excel. Por exemplo, esse tipo de vírus pode estar contido em arquivos de planilha.

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.

Polimórfico

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, ou seja, o vírus.

Vírus *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.

Vírus *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.

Vírus de 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.

Vírus 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.

Vírus 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.

Atente-se para as seguintes orientações:

1

Antivírus

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

Atualização

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

3 Verificação

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

Atenção com dispositivos

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.

5

Atenção com fontes externas

Os computadores e servidores de rede **nunca devem ser inicializados** a partir de um dispositivo externo recebido de uma fonte externa.

6

Software de proteção

O software de proteção contra vírus deve ser **carregado em cada computador** e servidor de rede como um programa residente para monitorar constantemente possíveis ataques de vírus e impedir que infectem a rede.

Sistemas de backup

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Backup é a criação de **cópias redundantes de informações**. Os sistemas de backups são utilizados como cópia de segurança de arquivos e dados.

> Você sabe por que o backup é tão importante?

Lembra-se do caso da empresa de Júlia?

Com o ataque, eles tiveram todo o banco de dados apagado. Caso eles tenham investido na realização de backups, o prejuízo sofrido pela empresa pode ser minimizado com a restauração dos dados. O ideal para uma empresa ou um usuário é realizar o backup de todos os dados em tempo real, para garantir que não haverá a perda de dados.

Na prática, quase sempre é inviável aplicar essa recomendação devido à concorrência de atividades que fazem parte do cotidiano de

uma empresa. No entanto, é muito importante que haja uma política específica para isso com a definição de responsáveis, periodicidade, locais de armazenamento e procedimentos de restauração, caso seja necessário.

A organização também deve ter uma **periodicidade para a manutenção dos backups**, ou seja, por quanto tempo devem ser guardados e se existe alguma legislação que seja aplicável de forma específica. Por exemplo, no caso de instituições de ensino, um questionamento comum é sobre o período que o histórico escolar de um aluno será guardado.

Atenção

É importante que as empresas realizem testes com os backups a fim de garantir que os dados salvos possam ser restaurados e disponibilizados quando for preciso.

Os backups são apenas um recurso de segurança usado para minimizar os problemas de uma companhia ou de um usuário em caso de perda de dados ou indisponibilidade nos sistemas. Quanto melhor for a **política de backup** (armazenamento e restauração de dados), menores serão os problemas para que a companhia possa continuar suas atividades. De acordo com Mayer (2017), existem alguns tipos de sistemas de backups, conforme apresentado a seguir:

Backup 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, entre outros, independentemente de terem sido modificados ou não.

Backup 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.

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.

Para garantir que as organizações possam continuar trabalhando em caso de perdas de dados, é extremamente recomendável possuir ferramentas conhecidas como *Disaster Recovery*. Essa infraestrutura tecnológica possibilita a operação da companhia em caso de falha de sistema.

Verificando o Aprendizado

Questão 1

Quais são os recursos que o controle de acesso visa proteger?

A

Apenas dados pessoais.

B

Apenas dados organizacionais.

C

Todos os programas da organização.

D

Todos os recursos que possam fornecer informação sobre a organização, seus funcionários, clientes e parceiros.

E

Softwares estratégicos para a organização.

A alternativa D está correta.

Aplicativos, arquivos de dados, utilitários e sistema operacional, arquivos de senha e arquivos de log. O objetivo do controle de acesso não é proibir ou dificultar o acesso, mas controlar o acesso aos recursos.

Questão 2

(Adaptado de CESPE – Polícia Federal – Papiloscopista – 2018) “São exemplos de vírus contidos em programas aparentemente inofensivos. Além disso, as suas ações são disfarçadas pelas funcionalidades do programa hospedeiro”. Considere a definição dada e selecione a opção que corresponde a esse tipo de vírus:

A

Cavalo de Troia.

B

Polimórfico.

C

Vírus *stealth*.

D

Vírus blindado.

E

Wardriving.

A alternativa A está correta.

Cavalos de Troia (*trojan*) são programas aparentemente inofensivos que trazem embutidos em si outro programa malicioso, ou seja, o vírus. Trata-se de um tipo de malware que, frequentemente, está disfarçado de software legítimo, ou seja, induz o usuário ao erro. Os criminosos virtuais e hackers utilizam esse tipo de vírus para obter acesso aos sistemas dos usuários e cometer crimes.

Vamos começar!

A importância da criptografia e certificado digital

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Criptografia

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Criptografia consiste no ato de codificar dados para que apenas pessoas autorizadas consigam ter acesso às informações.

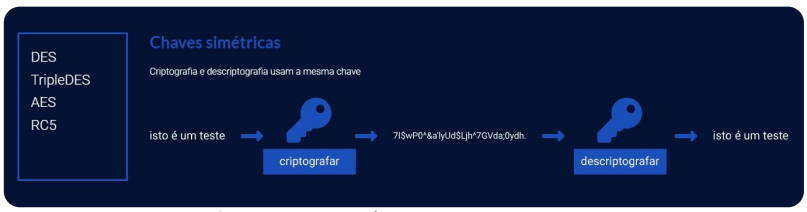
Segundo Stallings (2008), a criptografia das informações pode ser classificada em três tipos:

- Criptografia de chave simétrica
- Função Hash
- Criptografia de chaves assimétricas

Vamos entender melhor cada uma.

Criptografia de chave simétrica

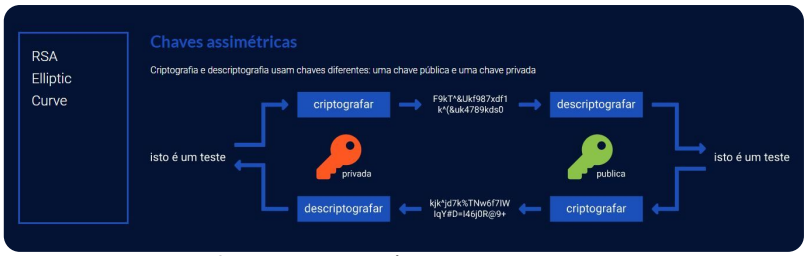
Também conhecida por **criptografia de chave privada ou secreta**. Aqui, o receptor da informação e o remetente usam uma única chave para criptografar e descriptografar a mensagem. O tipo frequente de criptografia usada nesse método é AES (*Advanced Encryption System*). Alguns exemplos de tipos de criptografia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



Exemplos de criptografia de chave simétrica.

Criptografia de chave assimétrica

Também 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. A imagem a seguir ilustra esse processo:



Exemplos de criptografia de chave assimétrica.

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*). A imagem a seguir ilustra esse processo:

Exemplos de algoritmos de Hash.

Por que existem tantos tipos diferentes de criptografia? Por que não é possível fazer tudo o que é necessário com apenas um? Porque cada esquema é otimizado para aplicações criptográficas específicas.

Observe:

Você quer garantir a integridade dos dados?

Use as **funções de hash**. Elas são adequadas para garantir a integridade dos dados, porque qualquer alteração feita no conteúdo de uma mensagem fará com que o receptor calcule um valor de hash diferente daquele colocado na transmissão pelo remetente. Como é altamente improvável que duas mensagens diferentes produzam o mesmo valor de hash, a integridade dos dados é garantida com muita confiança.

Você quer garantir a privacidade e confidencialidade?

Use a **criptografia de chave secreta**. Ela é ideal para criptografar mensagens, proporcionando privacidade e confidencialidade. O remetente pode gerar uma chave de sessão para criptografar a mensagem e o receptor precisará da mesma chave de sessão para descriptografá-la.

Você quer realizar a troca de chaves?

Use a **criptografia de chave pública**. Essa é uma importante aplicação desse tipo de criptografia. Esquemas assimétricos também podem ser usados para não repúdio e autenticação de usuário; se o destinatário puder obter a chave da sessão criptografada com a chave privada do remetente, somente esse remetente poderá ter enviado a mensagem.

A criptografia de chave pública também poderia, teoricamente, ser usada para **criptografar mensagens**, embora isso raramente seja feito, pois os valores de criptografia de chave secreta geralmente podem ser calculados muito mais rápido que os valores de criptografia de chave pública.

Quais são as principais diferenças entre **criptografia simétrica, assimétrica** e de **função hash**?

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.

É recomendável a utilização de métodos criptográficos para proteger documentos confidenciais — cujo conteúdo seja de grande importância para a empresa — com o objetivo de garantir que apenas pessoas autorizadas tenham acesso a eles. Além de arquivos, também é possível criptografar mensagens de e-mail como forma de evitar o acesso de conteúdo sigiloso por terceiros não autorizados. A expectativa para o futuro é de maior aprimoramento dos métodos de criptografia para tornar os dados pessoais mais seguros e seus padrões mais confiáveis.

Vamos a alguns exercícios:

Certificado digital

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

O **certificado digital** é um **documento eletrônico** que **identifica pessoas e instituições**, provando identidades e permitindo o acesso a serviços informatizados que garantam:

- Autenticidade
- Integridade
- Não repúdio

O certificado digital também é usado para assinar documentos digitalmente. Ele é destinado a qualquer pessoa, **física** ou **jurídica**, sendo emitido por uma **Autoridade Certificadora (AC)**. Com ele, pode-se anexar a chave pública, também chamada de infraestrutura de chave pública – do inglês *Public Key Infrastructure* (PKI) –, a um indivíduo ou entidade específica. Um certificado digital criptografado deve conter:

- O nome do sujeito (a organização ou indivíduo certificado);
- A chave pública do sujeito (usada para descriptografar mensagens e assinaturas digitais);
- Um número de série (para identificar exclusivamente o certificado);
- Uma data de validade;
- A assinatura digital da autoridade emissora do certificado e a mensagem.
- Qualquer outra informação relevante.

O caminho vinculado de verificação e validação de um certificado digital da entidade final para uma AC que atua como uma âncora de confiança é chamado de **cadeia de confiança**. Vejamos um exemplo de utilização de certificado digital:

Bancos

Os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor deles (aqui cabe lembrar o nome dessa característica de segurança da informação: autenticidade).

Cliente

Em contrapartida, o cliente, ao solicitar um serviço, como, por exemplo, acesso ao extrato da conta corrente, pode utilizar o seu certificado para autenticar-se perante o banco.

A figura a seguir mostra como os certificados digitais podem ser usados para validar a identidade de um provedor de conteúdo. Observe que os usuários de certificados digitais têm um vínculo de confiança comum com uma AC. Nele, é possível ver como o proprietário e o usuário do conteúdo trocam informações de identificação com a AC. Ambos possuem um relacionamento de confiança entre si.

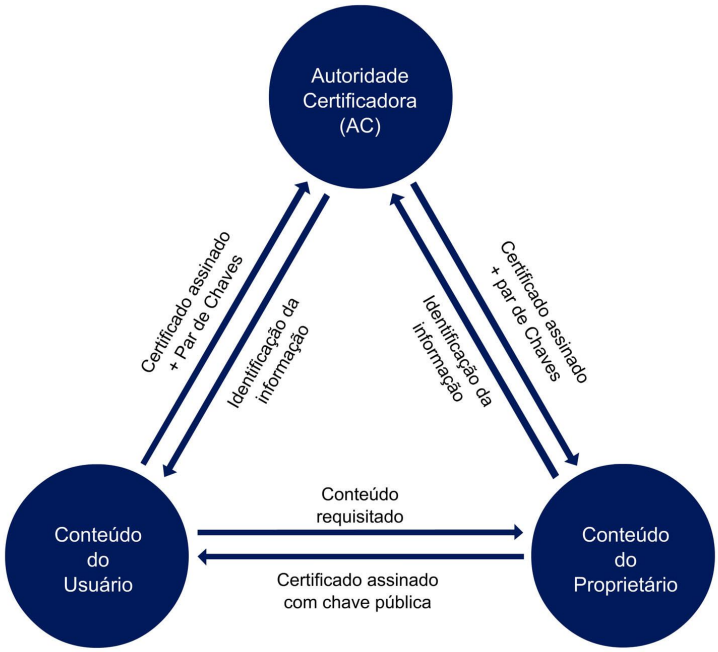


Diagrama do Certificado Digital.

O usuário do conteúdo se registra na AC e recebe um certificado; o proprietário do conteúdo se registra na AC e recebe um par de chaves e um certificado assinado pela AC. Quando o usuário solicita informações de um proprietário do conteúdo, ele envia sua chave pública presente no certificado assinado. Como o usuário pode validar a assinatura no certificado usando a chave pública da AC, ele pode confiar no certificado e usar a chave pública fornecida pelo proprietário do conteúdo.

A certificação digital no Brasil tomou impulso a partir de 2001 quando o governo federal criou a **Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)**, que teve um grande crescimento desde então. Os certificados são utilizados em diversas aplicações:

> Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)
>
> É uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão. Instituto Nacional de Tecnologia da Informação (2017).

- Automatização da prestação de informações fiscais à Receita Federal do Brasil.
- Nota fiscal eletrônica.
- Informatização do Poder Judiciário.
- Informatização de serviços cartoriais.
- Informatização de processos para abertura de empresas.
- Informatização de prontuários médico-odontológicos.
- Compras governamentais por meio de pregão eletrônico.

Os regulamentos sobre os quais se alicerça a ICP-Brasil são: **Medida Provisória 2.200-2** (BRASIL, 2001), **decretos, resoluções do Comitê Gestor da ICP-Brasil, instruções normativas da AC Raiz, documentos complementares**.

A Medida Provisória 2.200-2 (BRASIL, 2001) é o principal marco legal da ICP-Brasil. Publicada em 24 de agosto de 2001, tem força de lei, mesmo não tendo sido analisada no Congresso Nacional, uma vez que o mecanismo de caducidade das MPs não analisadas somente foi instituído pela Emenda Constitucional 32, de 11 de setembro de 2001. (BERTOL; SOUSA; PEOTTA, 2009)

Atenção

Cada usuário é responsável pela guarda e utilização de seu certificado digital, portanto, o usuário nunca deve fornecer o certificado digital a terceiros, pois é um documento pessoal e intransferível. Assim como outros documentos pessoais (CPF, RG e passaporte), não deve ser fornecido a terceiros por questões de segurança.

Com o objetivo de forçar os usuários a atualizarem seus pares de chaves periodicamente, **os certificados digitais possuem data de validade**. Caso uma chave privada seja comprometida antes da data de vencimento, o certificado digital pode ser cancelado e o usuário poderá obter um novo par de chaves e certificado digital. Os certificados cancelados e revogados são colocados em uma lista de certificados de revogação – do inglês *Certificate Revocation List* (CRL) –, mantida pela autoridade de certificação que emitiu os certificados. (DEITEL; DEITEL; CHOFFNES, 2005)

> O comércio eletrônico ainda é considerado inseguro por uma grande parcela da população, principalmente pela falta de conhecimento e inexperiência no uso dos recursos computacionais e, com especial destaque, da internet. Mas é necessário entender que as transações que usam certificados digitais são mais seguras do que informações pessoais trocadas através de meios que não garantam segurança por si mesmos, como comprar por telefone, ou entregar um cartão de crédito a um vendedor.

O avanço da ciência no desenvolvimento de algoritmos de criptografia mais robustos usados na maioria das transações on-line aumenta a segurança nas operações realizadas no mundo virtual. Cabe destacar que **o usuário continua a ser o centro de todo esse desenvolvimento** e é por meio da conscientização e educação nas boas práticas de segurança da informação que pode se sentir seguro e usufruir melhor das facilidades que a tecnologia pode fornecer no cotidiano.

Criptografia e certificado digital

Para saber mais sobre criptografia e certificado digital, assista ao vídeo a seguir.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Verificando o Aprendizado

Questão 1

Marque a alternativa que apresenta os tipos de "criptografias":

A

Chave simétrica, chave assimétrica e função Hash.

B

Quântica e Hash.

C

SHA, MD5 e PCK.

D

Firewall e antivírus.

E

Criptografia transsimétrica

A alternativa A está correta.

Criptografia de chave simétrica, criptografia de chave assimétrica e função Hash. O motivo da existência de três tipos de criptografia é que cada esquema é otimizado para alguma aplicação específica. As funções de hash, por exemplo, são adequadas para garantir a integridade dos dados. A criptografia de chave secreta, por sua vez, é ideal para criptografar mensagens, proporcionando privacidade e confidencialidade. A troca de chaves é uma aplicação importante da criptografia de chave pública.

Questão 2

Selecione a opção que apresenta todos os itens que compõem um certificado "digital":

A

Nome do titular do certificado, biometria, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado.

B

Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, cópia da chave pública do detentor de certificado.

C

Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas do envio do certificado, cópia da chave pública do detentor de certificado.

D

Nome do titular do certificado, número de série usado para identificar exclusivamente um certificado, o indivíduo ou a entidade identificada pelo certificado, datas de expiração, trechos criptografados da mensagem.

E

Nome do titular do certificado, chave criptográfica, data de nascimento, nome da mãe, datas deenvio do certificado, entidade identificada pelo certificado.

A alternativa B está correta.

O certificado digital destina-se a qualquer pessoa, física ou jurídica, sendo emitido por uma Autoridade Certificadora (AC). A AC emite um certificado digital criptografado contendo o nome do sujeito (a organização ou indivíduo certificado), a chave pública do sujeito, um número de série (para identificar exclusivamente o certificado), uma data de validade, a assinatura da autoridade de certificação confiável e qualquer outra informação relevante. O objetivo é garantir a autenticidade do usuário, ou companhia que faça uso do certificado digital, ou seja, certificar que o usuário ou a empresa são, de fato, quem dizem ser.

Considerações finais

Ao longo deste conteúdo, vimos que os recursos da informática, como a internet, o correio eletrônico, as redes sem fio etc., tornaram-se ferramentas indispensáveis para o desempenho das mais diversas atividades, principalmente as que ocorrem no ambiente de trabalho. Porém, tais recursos também se tornaram alvo de pessoas mal-intencionadas, sendo comumente explorados para fins ilícitos, como roubo de informações, disseminação de vírus, envio de spam, entre outros.

Em uma companhia, cada informação tem determinada importância, podendo ser classificada de acordo com o impacto que sua perda, alteração ou uso sem permissão pode causar. Por isso, para proteger esses dados de ataques virtuais, sugerimos, durante os módulos, diversas medidas de segurança, baseadas na ISO/IEC 27002, que podem ser adotadas para prevenir ou minimizar possíveis danos às instituições.

Essas medidas, conhecidas como **boas práticas em segurança da informação**, surgiram para proteger os instrumentos tecnológicos e computacionais usados para geração e uso da informação. O conhecimento e a aplicação delas nas organizações pode identificar, prevenir, proteger, detectar, responder e recuperar dados rapidamente perante uma ameaça virtual, garantindo, assim, a confidencialidade, a integridade e a disponibilidade dos ativos tecnológicos e informacionais.

Podcast

Encerraremos o tema falando sobre as boas práticas em segurança da informação.

Conteúdo interativo

Acesse a versão digital para ouvir o áudio.

Explore +

Para saber mais sobre o conteúdo visto, pesquise e leia os seguintes textos:

- **Segurança da informação: o que é e 12 dicas práticas para garantir**, do ECOIT.
- **Lei Geral de Proteção de Dados Pessoais** (Lei nº 13.709/2018).
- **Data Security**, do MIT Sloan Management Review.
- **Cyber Security and Information Sciences**, do Lincoln Laboratory.

O Apache é um servidor web muito popular e é, portanto, exposto a muitos ataques. Caso queira saber mais, procure o artigo **Detection of attack-targeted scans from the Apache HTTP Server access logs**, de Merve Baş Seyyar, Ferhat Özgür Çatak e Ensar Gül.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001** - Sistemas de gestão de segurança da informação. Rio de Janeiro, 2006.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27002** - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 16167** - Diretrizes para classificação, rotulação e tratamento da informação. Rio de Janeiro, 2013.

BERTOL, V.; SOUSA, R.; PEOTTA, L. **Um modelo para as normas sobre certificação digital no Brasil**. VI Conferência Internacional de Perícias em Crimes Cibernéticos. Natal, 2009.

BRASIL. Poder Executivo. **Medida Provisória no 2.200-2, de 24 de agosto de 2001**. Institui a Infraestrutura de Chaves Públicas Brasileira. Brasília, 2001.

DEITEL, H. M.; DEITEL, P. J.; CHOFFNES, D. R. **Sistemas Operacionais**. Pearson Prentice Hall, 3 ed., 2005.

DOCUSIGN. **How do digital signatures work?** Consultado em meio eletrônico em: 19 fev. 2020.

FONTES, E. **Praticando a segurança da informação**. Brasport, 2008.

GEEKS FOR GEEKS. **Types of Viruses**. Consultado em meio eletrônico em: 17 fev. 2020.

MAYER, A. **Backup Types Explained**: Full, Incremental, Differential, Synthetic, and Forever-Incremental. Nakivo Blog. Publicado em: 6 nov. 2017.

RED HAT. **Chapter 49. Security and Selinux**. Consultado em meio eletrônico em: 19 fev. 2020.

SALTZER, J. H.; SCHROEDER, M. D. **The Protection of Information in Computer Systems**. *In*: Proceedings of the IEEE, pp. 1278–1308, 1975.

SEYYAR, M. B.; ÇATAK, F. Ö., GÜL, E. **Detection of Attack-Targeted Scans from the Apache HTTP Server Access Logs**. *In*: Applied Computing and Informatics. Vol. 14, pp. 28-36, 2018.

SHAY R. *et al*. **Encountering stronger password requirements**: User attitudes and behaviors. *In*: Symposium on Usable Privacy and Security (SOUPS), Redmond, USA, pp. 14-16, 2010.

STALLINGS, W. **Criptografia e Segurança de Redes**. São Paulo: Pearson, 4 ed., 2008.

SUPORTE DO OFFICE. **Criar ou executar uma macro**. Consultado em meio eletrônico em: 19 fev. 2020.