Segurança de sistemas de bancos de dados

Segurança de sistemas de banco de dados

Ruy Flavio de Oliveira

© 2017 por Editora e Distribuidora Educacional S.A.
Todos os direitos reservados. Nenhuma parte desta publicação poderá ser reproduzida ou transmitida de qualquer modo ou por qualquer outro meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou qualquer outro tipo de sistema de armazenamento e transmissão de informação, sem prévia autorização, por escrito, da Editora e Distribuidora Educacional S.A.

Presidente
Rodrigo Galindo

Vice-Presidente Acadêmico de Graduação
Mário Ghio Júnior

Conselho Acadêmico
Alberto S. Santana
Ana Lucia Jankovic Barduchi
Camila Cardoso Rotella
Cristiane Lisandra Danna
Danielly Nunes Andrade Noé
Emanuel Santana
Grasiele Aparecida Lourenço
Lidiane Cristina Vivaldini Olo
Paulo Heraldo Costa do Valle
Thatiane Cristina dos Santos de Carvalho Ribeiro

Revisão Técnica
Juliana Schiavetto Dauricio
Roque Maitino Neto

Editoração
Adilson Braga Fontes
André Augusto de Andrade Ramos
Cristiane Lisandra Danna
Diogo Ribeiro Garcia
Emanuel Santana
Erick Silva Griep
Lidiane Cristina Vivaldini Olo

Dados Internacionais de Catalogação na Publicação (CIP)

Oliveira, Ruy Flavio de
O48s Segurança de sistemas de banco de dados / Ruy Flavio de Oliveira. – Londrina : Editora e Distribuidora Educacional S.A., 2017.
192 p.

ISBN 978-85-8482-866-1

1. Banco de dados – Medidas de segurança. I. Título.

CDD 001.64

2017
Editora e Distribuidora Educacional S.A.
Avenida Paris, 675 – Parque Residencial João Piza
CEP: 86041-100 — Londrina — PR
e-mail: editora.educacional@kroton.com.br
Homepage: http://www.kroton.com.br/

Sumário

Unidade 1 | Contextualização sobre segurança de sistemas de bancos de dados 7

Seção 1.1 - Contextualização sobre segurança de sistemas de bancos de dados 9
Seção 1.2 - Princípios de segurança e principais fragilidades em sistema de bancos de dados 23
Seção 1.3 - Mecanismos de segurança de sistemas de bancos de dados: casos reais de problemas na segurança de sistemas de banco de dados 37

Unidade 2 | Gerenciando usuários e permissões 51

Seção 2.1 - Introdução a Data Control Language (DCL) – linguagem de controle de dados 53
Seção 2.2 - DCL: comandos e estrutura 67
Seção 2.3 - Controle de acesso de usuários em DCL. Gerenciando permissões de usuários em DCL 81

Unidade 3 | Segurança em bancos de dados móveis 99

Seção 3.1 - Áreas de segurança em bancos de dados móveis 101
Seção 3.2 - Acesso e gerenciamento de dados e metadados 113
Seção 3.3 - Mecanismos e técnicas de segurança. Segurança de banco de dados comerciais móveis 127

Unidade 4 | Segurança em servidores de banco de dados 143

Seção 4.1 - Introdução ao SQL Inject 145
Seção 4.2 - Controle de acesso não autorizado 159
Seção 4.3 - Políticas de segurança para bancos de dados 173

Palavras do autor

Olá! Seja muito bem-vindo(a) ao nosso módulo de Segurança de Sistemas de Bancos de Dados!

Desde que começamos a utilizar comercialmente os computadores para armazenamento de dados — ainda na década de 1960 —, que um ramo da Ciência da Computação vem ganhando importância: o estudo dos Sistemas de Bancos de Dados. Cada vez mais vemos aspectos de nossas vidas armazenados nessas estruturas e hoje em dia seria simplesmente impossível obter informações digitalmente disponíveis sem consultar bancos de dados.

E com informações valiosíssimas a nosso respeito armazenadas em inúmeros bancos de dados espalhados pela internet afora, uma questão se torna fundamental: como proteger estas informações? É claro que a disciplina de Segurança da Informação já oferece subsídios importantíssimos para auxiliar na proteção de informações e ativos, contudo, é necessário fazer ainda mais. Há usuários que, apesar de cumprirem todas as regras a eles impostas pela Segurança da Informação, ainda ativamente buscam acesso não autorizado a informações armazenadas em bancos de dados. Uma camada a mais de medidas de segurança é necessária para proteger os dados.

Esta disciplina está dividida em quatro unidades, e é composta pelos seguintes temas:

Na Unidade 1, você vai conhecer o contexto dentro do qual se desenvolvem as principais técnicas de segurança em bancos de dados, entendendo quais são os problemas envolvidos, bem como os mecanismos de segurança dos sistemas de bancos de dados.

Na Unidade 2, você vai aprender a gerenciar usuários e suas permissões, além de entrar em contato com a Linguagem de Controle de Dados, utilizada para operacionalizar este gerenciamento.

Na Unidade 3, você entenderá os desafios ligados à segurança de bancos de dados móveis, bem como vai conhecer os mecanismos específicos para a proteção deste tipo de banco de dados.

Na Unidade 4, você entrará em contato com as técnicas de proteção dos

servidores de bancos de dados e vai conhecer as políticas de proteção a estes ativos.

Em resumo, com seu empenho no quesito autoestudo e sua participação em aula, este módulo vai ser bastante produtivo, e vai abrir para você enormes horizontes principalmente no âmbito profissional, mas também no acadêmico.

Pronto(a) para este desafio?

Então, mãos à obra!

Contextualização sobre segurança de sistemas de bancos de dados

Convite ao estudo

Com que frequência você pensa em "bancos de dados" em seu dia a dia? A menos que você seja um profissional da área, a resposta deve ser algo como: "eu não penso em bancos de dados em meu dia a dia". Ainda que estejam longe de nossa lista de preocupações diárias, os bancos de dados são elementos importantíssimos em nossas vidas, pois esta tecnologia é responsável pelo armazenamento de todas as informações disponíveis, por exemplo, na internet. Quando um webmaster (pessoa responsável pela manutenção de um website) começa a configurar o ambiente onde seu website vai ficar hospedado, por exemplo, uma das primeiras definições que lhe serão pedidas — logo depois do registro do nome do do website e muito antes da primeira linha de código HTML ser digitada — é o banco de dados que será usado para armazenar as informações das páginas, dos dados e dos usuários do website. Seus dados bancários, seus dados de imposto de renda, seus dados profissionais que o departamento de RH mantém na empresa onde você trabalha, tudo isso e muito mais é mantido em bancos de dados. Dá para entender o quanto eles são importantes? E dá para entender o quanto é importante proteger esta infraestrutura e os dados que ela mantém? Pois bem, nessa unidade curricular você vai conhecer e ser capaz de definir políticas de segurança lógica e física de dados.

Esta unidade tem, no contexto mais amplo, três grandes objetivos. O primeiro deles é que o aluno entenda o que é e para que serve a segurança da informação, em um contexto geral; entrar em contato com as dimensões da segurança, isto é, com os conceitos de confidencialidade, integridade e disponibilidade; descobrir quais são os objetos da segurança: pessoas,

informações e ativos; e entender onde os bancos de dados se encaixam no contexto da segurança. O segundo é que o aluno entenda o que é segurança em bancos de dados, especificamente; aprender o que deve ser protegido nos bancos de dados; conhecer as principais fragilidades em bancos de dados; entender quais são as ameaças e os agentes de ameaças aos bancos de dados. Finalmente, o terceiro é que o aluno possa conhecer casos relevantes de violações de bancos de dados e deles extrair aprendizados, para evitar que casos semelhantes ocorram novamente.

O jovem empreendedor Jonas, residente na bela cidade de Campos do Jordão, decidiu criar uma aplicação móvel por meio da qual o usuário que passa em frente a um estabelecimento comercial da cidade — em especial hotéis, pousadas, bares, restaurantes e lojas de interesse turístico — recebe notificações acerca de promoções feitas por estes estabelecimentos. Promoções em diárias, refeições e ofertas de vários tipos de bens são exibidas nas telas dos usuários que tiverem o "app" de Jonas. O empreendedor sabe que sua aplicação dependerá pesadamente de sistemas de bancos de dados e a questão da segurança o preocupa bastante. Em função dessa preocupação, ele buscou sua empresa, com o intuito de dirimir suas dúvidas e lançar seu produto sem dores de cabeça.

Será que é relevante falarmos em segurança de bancos de dados no contexto do projeto de Jonas? Se sim, por quê? Temos, neste caso, apenas um banco de dados a proteger? Quais são os desafios encontrados no processo de proteger os bancos de dados envolvidos?

Na presente unidade, será contextualizada a segurança de bancos de dados, isto é, veremos o que é um banco de dados, o que é a proteção a um banco de dados e por que é importante proteger os bancos de dados. Serão apresentados, também, os princípios de segurança, bem como as principais fragilidades dos bancos de dados. Por fim, serão apresentados alguns casos reais em que a segurança dos bancos de dados falhou e houve consequências tanto para as empresas como para os usuários.

Você está pronto para embarcar nesse desafio? Então, vamos seguir a leitura do material.

Seção 1.1

Contextualização sobre segurança de sistemas de bancos de dados

Diálogo aberto

Não é possível imaginarmos hoje em dia um sistema de informações que não dependa pesadamente de um sistema de bancos de dados. Até mesmo aqueles de nós que ainda utilizam agendas telefônicas em papel estão inconscientemente criando e mantendo um sistema de bancos de dados. Os dados processados em qualquer computador (dos supercomputadores aos smartphones) residem em bancos de dados e é nestes bancos de dados que é possível impor ordem a uma massa que de outra forma não faria sentido. Elmasri e Navathe (2005) resumem bem a situação quando afirmam que tanto banco de dados como sistemas de bancos de dados (sistemas computacionais que gerenciam e manipulam bancos de dados) são componentes essenciais no cotidiano da sociedade moderna.

Se os dados são assim tão importantes, não seria lógico protegê-los? Sim, pois se nenhuma outra ameaça existisse, deveríamos nos preocupar pelo menos em manter seguros os dados contra a deterioração dos componentes computacionais físicos que os armazenam. Discos rígidos falham, curtos-circuitos comprometem computadores inteiros, perigos de incêndios e inundações estão sempre aí a nos assombrar e muitos outros perigos rondam a massa de dados que só aumenta em nossos computadores. Proteger esses dados é fundamental, uma vez que não é exagero afirmar que boa parte da civilização depende deles mas, diante de uma tarefa potencialmente colossal como esta, duas perguntas nos vêm à mente: o que, exatamente, é "proteger dados"? e "como proteger os dados?". Em suma: qual é o contexto da segurança de sistemas de bancos de dados?

Pois bem, nesta primeira etapa no projeto que sua empresa pretende desenvolver com Jonas, você deverá contextualizar segurança de bancos de dados para o jovem empreendedor. Para tanto, você primeiro deve apresentar conceitos inerentes à segurança da informação tais como as dimensões da segurança e o conjunto de elementos a serem protegidos. Em seguida, será preciso contextualizar os bancos de dados, suas funções e o porquê da importância protegê-los. Esta consultoria será a

base para justificar um projeto de segurança para a aplicação de Jonas, e você deve apresentar um relatório contendo todas estas informações.

Nesta seção, você vai entender o que é e para que serve a segurança da informação, em um contexto geral; vai entrar em contato com as dimensões da segurança, isto é, com os conceitos de confidencialidade, integridade e disponibilidade; vai descobrir quais são os objetos da segurança: pessoas, informações e ativos; e, por fim, vai entender onde os bancos de dados se encaixam no contexto da segurança (já adianto: eles ocupam uma posição bastante central).

Não pode faltar

Bancos de dados são ferramentas que, como veremos à frente, permitem a organização, o armazenamento e o acesso fácil à informação. São ferramentas, em suma, que giram em torno da informação e existem para facilitar o nosso manuseio da gigantesca quantidade de informações que nos cercam na sociedade contemporânea. Para entendermos como prover segurança aos bancos de dados, é importante, antes, reforçarmos os conceitos de segurança da informação, a disciplina que engloba, entre outras coisas, a segurança de sistemas de bancos de dados.

O princípio da segurança em sistemas de bancos de dados: segurança da informação

Procure a definição acadêmica da expressão "segurança da informação", caro(a) aluno(a), e você vai perceber que não é tão fácil encontrar uma definição. Muitos autores tratam sobre o que a segurança endereça (pessoas, informações, ativos etc.) e muitos outros enfatizam as dimensões de segurança (confidencialidade, integridade, disponibilidade), mas raros são os que se aventuram a responder explicitamente a pergunta mais óbvia: o que é segurança?

Brostoff (2004) oferece uma definição interessante: segurança é a aplicação de um conjunto de salvaguardas ao elemento a ser protegido. Em suma: segurança é a aplicação de ações para proteger um ativo qualquer. Proteger contra o quê? Contra os impactos que possam ocorrer se algo indesejável ocorrer com este ativo.

Segurança é um assunto antigo, que preocupa a humanidade desde seus primórdios. Em seu artigo de 1943, Abraham Maslow estabeleceu sua "hierarquia das necessidades humanas", em que a segunda necessidade mais básica do indivíduo é a proteção, perdendo apenas para suas necessidades biológicas (alimentação, respiração, descanso, reprodução etc.). Em outras palavras, a primeira necessidade do indivíduo é existir e a segunda é proteger sua existência.

A Figura 1.1, a seguir, mostra a pirâmide que ilustra esta hierarquia. Nossa maior necessidade é a biológica, que garante nossa existência; em seguida temos a necessidade de segurança, de nos protegermos contra o meio; logo em seguida, temos a necessidade de amor, afeto, de nos sentirmos bem-vindos em um grupo; nossa próxima necessidade, garantido o amor de um grupo, é a de sermos respeitados, bem-vistos pelos que nos cercam; e, por fim, garantido o respeito, nossa necessidade final, segundo Maslow, é a autorrealização:

Figura 1.1 | Hierarquia das necessidades de Maslow

Fonte: adaptada de Maslow (1943).

Podemos transpor esta necessidade para a atual era da informação: as informações que são um dos bens mais preciosos à nossa disposição (alguns argumentariam, inclusive, que são os mais preciosos, aliás) precisam ser protegidas.

Assim como a informação precede a Tecnologia da Informação (TI) em alguns milênios, também a segurança da informação precederá as modernas técnicas de proteção digital das informações em alguns milênios. Como nos mostra Singh (2010), a proteção de informações sensíveis é praticada desde que em 480 a.C. um grego exilado na Pérsia conseguiu enviar uma mensagem secreta para os exércitos espartanos e gregos, anunciando a invasão que Xerxes, rei dos persas, planejava. O cidadão exilado entalhou a mensagem em tabletes de madeira e escondeu os escritos com cera. Estava inventada ali a técnica da esteganografia, que visa esconder a existência de uma mensagem, protegendo assim a informação.

Exemplificando

Singh (2010) relata que uma das primeiras formas sistematizadas de criptografia era enrolar um cinto de couro em um bastão cilíndrico e escrever uma mensagem neste cinto. Desenrolado o cinto, as letras se

> desalinham, e a mensagem só pode ser lida por alguém que saiba qual o diâmetro correto do cilindro onde enrolar o cinto. Este é ou não é um mecanismo muito inteligente?

Ao longo dos séculos, a criatividade humana propiciou inúmeras formas de esconder mensagens. Por outro lado, a sagacidade humana encontrou formas de decifrar as mensagens escondidas. Uma leitura de Singh (2010) nos mostra que a busca pelo fortalecimento e pela quebra da segurança das informações moldou o mundo em que hoje vivemos e é responsável pelo bom (ou mau) funcionamento da sociedade moderna. Tanto, que não é nada difícil concordar com o autor: a civilização moderna não seria possível sem a possibilidade de protegermos a informação.

As dimensões da segurança da informação

Devemos considerar que a segurança da informação é composta por três dimensões, como afirma Sêmola (2014, p. 9): "Toda informação é influenciada por três propriedades principais: confidencialidade, integridade e disponibilidade". Podemos definir estas dimensões (a que Sêmola identifica como "propriedades principais") da seguinte forma:

• **Confidencialidade** – a informação deve ser mantida em sigilo, sendo acessível apenas ao seu receptor designado.

• **Integridade** – a informação deve manter todas as características de conteúdo que tinha quando foi enviada por seu emissor, não podendo ser modificada a caminho do receptor.

• **Disponibilidade** – a informação deve estar disponível a qualquer destinatário que a ela tiver direito de acesso a qualquer momento.

Sob o ponto de vista das ações a serem tomadas, portanto, a segurança da informação implica em proteger estes três aspectos da informação, isto é:

• Garantir a confidencialidade da informação contra acessos não autorizados.

• Garantir a integridade da informação contra alterações não autorizadas.

• Garantir a disponibilidade da informação contra falhas no acesso, sejam elas frutos de acidentes ou provocadas por agentes não autorizados.

Sêmola (2014) levanta ainda alguns aspectos de segurança pertinentes não à informação, mas ao emissor e ao receptor da informação. São eles:

• **Autenticidade** – garantia quanto à identidade do emissor e do receptor da mensagem, impedindo que esta identidade seja mascarada por agentes não

autorizados.

• **Irretratabilidade (ou não repúdio)** – garantia de que o emissor de uma informação não negará sua ação, nem o receptor negará que acessou esta informação, sendo ambos sempre responsáveis por estes atos.

Exemplificando

É importante observar que um ataque contra a autenticidade ocorre quando um indivíduo não autorizado se passa pelo emissor da mensagem. O atacante, se fazendo passar pelo emissor oficial "A" envia uma mensagem para o receptor oficial "B". "B", por sua vez, toma alguma atitude pensando que a mensagem vem de "A" e é enganado. Se "B" é o tesoureiro de uma organização e "A" é o executivo responsável por pagamentos, o atacante "C" poderia se passar por "A" e enviar uma mensagem na linha de: " transfira R$X mil para a conta do Sr. Fulano de Tal", que seria recebida por "B". Pensando que a mensagem vem de fonte oficial, "B" transferiria o dinheiro, beneficiando o Sr. X, comparsa do atacante "C".

O que proteger?

Já que estamos tratando sobre segurança da informação, a resposta à questão "o que proteger?" parece óbvia, não? "Ora", dirá o leitor mais astuto, "temos que proteger a informação, claro!". Não deixa de ser verdade, obviamente, mas a informação é um conceito um tanto fugaz e abstrato. A informação deve ser protegida, mas como fazê-lo? Um caminho útil para chegarmos à proteção da informação é proposto por Nakamura e Geus (2007) e consiste em observar onde a informação reside. Afirmam os autores que a informação pode residir:

• Na cabeça das pessoas, onde geralmente é criada ou observada originalmente.

• Em artefatos físicos, tais como livros, revistas, cadernos, outdoors, cartazes e mesmo — pensando em nossa história — em cavernas ancestrais, por exemplo.

• Em dispositivos digitais, tais como computadores, pendrives, discos rígidos, redes (quando estão em trânsito), por exemplo.

Observando esses elementos e suas relações com a informação, Nakamura e Geus (2007) propõem os seguintes elementos a serem protegidos pela segurança da informação:

• **Pessoas** – devem ser o objeto principal de toda segurança, ou seja, protegemos "xis" com o objetivo maior de proteger as pessoas relevantes no contexto de "xis". Em segurança da informação esta relação é "de mão dupla": devemos proteger a informação para que assim protejamos também as pessoas e devemos proteger

as pessoas porque são detentoras da informação, ou seja: protegendo as pessoas estaremos também protegendo a informação.

• **Ativos** – chamamos de ativos a todos os elementos que contenham informações que não sejam as pessoas. Podem ser digitais (computadores, redes, dispositivos de armazenamento digital) ou não digitais (livros e outros dispositivos físicos onde podemos representar informações).

• **Informações** – além de proteger os receptáculos das informações, devemos também proteger as informações em si, para que se mantenham sempre sigilosas (acessíveis apenas aos que têm privilégio de acesso), fidedignas (sem adulterações) e disponíveis (acessíveis sempre que os usuários autorizados queiram acessá-las).

Assimile

As dimensões da segurança da informação são Confidencialidade, Integridade e Disponibilidade. As dimensões dos interlocutores da informação são Autenticidade e Não-Repúdio. O que deve ser protegido são as pessoas, os ativos e as informações.

O cerne da segurança: o risco

O estudo do risco é uma prática bastante utilizada por vários ramos do conhecimento, desde a psicologia, passando pela economia e chegando até a engenharia. O risco é uma medida quantitativa e qualitativa de o quanto um determinado elemento está ameaçado por uma determinada circunstância ou evento (NIST, 2012).

Entender segurança da informação passa obrigatoriamente por compreender o conceito de risco e seus componentes. Vejamos os conceitos que formam o risco, tomando por base um elemento qualquer a ser protegido:

• **Vulnerabilidade** – qualquer fraqueza inerente ao elemento a ser protegido. Vulnerabilidade é uma característica interna deste elemento, faz parte do elemento, estando sob seu controle uma vez descoberta. Por exemplo: um erro na codificação de um sistema que permite o acesso não autorizado a ele. Uma falha estrutural em um ponto do casco de um navio que torna este ponto suscetível de ruptura com um impacto de baixa potência.

• **Ameaça** – qualquer circunstância ou evento que possa afetar negativamente o elemento a ser protegido. As ameaças são externas ao elemento a ser protegido, estando fora de seu controle. Por exemplo: uma invasão do sistema por meio da exploração da vulnerabilidade que permite acesso não autorizado. A ruptura do casco do navio no ponto vulnerável.

• **Fonte (ou agente) de ameaça** – intenção, método que visa explorar uma

vulnerabilidade, ou situação que pode acidentalmente gerar resultados negativos por meio de uma vulnerabilidade. Por exemplo: um ex-funcionário que conhece a vulnerabilidade do sistema e está insatisfeito com seu desligamento da empresa. Um jet ski sem controle que segue em direção ao ponto vulnerável do casco do navio.

• **Impacto** – resultado da concretização de uma ameaça. Por exemplo: os prejuízos causados pelo roubo de informações resultante da invasão do sistema pelo ex-funcionário insatisfeito. A morte da tripulação, a perda do navio e a perda dos bens sendo transportados pelo navio depois de seu afundamento resultante do impacto com o jet ski.

• **Risco** – probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para a organização. Por exemplo: em função do alto valor das informações do sistema, do alto grau de insatisfação do ex-funcionário e da facilidade de exploração da vulnerabilidade, a consultoria XYZ estima em 80% a probabilidade de a ameaça se concretizar, ou seja, o risco é de 80%. Em função da posição traseira do ponto vulnerável e do histórico de colisões navais, a empresa dona do navio estima em 0,01% a probabilidade de uma colisão, ou seja, o risco é de 0,01%.

Bancos de dados

Pois bem, isso é o que havia por ora sobre segurança da informação. Nos próximos itens você estudará os fundamentos de banco de dados. Adiante!

Elmasri e Navathe (2005) começam a definição de bancos de dados por seu componente fundamental, o dado. Segundo os autores, temos os seguintes elementos:

• **Dado** – representação de um elemento, um fato que possui significado e que pode ser registrado. São exemplos: um número telefônico, a idade de uma pessoa, um endereço, uma cor, uma data;

• **Banco de dados** – coleção de dados que guardam alguma relação entre si. São exemplos: uma agenda de telefones, um caderno de receitas, uma lista de presença de um curso qualquer, o conjunto de pacientes de um médico, um dicionário, um catálogo de tintas de um fabricante.

A definição acima, de banco de dados, é bastante genérica, como os exemplos mostram, a ponto de uma casa, com uma gama variada de objetos, como é sempre o caso, poder ser considerada um banco de dados, pois os objetos lá contidos têm significado próprio e são relacionados (pertencem a alguém que os julga úteis e/ou agradáveis em sua vida diária). Uma casa, porém, não tem todas as características que Elmasri e Navathe (2005) definem como fundamentais em um banco de dados:

1. Um banco de dados é um conjunto de abstrações de elementos reais (dados

acerca dos elementos reais) que representam um subconjunto de aspectos do mundo real, chamado de minimundo ou de universo de discurso. As mudanças neste minimundo são refletidas no banco de dados.

2. Um banco de dados é uma coleção lógica e coerente de dados, diferente de um conjunto de dados coletados ao acaso, sem relação nenhuma;

3. Um banco de dados armazena e organiza os dados de forma a facilitar que operações de busca e correlacionamento sejam executadas sobre estes dados.

Os computadores são ferramentas perfeitas para a criação e manipulação de bancos de dados, uma vez que oferecem mecanismos rápidos e práticos para as operações sobre os dados que nos são úteis. A velocidade de processamento permite a busca precisa de dados em bancos com bilhões de elementos. Um exemplo disso é o Google. veja, na imagem a seguir, o resultado real de uma busca no Google pela expressão "banco de dados":

Figura 1.2 | Resultado de uma busca no Google

Fonte: elaborada pelo autor.

Observe que o Google pode ser encarado como um gigantesco banco de dados, com trilhões de registros sobre uma enorme diversidade de Assuntos, em várias línguas. Observe na figura que a busca pela expressão "banco de dados" gerou mais de vinte milhões de resultados, que foram agregados e colocados à disposição do usuário em 0,68 segundos. Ou seja, em menos de 7/10 de segundo o sistema de banco de dados do Google encontrou mais de vinte milhões de registros que atendem a minha chave de busca. Um sistema informatizado de banco de dados é ou não é uma ferramenta eficiente para manipular dados?

Reflita

Vale a pena organizar dados em um banco de dados? Imagine um guarda-roupa onde as camisas estão em cabides, as camisetas estão em uma gaveta e as meias e roupas íntimas estão em outra gaveta. Compare a facilidade de encontrar uma roupa específica neste guarda-roupa com a facilidade de encontrar esta mesma roupa se todas as peças estivessem dentro de um saco de estopa.

Componentes dos bancos de dados

Muitos são os modelos de arquitetura de bancos de dados, como afirmam Elmasri e Navathe (2005), e cada forma diferente de encarar os bancos de dados têm vantagens e desvantagens, sendo apropriadas para propósitos diferentes de estudo e manipulação. Como nossos propósitos são ligados à segurança, podemos adotar um modelo simplificado, baseado na estrutura lógica de organização dos dados e dos atores que manipulam estes dados:

• **Campos** – um campo é um espaço que permite o armazenamento de um tipo específico de dado. Pode ser um número, uma cifra (dinheiro), uma data, um conjunto de caracteres etc.

• **Registros** – um registro é o conjunto de campos que descreve uma entidade no banco de dados. Um registro do tipo endereço conterá um identificador único para o endereço, o nome da rua, o número, o complemento, o telefone (se tiver), o CEP, a cidade, o estado e o país.

• **Tabelas** – uma tabela é um conjunto de registros.

• **Banco de dados** – um banco de dados é um conjunto de tabelas que guardam alguma correlação. Um banco de dados, por exemplo, pode conter uma tabela de endereços de vários empregados, mais outra tabela de dados pessoais destes vários empregados, mais dados profissionais destes.

• **Instâncias** – uma instância de um banco de dados é um conjunto de registros que diz respeito a um contexto qualquer. No banco de dados do exemplo anterior, podemos ter uma instância pra uma empresa com sede em São Paulo e outra instância para a filial da mesma empresa localizada em Curitiba.

• **Índices** – um índice é uma chave de organização de um banco de dados. No exemplo anterior podemos organizar o banco de dados pelo nome dos empregados, ou organizar de outra forma, pelo endereço dos empregados, ou ainda de outra forma: pela profissão dos empregados e assim por diante. A indexação de um banco de dados ajuda a encontrar e correlacionar dados da forma que mais é útil ao usuário.

• **Relações** – relações são formas de se agrupar os dados e os registros. Podemos,

por exemplo, agrupar os funcionários que tenham a profissão de engenheiros com os funcionários que residem em um determinado bairro, gerando uma relação dos engenheiros que trabalham na empresa que residem no bairro especificado.

• **Usuários** – são os indivíduos que de alguma forma têm acesso às informações de um banco de dados e podem realizar operações de busca e correlacionamento neste banco de dados.

• **Administradores** – são usuários responsáveis pelo gerenciamento do sistema de banco de dados e pelos dados ali contidos, bem como dos usuários que têm acesso a este sistema de banco de dados e aos privilégios atribuídos a estes usuários.

Por que proteger bancos de dados?

Hoje em dia, todas as organizações de porte médio ou superior usam bancos de dados para armazenar e utilizar suas informações. Dados financeiros, contábeis, técnicos, de pessoal, entre outros, residem em bancos de dados. O saldo bancário de um correntista é uma entrada em um banco de dados. O acesso aos sistemas, isto é, o usuário e o hash da senha (resultado de uma operação matemática com a senha, que é armazenado no lugar desta) é armazenados em bancos de dados. Os inventários das empresas estão organizados em bancos de dados. As informações dos websites estão armazenadas em bancos de dados. Segundo Aveda (2015, p. 1):

> **Um sistema de gerenciamento de banco de dados é importante porque gerencia dados de forma eficiente e permite aos usuários executar várias tarefas com facilidade. O sistema banco de dados armazena, organiza e gerencia uma grande quantidade de informações dentro de uma única aplicação de software. A utilização deste sistema aumenta a eficiência das operações de negócios e reduz os custos gerais.(2015, p.1)**

Um computador sem banco de dados nada mais é que uma calculadora extremamente rápida, com memória e capacidade para bilhões de cálculos por segundo. Com o banco de dados, o computador passa a ser uma máquina capaz de executar um sistema de informação.

Não é à toa que a maioria dos ataques a sistemas na internet hoje em dia ocorre por meio dos bancos de dados ou neles mirando.

Agora que você já consegue se situar em segurança da informação e entende um pouco melhor o que são e qual a importância dos bancos de dados, nas próximas seções veremos quais são as vulnerabilidades e ameaças específicas a eles e como protegê-los dos impactos resultantes dessas ameaças.

Pesquise mais

Para entender um pouco mais a fundo a importância dos bancos de dados para uma empresa, leia o artigo "*Entenda a importância dos bancos de dados da sua empresa*", que traz importantes informações sobre o assunto GMPE, Gestão de Micro e Pequenas Empresas. Entenda a importância dos bancos de dados da sua empresa, 26 jul. 2014, disponível em: <https://gmpe.com.br/blog/-entenda-a-importancia-do-banco-de-dados-da-sua-empresa-18.html>. Acesso em: 24 jul. 2016.

Sem medo de errar

O jovem empreendedor Jonas é, como todos os que buscam construir seu próprio negócio, afeito a simplificar o cenário, de forma a enxergar apenas os obstáculos diretamente ligados ao alcance de seus objetivos. Ele quer criar um "app" e conectar empresas da cidade de Campos do Jordão. Enxerga como desafios a captação das empresas que disponibilizarão suas promoções e busca por uma forma de conseguir usuários para seus serviços. Jonas busca, também, alavancar investimentos para o negócio e parcerias que sejam benéficas para todos os envolvidos. Em suma: bancos de dados e segurança de informações não ocupam posições privilegiadas em seu rol de preocupações diárias. Quando um empreendedor pensa em segurança, normalmente acredita que está em um carro de Fórmula 1, tentando vencer uma corrida levando seu carro ao limite da velocidade em cada trecho da pista. Enquanto isso, o pessoal da segurança arruma um jeito de colocar quebra-molas ao longo da pista para evitar acidentes.

A primeira tarefa é tirar essa noção da cabeça de Jonas. Fazemos isso mostrando a ele que a função da segurança é encontrar o limite de velocidade que permite que o carro corra o máximo possível sem sofrer um acidente, e isso nem de longe passa por instalar quebra-molas na pista. Ou seja: o objetivo da segurança não é impor empecilhos ao negócio, mas sim dizer até onde o negócio pode ir sem por em risco sua própria existência.

Neste sentido, para auxiliar o empreendedor a entender a importância da segurança dos bancos de dados, você deverá seguir os seguintes passos:

1. Apresentar um resumo do que é e quais são os componentes da segurança da informação, pontuando que a segurança dos bancos de dados é um subconjunto específico desta disciplina, cujos atores são exatamente os mesmos;

2. Apresentar as dimensões da segurança da informação, mostrando sua relevância para que o negócio de Jonas seja um sucesso. Neste sentido, você pode mostrar exemplos de como o comprometimento da confidencialidade, integridade

e disponibilidade (e, adicionalmente, da autenticidade e do não repúdio) podem prejudicar o negócio, mostrando que a segurança da informação vai ajudar a prevenir estes efeitos nocivos.

3. Apresentar o que são bancos de dados e quais são seus componentes, pontuando sua importância para o negócio.

4. Por fim, você poderá apontar o quanto os bancos de dados são relevantes para o negócio de Jonas e qual a importância de protegê-los, encontrando exemplos de bancos de dados nos vários negócios que serão parceiros de Jonas.

Atenção

Não se esqueça que cada um dos negócios de Campos do Jordão, que são parceiros em potencial de Jonas usam bancos de dados a todo momento.

Avançando na prática

Fazer recall ou não fazer recall: eis a questão

Descrição da situação-problema

A empresa M@M Motors, fabricante do Capri, uma caminhonete 4x4 para uso na estrada e no campo, descobriu que em função de uma pequena falha no processo de fabricação de algumas peças o veículo é passível de acidente em algumas situações. Os engenheiros determinaram que se o automóvel ultrapassar os 120km/h com uma carga superior a 300kg, uma falha estrutural provoca vibrações que têm 20% de chance de romper a ponta dianteira esquerda do eixo do veículo.

O Capri foi um sucesso comercial, tendo sido vendido para mais de 350 mil compradores antes que a falha fosse descoberta e corrigida. Agora, a empresa busca entender qual seria o melhor caminho a seguir diante do problema potencial que tem à frente.

Um recall do veículo seria uma operação cara, custando por volta de R$2.000,00 por veículo para se corrigir o problema.

Sua empresa, experiente em questões de análise de risco, foi chamada para explicar a situação em termos de elementos dos riscos envolvidos e sugerir se o recall deve ou não ser feito. Sob seu ponto de vista, quais são os elementos de risco presentes nesta situação? Qual sua recomendação para a M@M Motors?

Resolução da situação-problema

Sob o ponto de vista do risco, você deve, primeiramente, organizar os elementos presentes na situação nos vários fatores que envolvem a questão do risco. Uma organização possível é a seguinte:

• Vulnerabilidade – falha estrutural na ponta de eixo dianteira esquerda.

• Ameaça – quebra da ponta de eixo dianteira esquerda.

• Fonte (ou agente) da ameaça – situação em que o veículo carrega mais de 300kg de carga e ultrapassa os 120km/h de velocidade.

• Impacto – uma quebra na ponta de eixo em velocidade superior a 120km/h provocará a perda de controle do veículo, o que tem grandes chances de gerar um acidente com perda do veículo e da carga, bem como de fatalidades dos ocupantes e de ocupantes de outros veículos atingidos pelo Capri desgovernado.

• Risco – um veículo do tipo caminhonete é projetado para carregar até 2.000kg e, contando com o peso dos ocupantes, devem ser muitos os casos reais em que a carga do Capri ultrapasse os 300kg. A velocidade de 120km/h, apesar de ser proibida em mais de 90% das estradas brasileiras, não é incomum em situações de ultrapassagem. Um veículo do porte de uma caminhonete desgovernado a mais de 120km/h em situação de ultrapassagem (em que obrigatoriamente há outro veículo envolvido) tem alta probabilidade de provocar um acidente grave, com múltiplas perdas de vida, gerando alto risco de acionamento judicial por parte dos parentes das vítimas contra a M@M Motors. Cada acionamento judicial desta natureza tem o potencial de custar mais de R$1.000.000,00 para a empresa.

Diante destas circunstâncias, você deve apresentar os resultados de sua análise ao corpo diretor da M@M Motors e indicar que o recall seja iniciado imediatamente.

Faça valer a pena

1. O Doutor Roberto e seu filho, Dr. Roberto, são sócios na Advogados Associados. Eles são procurados pela Sra. Gisele, uma enfermeira que está sendo processada por seu ex-marido, que tem intenção de obter a posse exclusiva do imóvel que antes pertencera a ambos, e no qual Gisele cria os dois filhos do casal. Ao analisar o caso, o Dr. Roberto decide deixá-lo a cargo do filho, que, apesar de iniciante na carreira, é bastante competente. Além disso, o pai está envolvido com o projeto pessoal de escrever e publicar um livro contando os principais casos que tratou em sua longa e bem-sucedida carreira como advogado.

O contexto acima coloca cada um dos três participantes em um

ponto específico da hierarquia das necessidades criada por Abraham Maslow. Assinale a alternativa que aponta adequadamente o patamar da hierarquia das necessidades de Maslow que cada um ocupa:

a) Dr. Roberto – 3; Dr. Roberto – 4, Gisele – 1

b) Dr. Roberto – 5; Dr. Roberto – 3, Gisele – 2

c) Dr. Roberto – 1; Dr. Roberto – 2, Gisele – 3

d) Dr. Roberto – 5; Dr. Roberto – 4, Gisele – 2

e) Dr. Roberto – 3; Dr. Roberto – 2, Gisele – 1

2. Alice tem um pedido secreto a fazer para Beto e o chama para uma conversa privada, em uma sala de reunião na empresa onde os dois trabalham. Carlos, um funcionário da empresa que não gosta de Beto, se coloca do lado de fora da sala e, com o auxílio de um copo, ouve o pedido que Alice fez a Beto.

Na situação descrita acima, qual dimensão da segurança da informação foi violada?

a) Confidencialidade.

b) Integridade.

c) Disponibilidade.

d) Autenticidade.

e) Não repúdio.

3. Jorge é piloto de avião e opera uma pequena aeronave do tipo "taxi aéreo", no aeroporto de uma grande cidade brasileira. Há alguns anos, Jorge foi diagnosticado com diabetes, uma situação que o obriga a alimentar-se adequadamente a cada 4 horas, pois, do contrário, está sujeito a tonturas ou mesmo a perdas de consciência.

Na situação de Jorge, descrita acima, sua condição de saúde (diabetes) pode ser considerada um(uma):

a) Ameaça.

b) Fonte de ameaça.

c) Vulnerabilidade.

d) Risco.

e) Impacto.

Seção 1.2

Princípios de segurança e principais fragilidades em sistema de bancos de dados

Diálogo aberto

Olá, aluno(a)! Você já reparou que, de vez em quando, sai na imprensa uma notícia informando que uma empresa qualquer — geralmente alguma rede varejista — teve grande quantidade de números de cartão de crédito furtados por bandidos que invadiram a rede? Pois bem, preste atenção que este tipo de incidente de segurança tem acontecido com certa frequência pelo mundo afora. Ocorre que os números de cartão de crédito são armazenados em bancos de dados, os quais podem apresentar falha de segurança, expondo as informações que deveriam ser confidenciais e causando dor de cabeça para as empresas e principalmente para os donos dos cartões expostos.

Jonas, nosso jovem empreendedor, está empenhado em criar um "app" que vai depender pesadamente de bancos de dados e procurou sua empresa para ajudá-lo a proteger sua infraestrutura. Nesta fase, é importante preparar o terreno para as medidas de segurança que no futuro serão implementadas. Jonas precisa entender quais são os princípios de segurança que envolvem os bancos de dados e também precisa saber onde estão e quais são as fragilidades comuns em bancos de dados. Sua tarefa, portanto, é garantir que ele adquira este entendimento e possa usá-lo para desenvolver um aplicativo robusto em todos os aspectos que envolvam bancos de dados, para garantir a segurança. Você deve, após coletar as informações adequadas, realizar uma apresentação para Jonas com as informações sobre o assunto.

A partir de agora, você entenderá o que é segurança em bancos de dados, especificamente. Em seguida, você aprenderá o que deve ser protegido nos bancos de dados, conhecerá as principais fragilidades em bancos de dados e também entenderá quais são as ameaças e os agentes de ameaças aos bancos de dados.

Não pode faltar

Quais são os princípios envolvidos em segurança de sistemas de bancos de dados? E, tão importante quanto os princípios, é preciso saber quais são as fragilidades a que os sistemas de bancos de dados estão sujeitos. Na verdade, estas questões estão intimamente ligadas e as respostas para ambas vêm lado a lado. Vamos, a partir de agora, respondê-las.

O que é segurança em bancos de dados?

Antes de começarmos a analisar aspectos ligados à sua segurança, é importante definirmos o que são e para que servem os bancos de dados. Sharma et al (2010) definem bancos de dados como repositórios de dados criados para dar apoio ao armazenamento eficiente, bem como à busca e manutenção dos dados ali armazenados.

Neste contexto, Elmasri e Navathe (2005) afirmam que o assunto segurança, quando aplicado aos bancos de dados, é bastante amplo e inclui várias questões. Dentre elas, os autores mencionam inicialmente as seguintes questões ligadas à restrição de acesso:

• **Questões legais e éticas** – referem-se ao direito de acesso às informações armazenadas em bancos de dados. Quem pode acessar o quê?

• **Questões políticas (níveis governamental, institucional e corporativo)** – algumas informações devem ser mantidas sigilosas por serem sensíveis: informações de cunho fiscal de uso exclusivo para imposto de renda, informações de crédito do consumidor, informações, prontuários e históricos médicos. O direito político à privacidade deve ser preservado.

• **Questões de níveis de segurança** – a política de segurança da instituição deve estabelecer níveis de sensibilidade das informações, níveis de privilégio de acesso. Esses níveis vão desde informações não classificadas, ou seja, de acesso livre (dados de histórico da instituição presentes no website, por exemplo), passando por vários graus de menor para maior necessidade de sigilo, até chegar em informações ultrassecretas.

Reflita

Como o acesso aos bancos de dados médicos para fins de pesquisa pode conviver eticamente com a necessidade de sigilo individual dos pacientes, cujos dados estão armazenados e precisam ser pesquisados?

Macedo (2011) afirma que a segurança de bancos de dados herda as mesmas tarefas e os mesmos desafios da segurança da informação, a saber: prover a confidencialidade, integridade e disponibilidade dos dados, garantindo ainda a autenticidade das partes e o não repúdio das transações, como vimos anteriormente.

Quando aplicados aos bancos de dados, os conceitos de segurança podem assim ser interpretados (MACEDO, 2011):

• **Confidencialidade** – proteção dos dados contra exposição não autorizada.

• **Integridade** – Garantia de não modificação dos dados armazenados sem a devida autorização.

• **Disponibilidade** – garantir disponibilidade dos dados aos usuários autorizados sem interrupções não programadas.

Devemos ainda adicionar os dois elementos de segurança que dizem respeito aos que geram e acessam os dados:

• **Autenticidade** – garantir que quem acessa ou gera dos dados é a parte autêntica e não um impostor.

• **Não repúdio** – garantir que uma transação qualquer com os dados, uma vez realizada, não possa ser negada por quem a realizou.

O que proteger em sistemas de bancos de dados?

Macedo (2010) estabelece os parâmetros de segurança em bancos de dados sob o ponto de vista de o que deve ser protegido. Sabemos, de antemão, que os dados precisam ser protegidos. No entanto, ainda precisamos entender o que isso significa e como podemos fazê-lo. Poderíamos, por exemplo, juntar os dados protegidos em um HD, remover este HD do computador onde ele se encontra, colocá-lo em um cofre e esconder o cofre. Os dados estariam protegidos? Sim. Nesta situação, os dados seriam úteis para alguma coisa? Não, obviamente. É necessário proteger os dados permitindo que o acesso a eles seja garantido.

Sob este ponto de vista, o autor levanta que o principal item de proteção em bancos de dados é o acesso aos dados, ou seja, o que deve ser protegido é o acesso que se permite aos dados, controlando e estipulando os parâmetros dentro dos quais este acesso é permitido. Estabelece-se, assim, o controle de acesso como o pivô de todos os esforços da segurança (MACEDO, 2010).

Ainda segundo Macedo (2010), o controle de acesso é o conjunto de mecanismos que regulam o acesso aos bancos de dados, impondo aos usuários regras que restringem os privilégios de acesso com base nas necessidades dos usuários, por meio de suas credenciais (nome de usuário e senha de acesso).

Segundo Martins e Candido Jr. (2014), o controle de acesso é a principal ferramenta disponível ao DBA (Data Base Administrator, o administrador dos bancos de dados, responsável tanto pelo gerenciamento como pela segurança dos bancos de dados) para garantir confidencialidade, integridade e disponibilidade dos dados sob sua responsabilidade.

Exemplificando

Nos edifícios comerciais modernos, os crachás dos funcionários utilizam bancos de dados para controlar o acesso desses funcionários, permitindo-lhes a entrada apenas nos locais e andares aos quais estejam autorizados.

Os mecanismos de segurança utilizados pelo DBA para controlar o acesso aos dados podem ser de dois tipos, com duas filosofias de trabalho diferentes (MARTINS; CANDIDO JUNIOR, 2014):

• **Mecanismos discricionários de acesso**: concedem ou negam privilégios ao usuário, a critério do DBA. Privilégios de leitura, inclusão, exclusão, atualização de dados e registros são atribuídos pelo DBA de acordo com as necessidades individuais de cada usuário.

• **Mecanismos obrigatórios de acesso**: os usuários são classificados em categorias diferentes, cada uma com um nível preestabelecido de acesso quanto às possiblidades de leitura, inclusão, exclusão e atualização de dados Os privilégios de acesso concedidos ou negados aos usuários visam proteger os dados de várias formas diferentes, como nos mostram Macedo (2010), Martins e Candido Jr. 2014).

• **Restrição de acesso à manipulação dos dados** – há usuários que podem enxergar dados e com eles realizar operações de combinação. Em outros casos, há usuários que podem, além disso, inserir dados na base. Há, ainda, usuários que podem modificar dados existentes. Por fim, há usuários que podem remover dados da base, além de realizar as demais atividades.

• **Restrição de acesso aos dados** – há usuários que têm restrição de acesso aos dados, podendo ter acesso a apenas um subconjunto desses dados. Outros usuários podem ter acesso a subconjuntos diferentes, ou mesmo a todos os dados da base.

• **Restrição de inferência** – em algumas bases de dados, os usuários poderão ter acesso apenas aos dados de inferência, isto é, aos dados estatísticos coletivos, não sendo permitido o acesso a dados individuais.

• **Restrição de fluxo de dados** – o fluxo de dados ocorre naturalmente entre objetos (processos e aplicativos, por exemplo). O mecanismo de restrição de fluxo de informações tem o objetivo de prevenir que um objeto com menor privilégio de acesso receba informações a que não tem direito, provenientes de um objeto com

maior privilégio. É como se um general obtivesse uma informação estratégica em uma reunião de cúpula e, ao tentar passar esta informação para, digamos, um soldado raso, fosse impedido por uma "polícia militar da informação".

O controle de acesso aos dados é feito por meio de combinações únicas de usuário e senha, que levam o usuário em questão à área do aplicativo que lida diretamente com o banco de dados que lhe atribui os privilégios de acesso a que tem direito.

A proteção dos dados ocorre, também, por meio da criptografia, que, a priori, protege o sigilo (confidencialidade) dos dados, mas não para por aí. Azevedo, Castro e Serrão (2011) afirmam que as proteções fornecidas pela criptografia dos dados garantem:

• **Confidencialidade** – os dados só são acessíveis (legíveis) por quem tem a chave de criptografia para decifrá-los. Garante-se, assim, o sigilo dos dados.

• **Integridade** – a criptografia garante que os dados não serão modificados sem autorização, pois alguém não autorizado só teria acesso aos dados "embaralhados". Qualquer tentativa de modificação nos dados neste estado seria facilmente identificável, pois os dados estariam corrompidos quando decifrados.

• **Autenticidade** – a criptografia utilizada nos dias de hoje para cifrar informações de bancos de dados é a criptografia de chave pública. Este tipo de mecanismo de criptografia é baseado em duas chaves: uma chave pública, utilizada para cifrar a mensagem e verificar a assinatura da mensagem, e outra chave privada, usada para decifrar a mensagem e assiná-la. O processo de assinatura e verificação da assinatura garante a autenticidade dos usuários.

• **Não repúdio** – uma vez assinada uma mensagem pelo usuário – que é o único que tem acesso à sua própria chave privada — não há como este usuário negar que foi ele quem fez a transação de dados.

Outros elementos a serem protegidos, obviamente, são ligados à infraestrutura sobre a qual os bancos de dados estão alicerçados, a saber (ELMASRI; NAVATHE, 2005):

• **Servidores** – o acesso físico e lógico aos servidores onde estão instalados os sistemas de gerenciamento de bancos de dados, bem como onde estão armazenados os dados em si, devem ser protegido.

• **Sistemas operacionais** – Os sistemas operacionais das máquinas onde os sistemas de gerenciamento de bancos de dados estão instalados (bem como onde os dados em si estão armazenados) devem ser protegidos e estar sempre atualizados com os últimos patches de segurança (patches são segmentos de código enviados pelo fabricante do sistema operacional com o objetivo de corrigir alguma vulnerabilidade).

• **Rede** – a proteção à rede é fundamental, pois, por meio dela, não autorizadas

podem ter acesso ao SGBD (Sistema de Gerenciamento de Bancos de Dados) de qualquer parte do mundo. Incidentalmente, a vasta maioria das violações de segurança sobre as quais falaremos posteriormente começam com a violação da segurança da rede.

• **Pessoas** – uma das formas mais simples e efetivas de burlar a segurança de um sistema qualquer é por meio das pessoas. O conhecimento das pessoas deve ser protegido e, para tanto, elas devem saber como evitar que se tornem o elo mais fraco na corrente de segurança.

Assimile

O não repúdio é um elemento de segurança da informação fundamental para as transações feitas em bancos de dados, pois garante que as transações feitas dentro das regras não possam ser renegadas por seu originador.

Fragilidades em bancos de dados

Azevedo, Castro e Serrão (2011) citam as pessoas como ponto inicial de fragilidade dos bancos de dados. Apesar de haver um contingente de usuários que são autorizados a acessar os bancos de dados, existem aqueles que não têm permissão, pois isso, é necessário criar mecanismos para impedir acessos não autorizados. Estes usuários expõem duas fragilidades inerentes aos bancos de dados:

• **Acesso a credenciais por parte de pessoas não autorizadas** – o atacante, ao invés de buscar uma falha na infraestrutura por meio da qual possa atacar o sistema, concentra seus esforços em roubar as credenciais de alguém que de fato esteja autorizado a acessar este sistema.

• **Acesso mal-intencionado por parte de pessoas autorizadas** – de acordo com Dan Codling, ex-chefe da divisão de cibercrimes do FBI, sob o ponto de vista humano, as principais ameaças vêm de dentro e incluem funcionários descontentes em busca de ganhos elícitos, com as informações à sua disposição (ASHFORD, 2015).

Martins e Candido Jr. (2014) apontam a falta de atualizações em software — em toda a cadeia que compõe a infraestrutura de bancos de dados — como uma fonte importante de fragilidades destes sistemas. Para evitar os danos causados por este tipo de fragilidade, dois tipos de medidas são necessárias

1. Manter todo o software da cadeia atualizado – muitas fragilidades são descobertas pelos fabricantes e resolvidas por meio de patches antes de serem exploradas por agentes de ameaça. Infelizmente, não são todos os responsáveis pela infraestrutura de

TI das empresas que se preocupam em manter seus sistemas atualizados. Isto é um problema, pois quanto mais antiga for uma brecha, mais eficientes serão as formas de explorá-la.

2. Adotar software de firewall específico contra ataques ao software – em alguns casos — bem documentados, aliás —, a fragilidade não está no software em si, isto é, não é fruto de alguma vulnerabilidade casual, mas sim de como o software é operado. Um usuário autorizado, com restrição de privilégios adequada, apenas acessando os aplicativos e comandos a que tem acesso, ainda assim pode causar dano ao sistema ou acessar dados aos quais não tenha direito. Isso simplesmente pode ocorrer se o usuário executar comandos de maneira diferente do mecanismo para os quais foram criados. Os firewalls específicos de software avaliam os comandos e as sequências de comandos executados e conseguem identificar quando estas sequências de comandos configuram ataques, bloqueando-os.

Outras fragilidades a serem cuidadas são mais genéricas e dizem respeito à infraestrutura de hardware (servidores) e rede, sob a qual os sistemas de bancos de dados estão implantados. Por mais que a segurança desta infraestrutura tenha melhorado sensivelmente nos últimos anos, ainda deve ser fonte de preocupação constante para os administradores de TI da organização.

Principais ameaças e agentes de ameaças aos bancos de dados

Para identificarmos as ameaças e os agentes de ameaças aos bancos de dados, podemos começar observando as três principais dimensões da segurança (confidencialidade, integridade e disponibilidade) à luz dos bancos de dados e do valor destes bancos de dados para os usuários e para a sociedade em geral.

Em primeiro lugar, por que a confidencialidade dos bancos de dados estaria em cheque? Bem, como afirmam Nakamura e Geus (2007), a informação tem valor para além dos bits e bytes, tendo significado maior para quem a possui e para entidades com as quais essa pessoa se relaciona. O saldo de sua conta bancária não é apenas um número em um registro de um banco de dados: é valor que você e o banco concordam que existem e ao qual você tem direito. Preservar a confidencialidade das informações é garantir que este valor só será acessível por quem tem direito sobre ele.

Neste contexto, a ameaça à confidencialidade dos bancos de dados é a violação do sigilo das informações. É, em outras palavras, a possibilidade de alguém não autorizado acessar informações sobre as quais não tem direito. No exemplo do saldo bancário, a quebra de sigilo implica no conhecimento ilícito por partes não autorizadas de: caminho para acessar a conta em questão; usuário e senha do dono da conta; valores disponíveis para saque; valores investidos e de acesso aos valores.

Os agentes de ameaça, ou seja, aqueles que podem expor o sigilo das informações, são de fácil identificação:

• Cracker com conhecimento cibernético em busca de ganhos ilícitos.

• Funcionários do banco mal-intencionados, em busca de ganhos ilícitos.

• Ex-funcionários do banco que ainda tenham acesso ao sistema, mal-intencionados e em busca de ganhos ilícitos.

• Funcionários de empresas parceiras do banco, mal-intencionados, em busca de ganhos ilícitos.

No caso da **integridade** dos bancos de dados, a ameaça é a violação das informações ali armazenadas, tendo como resultado a modificação não autorizada dos dados armazenados. Segue alguns exemplos no caso da conta bancária (NAKAMURA; GEUS, 2007):

• Inclusão de transações inexistentes de transferência de fundos para outras contas (impacto: redução ou mesmo eliminação total do saldo).

• Inclusão de transações fraudulentas e/ou ilegais no fluxo transacional do usuário (impacto: implicações legais com possibilidade de prisão para o alvo).

Os agentes de ameaça, ou seja, aqueles que podem expor a integridade das informações, são de fácil identificação, são praticamente os mesmo que os descritos para o quesito confidencialidade:

• Cracker com conhecimento cibernético em busca de ganhos ilícitos.

• Funcionários do banco mal-intencionados, em busca de ganhos ilícitos.

• Ex-funcionários do banco que ainda tenham acesso ao sistema, mal-intencionados, e em busca de ganhos ilícitos.

• Funcionários de empresas parceiras do banco, mal-intencionados, em busca de ganhos ilícitos.

• Adversários e/ou inimigos em busca de prejudicar o indivíduo em questão.

No caso da disponibilidade dos bancos de dados, a ameaça é a indisponibilidade dos dados no momento em que o usuário precise acessá-los (e como há usuários ativos 24h/dia, na vasta maioria dos casos, esta disponibilidade deve ser 24x7, ou seja, 24 horas por dia, 7 dias por semana). O exemplo nas transações bancárias a que estamos nos referindo é simples:

• Impossibilidade de o cliente acessar seus dados e, por consequência, impossibilidade de fazer transações (investimentos, resgates, consultas, pagamentos

de contas, transferências etc.).

Os agentes de ameaça, ou seja, aqueles que podem causar rupturas na disponibilidade das informações são:

• Funcionários e ex-funcionários insatisfeitos buscando causar dano à instituição.

• Concorrentes interessados em melhorar relativamente sua reputação causando danos à reputação da instituição que disponibiliza as informações por meio dos bancos de dados.

Pesquise mais

O professor Rafael Obelheiro, da Universidade Estadual de Santa Catarina, publicou um excelente artigo sobre os conceitos importantes do controle de acesso. Confira!

OBELHEIRO, R. **Controle de acesso**. Disponível em: <http://www2.joinville.udesc.br/~dcc2rro/seg-bcc/2009.1/resumo-controle-acesso.pdf>. Acesso em: 9 ago. 2016.

Sem medo de errar

Jonas precisa entender como aplicar os conceitos de segurança que aprendeu ao seu caso específico, isto é, o "app" que está desenvolvendo, bem como à infraestrutura de bancos de dados que dará apoio a este aplicativo. Agora que você já juntou as informações necessárias, é hora de colocá-las em uma apresentação e mostrá-las a Jonas, para que ele fique ciente da necessidade de prezar pela segurança de seu sistema.

Você pode começar a explicar-lhe por meio de uma apresentação que, no que diz respeito aos dados armazenados nos bancos de dados da infraestrutura do aplicativo, ele precisar atentar para três aspectos pertinentes à segurança:

• Aspectos éticos – garantir que o acesso às informações não fira a ética. No caso de seu aplicativo, os usuários deverão concordar explicitamente em fornecer suas coordenadas físicas (onde estão) ao sistema, sabendo que isto significa que o sistema tem ciência de onde se encontram quando estiverem em Campos do Jordão.

• Aspectos legais – o acesso aos dados deve ser feito de forma legal, sempre para fins previstos e autorizado pela lei. No caso de Jonas, as informações a serem passadas são legais e legítimas: ofertas e condições de estabelecimentos comerciais.

• Questões de níveis de segurança – Jonas deve ser informado que a infraestrutura de seu app deve prever vários níveis de segurança, desde o administrador dos bancos

de dados que deve ter acesso a todo o sistema, inclusive a todos os dados, até o usuário final, que deve ter acesso apenas indireto aos dados.

Em seguida você deverá mostrar a Jonas que a segurança de bancos de dados alicerça-se sobre o controle de acesso, e que este controle é fundamental para que os dados se mantenham seguros. Vale ressaltar com Jonas que, no processo de controle de acesso aos bancos de dados, ele deverá se preocupar com dois tipos de restrição importantes:

• **Controle de acesso à manipulação dos dados** – os funcionários e parceiros comerciais de Jonas devem ser cadastrados no sistema de acordo com os privilégios de manipulação de dados permitidos a eles. Empresas parceiras deverão ter acesso à manipulação apenas dos dados gerados por elas mesmas (ofertas, artigos, preços, prazos de vigência etc.); funcionários de Jonas deverão ter acesso aos dados do próprio aplicativo e acesso de leitura aos dados enviados pelos parceiros (não lhes sendo permitido, por exemplo, alterá-los, o que feriria a integridade dos mesmos); usuários devem ter acesso de escrita apenas aos seus dados de cadastro e acesso de leitura aos dados que lhes forem apresentados.

• **Controle de acesso aos dados** – da mesma forma que o controle de acesso aos dados deve ser restrito, o acesso dos funcionários aos dados globais também devem ser de acordo com uma política de segurança da informação, os parceiros de negócios podem ter o acesso restrito aos seus próprios dados e os clientes poderão ter acesso aos dados que lhes forem apresentados à medida que se moverem pela cidade.

Em seguida, você deverá explicar a Jonas que além da segurança lógica dos bancos de dados, ele deverá se preocupar em assegurar também a infraestrutura e o ambiente físico. Isto inclui assegurar:

• **Sistemas operacionais** – sempre aplicar as últimas atualizações e manter-se atento às vulnerabilidades e aos boletins dos fabricantes.

• **Servidores** – o acesso físico aos servidores deve ser garantido.

• **Redes** – os equipamentos e protocolos devem ser devidamente cuidados para que não apresentem vulnerabilidades.

Finalizando, você poderá informar a Jonas a respeito das principais ameaças e agentes de ameaça aos bancos de dados, sempre os vinculando às dimensões da segurança;

Confidencialidade:

• Ameaças: exposição de informações sigilosas a pessoas não autorizadas.

• Agentes de ameaças: bandidos com conhecimento cibernético, funcionários e

ex-funcionários mal-intencionados.

• Integridade

• Ameaças: alteração não autorizada de informações e transações.

• Agentes de ameaças: bandidos com conhecimento cibernético, funcionários e ex-funcionários mal-intencionados, adversários e/ou inimigos.

• Disponibilidade

• Ameaças: indisponibilidade dos dados e serviços baseados nestes dados (negação de serviços).

•Agentes de ameaças: bandidos com conhecimento cibernético, funcionários e ex-funcionários insatisfeitos, concorrentes buscando danificar a reputação da empresa.

Atenção

Segurança de sistemas de bancos de dados é um caso especial da segurança da informação.

Avançando na prática

A ex-funcionária insatisfeita

Descrição da situação-problema

A analista de sistemas Gerusalina atuou como DBA (Administradora de Bancos de Dados) da loja virtual durante mais de 10 anos, com excelente desempenho. Após algumas mudanças estruturais na empresa, associadas a processos de avaliação de desempenho, Gerusalina foi demitida. Esta ficou bastante furiosa com sua dispensa e acha que a empresa não foi justa com uma funcionária que deu mais de 10 anos de sua vida ao seu trabalho, só porque cometeu alguns deslizes, causando prejuízos e deixando alguns clientes descontentes com a empresa. Infelizmente, os processos internos da Brilhante não eram robustos e a ex-funcionária descobriu, depois de alguns dias em casa, que ainda tinha acesso completo aos sistemas de bancos de dados da Brilhante.

Nesta situação, quais são as vulnerabilidades, as ameaças, os agentes de ameaça e os impactos possíveis desse acesso?

Resolução da situação-problema

O caso descrito na situação-problema infelizmente é grave e bastante comum. Vejamos as respostas às questões que a situação gerou:

• **Vulnerabilidade**: o processo de desligamento do funcionário apresenta uma vulnerabilidade enorme, pois a funcionária deveria ter tido seu acesso imediatamente revogado a partir do momento em que foi desligada de seu cargo. O acesso depois do desligamento é uma vulnerabilidade de processo inaceitável em uma empresa.

• **Ameaças**: com acesso de administradora de bancos de dados, Gerusalina pode realizar qualquer ação que quiser nos bancos de dados da loja virtual. Algumas das ameaças que podem surgir desta situação são:

• **Comprometimento de informações sigilosas**: Gerusalina pode ter acesso, por exemplo, às listas de preços e promoções futuras da Brilhante, pode ter acesso a negociações sigilosas da loja virtual com seus fornecedores, pode ter acesso a endereços, telefones e dados de clientes VIP (e dos demais clientes também) e pode ter acesso a informações de cartão de crédito dos clientes.

• **Comprometimento da integridade das informações**: a ex-funcionária pode gerar transações inexistentes como por exemplos, vendas de joias para clientes que não as compraram, o desvio de entregas para endereços falsos, criar transações entre a Brilhante e seus fornecedores que não ocorreram, entre outras.

• **Comprometimento da disponibilidade**: Gerusalina pode gerar problemas enormes para a loja virtual também cortando o acesso aos bancos de dados, o que pode ocorrer se a ex-funcionária, por exemplo, remover as contas de acesso dos demais funcionários da empresa. Ela pode, ainda, apagar todos os dados contidos nos bancos, destruindo registros de mercadorias, transações, dados de clientes, entre outros.

Faça valer a pena

1. Algumas informações devem ser mantidas sigilosas por serem sensíveis (informações de cunho fiscal de uso exclusivo para imposto de renda, informações de crédito do consumidor, informações, prontuários e históricos médicos). O direito político à privacidade deve ser preservado.

Quando nos referimos aos elementos acima, a que tipo de questões de restrição de acesso estamos falando?

a) Questões legais.

b) Questões éticas.

c) Questões morais.

d) Questões políticas.

e) Questões técnicas.

2. Azevedo, Castro e Serrão (2011) citam as pessoas como ponto inicial de fragilidade dos bancos de dados. Apesar de haver um contingente de usuários que são autorizados a acessar os bancos de dados, existem aqueles que não têm permissão, por isso é necessário criar mecanismos para impedir acessos não autorizados.

Estes usuários expõem duas fragilidades inerentes aos bancos de dados. São elas:

a) Acesso a credenciais próprias por parte de pessoas autorizadas e acesso mal-intencionado por parte de pessoas sem acesso.

b) Acesso por parte de programas automatizados e acesso por parte de dispositivos defeituosos.

c) Acesso a credenciais por parte de pessoas não autorizadas e acesso mal-intencionado por parte de pessoas autorizadas.

d) Acesso por parte de ex-funcionários cujas credenciais foram imediatamente revogadas e acesso por parte de parentes sem acesso aos sistemas.

e) Acesso por parte de clientes e acesso por parte de fornecedores.

3. Para identificarmos as ameaças e os agentes de ameaças aos bancos de dados, podemos começar observando as três principais dimensões da segurança (confidencialidade, integridade e disponibilidade) à luz dos bancos de dados e do valor destes dados para os usuários (e para a sociedade em geral).

Observe os elementos de segurança de bancos de dados na coluna da esquerda e os exemplos de ameaças no caso de uma loja on-line, na coluna da direita:

I. Confidencialidade	A. O cliente tenta buscar por um produto e recebe uma página vazia
II. Integridade	B. O cliente descobre que os dados de seu cartão de crédito estão nas mãos de bandidos
III. Disponibilidade	C. O cliente recebe a conta de um produto que não comprou

A alternativa que faz a correspondência correta entre as colunas é:

a) I-A, II-B, III-C.

b) I-A, II-C, III-B.

c) I-B, II-A, III-C.

d) I-C, II-B, III-A.

e) I-B, II-C, III-A

Seção 1.3

Mecanismos de segurança de sistemas de bancos de dados: casos reais de problemas na segurança de sistemas de banco de dados

Diálogo aberto

Olá, mais uma vez!

Estamos chegando ao final desta primeira unidade de estudo, em que fazemos uma contextualização da segurança em sistemas de bancos de dados. E, agora que você já conhece um pouco mais acerca dos conceitos que alicerçam este assunto, está na hora de tirarmos estas questões do campo teórico e trazê-las um pouco mais para próximo de nós todos, observando de perto alguns casos reais em que a violação de bancos de dados ocorreu, trazendo enormes prejuízos para usuários e para organizações no mundo todo.

Não pense que segurança de bancos de dados é um assunto distante e que não há como trazer esta questão para perto de nós. Para provar isso, faça um pequeno exercício: no Google, busque os termos "fraude" e "cartão de crédito", por exemplo, e veja a quantidade de artigos e vídeos disponíveis mostrando como o assunto é sério e comum.

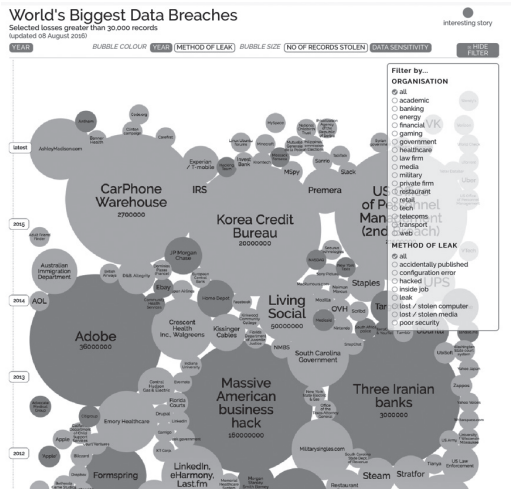
Bem, mas o fato é que Jonas, o empreendedor de Campos do Jordão, mesmo depois de ter entendido o que é segurança de sistemas de bancos de dados, ainda acha que não precisa se preocupar com o assunto. Como ele não tem tempo de fazer pesquisas sobre o assunto, você decidiu mostrar-lhe casos reais em que bancos de dados de clientes foram violados por bandidos, causando milhões em prejuízos, bem como as lições aprendidas com cada caso.

Então, vamos conhecer os casos corriqueiros e, infelizmente, cotidianos sobre o assunto.

Não pode faltar

Segundo Armerding (2012), violações de segurança ocorrem em números expressivos e em locais variados demais para que se mantenha uma conta precisa sobre elas. De fato, ao longo da história recente — mais especificamente desde a popularização da web — o número de violações só fez crescer. De acordo com pesquisa recém-publicada pelo grupo Information is Beautiful (2016), foram 220 casos nos quais mais de 30 mil registros foram ilegalmente obtidos e/ou expostos, entre os anos de 2004 e 2016, no mundo todo.

Figura 1.3 | Um mapa das violações recentes de bancos de dados



Fonte: <http://www.informationisbeautiful.net/visualizations/worlds-pbiggest-data-breaches-hacks/>. Acesso em: 13 set. 2016.

Os casos são muitos e, em diversas situações, os prejuízos gerados foram de milhões de dólares, sem falar nos problemas decorrentes para as empresas, como a perda de reputação.

A partir de agora veremos alguns destes casos. Foram escolhidos pela relevância dentro do assunto "segurança de bancos de dados", bem como pelos fatores que proporcionaram sua ocorrência. Alguns são mais antigos, e outros nem tanto, mas todos trazem valiosas lições para quem busca assegurar seus bancos de dados, uma vez que os erros cometidos nos casos visitados podem ser evitados se tivermos o cuidado devido.

O caso da America Online, 2004

- **Vulnerabilidade**: acesso a login/senha de um funcionário (processo).

• **Agente de ameaça**: ex-funcionário Jason Smathers.

• **Impacto**: 92.000.000 milhões de registros de clientes (nome, e-mail, endereço) foram roubados e vendidos a spammers (empresas especialistas no envio de mensagens de e-mail não solicitadas), que usaram os registros para envio de mais de 7 bilhões de mensagens de SPAM, gerando prejuízos de mais de 400 mil dólares para a Aol.

Segundo Ashford (2015), as maiores ameaças à segurança da informação vêm de dentro da própria organização, e este certamente é um caso contundente deste tipo de violação. Jason Smathers, que havia sido demitido da Aol. em 2003, conseguiu "emprestados" o login e a senha de um colega e, com estas informações, conseguiu furtar 92 milhões de dados de usuários, vendendo-os por 28 mil dólares para um grupo de spammers que queria enviar suas mensagens sobre jogos de cartas on-line para os clientes da Aol. (na época, dona do maior rol de clientes de acesso on-line do mundo). Resultado: os clientes passaram a receber periodicamente e-mails oferecendo sites de jogatina on-line, entupindo suas caixas de mensagem. As reclamações foram tantas que a Aol. passou a investigar a origem do caso e chegou até o colega de Smathers que havia "emprestado" as credenciais. Confessado o "empréstimo", a Aol. rapidamente chegou a Smathers. O ex-funcionário foi processado e condenado a pagar três vezes o valor que havia recebido como pagamento pelos spammers, ou seja, a soma de 84 mil dólares.

Uma coisa interessante a observar neste caso é que o valor recebido pelo crime foi irrisório em função do valor do banco de dados roubado. Só o prejuízo causado à Aol. (400 mil dólares, na conta mais conservadora) supera e muito o valor recebido por Smathers e, estima-se, o valor recebido pelos spammers, uma vez que se apenas uma fração dos clientes frequentaram e jogaram nos cassinos on-line anunciados, o valor faturado foi bem maior que os 28 mil dólares pagos.

Outro fator importante a observar é que ninguém entre spammers e anunciantes foi punido no caso: toda a culpa recaiu sobre Smathers. E todo o prejuízo ficou por conta da Aol. e dos clientes que passaram pelo inconveniente de receber, por meses mensagens, não solicitadas geradas em função do caso (NBCNEWS, 2005).

• **Lições aprendidas**: a organização deve fornecer treinamento claro para seus funcionários sobre os perigos de compartilharem informações sigilosas com ex-colegas (usuário e senha de sistemas internos, como no caso). Ex-funcionários, ainda que mantenham amizades na empresa, devem ser vistos como agentes externos potencialmente mais perigosos que outros e que podem causar dano, pois já tiveram experiência na organização, sabem onde as coisas estão e como funcionam.

Assimile

A maioria dos agentes de ameaça — e certamente os mais perigosos — vem de dentro da organização ou em algum momento pertenceram a ela.

O caso da TJMaxx, 2007

• **Vulnerabilidade** – falhas de segurança em redes wi-fi.

• **Agente de ameaça** – cyber-bandido Albert Gonzalez.

• **Impacto** – 45,7 milhões de credenciais completas de cartões de crédito e débito roubadas, gerando mais de 200 milhões de dólares em prejuízos.

Em janeiro de 2007, o grupo varejista norte-americano TJMaxx anunciou que 45,7 milhões de credenciais completas de cartão de crédito e débito foram roubadas de seus bancos de dados, expondo dados financeiros de clientes nos EUA e na Europa. O curioso deste caso é que o roubo não ocorreu de uma vez só, mas sim ao longo de dois anos.

Um jovem hacker que trabalhava como informante remunerado para o Serviço Secreto Americano, de nome Albert Gonzalez, usou um método simples para comprometer a segurança da TJMaxx: ele saía de carro com seu dispositivo wi-fi (um laptop) em busca de redes wireless abertas ou com segurança falha. Utilizando alguns procedimentos de teste, ele rapidamente conseguia avaliar se a rede era bem protegida ou não, invadindo aquelas que fossem precariamente protegidas. Chegou por acaso a um local onde conseguiu entrar na rede de uma loja da TJMaxx e percebeu que esta rede teria potencial para lhe dar informações valiosas. Em pouco tempo, conseguiu chegar até os bancos de dados locais da loja, que não eram protegidos, e identificou que lá havia credenciais de cartão de crédito dos clientes da loja. Passou, então, a sistematicamente roubar estes dados e a usar seu conhecimento para invadir outras lojas da rede e a roubar dados dessas lojas. Nos dois anos em que esteve ativo — nos quais a TJMaxx não foi capaz sequer de saber que estava sendo invadida e roubada — ele identificou formas de passar de uma rede para outra, estendendo seu alcance para muito além de sua localização geográfica, no estado de Nova Jersey, nos EUA.

Durante o processo judicial vieram à tona dados de outras investigações contra Gonzalez, implicando-o em outros casos de roubos digitais de cartões. Estima-se que ele tenha sido responsável pelo roubo de mais de 170 milhões de cartões no mundo todo, até ser preso. hoje, ele cumpre uma pena de 20 anos de prisão, iniciada em 2010 (ZETTER, 2010).

Lições aprendidas: a rede wi-fi e todos os elementos de perímetro (por meio dos quais se pode acessar a rede) devem ser motivo de constante preocupação por parte da segurança da empresa. Uma rede wi-fi insegura é uma porta aberta por onde

qualquer um pode entrar. Outra lição: não é porque não se vê nada acontecendo que nada esteja acontecendo. Gonzalez passou um tempo enorme invadindo as redes da TJMaxx sem que ninguém percebesse.

Reflita

Será que segurança de wi-fi tem alguma coisa a ver com segurança de banco de dados? Será que a instituição que mantém bancos de dados de valor deve se preocupar com o acesso de suas redes sem fio?

O caso da Advocate Health Care, 2012

• **Vulnerabilidade** – segurança física falha e falta de criptografia nos bancos de dados.

• **Agente de ameaça** – bandido desconhecido.

• **Impacto** – 4 milhões de registros médicos de pacientes do grupo foram comprometidos, violando a privacidade dessas pessoas e gerando vários processos civis contra a empresa.

Em 15 de julho de 2012, quatro computadores foram roubados de um escritório administrativo da empresa, que é uma operadora de plano de saúde nos EUA. O resultado foi a exposição de 4 milhões de registros de pacientes, contendo histórico médico, condição física, tratamentos pregressos, medicações pregressas e atuais, entre outras informações sensíveis e de cunho sigiloso. O problema não parou na fraca segurança física do local onde se encontravam os computadores, mas se agravou ainda mais porque os bancos de dados contidos nestes computadores não eram protegidos por criptografia, o que permitiu não só o acesso físico às máquinas, mas também o acesso lógico aos dados.

A empresa teve de pagar uma multa de 5,5 milhões de dólares pelas violações de privacidade, escapando de processos individuais, que certamente gerariam prejuízos maiores.

O perpetrador do roubo nunca foi apreendido pelas autoridades e não há pistas sobre quem tenha sido o responsável ou quem tenha orquestrado a ação (CONN, 2013).

• **Lições aprendidas**: não devemos negligenciar a segurança física. Computadores com informações sensíveis devem ser protegidos em salas cofre, sempre. Outra lição (e talvez mais importante que a primeira): é impensável manter um banco de dados com informações sensíveis sem que as mesmas sejam protegidas por criptografia de boa qualidade.

Exemplificando

Uma forma bastante interessante de se manter a segurança de bancos de dados e de outros aspectos da segurança da informação, também, é a política de mesa limpa, em voga em várias empresas de tecnologia.

Um exemplo em nosso país é a IBM Brasil, braço brasileiro da gigante americana. Ao final do dia, após o expediente, um grupo de funcionários da segurança visita todas as mesas e checa todos os papeis. Quando encontram algum documento marcado como "Confidencial", ele é confiscado e o funcionário deve buscá-lo — acompanhado de seu superior direto — na sala da segurança e recebendo uma reprimenda pelo erro.

O caso do Facebook, 2013

• **Vulnerabilidade** – erro na lógica de programação.

• **Agente de ameaça** – usuários do Facebook.

• **Impacto** – um erro na lógica de programação do acesso aos dados pessoais, por um breve tempo levava o usuário que ali clicasse à lista de e-mails e números telefônicos de todos os componentes de sua lista de amigos. O erro foi comentado na própria rede social e, em poucas horas, estima-se que 6 milhões de dados considerados sigilosos pelo Facebook tenham sido comprometidos.

Não são só as ações maliciosas que podem causar dano: os erros não intencionais também podem. Foi o que aconteceu em junho de 2013, quando uma atualização interna no módulo de configuração de perfil do usuário chamou uma rotina de uso interno da empresa, que acessa os dados pessoais ocultos dos usuários, tais como e-mail e número telefônico.

O erro permitia que um usuário alterando seu perfil tivesse acesso aos dados pessoais ocultos de todos em sua lista de amigos. Ocorre que não há lugar melhor para se divulgar uma vulnerabilidade dessas do que o próprio Facebook, e foi isso que os usuários começaram a fazer. Em poucas horas, estima-se que 6 milhões de registros de usuários tenham sido comprometidos, antes que o erro fosse descoberto e corrigido.

Um dado interessante é que a vulnerabilidade ficou ativa durante mais de um ano até que alguém a descobrisse e identificasse uma maneira de usá-la. Esta é uma preocupação enorme para as empresas que desenvolvem software: os "erros dormentes", ou seja, vulnerabilidades e erros no software que ninguém conhece e que ficam desconhecidos até que tenham sido explorados (SHIH, 2013).

• **Lições aprendidas**: testar software é uma atividade tão séria e importante quanto

criar software. Outra lição: não é porque seu software roda por longos períodos de tempo sem percalços que não haja erros escondidos.

Pesquise mais

Em 2015, a consultoria Proof publicou um artigo interessante acerca do custo, para as empresas, das violações de bancos de dados. Leia mais a respeito em "*Custo das Violações de dados no Brasil*", disponível em: <http://www.proof.com.br/blog/seguranca-da-informacao/custo-das-violacoes-no-brasil/>. Acesso em: 20 ago. 2016.

O caso do banco de dados dos eleitores dos EUA, 2015

• **Vulnerabilidade**: erro na configuração do banco de dados.

• **Agente de Ameaça**: consultor de segurança Chris Vickery.

• **Impacto**: consultor conseguiu acesso à base completa, contendo 191 milhões de registros de todos os eleitores dos EUA. Não se sabe se outros indivíduos conseguiram o mesmo acesso.

Em dezembro de 2015, o consultor de segurança Chris Vickery, que buscava falhas em bancos de dados para alertar seus clientes para a necessidade de melhorarem a segurança de seus ambientes, inadvertidamente conseguiu acesso a todo o banco de dados de eleitores dos EUA, demorando mais de 24 horas para fazer download de todos os registros. Até o momento, não se sabe se mais alguém conseguiu acessar e descarregar os dados como fez Vickery, mas a possibilidade certamente existe.

O consultor conseguiu acesso porque uma falha na configuração do banco de dados permitia acesso sem checagem de credenciais (FINKLE; VOLZ, 2015).

• **Lições aprendidas**: por mais óbvio que seja um passo na implantação de bancos de dados, por mais triviais que pareçam as atividades, elas devem ser planejadas, realizadas e conferidas. Apesar de parecer óbvia, esta lição é relevante, como Chris Vickery tão eloquentemente demonstrou.

Faça você mesmo

No infográfico da Information is Beautiful há centenas de casos de violações de bancos de dados. Explore o gráfico e identifique novas situações que certamente apresentarão elementos úteis ao aprendizado de segurança em bancos de dados. Disponível em: <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>. Acesso em: 20 ago. 2016.

Finalizando

Aprendemos aqui vários pontos importantes sobre segurança de bancos de dados, que devemos ter em mente sempre, quando tratamos do assunto. Vejamos:

• Engenharia social é provavelmente a principal fonte de problemas para um sistema de bancos de dados; e a única prevenção é o treinamento constante dos colaboradores.

• As vulnerabilidades são muitas, potencialmente, e vale o jargão que usamos em segurança da informação: a corrente sempre quebra no elo mais fraco. De nada adianta, por exemplo, ter uma sala-cofre de altíssima tecnologia para garantir que ninguém roubará os computadores se a rede wi-fi é vulnerável e o hacker pode furtar os dados sem estar fisicamente presente.

• Criptografia não é só uma boa ideia: é mandatório.

• Erros de software devem ser perseguidos sem descanso o tempo todo. Neste sentido, os três imperativos são: testar, testar e testar.

• Erros de configuração podem entregar dados facilmente a bandidos, sem que eles tenham de se esforçar. Novamente vale a máxima do teste.

Sem medo de errar

Se, mesmo depois de entender a seriedade nos conceitos de segurança da informação e em bancos de dados, Jonas ainda não está sensibilizado pela necessidade de se preocupar — e muito — com o assunto, agora é a hora de usar a tática da conscientização pelo medo. Sim, pois quem não tem medo de ter seus bancos de dados violados não está encarando a segurança de maneira responsável.

Você deve apresentar a Jonas alguns casos em que esta segurança foi violada e apresentar os perigos por meio dos prejuízos reais e potenciais e que foram gerados pelos fatos. Uma estratégia interessante para convencê-lo é a seguinte (e, obviamente, você pode pensar em outras formas de fazê-lo, se quiser):

1. Comece mostrando a Jonas que a segurança de bancos de dados depende de vários aspectos de segurança, pois os bancos de dados estão sempre no centro das operações, e há várias camadas a serem ultrapassadas até chegarmos até eles. Ocorre, porém, que à medida que atravessamos estas camadas, já estamos mais próximos, com acesso a mais recursos que nos ajudam a penetrar mais fundo as defesas.

2. Mostre a Jonas que há vários pontos pelos quais os dados podem vazar, e que em todos eles os resultados podem ser desastrosos.

3. Apresente a ele exemplos de violações de dados que ocorreram de formas variadas (os exemplos providos no "Não Pode Faltar" são excelentes pontos de partida). Utilize a tabela a seguir para organizar os casos na hora de apresentá-los:

Caso (Ano)	Vulnerabilidade	Agente de Ameaça	Impacto	Descrição

Atenção

Há uma variedade enorme de vulnerabilidades, agentes de ameaça, impactos e histórias por trás das violações de segurança. E, principalmente, de lições a serem aprendidas com cada caso.

Avançando na prática

Ajudando o cliente assustado

Descrição da situação-problema

O lojista Breno, há alguns meses abriu um site para comercializar também on-line os produtos que vende em sua loja. Ele acaba de sair assustado de uma apresentação a que foi convidado por seu amigo Jonas (um empreendedor), em que viu vários casos de "horror", nos quais empresas e organizações viram seus bancos de dados violados.

Na saída, ele já demonstrou a preocupação que certamente lhe tiraria o sono por muitos dias: como fazer para assegurar seu ambiente e, sobretudo, seus bancos de dados.

Breno viu apresentações sobre os seguintes casos:

- Aol., 2004;
- TJMaxx, 2007.

Ele está muito preocupado com as vulnerabilidades e com os agentes de ameaça que encontrou em cada um destes casos. Sua tarefa é apresentar a Breno um caminho que pode tomar no sentido de proteger seus bancos de dados

Resolução da situação-problema

Para solucionar esta questão, isto é, para que Breno fique mais tranquilo, você deve apontar formas de evitar os problemas em duas frentes:

• mitigar ou eliminar as vulnerabilidades;

• impedir que os agentes de ameaça ajam no ambiente.

Para tanto, podemos apontar os seguintes caminhos nos casos citados:

• Aol., 2004

• **Vulnerabilidade**: no caso da Aol., a vulnerabilidade era o acesso a informações de login por parte de pessoas não autorizadas. O que aponta para uma falha nos processos de segurança da Aol. Os profissionais devem ser devidamente treinados a não fornecer suas credenciais a ninguém, sendo inclusive passíveis de processos judiciais caso isto ocorra. Não há como remover 100% desta vulnerabilidade, mas o treinamento e a passividade judicial são ferramentas efetivas na minimização de sua probabilidade de incidência.

• **Agente de ameaça**: o treinamento quanto aos perigos da engenharia social (terceiros que se aproximam dos funcionários com objetivos de amizade, mas que, no fundo, escondem o interesse em ter acesso ilícito a recursos e informações) é essencial para evitar que ex-funcionários (e outros agentes) tenham acesso a informações que possam colocar a organização em risco.

• TJMaxx, 2007

• **Vulnerabilidade**: no caso da TJMaxx, a vulnerabilidade era um perímetro de rede (wi-fi, mais especificamente). É fundamental, neste caso, que todos os pontos de entrada sejam assegurados contra vulnerabilidades, isto é, estejam atualizados e sejam regularmente testados. Firewall em dia e um bom IDS/IPS (Intrusion Detection/Prevention System) também são úteis na prevenção, assim como manter todos os softwares básicos (sistemas operacionais, pilhas de protocolos etc.) atualizados.

• **Agentes de ameaça**: no caso, estamos falando de um hacker e não há como remover esta possibilidade. Ocorre que hackers são, como qualquer outro tipo de bandido, afeitos ao caminho de menor esforço. Eles vão mexer em uma rede por algum tempo, usando suas ferramentas preferidas. Se encontrarem um caminho possível, insistem, claro, mas, se não acham um caminho viável em suas primeiras tentativas, vão passar aos próximos alvos potenciais (são tantos, afinal de contas!), o que indica uma ação: manter as portas de entrada no sistema sempre muito bem fechadas e guardadas.

As informações coletadas transmitem uma mensagem bastante clara, que você pode reforçar junto a Breno: antes de nos assustarmos com as notícias de violações de segurança, temos que buscar aprender com elas. Há um antigo ditado anônimo que afirma que inteligência é aprender com os próprios erros, enquanto sabedoria é aprender com os erros dos outros. Os casos que chegaram à atenção de Breno são

claros neste sentido. As vulnerabilidades e os agentes de ameaça que contribuíram para todos os transtornos sofridos por Aol. e TJMaxx devem servir de insumo para que Breno tome as ações necessárias, para melhorar seu próprio ambiente e não vir a sofrer problemas semelhantes no futuro.

Faça valer a pena

1. Segundo Armerding (2012), violações de segurança ocorrem em números expressivos e em locais variados demais para que se mantenha uma conta precisa. De fato, ao longo da história recente — mais especificamente desde a popularização da web — o número de violações cresceu. De acordo com pesquisa recém-publicada pelo grupo Information is Beautiful (2016), foram _____ casos que mais de _____ registros foram ilegalmente obtidos e/ou expostos entre os anos de ____ e ____, no mundo todo.

Levando em consideração as informações da pesquisa do grupo Information is Beautiful, qual das alternativas apresenta elementos que adequadamente preenchem as lacunas?

a) 220, 10 mil, 2004, 2016.

b) 220, 30 mil, 2004, 2016.

c) 200, 100 mil, 2000, 2016.

d) 200, 30 mil, 2004, 2016.

e) 220, 100 mil, 2004, 2016.

2. No ano de 2004, 92 milhões de registros de clientes (nome, e-mail, endereço) da empresa americana Aol. foram roubados e vendidos a spammers (empresas especialistas no envio de mensagens de e-mail não solicitadas). Os spammers usaram os registros para envio de mais de 7 bilhões de mensagens de spam, gerando prejuízos de mais de 400 mil dólares para a Aol.

No caso da Aol. mencionado acima, o agente de ameaça responsável por concretizar a ameaça e gerar os impactos relacionados foi:

a) Um hacker profissional.

b) Um acidente.

c) Um usuário do sistema.

d) Um ex-funcionário.

e) Um executivo da empresa.

3. Um erro na lógica de programação do acesso aos dados pessoais, por um breve tempo, levava o usuário que ali clicasse à lista de e-mails e números telefônicos de todos os componentes de sua lista de amigos. O erro foi comentado na própria rede social e em poucas horas estima-se que 6 milhões de dados considerados sigilosos pelo Facebook tenham sido comprometidos.

Com relação à violação do banco de dados com informações de contato de usuários do Facebook, em 2013, qual foi o fato mais curioso acerca da situação?

a) Um hacker trabalhou mais de um ano até descobrir a vulnerabilidade.

b) O Facebook havia corrigido a vulnerabilidade havia um ano quando a mesma foi descoberta e explorada.

c) A vulnerabilidade ficou mais de um ano ativa antes de ser descoberta e explorada.

d) O Facebook ficou mais de um ano tentando resolver a vulnerabilidade.

e) Os usuários que descobriram a vulnerabilidade a exploraram por mais de um ano.

Referências

ARMERDING, Taylor. The 15 worst data security breaches of the 21st Century, **Revista CSO On-Line**, 15 fev. 2012. Disponível em: <http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html>. Acesso em: 19 ago. 2016.

ASHFORD, Warwick. Internal threat among biggest cyber security challenges, says former FBI investigator. **Computer Weekly**, 29 jun. 2015. Disponível em: <http://www.computerweekly.com/news/4500248908/Internal-threat-among-biggest-cyber-security-challenges-says-former-FBI-investigator>. Acesso em: 4 ago. 2016.

AVEDA, Scott. What is the importance of a database Management System? **Linkedin**. Disponível em: <https://www.linkedin.com/pulse/what-importance-database-management-system-scott-aveda>. Acesso em: 24 jul. 2016.

BROSTOFF, A. **Improving password system effectiveness**. 2004. 316 f. Tese (Doutorado em Ciência da Computação) — Departamento de Ciência da Computação, Universidade de Londres, Londres, 2004.

CONN, Joseph. Advocate data breach highlights lack of encryption, a widespread issue, **Modern Healthcare**, 30 ago. 2013. Disponível em: <http://www.modernhealthcare.com/article/20130830/NEWS/308309953>. Acesso em: 20 ago. 2016.

ELMASRI, Ramez; NAVATHE, Shamkant B. **Sistemas de bancos de dados**. São Paulo: Pearson Addison Wesley, 2005.

MACEDO, Diego. **Conceitos sobre segurança em bancos de dados**. Disponível em: <http://www.diegomacedo.com.br/conceitos-sobre-seguranca-em-banco-de-dados/?print=pdf>. Acesso em: 1 ago. 2016.

MARTINS, Fábio Crepaldi; CANDIDO JUNIOR, Eli. Segurança em banco de dados: conceitos e aplicações. **Revista ETIC**, Presidente Prudente, v. 10, n. 10, out. 2014. Disponível em: <http://intertemas.toledoprudente.edu.br/revista/index.php/ETIC/article/viewFile/4412/4172>. Acesso em: 2 ago. 2016.

MASLOW, Abraham Harold. A theory of human motivation. **Revista Psychological Review**, v. 50, n. 4, p. 370-396, 1943.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec. 2007.

NBC NEWS, **Ex-AOL worker who stole mail list sentenced**, 17 ago. 2005. Disponível em:

<http://www.nbcnews.com/id/8985989/#.V7hpqWXcvNV>. Acesso em: 20 ago. 2016.

NIST – National Institute of Standards and Technology, **NIST Special Publication 800-30 – Guide For Conducting Risck Assessment**. Revision 1, Washington: NIST Publications, 2012.

SHARMA, Neeraj et al. **Database fundamentals**. Toronto: DB2University, 2010.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. São Paulo: Campus, 2014.

SHIH, Gerry. Facebook admits year-long data breach exposed 6 million users, **Reuters**, 21 jun. 2013. Disponível em: <http://www.reuters.com/article/net-us-facebook-security-idUSBRE95K18Y20130621>. Acesso em: 20 ago. 2016.

SINGH, Simon. **O livro dos códigos**. 7. ed. São Paulo: Record, 2010.

REUSTERS. VOLZ, Dustin; FINKLE, Jim. **Exclusivo**: EUA acusam Irã de ataques cibernéticos contra bancos, fontes de Nova York. Mar/2016. http://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WP2NM. Acesso em: 21/02/2017.

ZETTER, Kim. TJX hacker gets 20 years in prison. **Wired**, 25 mar. 2010. Disponível em: <https://www.wired.com/2010/03/tjx-sentencing/>. Acesso em 20 ago. 2016.

Gerenciando usuários e permissões

Convite ao estudo

Olá, aluno!

Na unidade anterior, vimos os conceitos fundamentais de segurança da informação, que constituem o caso genérico da segurança de bancos de dados. Vimos também a definição de bancos de dados e os elementos da segurança específica dessa tecnologia. Vimos, ainda, um conjunto de casos reais em que a violação da segurança dos bancos de dados gerou enormes prejuízos para pessoas e empresas, além de lições que cada caso nos pode ensinar.

É importante reiterar que com esta disciplina buscamos atingir a competência geral que é conhecer e ser capaz de definir políticas de segurança lógica e física de dados. Nesta unidade, buscamos ainda atingir a competência técnica, que é conhecer e ser capaz de gerenciar usuários e permissões em sistemas de bancos de dados.

Os objetivos a serem atingidos com os estudos desta unidade são:

• conhecer o que é e para que serve o SQL (Structured Query Language, linguagem estruturada de consultas), bem como entender quais as linguagens que fazem parte de sua estrutura;

• conhecer os comandos básicos, intermediários e avançados do DCL, bem como a integração do DCL com outras linguagens de programação;

• conhecer quais são os perfis de uso de um banco de dados, com seus privilégios e responsabilidades. Também, é objetivo entender quais são os abusos cometidos por meio dos privilégios, suas causas, consequências e prevenção.

A M@@M é uma cadeia de restaurantes coreanos que funciona no sistema de franquia. Eles contam com um sistema interno que depende pesadamente de vários bancos de dados (franqueados, restaurantes, estoques, fornecedores, entre outros). O Sr. Kim, dono da cadeia, decidiu expandir a capacidade do sistema, de forma a permitir uma interação maior e mais próxima com os franqueados. Para tanto, ele contratou você para cuidar da segurança de acesso aos bancos de dados. Será que é possível liberar acesso a informações sem colocá-las em risco? É possível atribuir privilégios de acesso diferentes a usuários diferentes? É possível modificar e revogar privilégios de acesso?

Veremos as respostas a essas questões nesta unidade que se inicia agora, pois abordaremos a estrutura do SQL para em seguida entrarmos na estrutura da DCL, seus comandos e sua utilização.

Seção 2.1

Introdução a Data Control Language (DCL) – linguagem de controle de dados

Diálogo aberto

O controle de acesso aos bancos de dados é simplesmente fundamental nos dias de hoje, principalmente porque quase todos os nossos dados presentes no ambiente virtual (computadores, tablets, smartphones, nuvem e internet) estão armazenados em bancos de dados. Para que apenas usuários autorizados tenham acesso às nossas informações, é necessário que o controle seja eficiente. Felizmente, há mecanismos robustos para exercer esse controle de acesso.

O Sr. Kim, dono da franquia M@@M, uma rede de restaurantes de comida coreana, contratou-o para cuidar da segurança de acesso aos bancos de dados da empresa, que são vários e fundamentais para o bom andamento do estabelecimento.

O Sr. Kim tem dúvidas sobre como o controle pode ser exercido e, nesta fase, sua missão é explicar-lhe os fundamentos da linguagem estruturada de consultas (SQL), bem como o controle que pode ser exercido sobre os bancos de dados por meio da Data Control Language (DCL).

Nesta seção, veremos o que é a linguagem estruturada de busca (a que nos referiremos como SQL, seu nome mais conhecido e usado) e, a partir dela, entenderemos o que é a DCL, caracterizada por ser um subconjunto de comandos e ações destinado a controlar os dados de um banco de dados.

Não pode faltar

A partir de agora, vamos conhecer um pouco mais acerca das linguagens de manipulação de dados em bancos de dados, construindo nosso conhecimento até chegarmos na porção que mais nos interessa para segurança de sistemas de bancos de dados: a linguagem de controle de dados.

Antes, porém, vamos relembrar alguns conceitos acerca do SQL, que é a linguagem que fornece o alicerce sobre o qual o DCL se apoia.

SQL

Segundo Pratt e Last (2008), o SQL, ou linguagem estruturada de consultas (Structured Query Language), é uma das linguagens mais populares e amplamente utilizadas na manipulação de dados em bancos de dados. De fato, Elmasri e Navathe (2005) afirmam que SQL é uma das principais responsáveis pelo sucesso dos sistemas de gerenciamento de bancos de dados (SGBD).

Desenvolvida no início dos anos 1970 pelo laboratório da IBM em San Jose, na Califórnia, SQL é uma linguagem que visa permitir a manipulação de dados de forma estruturada, considerando que esses dados estão armazenados em um ou mais bancos de dados, em registros e tabelas organizadas (PRATT; LAST, 2008).

A justificativa por trás do SQL é fornecer uma ferramenta que permita, entre outras ações:

- buscar dados armazenados em um banco de dados relacional;
- correlacionar dados;
- encontrar subconjuntos de dados com base em características e atributos destes dados;
- combinar dados, formando subconjuntos que de alguma forma se relacionem;
- definir estruturas para armazenamento de dados;
- manipular usuários de bancos de dados;
- estabelecer privilégios de acesso a bancos de dados;
- restringir o acesso a bancos de dados com base em privilégios.

A linguagem SQL é declarativa, isto é, descreve o que deve ser realizado, sem se preocupar com como a ação será realizada (que é uma característica básica das linguagens procedurais). Como linguagem para manipulação de bancos de dados relacionais tornou-se padrão norte-americano (ANSI) em 1986 e padrão internacional (ISO) em 1987 (ISO/IEC 9075-1, 2008).

Assimile

A linguagem SQL é declarativa, isto é, define o que deve ser feito, sem que o usuário precise se preocupar com como as ações serão realizadas. O sistema por trás da SQL está preparado para realizar as ações, sendo que a preocupação do usuário se limita apenas em garantir que os comandos

> sejam compostos com coerência sintática e que os privilégios para os realizar estejam presentes. As linguagens declarativas se contrapõem às linguagens procedurais, nas quais o usuário mostra ao compilador o que quer por meio de um conjunto de comandos que especifica como as ações deverão ser realizadas.

SQL é uma linguagem composta por vários elementos que definem seus comandos e ações. Estes elementos são (PRATT, LAST, 2008):

• cláusulas ou comandos – ações individuais possíveis de serem realizadas com o banco de dados, com os dados, com os usuários e com os privilégios. Exemplos:

• **SELECT** – permite selecionar elementos (dado ou registros) de uma tabela;

• **JOIN** – permite unir duas tabelas, sem se preocupar em eliminar duplicações;

• **MERGE** – permite unir duas tabelas, tratando as duplicações;

• **GROUP** – permite agrupar dados semelhantes em uma tabela;

• **UPDATE** – permite atualizar um ou mais registros com base nos critérios definidos;

• **DELETE** – permite apagar dados de uma tabela.

• expressões – combinações de cláusulas que produzem valores escalares ou tabelas constituídas de linhas e colunas. Exemplo:

• **CASE** – permite realizar um comando condicional com base em um conjunto de possíveis condicionantes (caso X, faça X1; caso Y, faça Y1; caso Z, faça Z1...).

• predicados – condições que podem ser avaliadas de forma booleana (verdadeiro/falso). Exemplos:

• **IS** – um valor é igual a um comparativo;

• **IS NOT** – um valor é diferente de um comparativo;

• **IN** – um valor faz parte de um conjunto;

• **BETWEEN** – um valor está linearmente entre dois comparativos.

• Consultas – combinações de expressões e predicados que buscam dados com base em critérios específicos. Exemplo:

• **SELECT** Titulo, Autor, Editora, Preco

FROM Livros

WHERE Preco < 50

ORDER BY Titulo

• O comando "SELECT" seleciona da tabela "Livros", indicado pelo comando "FROM", as colunas "Título", "Autor", "Editora" e "Preço". Dessa forma, expõe apenas os livros cujos preços sejam inferiores a R$50,00. Observe a semântica e a sintaxe de uso do comando WHERE e os ordena pelo título em ordem alfabética crescente, devidamente descrito com o comando "ORDER BY".

Componentes de SQL

A SQL é uma linguagem formada por três blocos principais de comandos, os quais também são chamados de "linguagem". Esses blocos dividem-se por organização funcional e cada um é responsável por um conjunto de ações de função semelhante, dentro do gerenciamento de bancos de dados relacionais.

Os três principais módulos funcionais que compõem a linguagem SQL são (PRATT; LAST, 2008):

• DDL, *data definition language* (ou *data description language*, linguagem de definição/descrição de dados) – o propósito deste módulo funcional é definir as estruturas de dados de um banco de dados relacional. Os comandos dizem respeito à criação, definição e remoção de tabelas, bem como de suas estruturas ("schemas", que são registros e sua organização, os quais compõem essas tabelas).

• Principais comandos:

• CREATE – criação de tabelas;

• ALTER – alteração de tabelas;

• RENAME – modificação de nomes de tabelas;

• DROP – remoção de tabelas.

• DML (*data manipulation language*, linguagem de manipulação de dados) – o propósito deste módulo funcional é efetivamente manipular os dados das tabelas, permitindo sua correlação e consulta. Esse é o módulo funcional mais ativo durante a operação de um sistema de gerenciamento de bancos de dados relacionais (SGBD).

• Principais comandos:

• SELECT – comando de seleção de dados de acordo com especificações estabelecidas na própria linha de comando. Os dados de tabelas previamente criadas por meio de comandos da DDL são selecionados. Esse é o comando principal das consultas realizadas em bancos de dados relacionais;

• INSERT – comando de inserção de dados em uma tabela. Permite que novos registros sejam criados e passem a fazer parte de uma tabela. Durante o processo de coleta de dados e organização do banco de dados, é um dos comandos mais utilizados;

• UPDATE – comando que permite a alteração dos dados (registros) contidos em uma tabela;

• DELETE – comando que permite a remoção de um ou mais registros de uma tabela.

• DCL (Data Control Language, linguagem de controle de dados) – este módulo funcional é o objeto dos próximos tópicos discutidos nesta seção.

Exemplificando

Para criarmos uma tabela com os dados: número de registro, nome, sobrenome e data de nascimento de um paciente, determinando que estes valores devem ser preenchidos sempre (não podem ser vazios), poderíamos usar o seguinte comando em SQL:

```
CREATE TABLE paciente (
    numeroderegistro INTEGER PRIMARY KEY,
    primeiro_nome VARCHAR(50) not null,
    sobrenome VARCHAR(75) not null,
    data_de_nasc DATE not null
);
```

DCL, o que é e para que serve

O módulo funcional do SQL intitulado DCL (Data Control Language) é, segundo Murray (2010), o módulo responsável pelo controle de acesso aos bancos de dados relacionais. Esse acesso é garantido, alterado e revogado por meio de comandos definidos, os quais atribuem, alteram ou removem privilégios de acesso.

É fundamental, aqui, entender que o controle de acesso deve ser um processo, isto é, deve ser composto por procedimentos e políticas que vão muito além da tecnologia. Esse processo deve definir como a tecnologia será utilizada para garantir a segurança dos sistemas de bancos de dados, e apenas após essas definições terem sido criadas

é que utilizaremos a tecnologia (neste caso, sob forma dos comandos de DCL) para implementar a parte do processo que diz respeito à operacionalização da segurança.

Sob esse prisma, DCL é uma ferramenta à disposição dos processos de segurança de bancos de dados e apenas isso. Podemos fazer uma analogia dessa ferramenta com uma pá à disposição de um trabalhador. A pá é perfeitamente capaz de permitir que o trabalhador produza um buraco na terra, contudo, não é a pá que cava o buraco, mas sim o trabalhador. Se o buraco não é cavado, ou se é cavado no local errado, ou se não é cavado nas especificações necessárias, o responsável é o trabalhador e quem lhe deu as ordens, mas nunca a pá. De maneira análoga, a DCL é apenas uma ferramenta à disposição dos responsáveis pela segurança para atribuir, ajustar e revogar os direitos de aceso de usuários do sistema a bancos de dados específicos. Os comandos realizarão exatamente aquilo que deles for demandado, desde que esses comandos sejam sintaticamente corretos e quem os tente executar tenha os privilégios adequados para tais operações. Contudo, se os privilégios atribuídos a um usuário forem superiores aos que ele de fato tem direito, por exemplo, não podemos credenciar os problemas daí provenientes à DCL, mas sim ao processo de segurança, que se mostra falho.

E para que serve a DCL?

A DCL é um subconjunto de comandos da SQL (chamamos a esse subconjunto de comandos com funcionalidades semelhantes de "módulo funcional", para propósitos desta disciplina) cuja função é atribuir privilégios de aceso a bancos de dados, alterar privilégios atribuídos e revogar privilégios de acesso quando os mesmos já não forem mais mandatórios (MURRAY, 2010).

Observe que, na definição do parágrafo anterior, o termo utilizado é "mandatório". Este é um ponto fundamental a ser observado no tocante à segurança de sistemas de bancos de dados: privilégios de acesso devem estar à disposição do usuário apenas quando forem mandatórios, isto é, enquanto não houver outra alternativa a não ser dá-los aos usuários que acessarão as informações. No momento em que esses privilégios não forem mais mandatórios, devem ser revogados. Esse mecanismo de revogação deve ser previsto e implementado no processo de segurança a que nos referimos. Um usuário com acesso a bancos de dados sem necessidade mandatória para tanto é um risco de segurança que não deve ser tolerado em hipótese alguma, até porque é um risco de simples erradicação.

Reflita

Se os comandos da DCL são ferramentas à disposição da segurança de bancos de dados, faz sentido que um DBA (administrador de bancos de dados) entenda como criar uma política de segurança antes de se preocupar com os comandos à sua disposição. Ou ele deve entender

os comandos para mais bem saber como utilizá-los nas políticas a serem desenvolvidas?

Privilégios

Definimos, anteriormente, o controle de acesso como a atribuição, alteração e remoção de privilégios (MURRAY, 2010). Nesse contexto, é importante entendemos o que são privilégios sob o ponto de vista da DCL:

• privilégio pode ser definido como o direito de um usuário ou entidade de realizar uma ação em um banco de dados. Exemplos:

• a criação de um usuário;

• a criação de uma tabela;

• a conexão de um usuário com um ou mais bancos de dados;

• a consulta a um banco de dados;

• a inserção de dados em uma tabela;

• a alteração dos dados de uma tabela.

Há dois tipos de privilégios no que tange o gerenciamento de bancos de dados relacionais, a saber (RAJAN, 2011):

• **privilégios de sistema** – habilitam o usuário a realizar ações específicas no sistema de bancos de dados. Só podem ser exercidos por usuários administrativos. Exemplos:

• criação de tabelas;

• atribuição de privilégios a usuários.

• **privilégios de objetos** – habilitam o usuário a acessar e a manipular objetos específicos, como tabelas pertencentes a outros usuários. Exemplos:

• consultas a tabelas;

• inserção de dados em tabelas.

Em um SGBD há mais de 200 privilégios de sistema diferentes (BURLESON, 2015). Uma lista dos nomes dos privilégios de sistema pode ser encontrada em uma view chamada SYSTEM_PRIVILEGE_MAP, que pode ser consultada em vários sistemas de bancos de dados, tais como o SQLite e o Oracle.

Pesquise mais

Os pesquisadores Gustavo H. M. B. Motta, da Universidade Federal da Paraíba, e Sergio Furuie, da Universidade de São Paulo, criaram uma ferramenta de autorização e controle de acesso a prontuários de pacientes com base nas técnicas de controle de acesso de bancos de dados. Pesquise mais a respeito no excelente artigo publicado por eles.

MOTTA, G. H. M.; FURUIE, S. **MACA**: uma ferramenta de autorização e controle de acesso para o prontuário eletrônico de pacientes. ResearchGate, 2014. Disponível em: <https://www.researchgate.net/profile/Gustavo_Motta2/publication/268416335_MACA_Uma_Ferramenta_de_Autorizacao_e_Controle_de_Acesso_para_o_Prontuario_Eletronico_de_Pacientes/links/54bd3f700cf218da9391acd1.pdf>. Acesso em: 21 nov. 2016.

Sem medo de errar

Para auxiliar o sr. Kim sobre como podemos exercer controle sobre os bancos de dados, podemos começar explicando-lhe o que é SQL, a linguagem por meio da qual os sistemas de gerenciamento de bancos de dados relacionais permitem o acesso e a manipulação de bancos de dados. Um resumo de SQL pode assim ser apresentado:

• trata-se de uma linguagem declarativa de alto nível, em que a preocupação do usuário é definir o que deve ser feito, deixando para o sistema a preocupação de como as ações serão realizadas. Dessa forma, os administradores e usuários podem se preocupar com suas tarefas pertinentes ao negócio, ao invés de terem que despender tempo com os intrínsecos da infraestrutura;

• a linguagem SQL é composta por três módulos funcionais, cada um cuidando de um conjunto de ações específico, a saber:

• DDL (data definition/description language) – responsável pelas definições e criações de tabelas e usuários;

• DML (data manipulation language – responsável pela manipulação de dados e tabelas, permitindo também as correlações e consultas aos bancos de dados disponíveis;

• DCL (Data Control Language) – responsável pelo controle de acesso aos bancos de dados disponíveis.

• o módulo funcional DCL auxilia na implementação dos controles de acesso por meio da atribuição e revogação de privilégios aos usuários e entidades que manipulam

os bancos de dados.

• privilégios podem ser de dois tipos:

• privilégios de sistema – ações ligadas ao sistema de bancos de dados em si;

• privilégios de objeto – ações ligadas aos objetos (bancos de dados, tabelas, registros etc.);

• é importante ressaltar que a DCL é uma ferramenta, que deve ser sempre colocada ao serviço de uma política de segurança de bancos de dados. Os comandos dessa linguagem realizam o que pedimos a eles, mas devemos cuidar para que sejam realizados no sentido de habilitar uma política robusta de segurança.

Agora, para você conseguir fazer esse trabalho, abaixo estão algumas orientações:

1. Com os computadores ligados e o Google Chrome (navegador) iniciado, deverão entrar no site: <http://www.w3schools.com/sql/trysql.asp?filename=trysql_select_all> (acesso em: 20 nov. 2016) que é um simulador de linguagem SQL.

2. A fim de conhecer a base de dados já inserida "de fábrica" no simulador, vocês deverão inserir o seguinte comando no editor:

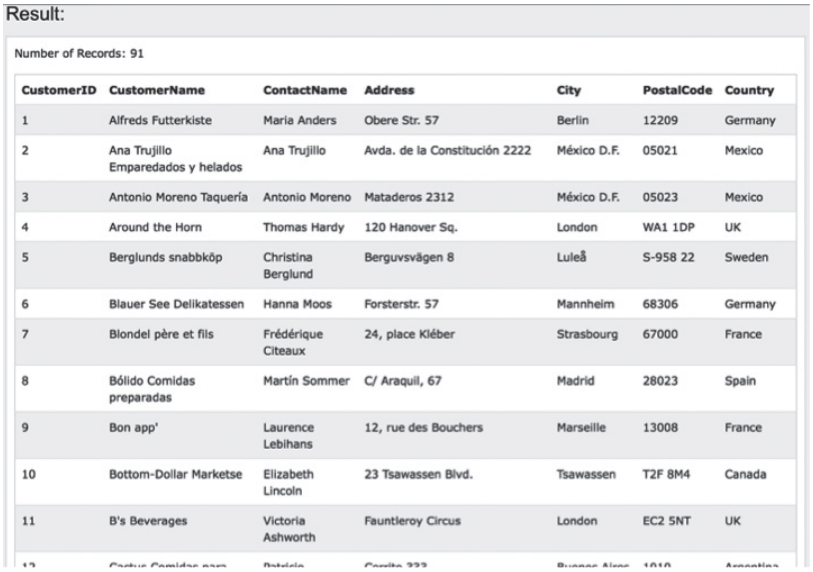
SELECT * FROM Customers;

Esse comando seleciona (SELECT) todos os campos (o "*" é o símbolo que indica "tudo) da tabela "Customers" (Clientes, uma tabela já inserida "de fábrica" no simulador).

3. Clicar no botão "Run SQL >>", que executa o comando (ou os comandos, se houver mais de um).

4. Observar que o resultado é uma tabela com 91 registros, exemplificados na figura a seguir:

Figura 2.1 | Resultado da execução da consulta



Result:

Number of Records: 91

CustomerID	CustomerName	ContactName	Address	City	PostalCode	Country
1	Alfreds Futterkiste	Maria Anders	Obere Str. 57	Berlin	12209	Germany
2	Ana Trujillo Emparedados y helados	Ana Trujillo	Avda. de la Constitución 2222	México D.F.	05021	Mexico
3	Antonio Moreno Taquería	Antonio Moreno	Mataderos 2312	México D.F.	05023	Mexico
4	Around the Horn	Thomas Hardy	120 Hanover Sq.	London	WA1 1DP	UK
5	Berglunds snabbköp	Christina Berglund	Berguvsvägen 8	Luleå	S-958 22	Sweden
6	Blauer See Delikatessen	Hanna Moos	Forsterstr. 57	Mannheim	68306	Germany
7	Blondel père et fils	Frédérique Citeaux	24, place Kléber	Strasbourg	67000	France
8	Bólido Comidas preparadas	Martín Sommer	C/ Araquil, 67	Madrid	28023	Spain
9	Bon app'	Laurence Lebihans	12, rue des Bouchers	Marseille	13008	France
10	Bottom-Dollar Marketse	Elizabeth Lincoln	23 Tsawassen Blvd.	Tsawassen	T2F 8M4	Canada
11	B's Beverages	Victoria Ashworth	Fauntleroy Circus	London	EC2 5NT	UK

Fonte: adaptada de: <http://www.w3schools.com/sql/trysql.asp?filename=trysql_select_all>. Acesso em: 1 dez. 2016.

5. Entre nos sites Diego Macedo (disponível em: <http://www.diegomacedo.com.br/introducao-a-linguagem-sql-comandos-basicos-e-avancados-parte-1/>. Acesso em: 21 nov. 2016) e Linha de Código (disponível em: <http://www.linhadecodigo.com.br/artigo/2975/comandos-basicos-em-sql-insert-update-delete-e-select.aspx>. Acesso em: 21 nov. 2015) e pesquise os comandos básicos do SQL, testando-os com a base de dados presente no simulador.

6. Caso você "acidentalmente" destrua a base, não entre em pânico: é só recarregar a página do simulador e tudo volta a ser como era antes.

7. Experimente com os seguintes comandos:

SELECT;

INSERT;

UPDATE;

DELETE;

CREATE TABLE.

8. Quais desses comandos pertencem à DDL?

9. Quais desses comandos pertencem à DML?

Avançando na prática

A ordem adequada das coisas

Descrição da situação-problema

O jovem Érico herdou de seu pai uma pequena rede de cinco farmácias em Belo Horizonte, cidade onde reside. A fim de automatizar os estoques das farmácias, decidiu investir em um sistema de bancos de dados e em uma aplicação que lhe permita controlar o sistema de seu computador e de seu celular. Após o sistema entrar em funcionamento, Érico começou a pensar em estendê-lo no sentido de oferecer aos clientes a possibilidade de comprar produtos, que não precisam de receita, pela internet com entrega em domicílio, ou produtos que demandam receita com retirada na própria farmácia. Para tanto, seu amigo, que é consultor, afirmou que ele precisaria tomar várias providências, após definir como será o sistema, entre elas:

- implementar controles de segurança nos bancos de dados;
- criar os perfis dos usuários;
- criar as novas estruturas e os novos bancos de dados para acesso dos clientes;
- disponibilizar o sistema para acesso dos usuários;
- atribuir os privilégios de acesso adequados a todos os usuários do sistema;
- testar a política de segurança do sistema em um ambiente controlado, com usuários de teste apenas;
- criar uma política de segurança robusta para o sistema.

Érico precisa, agora, definir como realizar tudo isso. Você pode auxiliá-lo definindo e justificando a ordem em que todas essas ações deverão ser implementadas. Será que tanto faz? Será que há vantagem em se definir conforme uma determinada ordem? Ajude Érico a resolver esse problema.

Resolução da situação-problema

Em se tratando de segurança de sistemas de bancos de dados, há pouco espaço para improvisos, e a lista de tarefas que o amigo de Érico compôs é um exemplo disso: Érico incorreria em sérios riscos se desrespeitasse uma ordem coerente para as ações.

Podemos definir como a ordem adequada para as tarefas:

1. Criar uma política de segurança robusta para o sistema.

2. Criar as novas estruturas e os novos bancos de dados para acesso dos clientes.

3. Implementar os controles de segurança nos bancos de dados.

4. Criar os perfis dos usuários.

5. Atribuir os privilégios de acesso adequados a todos os usuários do sistema.

6. Testar a política de segurança do sistema em um ambiente controlado, com usuários de teste apenas.

7. Disponibilizar o sistema para acesso dos usuários.

Como justificativa para essa ordem dos acontecimentos, temos:

1. Criar uma política de segurança robusta para o sistema – uma vez definido o sistema, a primeira atitude a ser tomada, antes mesmo da implantação das estruturas de dados, é a criação de uma política de segurança que seja robusta no gerenciamento de segurança do sistema.

2. Criar as novas estruturas e os novos bancos de dados para acesso dos clientes – uma vez criada a política de segurança, as estruturas e os bancos de dados (ainda sem acesso disponibilizado a ninguém, a não ser aos administradores) devem ser criadas.

3. Implementar os controles de segurança nos bancos de dados – criadas as estruturas e os bancos de dados, os controles de segurança devem ser implantados sobre estes, já seguindo estritamente a política de segurança definida no primeiro passo.

4. Criar os perfis dos usuários – definidos os controles de segurança para as estruturas e bancos de dados, é hora de criar os perfis dos usuários.

5. Atribuir os privilégios de acesso adequados a todos os perfis dos usuários do sistema – uma vez que os perfis estão definidos, é hora de atribuir os privilégios previamente definidos, permitindo que quando os usuários se cadastrarem no sistema, já entrem estando em concordância com a política de segurança.

6. Testar a política de segurança do sistema em um ambiente controlado, com usuários de teste apenas – o teste do sistema para averiguar a adequação da política de segurança deve ocorrer antes da disponibilização do sistema para o público em geral.

7. Disponibilizar o sistema para acesso dos usuários – testado o sistema e comprovada a adequação da política de segurança para os perfis e privilégios, é hora de liberar o sistema para uso do público.

Faça valer a pena

1. Desenvolvida no início dos anos 1970 pelo laboratório da IBM em San Jose, na Califórnia, SQL é uma linguagem que visa permitir a manipulação de dados de forma estruturada, considerando que esses dados estão armazenados em um ou mais bancos de dados, em registros e tabelas organizadas (PRATT, LAST, 2008).

Sabendo que SQL é uma linguagem que visa a manipulação de dados, qual o significado da sigla SQL?

a) Serial query language.

b) Sructured query language.

c) Sequential queasy language.

d) Structured query limits.

e) Serial queasy limits.

2. SQL é uma linguagem formada por três blocos principais de comandos, cada um deles chamado, também, de "linguagem". Esses blocos dividem-se por organização funcional e cada um deles é responsável por um conjunto de ações de função semelhante, dentro do gerenciamento de bancos de dados relacionais.

Sobre o módulo funcional cuja sigla é DDL, podemos afirmar que sua função básica é:

a) Disponibilizar as estruturas e os dados.

b) Desencriptar as estruturas e os dados.

c) Garantir que as estruturas e os dados sejam controlados com relação aos privilégios de acesso.

d) Permitir a criação de novos registros em tabelas, com novos dados em cada registro.

e) Definir as estruturas de dados.

3. Definimos o controle de acesso como a atribuição, alteração e remoção de privilégios (MURRAY, 2010). Nesse contexto, é importante entendermos o que são privilégios sob o ponto de vista da DCL. Privilégios, afinal de contas, são o cerne de todo o processo de controle de acesso aos bancos de dados.

No contexto de controle de acesso aos bancos de dados, como podemos definir privilégio?

a) O direito de um usuário ou entidade de reivindicar acesso a um banco de dados.

b) O dever de um usuário de cuidar adequadamente de um banco de dados.

c) O direito de um usuário ou entidade de realizar uma ação em um banco de dados.

d) O direito de um usuário ou entidade de inserir dados em uma tabela.

e) O dever de um usuário de relatar anomalias que presencie em bancos de dados.

Seção 2.2

DCL: comandos e estrutura

Diálogo aberto

Os pares de aminoácidos estão para uma cadeia de DNA assim como os comandos em uma linguagem de programação qualquer estão para um programa pronto: são simples e de fácil compreensão, mas, quando encadeados, podem produzir verdadeiras maravilhas. O DNA produz toda a vida na Terra. E os programas facilitam nossa vida de formas tão impressionantes e diversas que é seguro afirmar que retornaríamos quase cem anos no tempo, em termos de progresso, sem eles. Com SQL — e, mais especificamente, com o módulo funcional DCL — não é diferente. Poucos comandos permitem que realizemos diversas e importantes tarefas no que tange o uso de bancos de dados.

O Sr. Kim, dono da franquia de comida coreana M@@M, contratou você para cuidar da segurança de seus bancos de dados, agora que ele decidiu estender o sistema para uso dos franqueados. Nesta etapa, você recebeu uma lista com 20 franqueados — que comporão o projeto piloto — e deverá dar-lhes acesso adequado ao sistema. Eles deverão ter acesso de leitura a todos os bancos de dados de estoque, mas não deverão ter acesso qualquer aos bancos de dados administrativos do sistema, que é de responsabilidade da matriz, e não dos franqueados. Como garantir o acesso de forma adequada e consistente aos franqueados? Como proteger as porções a que eles não devem ter acesso?

Nesta seção, você vai conhecer os comandos básicos, intermediários e avançados do DCL, bem como a integração do DCL com outras linguagens de programação.

Pronto para mais uma etapa de aprendizado?

Não pode faltar

Uma vez que você compreende como funciona a linguagem SQL e para que servem seus módulos funcionais, é hora de nos concentrarmos na Data Control

Language (DCL), o módulo funcional que efetivamente permite o controle dos bancos de dados.

Uma classificação arbitrária, porém útil

Em uma análise mais rigorosa do assunto, não é difícil enxergar que a divisão em comandos básicos, intermediários e avançados de DCL é arbitrária. Isso se deve ao fato de que toda a DCL é baseada em dois comandos:

- GRANT;
- REVOKE.

No entanto, se esse é o caso, como podemos, então, fazer a classificação em comandos básicos, intermediários e avançados? Bem, para fins de estudo, essa classificação pode ser feita com base nos objetos aos quais os privilégios serão atribuídos ou revogados.

Há, também, outra forma de encararmos essa questão de comandos básicos, intermediários e avançados: as circunstâncias nas quais se utilizam os comandos. Como analogia, tomemos as técnicas de cirurgia. De maneira simplificada, existem duas ações básicas que um cirurgião pode tomar: romper tecidos (geralmente por meio de um bisturi) e unir tecidos (geralmente por meio de suturas). Essas duas ações resumem o que ocorre em 100% das cirurgias, mas ninguém em sã consciência classificaria a cirurgia de remoção de uma verruga no mesmo grau de complexidade de uma cirurgia para implantação de uma ponte de safena, não é verdade?

Da mesma forma, os dois comandos simples do módulo funcional DCL podem ser usados tanto para a execução de comandos simples no controle de privilégios como para ações mais elaboradas e complexas.

Assimile

Por mais simples que a DCL seja (e com apenas dois comandos fica difícil ser mais simples, em teoria), é um módulo funcional poderosíssimo, pois permite e limita acesso a todos os recursos de um sistema de bancos de dados. É necessário, portanto, que se aprenda com dedicação e detalhe como manejá-la, para que os bancos de dados sejam por ela assegurados e mantidos seguros e sem risco.

Tipos de privilégios

Como já vimos, o módulo funcional DCL é utilizado para controlar privilégios em bancos de dados. Privilégios são necessários sempre que quisermos realizar alguma operação sobre bancos de dados, tais como criar tabelas, e são concedidos apenas por usuários administradores do banco. Os privilégios podem ser de dois tipos, a saber (GUPTA, 2010):

• **privilégios de sistema** – são privilégios concedidos no nível dos "Schemas" do SGBD. Permitem a criação de usuários, seções, tabelas, bem como a execução de ações que têm efeito sobre o ambiente ou sobre partes deste. São privilégios com consequências potenciais mais sérias, pois podem afetar todos os usuários de um sistema de bancos de dados;

• **privilégios de objeto** – são privilégios que podem ser concedidos pelo dono de um objeto a outros usuários do sistema. Permitem a ação sobre objetos (manipulação, consulta, inserção, alteração, entre outros). São privilégios mais localizados, e suas consequências se limitam aos elementos a que as ações podem ser aplicadas com a anuência de seus donos.

Essa classificação de tipos de privilégios será importante na compreensão da divisão de comandos do módulo funcional em básicos, intermediários e avançados, que veremos a seguir. Observe, porém, que se trata de mais um caso de divisão arbitrária, adotada para facilitar (ou, no caso, para tentar facilitar) a compreensão dos conceitos.

Reflita

Quem pode fazer mais "estragos" em um sistema de bancos de dados: um usuário que inadvertidamente obtenha privilégios de objetos ou um usuário que indevidamente obtenha privilégios de sistema?

Comandos básicos

Em sua expressão mais simples, o módulo funcional DCL é baseado em dois comandos apenas, a saber (STUDYTONIGHT, 2014):

• **GRANT (do inglês "conceder")** – é o comando que concede um privilégio qualquer ao usuário;

• **REVOKE (do inglês "revogar")** – é o comando que revoga um privilégio qualquer do usuário.

Esses dois comandos podem ser utilizados em uma miríade de situações nas operações diárias de um banco de dados; ambos têm uma sintaxe simples de ser compreendida.

Vejamos, primeiramente, a sintaxe do comando GRANT (GUPTA, 2010):

GRANT [privilégio]

ON [objeto]

TO {usuário | papel | PUBLIC}

[**WITH** {ADMIN | GRANT} OPTION];

Observemos o significado do comando genérico **GRANT**, mostrado acima, em uma análise linha a linha (GUPTA, 2010):

1. Na primeira linha, temos os termos: **GRANT** [privilégio]. O comando começa com a concessão de um privilégio qualquer, por meio da cláusula "GRANT". O "privilégio" que deve vir a seguir é uma cláusula qualquer. Se for uma cláusula de sistema, o comando concede um privilégio de sistema e, se for uma cláusula de objeto, o comando concede um privilégio de objeto. São exemplos de cláusulas que podem ser "concedidas" como privilégio:

a. Privilégios de sistema: CREATE, DROP, DEBUG, FLASHBACK, LOCK, CONNECT, EXECUTE, RESOURCE ALTER (atributo de sistema);

b. Privilégios de objeto: SELECT, INSERT, DELETE, UPDATE, INDEX, READ, WRITE, ALTER (objeto).

2. Na segunda linha, temos os termos: **ON** [objeto]. O privilégio é concedido sobre ("ON") algum objeto, que, no caso, pode ser uma tabela ou uma sequência, por exemplo.

3. Na terceira linha, temos os termos: **TO** {usuário | papel | PUBLIC}. O privilégio sendo concedido sobre um objeto qualquer deve ser concedido para ("TO") alguém ou alguma coisa. Esse "alguém ou alguma coisa" pode ser um usuário, um papel ("papel" é um conjunto de características que definem um tipo de usuário do SGBD), ou para todo mundo, por meio do qualificador "PUBLIC". Trataremos dessa questão mais à frente, quando falarmos sobre os comandos intermediários.

4. A última linha especifica duas possibilidades de qualificadores administrativos de alta hierarquia. Trataremos dessa questão mais à frente, quando falarmos sobre os comandos avançados.

Como exemplo de comando básico de concessão de privilégios, podemos apresentar o seguinte:

GRANT SELECT ON Tabela01 **TO** Usuario35;

O comando acima concede o direito de executar o comando "SELECT" (seleção combinada de dados) na tabela "Tabela01" ao usuário designado por "Usuario35".

É importante observar que uma de duas condições deve estar presente para que esse comando seja aceito e executado pelo sistema:

1. O comando deve ser emitido pelo dono da "Tabela01"; ou

2. O comando deve ser emitido por um usuário com privilégios administrativos.

Do contrário, isto é, se quem está emitindo esse comando não é dono da tabela em questão, nem tem privilégios administrativos, o sistema emitirá uma mensagem de erro informando que se trata de um comando inválido, nas condições em que é emitido, e não realizará as ações ali estipuladas.

Segundo Microsoft (2016), o comando GRANT pode ter como argumento vários tipos de privilégio, a saber:

• **ALL** – o significado do termo ("tudo", em inglês) pode dar uma ideia errada deste argumento. Na verdade, não significa que todos os privilégios estejam sendo atribuídos a um objeto, mas todos aqueles, entre os 92 tipos possíveis de privilégios do SQL ANSI (padrão de SQL definido pelo American National Standards Institute), que são aplicáveis ao comando em questão;

• **Privilégios de função escalar** – comandos aplicáveis: EXECUTE, REFERENCES;

• **Privilégios de função com valor de tabela** – comandos aplicáveis: DELETE, INSERT, REFERENCES, SELECT, UPDATE;

• **Privilégios de procedimento armazenado** – comando aplicável: EXECUTE;

• **Privilégios de tabela** – comandos aplicáveis: DELETE, INSERT, REFERENCES, SELECT, UPDATE;

• **Privilégio de exibir privilégios** – comandos aplicáveis: DELETE, INSERT, REFERENCES, SELECT, UPDATE.

Já o comando REVOKE — o segundo comando básico do módulo funcional DCL, que significa "revogar" ou "cancelar" — tem a seguinte sintaxe (GUPTA, 2010):

REVOKE [privilégio]

ON [OBJETO] [esquema].objeto [(coluna [,...n])]

FROM [privilegiado] [,...n]

Observemos o significado do comando genérico REVOKE, mostrado acima, em uma análise linha a linha (MICROSOFT, 2016a):

1. Na primeira linha, temos o comando "REVOKE" em si, que pode ser aplicado a um ou mais privilégios.

2. Na segunda linha, temos o(s) objeto(s) ou o(s) elemento(s) de objeto para o qual o privilégio está sendo revogado.

3. Na terceira linha, temos o privilegiado (ou os privilegiados, caso haja mais de um) para quem o(s) privilégio(s) está(ão) sendo revogado(s).

Como exemplo de comando básico de revogação de privilégios, podemos apresentar o seguinte:

REVOKE EXECUTE **ON** Procedimento01 **FROM** Usuário12;

Esse comando revoga a possibilidade de executar comandos SQL presentes no procedimento "Procedimento01" para o usuário "Usuário12".

Mecanismos discricionários x mecanismos obrigatórios de acesso

Se você se lembra, na Seção 1.2, falamos de mecanismos discricionários de acesso e também de mecanismos obrigatórios de acesso. Pois bem, quando aplicamos os comandos GRANT e REVOKE a usuários definidos ou a grupos definidos de usuários, estamos realizando mecanismos discricionários de controle de acesso (MARTINS; CANDIDO JUNIOR, 2014).

Os comandos aplicados a objetos de um banco de dados são considerados básicos, conforme a divisão arbitrária entre os comandos GRANT e REVOKE.

Veremos os demais nos itens a seguir.

Comandos intermediários

Tanto o comando GRANT como o comando REVOKE podem ser aplicados não apenas a usuários individuais ou a conjuntos definidos de usuários (estipulados um a um no próprio comando, a que chamamos de "objetos discricionários"), mas também ao que chamamos de "papéis", que são perfis definidos de antemão.

Um papel, antes de tudo, deve ser criado e, em seguida, usuários devem ser adicionados a ele. No fundo, um papel é um conjunto de usuários que têm um nome. Existem duas vantagens sobre conjuntos de usuários definidos no corpo de um comando:

• **organização** – uma vez que conhecemos os papéis que os vários usuários de um sistema de banco de dados vão desempenhar, o ideal é agruparmos estes usuários em papéis, uma vez que com essa organização podemos concentrar nossas ações em dois pontos apenas: a atribuição correta de papéis e o gerenciamento dos papéis em si, sem que precisemos nos preocupar com o gerenciamento de usuários individuais;

• **otimização** – em um sistema com algumas centenas de usuários, a atuação individual sobre esses usuários rapidamente se transforma em um pesadelo. O volume

de trabalho é enorme, e erros fatalmente são cometidos. Por meio desse agrupamento, a atuação sobre o papel "economiza" um trabalho enorme e evita esquecimentos ou inclusões indevidas (obviamente que é necessário garantir que todos os usuários requisitados — e somente estes — façam parte do papel em questão, mas essa é uma tarefa que pode ser realizada com bastante precisão em um processo de gestão de usuários).

É importante observar que a criação de um papel é considerada uma ação administrativa e, portanto, apenas os usuários com status de administradores (DBAs) devem ter o privilégio de cria-los.

O comando para a criação de um papel é bastante simples, a saber. (MICROSOFT, 2016b):

CREATE ROLE nome_do_papel [**AUTHORIZATION** dono_do_papel]

No comando, podemos observar que um nome deve ser fornecido (um nome a critério do administrador que está criando o papel). O papel também deve ter um responsável, que é designado pelo atributo AUTHORIZATION. Caso o atributo AUTHORIZATION e o nome do responsável sejam omitidos, o sistema assume que o administrador que está criando o papel seja o dono deste papel.

Uma vez criado um papel, o próximo passo é popular este papel com os usuários que farão parte do grupo em questão. Esse processo se dá por meio do comando ALTER ROLE. Uma vez que um papel não tem mais utilidade, ele deve ser removido permanentemente do sistema (apagado), por meio do comando DROP ROLE.

No processo de atribuição de privilégios, o comando de concessão GRANT é considerado um comando intermediário do módulo funcional DCL quando é aplicado a um papel, ao invés de ser aplicado a um usuário ou a um grupo de usuários definido no próprio comando. Essa aplicação do comando a um papel pode ocorrer em dois pontos do comando, como podemos ver a seguir (GUPTA, 2010):

• **ON** – um privilégio é concedido sobre ("ON") um objeto qualquer, como já vimos nesta mesma seção. Pois bem, esse objeto pode ser também um papel. O comando parcial "GRANT ALTER ON nome_do_papel" permitiria que o usuário a quem o privilégio é concedido faça alterações no papel "nome_do_papel";

• **TO** – um privilégio é concedido a ("TO") alguém, como já vimos nesta mesma seção. Pois bem, esse alguém pode também ser um papel. O comando "GRANT SELECT ON tabela01 TO papel_correntista" permite que qualquer usuário que faça parte do papel "papel_correntista" execute o comando SELECT na tabela de nome "tabela01".

Exemplificando

Para criarmos um papel chamado "pesquisadores" pertencente ao usuário Lucas, inserirmos os usuários Paulo e Jorge a esse papel, e permitirmos que os componentes desse papel possam realizar consultas à Tabela01, teríamos a seguinte sequência de comandos:

CREATE ROLE pesquisadores **AUTHORIZATION** Lucas

ALTER ROLE pesquisadores **ADD MEMBER** Paulo

ALTER ROLE pesquisadores **ADD MEMBER** Jorge

GRANT SELECT ON Tabela01 **TO** pesquisadores

A concessão e a revogação de privilégios sobre papéis são bem mais cômodas e permitem uma organização bem melhor que no caso das concessões e revogações de privilégios a usuários individuais. Ela também demanda, como podemos observar, critérios bem mais rigorosos para que sejam aplicadas, uma vez que tem o potencial de afetar um contingente bem maior de usuários de uma vez.

Os comandos intermediários também podem conceder ou revogar privilégios de sistema, isto é, privilégios que estejam relacionados não a objetos ou papéis, mas também a elementos de funcionamento do próprio sistema. Um exemplo que podemos citar é o privilégio de execução de comandos que pode ser atribuído a procedimentos externos.

Funciona assim: outros sistemas que acessam os bancos de dados — interfaces Web, programas em JAVA ou outras linguagens, aplicativos que fazem interface com bancos de dados, entre outros — podem requisitar a execução de comandos SQL, desde que devidamente autorizados por meio de privilégios concedidos pelo sistema.

Vejamos um exemplo do comando GRANT para execução de comandos por procedimentos (GUPTA, 2010):

GRANT EXECUTE ON Procedimento01 **TO** Usuario03;

Esse comando permite que o "Usuario03" execute comandos por meio do "Procedimento01.

Há vários comandos que se referem ao sistema, e não a objetos de bancos de dados. O comando ALTER, bem como o comando CONNECT são exemplos de comandos de sistema. Quando usamos o DCL para conceder privilégios sobre elementos de sistema, estamos usando o DCL em sua modalidade de comandos intermediários.

Comandos avançados

O módulo funcional DCL permite, por fim, a utilização dos comandos GRANT e REVOKE no que podemos chamar, nessa nossa classificação arbitrária, de "comandos avançados". Trata-se dos casos em que os comandos são aplicados para conceder e revogar direitos sobre a criação de elementos no banco de dados ou sobre a administração de elementos do sistema de banco de dados.

Retomando o comando GRANT, temos (GUPTA, 2010):

GRANT [privilégio]

ON [objeto]

TO {usuário | papel | PUBLIC}

[**WITH** { GRANT | ADMIN } **OPTION**];

O que nos interessa neste momento, para fins dos comandos avançados, é a quarta linha do comando, em que o privilégio sobre o objeto é concedido ao usuário (ou ao papel ou ao público em geral) com uma de duas opções: GRANT ou ADMIN.

O qualificador GRANT permite que o usuário que recebe o privilégio possa, ele próprio, atribuir privilégios. Já o qualificador "ADMIN" permite que o usuário que recebe a concessão a receba com privilégio de administrador do sistema, ou seja, pode emitir o comando para o qual recebe privilégio em qualquer situação, para quaisquer objetos que o privilégio encampa. Ambos só podem, obviamente, ser emitidos por usuários com privilégios administrativos, e o "ADMIN" só pode ser emitido por usuários que, além de poder conceder privilégios, também possuam privilégios administrativos completos (possibilidade de atuar sobre todo o sistema de banco de dados).

Um exemplo dessa aplicação de comandos avançados:

GRANT CREATE INDEX TO Usuario01 **WITH GRANT OPTION**

Nesse exemplo, estamos atribuindo o privilégio de poder criar índices ao usuário "Usuario01" e, ao mesmo tempo, permitindo a esse usuário que atribua privilégios de criação de índices a outros usuários.

É importante frisar que as opções GRANT e ADMIN são bastante delicadas e devem ser aplicadas apenas com rigorosos critérios, que façam parte de um rigoroso processo de segurança e de administração dos bancos de dados.

Pesquise mais

Os comandos GRANT e REVOKE são comandos muito importantes no contexto do SQL, em geral, e do módulo funcional DCL, em especifico. Estude mais a respeito desses comandos no artigo de Sauragh K. Gupta:

GUPTA, S. K. **Oracle DCL Data Control Language**. Site ClubOracle, 8 nov. 2010. Disponível em <http://www.club-oracle.com/threads/oracle-dcl-data-control-language.16248/>. Acesso em: 22 nov. 2016.>

Sem medo de errar

Para dar acesso de leitura à lista de 20 franqueados da M@@M aos bancos de dados de estoque, garantindo que não tenham acesso aos demais bancos de dados (todos administrativos), devemos começar com a identificação dos franqueados. Para fins de simplificação, assumimos aqui que esses franqueados têm identificação no sistema como "FranqueadoXX", sendo que "XX é um número de dois algarismos que vai de 01 a 20. Assumimos, também, que os bancos de dados de estoque são divididos em três, assim nomeados:

- Estoque_de_alimentos;
- Estoque_de_material_de_consumo;
- Estoque_de_material_de_escritorio.

Em primeiro lugar, para garantirmos que os franqueados não terão acesso a nenhuma porção administrativa do sistema, não precisamos fazer rigorosamente nada a partir do momento que são criados no sistema, pois são criados sem privilégio algum. Garantir a segurança, portanto, passa por atribuirmos apenas os privilégios aos que de fato têm direito.

Sabendo disso, podemos nos tranquilizar e criar, primeiramente o papel "Franqueados", pertencente, por definição, ao administrador dos bancos de dados. Para tanto, precisamos inserir o seguinte comando no sistema:

```
CREATE ROLE Franqueados;
```

Uma vez criado o papel, podemos inserir a sequência de comandos que adicionam os usuários já criados ao papel:

```
ALTER ROLE Franqueados ADD MEMBER Franqueado01;
ALTER ROLE Franqueados ADD MEMBER Franqueado02;
ALTER ROLE Franqueados ADD MEMBER Franqueado20;
```

Alternativamente, poderíamos ter desenvolvido um pequeno procedimento que lê uma lista onde constam todos os nomes dos franqueados e, com cada um deles, executa o comando de alterar o papel Franqueados, inserindo-os. Esse laço de repetição é simples e será visto extensamente nas disciplinas de programação.

O próximo passo é atribuir o privilégio de consulta (essencialmente, o privilégio de os usuários lerem o conteúdo das tabelas) aos bancos de dados de estoque para o papel de franqueados, recém-criado e recém-populado. Para tanto, nos valeremos dos seguintes comandos:

GRANT SELECT ON Estoque_de_alimentos **TO** Franqueados;

GRANT SELECT ON Estoque_de_material_de_consumo **TO** Franqueados;

GRANT SELECT ON Estoque_de_material_de_escritorio **TO** Franqueados;

E pronto! O privilégio de consulta (leitura) foi atribuído aos franqueados, que agora têm acesso aos bancos de dados de estoque da M@@M.

Atenção

Privilégios só devem ser atribuídos quando forem necessários, do contrário não devem ser atribuídos, mantendo assim a segurança do ambiente.

Avançando na prática

Removendo privilégios desnecessários

Descrição da situação-problema

A farmacêutica Lígia é dona de uma farmácia bem frequentada na cidade onde mora. O negócio cresceu, e Lígia adotou um sistema de bancos de dados para facilitar a organização e venda de seus produtos.

Para tanto, Lígia cadastrou os funcionários à época como usuários e atribuiu a todos o direito de consultar os bancos de dados. Eram, à época, quatro funcionários: Aldo, Cesar, Jairo e Denise. O funcionário Jairo, que se mostrou bastante eficiente na administração da farmácia, rapidamente se tornou o "segundo em comando" de Lígia e ficou responsável pela administração do acesso dos demais funcionários.

Hoje, observando a situação do acesso aos bancos de dados da farmácia, Lígia percebeu que a ex-funcionária Denise ainda consta como usuária, e que Jairo — que se mudou de cidade e hoje trabalha em sua própria farmácia — ainda consta como administrador dos funcionários.

Quais as providências que Lígia teria tomado para criar o acesso aos funcionários quando criou o sistema? Que providências deverá tomar agora, para manter a consistência da segurança do ambiente?

Resolução da situação-problema

Lígia, à época, teria que ter tomado as seguintes providências:

• criar os usuários dos funcionários no sistema;

• criar o papel "Funcionario" no sistema, atribuindo sua administração para Jairo;

• inserir todos os funcionários no papel "Funcionario";

• atribuir privilégio de consulta aos bancos de dados para todos os funcionários.

Hoje, Lígia deve tomar as seguintes providências:

• remover a ex-funcionária Denise do papel "Funcionario";

• remover o ex-funcionário Jairo do papel "Funcionario;

• se Lígia tem outro "braço direito", que é responsável pelo ambiente de bancos de dados, pode alterar o papel Funcionário, atribuindo a responsabilidade de administração desse papel ao funcionário em questão, senão essa função passa naturalmente a ela (administradora), uma vez que Jairo foi excluído.

Faça você mesmo

Que comandos Lígia teria usado nas situações descritas acima? Escreva-os usando a linguagem SQL.

Faça valer a pena

1. Em uma análise mais rigorosa acerca da classificação dos comandos do módulo funcional DCL, não é difícil enxergar que a divisão em básicos, intermediários e avançados é arbitrária. Isso se deve ao fato de que toda a DCL é baseada em dois comandos.

Quais são os comandos que efetivamente fazem parte do módulo funcional DCL?

a) CREATE e ALTER.

b) CREATE e ROLE.

c) GRANT e REVOKE.

d) GRANT e ROLE.

e) REVOKE e ROLE.

2. Tanto o comando GRANT quanto o comando REVOKE podem ser aplicados não apenas a usuários individuais ou a conjuntos definidos de usuários (estipulados um a um no próprio comando), mas também ao que chamamos de "papéis", que são perfis definidos de antemão.

Por que a definição de papéis é mais vantajosa que os conjuntos de usuários definidos no corpo de um comando?

a) Porque é mais rápido e não consome tantos recursos de processamento do sistema.

b) Porque apesar de ser mais inseguro, é mais indicado.

c) Porque é a tradição que define como devemos fazer; e a tradição especifica que deve ser assim.

d) Porque, apesar de dar mais trabalho, é mais fácil.

e) Porque permite que a operação fique mais organizada e otimizada.

3. O módulo funcional DCL permite, por fim, a utilização dos comandos GRANT e REVOKE no que podemos chamar, nessa nossa classificação arbitrária, de "comandos avançados". Trata-se dos casos em que os comandos são aplicados para conceder e revogar direitos sobre a criação de elementos no banco de dados ou sobre a administração de elementos do sistema de banco de dados.

O que determina o uso dos comandos do módulo funcional DCL avançado é:

a) O uso dos qualificadores GRANT ou ADMIN.

b) O uso dos comandos GRANT e REVOKE.

c) O uso de papeis para identificar os usuários.

d) O uso de um usuário sem privilégios administrativos.

e) O uso dos qualificadores SELECT e EXECUTE.

Seção 2.3

Controle de acesso de usuários em DCL. Gerenciando permissões de usuários em DCL

Diálogo aberto

Olá, aluno! Vamos a mais uma etapa de nosso aprendizado!

Imagine uma organização informatizada qualquer, que tenha um ou mais sistemas distribuídos que devam ser acessados por múltiplos usuários. Pode ser qualquer organização: um banco, uma rede de lojas, uma indústria ou um hospital. Observe que nesta organização os usuários do sistema podem ser de alguns poucos (o sistema de uma padaria, por exemplo) até muitos milhões (o sistema da Receita Federal, por exemplo). Contudo, independentemente da quantidade de usuários, teremos sempre alguns poucos perfis de uso para o sistema, dentro dos quais todos os usuários se encaixarão.

Alguns poucos perfis de administrador — se é que teremos mais de um —, alguns poucos perfis de fornecedores e parceiros, um ou dois perfis de usuários internos, um ou dois perfis de usuários externos (usuários finais) e pronto: o sistema não precisa de mais do que esse punhado de perfis para que neles consigamos definir todos aqueles que precisarão de acesso, sejam poucos ou milhões de usuários.

O que diferencia esses usuários? Em essência, é o tipo de acesso ao sistema a que eles têm direito. Em suma: o que os diferencia são seus privilégios de acesso. Agora, imagine que um desses usuários "dá um jeito" de aumentar seus privilégios, acessando porções do sistema a que normalmente não teria direito. Seria um problema e tanto, não é verdade? Pois é, é principalmente com isso que os gestores de segurança de sistemas de bancos de dados devem se preocupar diariamente.

O sr. Kim, dono da cadeia de restaurantes franqueados M@@M, está expandindo o acesso aos sistemas da empresa aos franqueados. Nesta etapa do trabalho, você, que foi contratado para cuidar da segurança dos sistemas de bancos de dados, deve criar um mapa contendo os perfis dos usuários do sistema, bem como de seus privilégios, justificando suas escolhas. Apresente seu trabalho ao Sr. Kim por meio de uma tabela organizada.

Nesta seção, você vai estudar os tipos de usuários de bancos de dados e os principais tipos de ataques a permissões de bancos e dados. Também, vai estudar o uso do DCL para gerenciar as permissões de acesso, bem como a integração do gerenciamento de permissões de bancos de dados com outros sistemas de permissão e autenticação. O objetivo é entender quais são os perfis de uso de um banco de dados, com seus privilégios e responsabilidades. Também é nosso objetivo entender quais são os abusos cometidos por meio dos privilégios, suas causas, consequências e prevenções.

Não pode faltar

Para entendermos quais são os ataques às permissões de um banco de dados e entendermos como podemos usar o módulo funcional DCL (Data Control Language ou linguagem de controle de dados) para nos defendermos destes ataques, é importante primeiro conhecermos os perfis básicos de usuários de um sistema genérico de bancos de dados.

Vamos nos familiarizar com esses perfis a partir de agora:

Tipos de usuários de bancos de dados

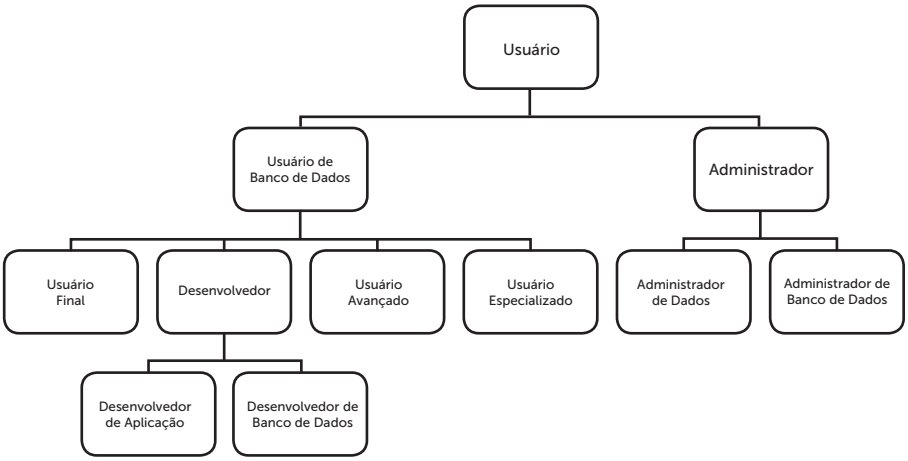
No uso de banco de dados, há a necessidade de categorizarmos (para fins de organização) vários tipos de usuário, como nos mostra Pires (2009), dividindo os indivíduos que interagem com os bancos de dados em dois grupos básicos, a saber:

• **usuário de bancos de dados** – aquele que interage direta ou indiretamente com os bancos de dados, mas não tem responsabilidade administrativa sobre estes;

• **administrador** – aquele que interage diretamente com os bancos de dados, atende as necessidades dos usuários e zela pela organização e pela segurança de todos sob sua guarda, sejam eles bancos de dados ou usuários.

Com essas duas grandes categorias, podemos estabelecer um diagrama que organiza assim aqueles que interagem com os bancos de dados, como podemos ver na Figura 2.2, a seguir (PIRES, 2009):

Figura 2.2 | Pessoas em ambientes diversos realizando atividades diversas



Fonte: Pires (2009, p. 12).

Assimile

Há dois tipos de indivíduos com acesso aos bancos de dados: os usuários e os administradores.

Vamos analisar cada um dos elementos que compõem esse diagrama (PIRES, 2009):

• **usuário final** – é o indivíduo que se configura como o objetivo maior dos bancos de dados, pois é ele quem vai se beneficiar dos dados e informações ali armazenados.

• **tipo de interação** – indireta, por meio dos aplicativos disponibilizados pelos administradores;

• **tipo de acesso** – acesso de leitura restrito aos dados de sua alçada, geralmente, dados pessoais, por ele inseridos nos bancos de dados, ou que dizem respeito a ele e ao seu contexto nos aplicativos em questão. Acesso de escrita restrito, ainda, apenas para fins de correção, ou sobre dados que não afetarão o funcionamento do sistema (no caso dos privilégios de remoção de dados);

• **privilégios** – os mais básicos. Geralmente privilégios restritos de consulta aos dados pertinentes ao seu contexto de atuação e inserção/deleção restrita de dados, também aos dados pertinentes ao seu contexto de atuação;

• **exemplos** – cliente de um banco, paciente de um hospital, contribuinte da Receita Federal;

• **usuário especializado** – geralmente é um funcionário e/ou executivo da organização, que não somente interage com as aplicações, mas também tem acesso aos bancos de dados em si, consultando-os para fins administrativos.

• **tipo de interação** – direta, por meio do próprio SGBD, e indireta, por meio de aplicações. Seu acesso por meio do próprio SGBD se dá por meio da linguagem SQL e dos módulos funcionais do SQL aos quais tem acesso. Seu principal propósito para com os bancos de dados é a consulta para fins de análise estratégica e operacional, com vistas a beneficiar a organização;

• **tipo de acesso** – acesso de leitura sobre contextos de atuação pertinentes ao seu papel na organização, geralmente envolvendo dados estratégicos e operacionais da própria organização, que extrapolam os dados e contextos pessoais, englobando contextos de vários usuários e aplicações. Acesso de escrita menos limitado que os usuários finais, podendo os usuários avançados criar contextos de dados e tabelas a partir de outras tabelas e contextos;

• **privilégios** – privilégios amplos de leitura sobre todos os contextos e aplicações de sua alçada, privilégios de criação de esquemas e bancos de dados e de inserção de dados nos mesmos. Privilégios amplos em consultas (restrições, quando existem, se limitam aos dados de administração do próprio sistema);

• **exemplos** – executivos e gestores da organização, consultores prestando serviços à organização.

• **usuário avançado** – são "híbridos" de usuários e desenvolvedores, interagindo com o SGBD com o objetivo de desenvolver aplicações especializadas, a exemplo de datawarehouse, que é uma coleção de dados provenientes de vários bancos de dados, armazenados e organizados de forma a permitir análises que objetivam a combinação de dados para a identificação de padrões e informações (BALTZAN, PHILLIPS, 2013), com foco nos dados dos bancos de dados (ao invés de focar em uso para estes dados, como no caso dos demais tipos de aplicativos).

• **tipo de interação** – interação direta com os bancos de dados por meio das aplicações especializadas que desenvolvem, geralmente aplicações de datawarehouse;

• **tipo de acesso** – geralmente irrestrito de leitura dos dados, a menos que seja dos dados administrativos que não são foco das aplicações de *datawarehouse*. Acesso irrestrito para criação de estruturas de dados, uma vez que serão necessárias para as aplicações de *datawarehouse*, sendo desenvolvidas e refinadas;

• **privilégios** – bastantes amplos durante o desenvolvimento e refino de aplicações de datawarehouse, mas sempre dispensados com base nas necessidades impostas por esses fins. Apesar desse amplo grau de liberdade, os privilégios sempre estarão

atrelados à necessidade, sendo revogados quando a necessidade não mais existir (como é o caso de qualquer privilégio de qualquer tipo de usuário);

• **exemplos** – desenvolvedores de aplicações de datawarehouse, desenvolvedores de aplicações de gestão do conhecimento.

• **desenvolvedor de aplicação** – diferentemente do que ocorre com o que chamamos de "usuário avançado", no caso do "desenvolvedor de aplicação" temos um usuário cujo foco de atenção é no uso que se faz dos dados, e não nos dados em si. Seu interesse é mais amplo, mais genérico, pois visa atender necessidades dos demais usuários, por meio de aplicações criadas para o processamento e a análise dos dados.

• **tipo de interação** – o desenvolvedor de aplicações interage indiretamente com os bancos de dados, por meio das aplicações que desenvolve. Ainda assim, isto é, ainda que ele não tenha a necessidade de emitir comandos diretos na interface do SQL, esses comandos estão à sua disposição por meio dos aplicativos que ele desenvolve;

• **tipo de acesso** – por suas necessidades pessoais, o desenvolvedor de aplicações poderia ter acesso direto bastante restrito, se é que algum. Contudo, os aplicativos que desenvolve precisam de acesso praticamente irrestrito de leitura e escrita sobre os dados, uma vez que é para isso que são desenvolvidos. Dessa forma, para manter a coerência de restrições de acesso aos dados, os acessos de escrita e leitura do desenvolvedor de aplicações são tão amplos quanto das aplicações que ele desenvolve;

• **privilégios** – também, por força da necessidade de desenvolver software, os privilégios de acesso do desenvolvedor são tão extensos quanto os privilégios necessários às aplicações que ele desenvolve;

• **exemplos** – desenvolvedor de aplicações Web, desenvolvedor de aplicações móveis.

• **desenvolvedor de bancos de dados** – este é um caso diferente do desenvolvedor de aplicações, pois ele desenvolve visando principalmente os usuários avançados (gestores, executivos e consultores da empresa, como visto anteriormente) e não os usuários internos. Também pode desenvolver partes de aplicações genéricas que lidam diretamente com os bancos de dados (algo que ocorre com certa frequência, uma vez que, por questões de desempenho, há partes de código de interação com bancos de dados que ficam mais eficientes se desenvolvidas diretamente em procedimentos escritos em SQL).

• **tipo de interação** – esse usuário interage diretamente com os bancos de dados;

• **tipo de acesso** – geralmente têm acesso bastante amplo de leitura e escrita, assumindo, inclusive, papéis administrativos em alguns momentos do desempenho de suas funções como desenvolvedores;

• **privilégios** – bastantes amplos sobre estruturas, dados, usuários e o sistema em si;

• **exemplos** – desenvolvedor de aplicações internas para executivos da organização em busca de informações estratégicas nos dados armazenados.

• **administrador de dados** – se comparássemos os administradores de bancos de dados a médicos, o administrador de dados seria o psiquiatra: responsável pela saúde "mental" dos dados, isto é, por sua semântica, pelos relacionamentos que mantêm uns com os outros, com a consistência das informações. É o responsável por determinar o modo pelo qual as aplicações compartilham suas informações.

• **tipo de interação** – interage diretamente com os bancos de dados no desempenho de sua função;

• **tipo de acesso** – tem acesso irrestrito de leitura e escrita sobre quaisquer dados e quaisquer domínios e estruturas de dados, bem como amplo acesso sobre usuários e estruturas administrativas;

• **privilégios** – irrestritos no que tange domínios e estruturas de dados, podendo ter restrições apenas no que tange a administração física dos dados e do sistema;

• **exemplos** – administrador de dados, administrador do banco de dados (DBA, pois podem ser a mesma pessoa, ocupando duas funções).

• **administrador de bancos de dados (DBA)** – na analogia dos administradores como médicos, o DBA é o clínico geral, responsável pela saúde "física" dos dados. Ele tem participação nas definições lógicas do projeto, mas sempre com vistas à consistência física do ambiente como um todo, pois é ele que vai executar os projetos sob o ponto de vista físico. É responsável por todas as atividades de implantação e manutenção no sistema de bancos de dados e nos bancos de dados em si.

• **tipo de interação** – interage diretamente com os bancos de dados no exercício de suas funções;

• **tipo de acesso** – irrestrito de leitura e escrita;

• **privilégios** – privilégios de administrador, muitas vezes conhecido como "superusuário";

• **exemplos** – administrador de bancos de dados (DBA).

É importante salientar que apesar dessa lista não ser numerada/hierarquizada, podemos observar que nela existe uma ordem crescente no tocante aos privilégios, desde o usuário, que tem as maiores restrições, até o DBA, que tem todos os privilégios.

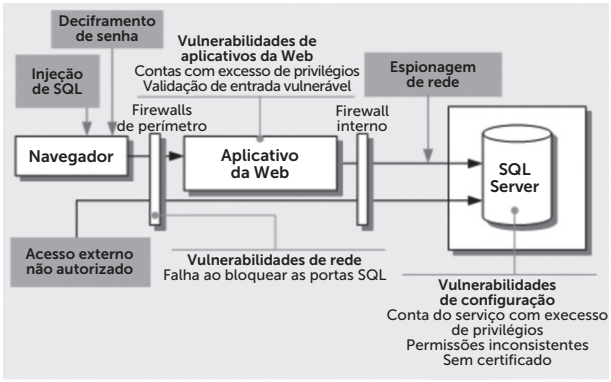
Reflita

Se um usuário especializado tem praticamente todos os privilégios de um administrador de dados, faz sentido que haja, então, perfis diferentes?

Tipos de ataques em permissões de bancos de dados

Antes de falarmos sobre ataques às permissões dos bancos de dados é útil observarmos um esquema lógico de uma implantação típica de bancos de dados. Na visão de Azevedo Filho e Costa (2008), podemos observar que o servidor SQL se encontra geralmente protegido por nada menos que dois firewalls (um firewall de perímetro e um firewall interno), como podemos ver na Figura 2.3:

Figura 2.3 | Principais ameaças ao servidor de bancos de dados



Fonte: Azevedo Filho e Costa (2008, p. 3).

Podemos notar também, que vários elementos propiciam pontos de ataque e que dois deles, em particular, nos remetem a ameaças com permissões em sua raiz:

• **aplicativos Web** – podem conter contas com excesso de privilégio e pontos vulneráveis de entrada;

• **servidor SQL** – pode conter contas com excesso de privilégio, bem como permissões inconsistentes de acesso ou acesso sem certificado.

Em que pese haver vários pontos delicados no que diz respeito à segurança da informação como um todo, vamos nos concentrar nos problemas que concernem às permissões (privilégios), nos bancos de dados.

Segundo Perallis (2015), entre as dez principais causas de ataques a bancos de dados no ano de 2015, as duas que ocupam as posições principais dizem respeito a privilégios. São elas:

1. Privilégios excessivos ou esquecidos.

2. Abuso de privilégios concedidos.

Outras causas muitas vezes em destaque em notícias da mídia, tais como malware, negação de serviço e SQL Injection ocupam posições menos proeminentes do que essas duas, o que já nos dá uma medida do problema de negligenciarmos a importância de um bom gerenciamento de privilégios em bancos de dados.

Vamos analisar em mais detalhes essas duas causas de ataques, entendendo como funcionam, as ameaças potenciais e — principalmente — como podemos trabalhar em sua prevenção. Para fins de análise, o primeiro item será quebrado em dois, uma vez que os problemas no caso de privilégios esquecidos tendem a ser mais graves, e as prevenções são diferentes (PERALLIS, 2015):

• **privilégios excessivos** – o usuário tem privilégios acima do que é necessário para realizar suas ações de direito, ou o nível de privilégios necessário para essas ações inclui privilégios não planejados.

• **ameaças potenciais** – uso dos privilégios para gerar benefícios indevidos (próprios ou a terceiros); uso dos privilégios para prejudicar outros usuários ou a própria organização;

• **prevenção** – começa por uma definição detalhada dos privilégios e as ações que permitem, passando por uma política robusta de atribuição e acompanhamento de privilégios, com auditorias periódicas, incluindo análises de como os usuários utilizam os privilégios a eles atribuídos.

• **privilégios esquecidos** – funcionários que mudam de função dentro da organização ou — pior — são desligados, mas mantêm-se os privilégios aos quais já não têm mais direito. O mesmo pode ocorrer com usuários externos do sistema.

• **ameaças potenciais** – os abusos, no caso de usuários que ainda pertencem à organização ainda podem ser "comedidos", uma vez que ainda há ligação trabalhista do indivíduo para com a organização em questão, mas ainda assim pode haver conflitos de interesse entre a função atual (que já não dá mais direito ao acesso) e a função anterior (cujos privilégios foram esquecidos). A possibilidade de roubo de informações e/ou abuso de informações ainda é presente, e não deve ser descartada;

• **prevenção** – a política de atribuição/revogação de privilégios deve contemplar especificamente tanto a mudança de posição do funcionário como o desligamento. No caso da mudança de função, o ideal é haver uma revisão detalhada de privilégios atribuídos contra os privilégios necessários a partir de agora, com a revogação imediata dos privilégios já desnecessários, bem como a atribuição dos novos privilégios. No caso do desligamento, o funcionário deve ter todos os seus privilégios de acesso a todos os sistemas removidos de imediato, preferencialmente antes mesmo de deixar o local físico da organização.

• **abuso de privilégios concedidos** – usuários podem utilizar privilégios concedidos para um fim com objetivos diversos daqueles para os quais foram concedidos, obtendo acesos indevidos e com eles podendo derivar benefícios ilícitos e/ou prejudicar outros usuários e a organização.

• **ameaças potenciais** – acesso, por meio de credenciais válidas, a sistemas com ferramentas não autorizadas. Um exemplo é o acesso a certos sistemas que permitem apenas o acesso individual a registros, por meio de uma interface gráfica. O usuário mal-intencionado pode usar, por exemplo, um programa de planilha eletrônica com suas credenciais de acesso e, através dessa planilha eletrônica acessar os dados em bloco, descumprindo o propósito do privilégio;

• **prevenção** – analisar criteriosamente os candidatos a privilégios antes de sua implantação, executando análises de cenários possíveis de utilização desses candidatos. Frequentar fóruns de segurança onde questões de abuso de privilégio são discutidas por administradores de bancos de dados, pois os problemas enfrentados por outros DBAs podem ser imensamente úteis na prevenção em nosso sistema.

Exemplificando

Em setembro de 2016, um escândalo no Wells Fargo Bank (o maior banco privado dos EUA) veio à tona. Empregados do banco abusaram dos privilégios de criação de contas, criando mais de 2 milhões de contas correntes e contas poupança em nome de correntistas, transferindo pequenas somas de dinheiro para estas contas, emitindo cartões de débito e de crédito, e cobrando taxas dos clientes para essas contas, tudo sem autorização ou mesmo conhecimento por parte dos clientes (GLAZER, 2016; WATSON, 2016).

Usando o DCL para gerenciar permissões de acesso

Já vimos o módulo funcional DCL em detalhes nas seções anteriores, mas é importante frisarmos o uso de alguns de seus principais comandos específicos de concessão e revogação de privilégios. Vejamos os comandos:

• CONNECT – conexão com o banco de dados. Permite que um usuário se conecte com o banco de dados e nele realize as ações que tem (ou terá) privilégios a realizar. Exemplo de concessão de privilégio para que o usuário "Usuario3" se conecte com o contexto de banco de dados sendo administrado por quem emite o comando GRANT:

GRANT CONNECT Usuario3;

• SELECT – acesso a consultas em tabelas específicas (estabelecidas no próprio comando) do contexto de banco de dados em que se está conectado. Exemplo que dá acesso de consulta à tabela "Tabela01" ao usuário "Usuario5";

GRANT SELECT ON Tabela01 **TO** Usuario5;

• INSERT – acesso de inserção de dados (registros) em uma tabela por um usuário ou papel. Exemplo de concessão de privilégio de inserção de registros na tabela "Tabela01" ao usuário "USUARIO7":

GRANT INSERT ON Tabela01 **TO** Usuario7;

• VIEW SERVER STATE – acesso dado a usuários avançados, desenvolvedores e administradores para que possam ver os metadados (variáveis de estado) do servidor. Exemplo de concessão de visualização de metadados ao usuário "Usuario10".

Essa lista não pretende ser extensa, obviamente. É, contudo, um subconjunto importante e significativo do uso do módulo funcional DCL para controle de acesso a elementos do banco de dados.

Pesquise mais

Para saber a extensão do que é possível fazer em termos de atribuição de privilégios, recomenda-se que o aluno estude a fundo os próprios comandos do SQL, que são passíveis de privilégios. 1KEYDATA, Tutorial de SQL, site 1keydata.com, 2016. Disponível em: <http://www.1keydata.com/pt/sql/>. Acesso em: 22 nov. 2016.

Integrando o gerenciamento de permissões de BD com outros sistemas de permissão

Antes de falarmos sobre a integração do gerenciamento de permissões dos bancos de dados com outros sistemas de permissões, é necessário relembrarmos alguns conceitos importantes aceca de sistemas de permissão. É necessário estabelecermos dois conceitos fundamentais sobre os sistemas de permissão. São eles (UBUNTU, 2013):

• **autenticação** – garantia de que o usuário requerendo acesso é quem diz ser. Pode ocorrer por meio de um fator (senha, token ou biometria) ou dois fatores (senha mais token, senha mais biometria, token mais biometria). Apenas o usuário com as credenciais adequadas é considerado autêntico, isto é, consegue demonstrar sua identidade o suficiente para ter acesso ao sistema;

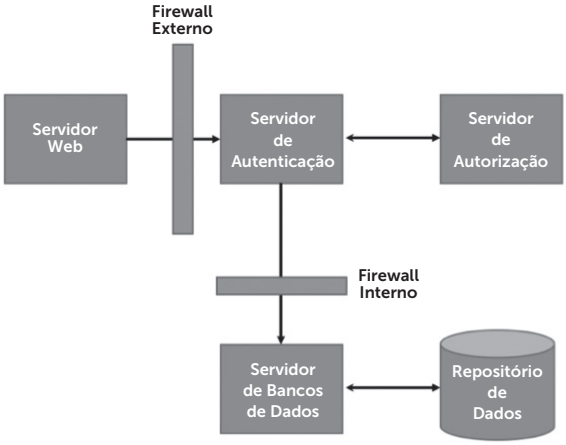
• **Exemplo**: Sistema Kerberos de autenticação, amplamente integrável aos SGBD para autenticação de usuários.

• **autorização** – Uma vez autenticado o usuário, ele deve ser autorizado, isto é, deve ocorrer uma verificação de sua identidade e uma atribuição de um conjunto de autorizações de acessos e ações a porções do sistema (que pode ser um sistema complexo, composto por rede, dispositivos e sistemas).

• **Exemplo**: sistema *lightweight directory access protocol*, ou protocolo leve de acesso a diretório (LDAP), um sistema de autorização de uso genérico também altamente integrável aos SGBD para delimitação de acesso, que se traduz em privilégios de acesso aos bancos de dados.

Em uma solução de bancos de dados — como é o caso para vários ambientes e soluções que exigem controle de acesso — é fundamental que ambas as tarefas sejam realizadas: autenticação e autorização do usuário, antes que esse tenha acesso ao sistema em si, seja diretamente ou por meio de alguma aplicação. Vejamos, a seguir, como os sistemas de autenticação e autorização se encaixam no ambiente (AZEVEDO FILHO; COSTA, 2008):

Figura 2.4 | Integração dos bancos de dados com os sistemas de autenticação e autorização



Fonte: adaptada de Azevedo Filho e Costa (2008).

Na Figura 2.4 temos que o ponto de entrada do sistema é o Servidor Web, por onde o usuário faz seu acesso. Esse acesso deve passar primeiro obrigatoriamente pela autenticação (Servidor de Autenticação), e caso o usuário apresente credenciais adequadas, deve passar pelo processo de autorização (Servidor de Autorização). Devidamente autorizado, só então terá acesso ao Servidor de Banco de Dados, por meio da aplicação, podendo acessar as porções desse sistema a que tenha direito.

Sem medo de errar

Como seu objetivo nesta etapa é criar um mapa contendo os perfis dos usuários do sistema, bem como de seus privilégios, esse trabalho deve ter início com uma política de segurança robusta, que inclua um levantamento criterioso de necessidades de acesso de todos os envolvidos, para daí definir perfis de uso. Os tipos de usuários estudados servem como guia para a definição dos perfis e de seus privilégios.

Podemos definir os seguintes passos na resolução desta situação-problema:

1. Estabelecer formalmente a necessidade de uma política de segurança para a M@@M, já englobando o novo sistema que dá acesso aos franqueados.

2. Estabelecer a necessidade de uma porção do plano que enderece as necessidades de acesso e os procedimentos e limites para esse acesso.

3. Criar e manter em mãos uma lista com os tipos genéricos de acesso aos bancos de dados.

4. Criar uma lista com os tipos de usuários do sistema, estabelecendo, em linhas gerais, os privilégios que lhes serão atribuídos.

5. Encaixar os tipos genéricos de acesso aos tipos de usuários do sistema da M@@M (não é um problema se o mesmo tipo genérico for atribuído a mais de um perfil de acesso ao sistema, desde que sejam identificadas necessidades de manter privilégios diferentes para cada perfil).

6. Apresentar o quadro em forma de uma tabela para o Sr. Kim.

Podemos usar a seguinte tabela para apresentar o trabalho:

Tabela 2.1 | Perfis de acesso

Nome do perfil	Tipo genérico	Tipo(s) de acesso	Privilégios	Restrições	Observações
DBA	Administrador de banco de dados	Direto	Totais de leitura e escrita	N/A	
Desenvolvedor					
Franqueado					
Cliente					

Fonte: elaborada pelo autor.

Atenção

É fundamental que a definição dos perfis e privilégios seja resultado de uma política ampla de segurança de acesso, e que essa definição ocorra no momento correto, sem queimar etapas, sendo testada e averiguada antes de sua implantação final.

Avançando na prática

Removendo privilégios desnecessários (e perigosos)

Descrição da situação-problema

Você foi contratado como gestor de segurança da D@@D, uma empresa que presta suporte telefônico a vários tipos de negócios, terceirizando serviços de atendimento para centenas de empresas. Recentemente, uma notícia vem tirando o sono dos executivos da D@@D: uma empresa concorrente no ramo de serviços de atendimento telefônico, chamada Pizza, anunciou que um de seus ex-empregados ganhou acesso ao sistema e apagou os registros em andamento de vários clientes, bem como marcou dezenas de registros como "fechados" ou "resolvidos", quando estes ainda precisavam de atenção. A ação indevida gerou caos durante vários dias na operação da Pizza, e só não foi pior porque, no fim de semana, a empresa decidiu parar as operações e restabelecer um backup do sistema.

Você está ciente de que o "giro" de empregados em uma empresa de atendimento telefônico é altíssimo, com empregados entrando e saindo do quadro de funcionários diariamente. O problema da Pizza, em suma, pode muito bem vir a ocorrer na D@@D. Que medidas devem ser tomadas para prevenir o acontecimento de uma situação semelhante?

Resolução da situação-problema

Uma avaliação criteriosa nos processos e procedimentos de segurança de acesso aos sistemas da D@@D deve ocorrer o mais brevemente possível. Uma sequência de ações recomendável é a seguinte:

1. Revisão na política de acesso da D@@D, identificando os privilégios de acesso de todos os funcionários, visando identificar privilégios indevidos que estejam sendo atribuídos (um funcionário não deveria ter o privilégio de apagar registros, como ocorreu na Pizza-Desk, por exemplo).

2. Revisão nos procedimentos de desligamento de funcionários, estabelecendo que a remoção de acesso ocorra imediatamente antes de o funcionário receber a

notícia de seu desligamento, ou imediatamente após este funcionário solicitar seu desligamento. Esse procedimento minimiza a possibilidade de ações maliciosas dos funcionários desligados ou que requisitam desligamento.

3. Estabelecer procedimentos de acompanhamento aleatório de uso do sistema por parte dos funcionários, identificando potenciais abusos de privilégio, o que permitirá agir sobre todos os funcionários quando for identificado um caso de exceção.

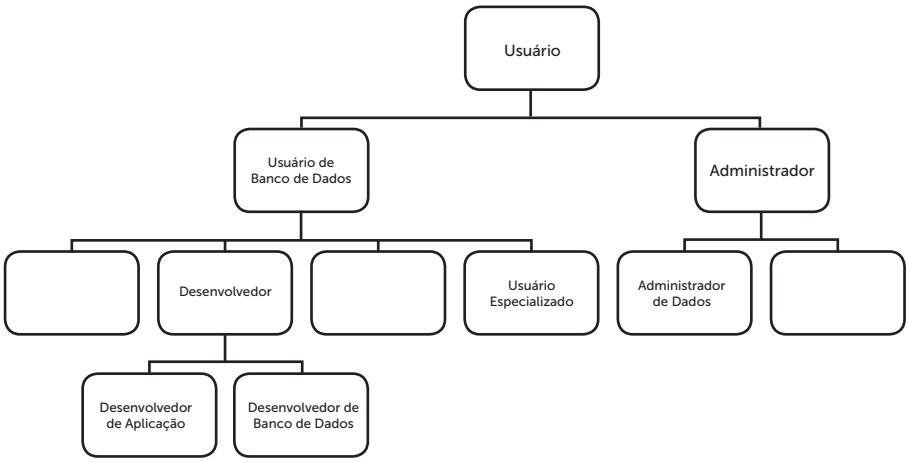
Faça valer a pena

1. No uso de banco de dados, há a necessidade de vários tipos de usuário, como nos mostra Pires (2009), dividindo os indivíduos que interagem com os bancos de dados em dois grupos básicos, a saber:

• **usuário de bancos de dados** – aquele que interage direta ou indiretamente com os bancos de dados, mas não tem responsabilidade administrativa sobre estes;

• **administrador** – aquele que interage diretamente com os bancos de dados, atende as necessidades dos usuários e zela pela organização e pela segurança de todos sob sua guarda, sejam eles bancos de dados ou usuários.

Com essas duas grandes categorias, podemos estabelecer um diagrama que organiza assim aqueles que interagem com os bancos de dados (PIRES, 2009, p. 12):



Assinale a alternativa que preenche corretamente os quadros vagos do diagrama acima:

a) Usuário Simples, Usuário Híbrido, Desenvolvedor de Dados.

b) Usuário simples, Usuário Final, Usuário Avançado.

c) Usuário Final, Usuário Avançado, Desenvolvedor de Dados.

d) Usuário Final, Usuário Avançado, Administrador de Dados.

e) Usuário Final, Administrador de Dados, Desenvolvedor de Dados.

2. Na visão de Azevedo Filho e Costa (2008), podemos observar que o servidor SQL encontra-se geralmente protegido por nada menos que dois firewalls (um firewall de perímetro e um firewall interno). Ou seja: há uma preocupação grande e constante com a segurança do servidor de bancos de dados.

Em que pese haver vários pontos possíveis de ataque em uma infraestrutura de bancos de dados, dois destes elementos propiciam ataques potenciais às permissões. São eles:

a) Firewall externo e firewall interno.

b) Servidor Web e firewall externo.

c) Aplicativos Web e servidor SQL.

d) Servidor Web e firewall interno.

e) Firewall externo e servidor SQL.

3. Em uma solução de bancos de dados — como é o caso para vários ambientes e soluções que exigem controle de acesso — é fundamental que ambas as tarefas sejam realizadas: _____ e _____ do usuário, antes que este tenha acesso ao sistema em si, seja diretamente ou por meio de alguma aplicação.

No que concerne às permissões de acesso aos bancos de dados, assinale a alternativa que completa corretamente as lacunas do texto anterior:

a) autenticação e autorização.

b) criptografia e login.

c) cadastro e atribuição.

d) cadastro e autorização.

e) login e atribuição.

Referências

AZEVEDO FILHO, E.; COSTA, M. C. L. **Segurança em servidores com banco de dados Microsoft SQL Server**: meios de proteção contra invasões. In: SEMINÁRIO DE EXCELÊNCIA EM GESTÃO E TECNOLOGIA, 5., 2008, Rio de Janeiro. **Anais**... Rio de Janeiro: SEGeT, 2008. 9 p. Disponível em: <http://www.aedb.br/seget/arquivos/artigos08/261_261_Seguranca.pdf>. Acesso em: 22 nov. 2016.

BALTZAN, P.; PHILLIPS, A. **Essentials of business driven information systems**. 4. ed. Nova York: McGraw-Hill, 2013.

BURLESON Consulting. **System_privilege_map tips**. 28 ago. 2015. Disponível em: <http://www.dba-oracle.com/t_system_privilege_map.htm>. Acesso em 22 nov. 2016.

ELMASRI, R.; NAVATHE, S. B. **Sistemas de bancos de dados**. São Paulo: Pearson Addison Wesley, 2005.

GLAZER, E. Wells Fargo to pay $185 million fine over account openings. **The Wall Street Journal**, 8 set. 2016. Disponível em: <http://www.wsj.com/articles/wells-fargo-to-pay-185-million-fine-over-account-openings-1473352548>. Acesso em: 22 nov. 2016.

GUPTA, S. K. Oracle DCL Data Control Language. **Club Oracle**, 8 nov. 2010. Disponível em: <http://www.club-oracle.com/threads/oracle-dcl-data-control-language.16248/>. Acesso em: 22 nov. 2016.

ISO/IEC 9075-1. **Information technology** – database languages – SQL – Part 1 – framework (SQL framework). Londres: International Organization for Standadization, 2008.

MARTINS, F. C., CANDIDO JUNIOR, E. **Segurança em Banco de Dados**: Conceitos e Aplicações. ETIC, v. 10, n. 10, out. 2014. Disponível em <http://intertemas.toledoprudente.edu.br/revista/index.php/ETIC/article/viewFile/4412/4172>. Acesso em: 2 ago. 2016.

MICROSOFT. **Permissões de objeto GRANT** (Transact-SQL). Microsoft, 2016. Disponível em: <https://msdn.microsoft.com/pt-br/library/ms188371.aspx>. Acesso em: 22 nov. 2016.

_____. **Permissões de objeto REVOKE** (Transact-SQL). Microsoft, 2016. Disponível em: <https://msdn.microsoft.com/pt-br/library/ms187719.aspx>. Acesso em: 22 nov. 2016.

_____. **Create Role** (Transact-SQL). Microsoft, 2016. Disponível em: <https://msdn.microsoft.com/pt-br/library/ms187936.aspx>. Acesso em: 22 nov. 2016.

MURRAY, M. C. Database security: what students need to know. **Journal of Information**

Technology and Education, v. 9, p. 61-77, 2010. Disponível em <http://jite.org/documents/Vol9/JITEv9IIPp061-077Murray804.pdf>. Acesso em: 22 nov. 2016.

MOTTA, G. H. M.; FURUIE, S. **MACA**: uma ferramenta de autorização e controle de acesso para o prontuário eletrônico de pacientes. ResearchGate, 2014. Disponível em <https://www.researchgate.net/profile/Gustavo_Motta2/publication/268416335_MACA_Uma_Ferramenta_de_Autorizacao_e_Controle_de_Acesso_para_o_Prontuario_Eletronico_de_Pacientes/links/54bd3f700cf218da9391acd1.pdf>. Acesso em: 21 nov. 2016.

ORACLECOACH. Oracle SQL Tutorial – Data Control Language – System Privilegies (Theory). 6 jan. 2011. Disponível em: <https://www.youtube.com/watch?v=MUqZ5U7VIMk>. Acesso em: 22 nov. 2016.

PERALLIS, V. R. C. 10 principais causas de ataques a bancos de dados. **Perallis IT Innovation**, 2015. Disponível em: <http://www.perallis.com/news/10-principais-causas-de-ataques-a-banco-de-dados>. Acesso em: 23 set. 2016.

PIRES, C. E. **Conhecendo os usuários de um sistema de bancos de dados**. Site de Ciências da Computação da Universidade Federal de Campo Grande, 9 dez. 2009. Disponível em: <http://www.dsc.ufcg.edu.br/~cesp/publications/Palestra_Grupo_PET_DSC_UFCG.pdf>. Acesso em: 22 nov. 2016.

PRATT, P. J.; LAST, M. Z. **A guide to SQL**. 8. ed. Boston: Course Technology, 2008.

STUDYTONIGHT. DCL Command. **Study Tonight**, 2014. Disponível em: <http://www.studytonight.com/dbms/dcl-command>. Acesso em: 22 nov. 2016.

UBUNTU. Kerberos e LDAP. **Ubuntu Documentation**, 2013. Disponível em: <https://help.ubuntu.com/lts/serverguide/kerberos-ldap.html>. Acesso em: 22 nov. 2016.

WATSON, P. W. Wells Fargo scandal shows next bank crisis coming. **Forbes**, 15 set. 2016. Disponível em: <http://www.forbes.com/sites/patrickwwatson/2016/09/15/wells-fargo-scandal-shows-next-bank-crisis-coming/#7e6d569a69ec>. Acesso em: 22 nov. 2016.

Segurança em bancos de dados móveis

Convite ao estudo

Aluno, seja bem-vindo à unidade três de nossos estudos acerca de segurança de bancos de dados.

Até o momento, revimos alguns conceitos importantes sobre segurança da informação na Unidade 1, entrando, depois, nos mecanismos de controle de acesso a bancos de dados, na Unidade 2. Agora, é chegado o momento de entendermos os aspectos de segurança em bancos de dados móveis.

Lembrando que, com esta disciplina, você vai conhecer as políticas de segurança lógica e física de dados e defini-las. Mais especificamente nesta unidade, você vai conhecer e utilizar técnicas para segurança de bancos de dados e seus servidores.

Os objetivos específicos desta unidade são:

- compreender o que são os bancos de dados móveis e para que servem, bem como os riscos inerentes aos bancos de dados móveis e também como fazer os controles e proteções aos bancos de dados móveis;

- entender o que são metadados e qual sua relação com os dados em uma aplicação, bem como o que é comprometimento de uma comunicação por via aérea e qual o papel dos metadados neste comprometimento; dessa forma, buscar entender a relação entre consistência e interrupção e os riscos inerentes aos metadados na comunicação de aplicativos móveis;

- compreender o que são e como funcionam os firewalls de bancos de dados, bem como o modo como deve ser aplicada a criptografia, para proteger as informações dos bancos de dados. Além disso, entender o que é, para que serve e, ainda, como realizar a auditoria de bancos de dados e a análise de privilégios em bancos de dados.

Você já percebeu como os dispositivos móveis cada vez mais têm um papel importante em nossas vidas? E não é de hoje: desde que os laptops começaram a se popularizar, ainda na década de 1990, o caminho tem sido o da miniaturização. Com a chegada dos celulares da Blackberry ao mercado, no final daquela década, inaugurava-se a era dos smartphones, pois, além de fazer e receber chamadas, os celulares passavam a desempenhar novas tarefas, como enviar e receber mensagens de correio eletrônico, manter agendas e muito mais. Desde então, os aparelhos têm crescido sem parar em potência e em versatilidade. Com mais de dois milhões de aplicativos disponíveis tanto na Apple App Store quanto na Google Play Store, as possibilidades de produtividade com os smartphones são gigantescas, e muitos são os profissionais que hoje dependem menos dos computadores convencionais. Muitos até mesmo os abandonam.

Pensando nessa mudança de foco para os dispositivos móveis, a empresária Talínia decidiu usar essa tecnologia para expandir seus negócios. Dona de uma rede de brechós em São Paulo, chamada Tutti Bella, ela decidiu investir em um aplicativo móvel por meio do qual seu time comercial — um grupo de dez funcionários cujo trabalho é visitar lojas, brechós e residências em busca de novos estoques, além de serem responsáveis por fazer girar os materiais parados há mais tempo — terá mais agilidade em catalogar produtos em oferta por lojas e pessoas físicas, bem como em vender estoques parados. Talínia contratou você para ajudá-la com os aspectos desse novo sistema, em específico com os bancos de dados móveis, que ela ainda não sabe direito para que servem ou que papel terão no sistema. Será que é necessário mesmo o uso de bancos de dados móveis? Quais são os riscos envolvidos? Como proteger os dados nesse ambiente?

Na primeira seção desta unidade, serão discutidos os riscos de segurança em bancos de dados móveis, bem como as prevenções contra a incidência dos impactos potencialmente resultantes desses riscos. Na segunda seção, serão abordados os detalhes da comunicação com bancos de dados móveis e como proteger essa comunicação. Na terceira seção, serão estudados os bancos de dados móveis comerciais, bem como as proteções que oferecem aos usuários.

Seção 3.1

Áreas de segurança em bancos de dados móveis

Diálogo aberto

Olá!

A expressão "revolução digital" diz respeito à adoção em massa dos computadores em todos os ramos da sociedade. Isso não é novidade: desde a introdução do computador, lá no início da década de 1940, temos visto estes dispositivos ocupando cada vez mais um papel central em nossas vidas, pois são ferramentas formidavelmente úteis onde aplicadas.

Mas em que pese essa revolução já ser profundamente importante, você já percebeu que temos ainda outra revolução em curso? Podemos até chamá-la de uma revolução dentro da revolução digital: a revolução dos dispositivos móveis.

Já percebeu o quanto nossas vidas, cada vez mais, são apoiadas por esses pequenos computadores de bolso? Sob forma de smartphones e tablets, cada vez mais dependemos deles para nossas atividades diárias e cada vez mais podemos ser produtivos e estar conectados, tudo graças a esses pequenos milagres digitais. Pois é, mas nem tudo são flores.

Quando você usa algum aplicativo no seu smartphone, há riscos inerentes aos bancos de dados móveis presentes no aparelho? Se há, quais são e como preveni-los?

Essas e outras questões inerentes aos riscos que surgem com a presença de bancos de dados móveis são a preocupação atual de Talínia, a empresária paulistana que te contratou para cuidar da segurança de sua nova aplicação, a qual auxiliará seus funcionários de campo a comercializar (comprar e vender) estoques de roupas para sua rede de brechós. Nessa etapa, você deverá mostrar à empresária que há, de fato, riscos inerentes aos bancos de dados móveis, bem como apresentar uma estratégia para prevenir os efeitos negativos desses riscos.

Na presente seção, estudaremos os riscos específicos tanto aos bancos de dados móveis quanto à mobilidade em si; entenderemos um pouco melhor os riscos inerentes

às redes wireless e terminaremos entendendo as diferenças entre a segurança nos ambientes móveis e a segurança nos ambientes estáticos.

Não pode faltar

Em que pese à segurança de bancos de dados móveis ser, em muitos aspectos, um caso particular da segurança de bancos de dados no contexto mais genérico, há vários pontos específicos que devem ser endereçados. Há, por exemplo, riscos específicos a que os bancos de dados móveis estão sujeitos, que diferem dos riscos mais genéricos estudados em segurança da informação. A partir de agora, vamos entender os riscos envolvidos em bancos de dados móveis.

Banco de dados móveis: riscos específicos

A segurança é mandatória para qualquer sistema que envolva bancos de dados e ainda mais importante quando esses sistemas estão em ambientes móveis, como afirmam Ghorbanzadeh et al. (2010).

Os aplicativos móveis são, em muitos casos, baseados em uma estrutura de bancos de dados conhecida como DDBMS, ou *Distributed Database Management System*, que, em português, traduz-se por sistema de gerenciamento de bancos de dados distribuídos (RAHIMI, HAUG, 2010). Diferentemente dos sistemas de gerenciamento de bancos de dados unitários, em que os bancos de dados são armazenados e gerenciados em apenas um local, os DDBMS (ou na sigla em português SGBDD) podem distribuir e gerenciar seus bancos de dados ao longo de vários computadores e em várias redes diferentes, desde que interligáveis (RAHIMI, HAUG, 2010).

Assimile

Nos aplicativos móveis vemos, em muitos casos, a presença de sistemas distribuídos de gerenciamento de bancos de dados, pois o usuário pode armazenar dados localmente e também ter acesso a dados armazenados em um servidor remoto.

No caso dos dispositivos móveis, Matthews e Gliser (2015) descrevem o uso de aplicativos em smartphones (principalmente) e tablets (secundariamente) como ocorrendo em pequenas "explosões", isto é, em momentos curtos de alta atividade. Os autores mencionam várias situações, entre elas (grifos nossos):

- em casa – receitas, mensagens instantâneas, jogos,
- em filas e salas de espera – redes sociais, e-mail, jogos,

- nas compras – buscas por ofertas,
- no trabalho – agenda, aplicativos corporativos,
- no trânsito – checagem de rotas.

Os grifos foram adicionados para destacar aqueles aplicativos que se valem de bancos de dados distribuídos. Um aplicativo de receitas, por exemplo, terá acesso a receitas armazenadas em algum servidor na internet, bem como um pequeno conjunto de receitas preferidas armazenadas no smartphone ou tablet, ou mesmo algumas receitas proprietárias, criadas pelo próprio usuário. Em outro caso, a agenda sincroniza as informações do usuário em vários dispositivos. A agenda do Google, por exemplo, pode ser sincronizada em computadores e em aplicativos no Android ou os que operam pelo iOS. Um evento criado no aplicativo do Android, por exemplo, vai se propagar para o servidor e será espelhado em todas as agendas do usuário, em todos os seus dispositivos.

Para esses e vários outros exemplos, é necessário que o aplicativo tenha acesso a bancos de dados no servidor, mas que também armazene dados em bancos de dados locais. Nada mais simples, uma vez que a tecnologia dos smartphones e tablets empacota poder computacional, que faz com que esses pequenos aparelhos equivalham a potentes computadores do passado.

Esses bancos de dados móveis, contudo, além de resolverem problemas e garantirem a mobilidade e a versatilidade dos dispositivos e seus aplicativos, também trazem problemas potenciais a seus usuários, problemas esses que devem ser endereçados.

O time de segurança de dispositivos móveis da OWASP (*Open Web Application Security Project*) criou uma lista, em 2014, com base em pesquisas próprias junto a usuários e provedores de aplicativos, com os dez principais riscos a que os aplicativos móveis estão sujeitos. Esses riscos são apresentados na lista "Top-10", a seguir (OWASP, 2014):

1. Controles fracos do lado do servidor,
2. Armazenamento inseguro de dados,
3. Proteção insuficiente na camada de transporte,
4. Vazamento não intencional de dados,
5. Autenticação e autorização insuficientes ou pobres,
6. Criptografia falha,
7. Injeções no dispositivo móvel,

8. Decisões de segurança baseadas em entradas não confiáveis,

9. Manipulação inadequada de sessões,

10. Falta de proteções binárias.

Os itens 1, 5 e 9 dizem respeito aos servidores de bancos de dados de aplicações móveis e já foram, de uma forma ou de outra, endereçados nas unidades 1 e 2. Os itens 6, 8 e 10 dizem respeito aos aplicativos móveis em si, e não aos bancos de dados. O item 3 diz respeito à segurança da rede de comunicação do dispositivo móvel com os servidores e será tratado mais à frente, nesta seção.

Já os itens 2, 4 e 7 dizem respeito especificamente aos bancos de dados móveis. Vamos analisá-los em maiores detalhes agora (OWASP, 2014):

- **Armazenamento inseguro de dados** – dados armazenados localmente devem estar seguros, isto é, devem estar abrigados de acessos não autorizados (confidencialidade), devem ser manipuláveis apenas por processos autorizados (integridade) e devem ser protegidos contra corrupções ou deleções não autorizadas (disponibilidade).

- **Quando ocorre** – quando os desenvolvedores assumem que o agente de ameaça não terá acesso ao sistema de arquivos do dispositivo, o que é um erro, visto que esse acesso é relativamente fácil para um atacante ou para um malware.

- **Como prevenir** – a regra número um de bancos de dados móveis, segundo a OWASP (2014, p. 1) é: "Não armazenar dados localmente, a não ser que seja absolutamente necessário". Isso porque a proteção local de dados é inerentemente mais difícil que no caso dos dispositivos não móveis, uma vez que o acesso físico aos aparelhos é bem mais factível, e o roubo de aparelhos é bem mais plausível. A criptografia é mandatória e, mesmo assim, credenciais de acesso não devem ser armazenadas no dispositivo. Durante o desenvolvimento, a decisão entre usabilidade e segurança deve sempre ter como resposta a "segurança".

- **Vazamento não intencional de dados** – ocorre quando dados de aplicações são armazenados em áreas acessíveis por aplicativos ou processos não autorizados, ou quando há falha na autenticação e autorização de elementos (usuários, aplicativos ou processos) no banco de dados, dando-lhes acesso indevido a dados que deveriam ser protegidos.

- **Como prevenir** – nesse caso, há duas frentes de prevenção: por um lado, uma política de autenticação e autorização que seja robusta e frequentemente avaliada tende a prevenir acessos indevidos de usuários, aplicativos e processos. Por outro lado, a arquitetura do sistema não deve permitir o armazenamento de dados em áreas que não sejam explicitamente protegidas pelo sistema operacional. Uma ferramenta de prevenção bastante útil nesses casos são os "pen-tests", ou "testes de penetração", que

devem ser conduzidos periodicamente sobre o sistema e sobre implantações móveis.

- **Injeções no dispositivo móvel** – a injeção de códigos ou comandos não autorizados nos aplicativos móveis se dá, em muitos casos, por meio dos bancos de dados, por meio de comandos SQL que revelam informações e atribuem privilégios não autorizados ao atacante. Esse tipo de ataque surgiu na web na década de 2000 e rapidamente migrou para os dispositivos móveis, a partir de sua popularização.

- **Como prevenir** – a forma mais eficaz de evitar as injeções de código ou comandos em dispositivos móveis é identificar e validar todas as fontes entrada que requerem acesso ao dispositivo móvel, antes de garantir o acesso. O acesso de escrita de dados deve pertencer exclusivamente ao aplicativo que manipula esses dados, sendo que outros aplicativos e processos devem ser impedidos de sequer enxergar áreas de armazenamento que não lhes tenham sido explicitamente designadas.

Reflita

O hábito de usar mecanismos de tunelamento tais como SSL e TLS apenas nos processos de autenticação e autorização do usuário data do início dos anos 2000, um tempo em que o aumento de dados e de tempo de tráfego causado pelo processo de tunelamento pesava sobre a rede. Desde então, as velocidades e capacidades de tráfego das redes cresceram sobremaneira. Será que ainda vale a pena a economia proporcionada por não se usar o tunelamento em toda a comunicação, deixando-o apenas para os processos de autenticação e autorização?

Riscos inerentes à mobilidade

É bastante importante observar que a própria natureza dos aparelhos móveis apresenta riscos visíveis para os usuários e para as organizações que os adotam: diferentemente dos dispositivos não móveis ou de outros dispositivos portáteis mais tradicionais (computadores de mesa e notebooks, por exemplo), os smartphones e tablets nos acompanham a todos os lugares que frequentamos, seja por motivos profissionais ou pessoais, e o primeiro risco inerente à mobilidade diz respeito à segurança física dos aparelhos. Ghorbanzadeh et al. (2010) citam o acesso aos dados em função de perda, furto (subtração sem a presença do proprietário e sem violência) ou roubo (subtração com a presença do proprietário e com violência ou grave ameaça) dos aparelhos como sendo uma fonte importante de preocupação para os donos, bem como para os desenvolvedores de aplicativos móveis.

Em que pese muitos roubos de aparelhos terem como objetivo apenas o aparelho em si, há casos de roubo que visam os dados do usuário.

Na primeira situação, o que o usuário pode fazer para se proteger — e, admitidamente,

estamos aqui saindo do assunto dos bancos de dados móveis — é tentar evitar a perda, ou o furto, ou roubo de seus aparelhos. Para tanto, o controle que deve adotar é a atenção sobre seus dispositivos, o que se pode melhorar por meio do treinamento. O usuário também deve usar ferramentas de segurança dos aparelhos que impeçam seu uso depois de roubados, como uma senha forte de acesso e o acionamento dos mecanismos de proteção pela nuvem, como no caso do iCloud (aparelhos iOS da Apple) e do Knox (aparelhos Android). Esses mecanismos impedem que um aparelho "zerado", isto é, apagado e levado ao seu estado de fábrica, seja acessível sem as credenciais do dono.

Na segunda situação, Ghorbanzadeh et al. (2010) sugerem as seguintes medidas:

- **Autenticação forte para acesso ao aparelho** – evitar senhas de 4 dígitos ou senhas óbvias. Horn (2012) cita as 20 senhas de 4 dígitos mais comuns em smartphones, e é inadmissível sob o ponto de vista de segurança que mais de 10% dos usuários ainda utilizem "1234" como senha. Equivale a usar um "durex" ao invés de uma fechadura para "trancar" a porta da frente de uma residência. Datas de aniversário (ou datas em geral) também são inadequadas, além de combinações óbvias de números.

- **Remoção de dados do aparelho por via remota** – os dispositivos móveis contam com ferramentas que permitem o apagar todo o seu conteúdo após certo número de senhas erradas, ou quando o dono aciona essas ferramentas por meio de um computador conectado à internet. Pela via das senhas erradas, essa ação é imediata, enquanto que por via do computador remoto, apagar esses dados é fácil, pois ocorre quando o smartphone se conectar à internet da próxima vez.

- **Criptografia no armazenamento removível** – muitos aparelhos permitem a adição de cartões de armazenamento em memória Flash (cartões SSD). Em que pese serem bastante úteis para aumentar a capacidade de armazenamento dos dispositivos, é fundamental que seu conteúdo seja criptografado, uma vez que podem ser removidos dos aparelhos e assim não terão mais a proteção oferecida pela senha.

- **Autenticação forte** – muitos aparelhos já contam com reconhecimento de digital, reconhecimento de face e reconhecimento de pupila. Esses mecanismos de autenticação, quando presentes, devem ser usados para aumentar o grau de proteção oferecido pelos smartphones.

Riscos inerentes às redes wireless

Ainda segundo Ghorbanzadeh et al. (2010), quando falamos em comunicações móveis, uma vez que o meio está disponível a todos, inclusive atacantes em potencial, os bancos de dados são inerentemente mais vulneráveis, uma vez que os meios por onde os dados trafegam são vulneráveis.

Além dos pontos de vulnerabilidade já descobertos para os protocolos tradicionais

(pilha TCP/IP e protocolos de redes locais), os protocolos envolvidos em comunicações de smartphones e tablets são menos testados pelo tempo e "também" se baseiam em novas tecnologias que são potencialmente vulneráveis. Nesse sentido, os protocolos 3G e os novos protocolos 4G adicionam pontos de preocupação quanto à confidencialidade, integridade e disponibilidade dos dados, uma vez que por meio deles trafegam de servidores para dispositivos móveis (GHORBANZADEH et al., 2010).

Além disso, Owasp (2014) ainda afirma que nas comunicações entre aplicativos móveis e servidores na Internet sofremos de um problema inerente à proteção insuficiente da camada de transporte. É comum que durante o processo de autenticação sejam utilizadas ferramentas de proteção, da camada de transporte, do tipo SSL (Secure Sockets Layer) ou TLS (Transport Layer Security). Ambas consistem na criação de um túnel criptografado por meio do qual as credenciais do usuário são apresentadas e checadas. Contudo, muitas aplicações que usam SSL ou TLS durante a autenticação deixam de usar essas ferramentas na comunicação de dados, deixando-os suscetíveis a escutas não autorizadas. O atacante só precisa identificar o fluxo de comunicação para ter acesso aos dados sendo comunicados, inclusive aos certificados.

Como prevenção para esse tipo de vulnerabilidade, Owasp (2014) recomenda, entre outros:

- assumir que a camada de transporte é insegura em todos os momentos, e não apenas na autenticação dos usuários;
- usar ferramentas SSL ou TLS durante toda a sessão de comunicação;
- não enviar dados sensíveis por canais alternativos no aparelho (mensagens SMS, MMS ou notificações);
- alertar usuários e — preferencialmente — parar a aplicação se for detectado algum certificado inválido.

Pesquise mais

O Cert.br, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil é o órgão que cuida da disseminação de informações de segurança para ambientes informatizados, em nosso país. O Cert.BR publicou, em 2012, uma cartilha com os principais pontos de segurança em ambientes e dispositivos móveis. Vale a pena conferir para aprender mais sobre o assunto:

CERT, Segurança em dispositivos móveis. Site Cert.br, publicado em 4 set. 2012. Disponível em: <http://cartilha.cert.br/dispositivos-moveis/>. Acesso em: 15 dez. 2016.

Riscos mobilidade x segurança estática

Existem várias diferenças entre a computação com dispositivos tradicionais (computadores de mesa e notebooks) e computação móvel, mas, talvez, uma das principais seja, como afirma Hansen (2014), a velocidade com que essas novas plataformas estão sendo adotadas, rapidamente tornando-se os dispositivos primários para tarefas informatizadas de uma grande parcela da população.

Segundo MobileIron (2014), há diferenças importantes entre segurança no ambiente computacional tradicional (chamado pelos autores de "PC-Cêntrico") e o ambiente móvel. São elas:

- **Controle reduzido sobre dispositivos móveis** – essa nova proposta, a que os autores chamam de "mobile first" (ou "móvel primeiro", no sentido de as soluções visarem primariamente o ambiente móvel), implica em foco no usuário final, e não no ambiente. No modelo tradicional, a empresa e o departamento de TI impunham o equipamento e os aplicativos, sendo que os usuários não tinham qualquer escolha. Já no modelo "mobile first", o usuário tem seu próprio equipamento pessoal, que espera poder usar em suas tarefas profissionais. Esse conceito, chamado de BYOD (Bring Your Own Device ou "traga seu próprio dispositivo"), implica que a empresa vai ter menos controle sobre os equipamentos e, entre os aplicativos de produtividade, o usuário certamente vai colocar seus aplicativos (e jogos) preferidos. Em outras palavras, diferente do ambiente PC-Cêntrico, no ambiente "mobile first" a empresa não tem mais controle absoluto sobre o equipamento e sobre o que o usuário faz com ele.

- **Soluções de segurança baseadas em agentes não se aplicam** – em ambientes PC-Cêntricos, é bastante comum que os "agentes", pequenos e leves aplicativos invisíveis para o usuário, monitorem o sistema, identificando eventos e ações que ameacem a segurança do ambiente. A arquitetura dos sistemas operacionais móveis é baseada em "caixas de areia" (sandboxes), ou seja, ambientes segregados e seguros, como as caixas de areia em parquinhos, que as mães permitem que seus filhos frequentem por serem seguras. Dentro de sua caixa de areia própria (e só lá), um programa pode fazer o que quiser, sabendo que está seguro das ações e monitorações de outros programas. Um agente não teria como monitorar outros programas em um dispositivo móvel, justamente por este, conceito de caixas de areia.

Exemplificando

A IBM Brasil criou uma estratégia de integração de dispositivos pessoais nas redes de seus clientes, apoiando-os na implantação e gestão desses dispositivos. Em 2013, no Fórum Mobile+, a empresa anunciou resultados positivos: uma média de retorno de 108% sobre o investimento dos clientes, ou seja, para cada R$100,00 que um cliente investia nessa estratégia, ele faturava R$108,00, ou seja, um sucesso absoluto (CHIECO, 2013).

Sem medo de errar

Nesta etapa do projeto de um aplicativo para a rede de brechós de Talínia, você deve mostrar-lhe que de fato há muitos riscos envolvidos aos bancos de dados operados e armazenados em aplicativos móveis, bem como propor-lhe uma estratégia para enfrentar os desafios nesta área.

O foco de seu trabalho será nos bancos de dados, mas não é prudente "mergulhar" nas questões de bancos de dados sem antes expor as questões da segurança em um contexto mais amplo para Talínia. Nesse sentido, podemos começar o trabalho expondo à empresária a lista "Top 10" de riscos de segurança em dispositivos e aplicativos móveis, da OWASP (Disponível em: <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks>. Acesso em: 15 dez. 2016, em inglês):

1. Controles fracos do lado do servidor.
2. Armazenamento inseguro de dados.
3. Proteção insuficiente na camada de transporte.
4. Vazamento não intencional de dados.
5. Autenticação e autorização insuficientes ou pobres.
6. Criptografia falha.
7. Injeções no dispositivo móvel.
8. Decisões de segurança baseadas em entradas não confiáveis.
9. Manipulação inadequada de sessões.
10. Falta de proteções binárias.

Uma rápida explanação de cada um destes dez pontos levantados será útil para contextualizar a situação para Talínia, e, para tanto, uma visita ao site do Owasp é bastante recomendável.

Em seguida, será bastante útil focar nos três pontos diretamente ligados aos bancos de dados móveis, os itens 2, 4 e 7. Você poderá detalhá-los e expor as formas indicadas de prevenção ou mitigação desses riscos.

Por fim, a título de estratégia para a condução do projeto, você pode apresentar uma lista de providências a serem tomadas:

A. Fazer um levantamento criterioso das necessidades de Talínia para o software;

B. Criar uma política de desenvolvimento seguro, levando em conta principalmente os riscos inerentes ao futuro aplicativo móvel;

C. Estudar criteriosamente os riscos, inserindo nos requisitos do software as prevenções e contramedidas que eliminam ou mitigam esses riscos.

D. Dentro da estratégia de BYOD, identificar os principais aparelhos móveis do mercado e entender que condições mínimas de hardware e software deverão ser estabelecidas para que seu uso seja permitido no ambiente.

Desta forma, a preparação para o desenvolvimento do aplicativo contemplará as necessidades de segurança inerentes à natureza móvel do aplicativo.

Avançando na prática

Uma família conectada no trabalho

Descrição da situação-problema

O Sr. Hiro é o proprietário de uma loja de flores e ornamentos na capital carioca. Ele, a esposa e os três filhos empregam alguns dias da semana na busca por novos fornecedores e também na venda de seus produtos para empresas de decoração. Para tanto, o Sr. Hiro decidiu que vai adotar smartphones para catalogar os produtos encontrados, bem como tirar pedidos das vendas que ele e a família realizam em campo.

O Sr. Hiro está preocupado com a segurança dos aparelhos e procurou você, um amigo da família e consultor de segurança, para ajudá-lo a criar um conjunto simples de instruções que possam ser seguidas pela família no sentido de evitar problemas no uso dos aparelhos em seus negócios.

Considerando que a família não lida com tecnologia em seus afazeres diários, as instruções devem ser claras, simples e úteis para todos.

Como ajudar a família Hiro neste caso?

Resolução da situação-problema

Entre as várias sugestões que podem ser apresentadas à família Hiro, a lista a seguir é um exemplo útil:

1. Estar sempre alerta para onde se encontra o dispositivo. Diferentemente de computadores maiores, os smartphones são alvos mais fáceis para os ladrões, devido

ao seu pequeno volume e alto valor.

2. Adotar formas de rastrear os aparelhos e/ou apagar remotamente os dados dos aparelhos em caso de roubo. No caso dos celulares com sistema operacional iOS, ambos os recursos estão disponíveis de fábrica, e no caso dos celulares com sistema operacional Android, há aplicativos que podem ser adotados para tanto. Os aplicativos Cerberus, Lookout, Prey e Android Lost, por exemplo, atuam no sentido de localizar um celular que foi roubado e permitem cópias remotas do conteúdo do celular, além de também apagar as informações remotamente.

3. Adotar uma senha forte, não trivial, que efetivamente proteja o celular. Evitar a qualquer custo senhas de 4 dígitos e senhas de fácil dedução.

4. Preferencialmente não usar cartões de memória, mas se for absolutamente necessário, adotar criptografia para os dados armazenados nessas mídias.

5. Se um aplicativo for desenvolvido para uso no negócio, toda a comunicação (e não apenas os processos de autenticação e autorização) deve ser protegida por tunelamento SSL ou TLS.

Com uma lista nesse sentido, contendo sugestões simples, práticas, mas bastante eficientes, o Sr. Hiro estará no caminho certo para proteger os dispositivos móveis em seu ambiente profissional.

Faça valer a pena

1. Nos aplicativos móveis vemos, em muitos casos, a presença de sistemas _____ de gerenciamento de bancos de dados, uma vez que o usuário pode armazenar dados _____ e também pode ter acesso a dados armazenados em um _____.

Assinale a alternativa que completa adequadamente as lacunas do texto acima:

a) abertos, inseguros, smartphone.

b) fechados, seguros, laptop.

c) distribuídos, localmente, servidor remoto.

d) distribuídos, seguros, smartphone.

e) fechados, localmente, laptop.

2. É importante observar, também, que a própria natureza dos aparelhos móveis apresenta riscos visíveis: diferentemente dos dispositivos não

móveis, os smartphones e tablets nos acompanham a todos os lugares, e o primeiro risco inerente à mobilidade diz respeito à segurança física dos aparelhos. Ghorbanzadeh et al. (2010) citam o acesso aos dados em função de perda, furto (subtração sem a presença do proprietário e sem violência) ou roubo (subtração com a presença do proprietário e com violência) dos aparelhos como uma fonte importante de preocupação para os donos, bem como para os desenvolvedores de aplicativos móveis.

No caso da ameaça de furto, qual dos controles de segurança é útil para prevenir que a ameaça se concretize?

a) Treinamento do usuário.

b) Firewall específico para dispositivos móveis.

c) Tunelamento SSL/TLS.

d) Banco de dados distribuído.

e) Antivírus.

3. Além dos pontos de vulnerabilidade já descobertos para os protocolos tradicionais (pilha TCP/IP e protocolos de redes locais), os protocolos envolvidos em comunicações de smartphones e tablets, além de menos testados pelo tempo, trazem novas tecnologias que também são potencialmente vulneráveis. Nesse sentido, os protocolos 3G e os novos protocolos 4G adicionam pontos de preocupação quanto à confidencialidade, integridade e disponibilidade dos dados que, por meio deles, trafegam de servidores para dispositivos móveis.

Podemos afirmar que as novas tecnologias de comunicação móvel (protocolos 3G e 4G, por exemplo):

a) contribuem para tornar o ambiente mais seguro, porque adicionam mais vulnerabilidades potenciais.

b) contribuem para tornar o ambiente mais inseguro, porque adicionam mais vulnerabilidades potenciais.

c) contribuem para tornar o ambiente mais seguro, porque são tecnologias mais modernas e menos passíveis de ataques.

d) contribuem para tornar o ambiente mais inseguro por conta do roubo de aparelhos.

e) não contribuem para tornar o ambiente nem mais seguro nem mais inseguro, uma vez que não afetam a segurança.

Seção 3.2

Acesso e gerenciamento de dados e metadados

Diálogo aberto

Olá! Seja muito bem-vindo a mais uma seção de estudos sobre segurança de sistemas de bancos de dados.

Você, profissional de segurança especializado em segurança de sistemas de bancos de dados, está empenhado em auxiliar a empresária Talínia em seu projeto de adoção de um aplicativo móvel, para auxiliar sua força de vendas. Tendo sido alertada para as vulnerabilidades impostas pelos metadados de uma aplicação (e sem conhecer muito acerca do assunto), Talínia foi taxativa: "não quero metadados em minha aplicação".

Será que isso é possível? Será que há como um aplicativo móvel que vai depender pesadamente de bancos de dados não utilizar metadados? Sua tarefa, nesse momento, é orientar Talínia se isso for possível e sobre o melhor curso de ação quanto à garantia de segurança do aplicativo, no que diz respeito aos metadados.

Para tanto, você vai conhecer o que são metadados e qual sua relação com os dados em uma aplicação; vai entender o que é comprometimento de uma comunicação por via aérea e qual o papel dos metadados neste comprometimento; vai entender a relação entre consistência e interrupção, além de conhecer os riscos inerentes aos metadados na comunicação de aplicativos móveis.

Pronto para mais essa etapa?

Não pode faltar

Um elemento da comunicação que fica "escondido" dos usuários e que contém informações sobre os dados são os metadados. Em que pese esses elementos serem fundamentais para a comunicação, como veremos a seguir, a vasta maioria das pessoas que se beneficiam da comunicação digital raramente está ciente de sua

existência. A partir de agora, você vai entender o que são, para que servem e como proteger os metadados.

Mensagens: dados e metadados

Para entender metadados, observemos inicialmente os envelopes enviados pelo correio. A mensagem é a carta que vai dentro do envelope, mas essa carta só tem como atingir seu destino se houver uma série de informações no envelope. Veja, na Figura 3.1, um exemplo:

Figura 3.1 | Exemplo de envelope postal

Fonte: <https://en.wikipedia.org/wiki/Airmail#/media/File:Cover_Canada_1932_Rae_air.jpg>. Acesso em: 18 out. 2016.

Podemos observar que o envelope contém os seguintes dados que não são relacionados com a mensagem em si (que é a carta que vai dentro do envelope):

- nome do destinatário;
- endereço do destinatário;
- selo, garantindo que o custo de envio foi pago;
- carimbo postal, garantindo que a carta foi transportada por agentes autorizados;
- data de saída da carta (no carimbo), garantindo que a carta foi entregue em tempo adequado para a relevância da mensagem.

Em que pese essas informações de fato não serem pertinentes ao contexto da mensagem (carta), elas (ainda assim) são fundamentais para que a comunicação possa ocorrer sem percalços.

Outro exemplo interessante e muito comum em tempos de Internet é o pacote TCP, como representado por Guerber (2007), na Figura 3.2, a seguir:

Figura 3.2 | Pacote TCP

<table>
<tr><td colspan="3">Porta origem</td><td>Porta destino</td></tr>
<tr><td colspan="4">Número de Sequência</td></tr>
<tr><td colspan="4">Acknowlegement</td></tr>
<tr><td>Tam.</td><td>Reser.</td><td>Flags</td><td>Window</td></tr>
<tr><td colspan="3">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="4">Opções (se houver)</td></tr>
<tr><td colspan="4">Dados</td></tr>
</table>

Fonte: Guerber (2007, p. 1).

No pacote TCP representado na figura, temos uma série de informações que não fazem parte da mensagem em si. A mensagem é, na verdade, limitada ao último campo intitulado "Dados". O que vem antes é uma coleção de informações que não empresta significado algum à mensagem em si, mas que é de suma importância para que a mensagem seja transportada e entregue corretamente. Informações como porta de origem, porta de destino, número de sequência e outras são fundamentais para que as informações de fato façam sentido para o interlocutor, no caso, o computador de destino.

Essas informações "extras", tanto no caso do envelope postal como no caso do pacote TCP, são chamadas de metadados. NISO (2004) define metadados como as informações estruturadas que descrevem, explicam, localizam ou facilitam a busca e recuperação, o uso e o gerenciamento de informações. De maneira simplificada, podemos definir metadados como informações acerca de informações (NISO, 2004).

Existem três tipos principais de metadados (NISO, 2004):

- **metadados descritivos** – descrevem um recurso qualquer para fins de identificação. Podem incluir elementos como nome, resumo descritivo, autor e descritores (palavras-chave);

- **metadados estruturais** – indicam como objetos compostos são agrupados, por exemplo: como as páginas de um livro são ordenadas para formar seções e unidades ou capítulos;

- **metadados administrativos** – fornecem informações para auxiliar no gerenciamento de um recurso qualquer. Exemplos: quando o recurso foi criado, como foi criado, tipo de arquivo, quem pode acessar o recurso. Existem vários subconjuntos de dados administrativos e dois deles em especial, às vezes, são apresentados como tipos de metadados separados;

- **metadados de gestão de direitos** – tratam dos direitos de propriedade intelectual;

- **metadados de preservação** – contêm informações necessárias para arquivar e preservar um recurso.

Os metadados podem ainda ser classificados quanto à sua estrutura. Baca (2008) provê uma definição útil acerca dessa classificação:

- **metadados não estruturados** – não possuem uma estrutura hierárquica ou organizacional. Todos os elementos descritivos são apresentados sem uma organização, a não ser do tipo mais básico (ordem alfabética ou ordem numérica crescente, por exemplo),

- **exemplos** – índice remissivo ao final de um livro; índice de ordenação (gerado por um usuário em uma operação qualquer) de um banco de dados;

- **metadados estruturados** – os metadados podem ser classificados de acordo com uma estrutura hierárquica e/ou organizada. Um metadado será agrupado com outros metadados com características semelhantes. As características de agrupamento (que também são, em si, metadados) igualmente podem ser agrupadas.

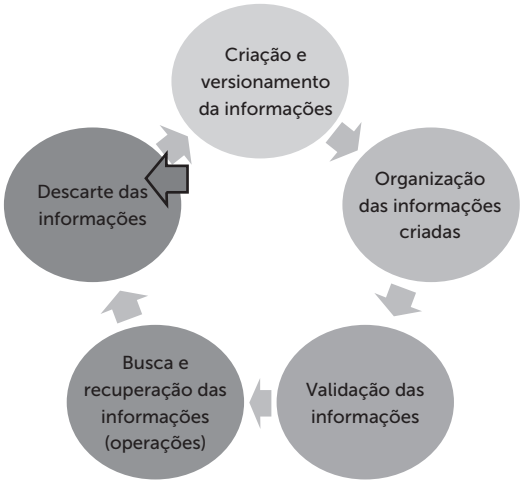
- **exemplo** – índice principal de um livro; dicionário de dados de um banco de dados.

Assimile

Metadados são "informação sobre a informação".

Os metadados têm participação fundamental no ciclo de vida das informações, como podemos ver na figura 3.3:

Figura 3.3 | Ciclo de vida das informações



Fonte: adaptado de Baca (2008, p. 18).

Segundo Baca (2008), à medida que um objeto de informação passa pelas fases de seu ciclo de vida, adquire novas camadas de metadados que permitem sua administração e organização. Cada fase tem seus metadados adequados adicionados às informações:

- **criação e versionamento das informações** – metadados usados para identificar a informação e seus responsáveis. Exemplos de metadados: nome, nome do criador/responsável, data de criação, número da versão;

- **organização das informações** – metadados usados para tipificar a informação. Exemplos de metadados: classificação da informação, classificação de sigilo, permissões de manipulação;

- **validação das informações** – metadados usados para aferir a fidedignidade da informação. Exemplos de metadados: quem referencia ou cita as informações, quantidade de acessos, grau de confiança de cada informação em uma escala arbitrária. Além de metadados dessa natureza, os mesmos das etapas anteriores são utilizados, sendo que os algoritmos os utilizam para aferir a validade e a fidedignidade das informações. Exemplos de aferições: qual a reputação do autor em prover informações adequadas? Qual a relevância das informações hoje, sendo que foram publicadas há x dias (ou semanas, ou meses, ou anos)?

- **busca e recuperação das informações** – metadados usados para facilitar o acesso à informação. Exemplos de metadados: localização física e lógica das informações,

- **descarte das informações** – metadados usados para auxiliar na eliminação de informações desatualizadas, imprecisas ou irrelevantes. Exemplos de metadados: data de validade das informações, índice de atividade (ou inatividade) das informações.

Comprometimento por via aérea

Na seção anterior foi discutida a questão da proteção insuficiente das comunicações móveis por via aérea (wireless). Especificamente, OWASP (2014) menciona os problemas inerentes da proteção por meio de tunelamento SSL/TLS apenas para os processos de autenticação/autorização da comunicação.

Ocorre que os metadados trafegados durante o processo de comunicação correm "em aberto" e podem prover vetores de ataque para os ciber-bandidos que estejam monitorando a comunicação. Sheldon (2012) exemplifica essa vulnerabilidade quando afirma que as operadoras de comunicação podem interceptar os metadados de cada pacote enquanto estes circulam em suas redes. Esses metadados, segundo o autor, incluem informações sobre origem e destino das informações, bem como sua natureza (tipo de dados). Casos registrados de violação de dados mostram que os ciber-bandidos usam (ilegalmente) os mecanismos de acesso das operadoras para

coletar metadados, identificando, assim, fluxos de comunicação que sejam de seu interesse violar.

A solução, como já foi analisada na seção anterior, é simples, mas fundamental: o uso constante do tunelamento (SSL – Secure Sockets Layer, ou sua versão mais nova, o TLS – Transport Layer Security) em todas as transações via rede wireless, uma vez que o fluxo de comunicação está ao alcance de qualquer um que tenha presença geográfica próxima ao dispositivo móvel.

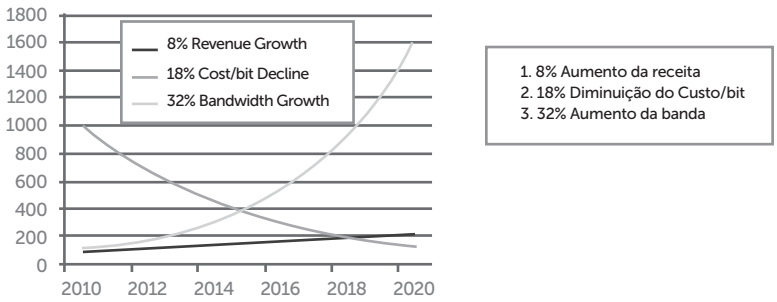
Há desvantagens e vantagens para o uso constante do tunelamento:

- **vantagem**: proteção de toda a comunicação, e não apenas das credenciais de autenticação e autorização;

- **desvantagem**: maior consumo de banda em função do *overhead* imposto pelo processo de tunelamento.

Com relação à desvantagem, é importante destacar que o mecanismo de tunelamento exclusivo dos processos de autenticação/autorização data de um tempo em que a banda disponível era bem menor, e bem mais cara, do que aquela que o usuário tem à sua disposição nos dias de hoje (KIPP, 2012). A Figura 3.4 representa o aumento exponencial da disponibilidade de banda e a redução equivalente dos custos de banda nos últimos anos, projetando-os para o futuro.

Figura 3.4 | Variação de disponibilidade e custos de banda de comunicação



Fonte: Kipp (2012, p. 1).

A linha (2) identifica o custo por bit para o usuário de banda larga. Ele vem caindo ano a ano e, em 2020, estima-se que ele estará 18% menor do que estava em 2010. A linha (3) identifica o crescimento da largura da banda, também desde o ano de 2010. Por fim, a linha (1) representa o crescimento da receita com a prestação do serviço da banda larga.

Consistência x interrupção

Há duas formas úteis de encararmos a questão da consistência x interrupção quando o assunto é a comunicação de informações de bancos de dados por meios sem fio (wireless). A primeira delas tem a ver com os metadados e a consistência que emprestam à comunicação. A segunda diz respeito ao fluxo de comunicação e o que ocorre com a consistência quando interrompemos esse fluxo.

No primeiro aspecto, os metadados, como afirma Baca (2008), auxiliam na organização das informações, emprestando-lhes maior valor por meio dessa organização. Os dados armazenados e as transações realizadas ganham maior consistência por meio dos metadados. O grau de certeza acerca de uma informação aumenta à medida que os metadados corroboram sua origem, versão, responsável, data de criação, dados de acesso e armazenamento além de tantos outros. Obviamente que há valor nos metadados e seu uso generalizado é um testemunho desse valor.

Contudo, é fundamental observarmos que os metadados dizem mais sobre as informações do que talvez os responsáveis por essa informação queiram deixar visível. Um ciber-bandido que não tenha acesso a uma informação em particular, mas tenha acesso aos seguintes metadados acerca dessa informação, já está bem encaminhado no sentido de obter acesso indevido:

- criador da informação;
- versão atual da informação;
- data de criação da informação;
- classificação de tipo da informação;
- classificação de sigilo da informação.

Esses dados facilitariam, por exemplo, um ataque com base em engenharia social, com o atacante personificando alguém que conhece o criador dos dados; sabe quando foi criado, e a que se refere, podendo convencer um técnico a lhe dar acesso, alegando que sua cópia foi perdida ou corrompida.

Nesse sentido, a interrupção dessa consistência de dados é útil porque protege a informação. Essa interrupção se dá de forma radical, porém bastante utilizada: por meio da remoção dos metadados. Chappie (2013) sugere que todos os metadados sejam removidos antes do envio de documentos sensíveis e que, se os metadados forem de fato úteis após o processo de comunicação, devem ser adicionados a documentos protegidos e devem, também, fazer parte da comunicação segura. Na visão do autor, os metadados de um documento só devem existir durante o breve momento em que sejam criados e não devem continuar fazendo parte de um documento após ser gerados.

Exemplificando

Em 2012, o hacker Higino, componente do grupo de hackers "Anonymous" e conhecido pelo pseudônimo de "Wormer", foi preso pelo FBI por conta dos metadados. Alguns meses antes da prisão, Higino havia tuitado uma foto sem antes remover os metadados. Ocorre que uma das informações que compõem os metadados de uma foto (conhecidos dos fotógrafos por "EXIF") são as coordenadas GPS de onde a foto foi tirada. De posse dessas coordenadas, o FBI pôde focar suas investigações, chegando rapidamente a Higino e prendendo-o (DIAZ, 2012).

O segundo aspecto do equilíbrio entre consistência x interrupção dá-se no nível da rede, durante o processo de comunicação.

É sabido que os metadados auxiliam no fluxo de comunicação, como nos mostra Guerber (2007) na Figura 3.2. Metadados tais como o número de sequência e o checksum (cálculo que determina a integridade do pacote) são fundamentais no fluxo de comunicação. Uma vez que ocorra uma interrupção nesse fluxo, os metadados são fundamentais para que a comunicação seja adequadamente restabelecida. Uma rápida averiguação na identificação da seção e o acompanhamento dos números dos pacotes que chegaram de forma bem-sucedida são suficientes para que esse fluxo seja restabelecido.

Contudo, essa conveniência tem seu preço: para que seja possível, ela depende pesadamente dos metadados. Ou seja: aumentando a consistência da comunicação, reduzimos, em teoria, a segurança. O contrário também é válido: quando dependemos menos dos metadados, reduzimos a consistência da comunicação, mas aumentamos a segurança do processo como um todo.

Reflita

Por que razão manter metadados quando os mesmos não têm mais utilidade em um arquivo?

Riscos inerentes aos metadados

Nas palavras de Lemos (2014, p. 1), "os metadados implicam ao mesmo tempo em riscos e em recompensas". As recompensas, como já foi apresentado nesta seção, se dão sob a forma das facilidades de organização e administração das informações.

Já os riscos podem ser classificados segundo as já conhecidas dimensões da segurança da informação: confidencialidade, integridade e disponibilidade:

- riscos dos metadados à confidencialidade – por serem disponíveis do lado

de fora" dos arquivos ou livres no fluxo de comunicação, os metadados são, por natureza, não confidenciais. Isso, porque fornecem dados que podem ser explorados pelos bandidos (criadores/responsáveis pelas informações, local de armazenamento das informações) para ganhar acesso às informações, comprometendo-lhes a confidencialidade. A alteração da classificação de segurança de um arquivo criptografado, por exemplo, de "confidencial" para "não confidencial" pode provocar a disponibilização desse arquivo e a remoção de sua criptografia por parte dos responsáveis;

- **riscos dos metadados à integridade** – a alteração dos metadados de um arquivo não só é possível como bastante fácil, havendo até mesmo aplicativos comerciais que permitem sua manipulação. Uma vez alterados os metadados de um arquivo, sua integridade já não existe mais. A alteração, por exemplo, da data de criação de um arquivo, do nome do criador, da classificação de tipos ou de segurança, por si só já elimina a integridade das informações referentes aos metadados alterados;

- **riscos dos metadados à disponibilidade** – a alteração de alguns metadados pode afetar diretamente a disponibilidade das informações. Por exemplo, a alteração do checksum de um pacote de comunicação provoca o descarte desse pacote por parte do sistema destinatário, uma vez que os dados do pacote não mais correspondem à checagem de integridade estampada no *checksum*.

Pesquise mais

Os pesquisadores Terezinha Batista de Souza, Maria Elisabete Catarino e Paulo Cesar dos Santos expõem os conceitos fundamentais dos metadados e a estruturação da descrição padronizada de documentos eletrônicos no artigo **Metadados – catalogando dados na Internet**.

SOUZA, T. B; CATARINO, M. E; SANTOS, P. C. Metadados: catalogando dados na internet, **Revista Transformação**, v. 9, n. 2, p. 93-105, maio-agosto, 1997. Disponível em: <http://periodicos.puc-campinas.edu.br/seer/index.php/transinfo/article/download/1586/1558>. Acesso em: 15 dez. 2016.

Sem medo de errar

Podemos começar explicando a Talínia que há metadados sem os quais as comunicações não são possíveis e que esses devem ser preservados e protegidos na medida do possível.

Um caminho viável de ser seguido para explanar à Talínia sobre a importância dos metadados é o seguinte:

1. Mostre-lhe em termos simples que os metadados são fundamentais. Para tanto, dê o exemplo do envelope com as informações de origem e destino de uma carta e explique que sem esses dados a carta não pode ser entregue ao destinatário, nem devolvida ao remetente em caso de erro.

2. Explique que há metadados estruturados e metadados não estruturados, exemplificando ambos.

3. Explique e exemplifique os tipos de metadados segundo a NISO.

4. Mostre o que é e como se dá o comprometimento por via aérea, no caso dos protocolos de comunicação sem fio.

5. Mostre à Talínia que a velocidade e a disponibilidade de banda nos dias de hoje já não justificam o uso de tunelamento apenas nos processos de autenticação e autorização, devendo esse tunelamento ocorrer durante todo o processo de comunicação.

6. Mostre à Talínia os dois tipos de contraste entre consistência e interrupção, explicando as vantagens e desvantagens de se remover os metadados de um conjunto de dados.

7. Exemplifique à Talínia o perigo dos metadados que permanecem junto à informação mesmo depois de perderem sua utilidade. O caso do hacker preso pelo FBI em função dos metadados disponíveis em uma fotografia é bastante útil para essa explicação.

8. Explique à Talínia quais são os riscos impostos pelos metadados tanto na confidencialidade como na integridade e na disponibilidade dos dados.

Pronto, agora Talínia sabe para que servem os metadados e como mais bem utilizá-los em seu favor, sem colocar as comunicações de seu aplicativo em risco. Além disso, apresente à Talínia os pontos técnicos a serem tratados e que fazem parte desse processo. Informações e especificações estão disponíveis em: <https://docs.oracle.com/cd/E36560_01/html/E36005/recdeploytopologies.html>. Acesso em: 15 dez. 2016.

Avançando na prática

O verdadeiro autor

Descrição da situação-problema

Você, profissional da segurança de sistemas de banco de dados, tem um problema e está determinado a auxiliar um cantor e compositor que o procurou com uma

situação inusitada, sob o ponto de vista tecnológico. Ele alega ter composto uma música romântica que faria parte de seu próximo álbum. Ocorre que, durante o processo de composição, o compositor contratou pintores, pois estava em reforma de seu apartamento, e desconfia que um deles se apropriou indevidamente de sua composição. Isso porque, duas semanas depois, um dos pintores lançou uma música que tem a letra quase que 100% idêntica à música que o compositor alega ser de sua autoria.

Você, um especialista em segurança com bastante experiência em metadados, foi chamado a ajudar na resolução do caso. Você recebeu o documento em Microsoft Word do pintor, datado de 25 de março do ano corrente, e também o documento em Microsoft Word do compositor, datado de 15 de abril, também do ano corrente. O pintor, agora também músico, alega que compôs a canção bem antes de começar o serviço na casa do cantor/compositor, oferecendo a data do documento como evidência.

Como você procederia para resolver essa situação?

Resolução da situação-problema

Uma maneira simples de decidir essa disputa entre o cantor/compositor e o pintor musicista é consultar os metadados dos arquivos Word, que podem ser facilmente encontrados na opção "Propriedades" no menu "Arquivo", do Word.

Mesmo que um arquivo tenha sua data modificada — e é bem fácil modificar essa data —, os metadados do arquivo não serão modificados. Lá podemos encontrar dois dados fundamentais para a resolução da disputa:

- data de criação do documento;
- autor do documento.

Se o pintor está falando a verdade, a data de criação estabelecida nos metadados será a mesma que ele apresenta: 25 de março do ano corrente. Caso contrário, se a data de criação estabelecida nos metadados for a data apresentada pelo compositor, ficará claro que houve adulteração do documento.

O nome do autor é outro elemento fundamental, pois ele é atribuído automaticamente a quem instalou e configurou o Microsoft Word na máquina. Se o nome do autor for o do pintor, ou se for o do compositor, teremos mais evidências claras de quem é o autor.

Faça valer a pena

1. As informações extras, tanto no caso de envelope postal como no caso de um pacote TCP, têm um nome específico. Niso (2004) as define como as informações estruturadas que descrevem, explicam, localizam ou facilitam a busca e recuperação, o uso e o gerenciamento de informações. De maneira simplificada, também podemos defini-las como informações acerca de informações.

Qual o nome das informações extras que contextualizam e auxiliam na comunicação das informações?

a) Endereço.

b) Cabeçalho.

c) Mensagem.

d) Metadados.

e) Comunicação.

2. Os metadados trafegados durante o processo de comunicação correm "em aberto" e podem prover vetores de ataque para os ciber-bandidos que estejam monitorando a comunicação. Sheldon (2012) exemplifica essa vulnerabilidade quando afirma que as operadoras de comunicação podem interceptar os metadados de cada pacote enquanto estes circulam em suas redes.

Analise as asserções a seguir:

I. Apesar de o tunelamento de toda a comunicação (e não apenas dos processos de autenticação e autorização) ser uma desvantagem em função de propiciar maior consumo de banda, nos dias de hoje isso tende a não ser um problema relevante.

PORQUE

II. A disponibilidade de banda e a velocidade média de banda são bem maiores hoje em dia do que alguns anos atrás, quando toda economia de banda era necessária para que a comunicação de dados fosse eficiente.

Analisando-se as asserções acima, conclui-se que:

a) As duas afirmações são verdadeiras e a segunda justifica a primeira.

b) As duas afirmações são verdadeiras e a segunda não justifica a primeira.

c) A primeira afirmação é verdadeira e a segunda é falsa.

d) A primeira afirmação é falsa e a segunda é verdadeira.

e) As duas afirmações são falsas.

3. Nas palavras de Lemos (2014, p. 1) "os metadados implicam ao mesmo tempo em riscos e em recompensas". As recompensas, como já foi apresentado nesta seção, se dão sob a forma das facilidades de organização e administração das informações. Já os riscos podem ser classificados segundo as já conhecidas dimensões da segurança da informação: confidencialidade, integridade e disponibilidade.

Assinale a alternativa que descreve um risco imposto pelos metadados à confidencialidade.

a) A eliminação do identificador da sessão de um fluxo de comunicação, impedindo que o pacote em questão seja adequadamente identificado no destino.

b) A alteração do nome do criador do documento para o nome de uma pessoa não autorizada, dando-lhe acesso ao documento.

c) A alteração do local onde um documento está armazenado, impedindo que ele seja adequadamente preservado e encontrado no futuro.

d) Alteração no índice das informações, incluindo dados que na verdade não fazem parte do conteúdo armazenado.

e) Eliminação de todos os metadados de um arquivo armazenado, impedindo o usuário de saber quem foi seu criador e quando ele foi criado.

Seção 3.3

Mecanismos e técnicas de segurança. Segurança de banco de dados comerciais móveis

Diálogo aberto

Desde que os computadores digitais foram introduzidos em nossas vidas, mais de 70 anos atrás, eles vêm sendo usados para organizar informações. O software para armazenamento e busca de dados sempre foi de importância capital para quem utiliza computadores, e a indústria não demorou a enxergar aí uma oportunidade de negócios.

E foi assim que surgiram as empresas cuja especialidade é produzir software para gerenciamento de bancos de dados, os chamados bancos de dados comerciais. Esses pacotes são especializados em coletar e organizar dados, atingindo alto grau de otimização, pois permitem que milhões de registros de informações (cada um contendo até centenas de dados individuais) sejam organizados de forma eficiente e encontrados em segundos. Quer ver um exemplo? Basta tirar um extrato bancário em seu smartphone para comprovar: todos os dados serão coletados e apresentados em questão de poucos segundos, e a maior parte desse tempo é empregada em transportar sua requisição do celular para o servidor e em seguida para transportar o resultado da requisição do servidor para seu smartphone. As operações no banco de dados em si são (de longe) a porção mais rápida desse processo.

A empresária Talínia, dona da rede de brechós Tutti Bella, está às voltas com seu projeto para criar uma aplicação móvel para sua força de vendas. Nesta etapa, você — especialista em segurança de bancos de dados — já convenceu Talínia da importância da segurança para seu projeto e, agora, deve mostrar-lhe que as soluções de bancos de dados disponíveis no mercado podem oferecer tudo aquilo que ela precisa, em termos de proteção para seu aplicativo. Você deve explicar-lhe como funcionam os mecanismos de proteção por firewall, como funciona a criptografia, o que é e para que serve a auditoria de bancos de dados bem como o funcionamento dos controles e a análise de privilégios.

São exatamente esses os conteúdos que veremos na presente seção: firewall, criptografia, eventos e controle de privilégios. O objetivo é conhecermos os

mecanismos de segurança em bancos de dados comerciais, entendendo como funcionam e como aplicá-los para proteger as informações.

Não pode faltar

Os sistemas de gerenciamento de bancos de dados de uso comercial (SGBDs comerciais), pelo valor intrínseco dos dados que mantêm, devem ser dotados de mecanismos próprios de segurança. E, obviamente, eles são, como veremos a partir de agora, na presente seção.

Bancos de dados comerciais: firewall

Antes de chegarmos ao firewall do banco de dados, primeiramente precisamos recordar o conceito de firewall. O termo firewall, que em inglês significa (em tradução livre) "porta corta fogo", foi criado para definir um tipo de dispositivo que se posta entre a rede externa (internet) e a rede interna de uma organização e permite a passagem apenas de tráfego autorizado (NAKAMURA e GEUS, 2007). Esses dispositivos, que em seu nascimento foram direcionados a proteger a rede, tiveram seu conceito expandido para outros níveis da comunicação. Podemos pensar em um firewall como uma barreira lógica que permite apenas a passagem de elementos autorizados. A imagem de uma porta de aço que impede a passagem do fogo, mas permite que as pessoas circulem é apropriada, não acha? A Figura 3.5 representa uma dessas portas de emergência, resistentes ao fogo:

Figura 3.5 | Porta de emergência, antifogo

Fonte: <https://www.flickr.com/photos/jeepersmedia/14120419530>. Acesso em: 16 dez. 2016.

Transportando o conceito de firewall para os bancos de dados, Lugo e Parker (2010) os definem como um filtro que se posta entre o sistema gerenciador de bancos de dados (SGBD) e os componentes de comunicação do sistema operacional além de decidir sobre que transações terão permissão de chegar ao SGBD e quais transações serão impedidas. Para tanto, o firewall de bancos de dados analisa os pedidos de

transação contra um conjunto de regras pré-estabelecidas. Esses pedidos de transação chegam formatados na linguagem SQL, ou seja: são comandos SQL que chegam de vários aplicativos e usuários presentes no sistema. Apenas as transações que estiverem explicitamente permitidas nesse conjunto de regras terão permissão para chegar até o SGBD. As demais serão sumariamente descartadas (podendo opcionalmente gerar uma mensagem em um *log* próprio ou uma mensagem na tela do requisitante).

As regras de firewall de bancos de dados são simples, pois o que é analisado é a origem do comando e o subsistema a que se destina (a porção do banco de dados que deverá atender a transação). Origens autorizadas para subsistemas autorizados são permitidos, enquanto origens não autorizadas ou subsistemas não autorizados são descartados (LUGO e PARKER, 2010). Regras adicionais com condicionantes também podem ser definidas, como:

- horário em que a transação foi solicitada;
- ponto de origem (endereço IP) da transação.

É importante observar que os firewalls tradicionais de banco de dados se atêm a essas informações, não entrando no comando SQL em si para averiguar seu conteúdo. Isso porque os firewalls de bancos de dados — os que funcionam na arquitetura tradicional desse tipo de aplicativo — buscam ser ágeis e não inserir um *overhead* grande demais no processo de comunicação (LUGO e PARKER, 2010).

Nesse contexto, devemos entender *overhead* como excesso de processamento durante o processo de comunicação.

Assimile

Os firewalls de aplicação tradicionais não abrem o pacote para analisar o que tem dentro, mas, sim, o avaliam contra um conjunto de regras quanto à origem e ao destino do pacote.

Vejamos as características de alguns dos principais firewalls comerciais desenvolvidos especialmente para bancos de dados:

- **firewalls especializados de uso genérico (compatíveis com vários SGBD de mercado)** – Segundo Shetty e Hanna (2016), esses firewalls são suítes completas de proteção e monitoração para bancos de dados de vários fabricantes, podendo ser integrados com vários SGBDs de mercado (daí o fato de serem genéricos), entre eles: Oracle, Oracle MySQL, Microsoft SQL Server, IBM DB2, SAP, Sybase e ASE. Um dos pacotes mais conhecidos dessa categoria, por exemplo, tem duas funções básicas dentro de um sistema de banco de dados: coletar e organizar informações de auditoria (que veremos mais à frente ainda nesta seção) e prover proteção por meio de um firewall de bancos de dados (ORACLE, 2015);

- Características

- Diferentemente dos firewalls de bancos de dados tradicionais, os firewalls mais modernos abrem o pacote e fazem uma análise gramatical e semântica completa em seu conteúdo, funcionando de maneira análoga a um IPS (*Intrusion Prevention System*);

- Funcionam em modo passivo (monitoração com alertas emitidos aos administradores quando alguma transação fora do padrão adequado for detectada) ou ativo (monitoração com interrupção da transação quando a mesma for identificada como fora do padrão adequado).

- **firewalls específicos** – trata-se dos firewalls criados para atuar junto com um SGBD específico, sendo limitado a esta solução. No mais das vezes, como no caso de um dos mais populares, atuam como os firewalls tradicionais, isto é, não avaliam o conteúdo do pacote, mas, sim, se baseiam nas regras estabelecidas de usuário de origem (que pode ser uma pessoa ou um aplicativo) e destino do pacote (subsistema de destino dentro do SGBD), podendo no máximo se estender para o horário e o endereço de origem da transação (MYSQL, 2016).

- Características

- Funcionamento baseado em *whitelists* (listas de autorização): as transações permitidas devem fazer parte de uma *whitelist*. Se a transação que chega ao firewall foi prevista na *whitelist*, a transação é permitida; do contrário, se a transação não está explicitamente prevista na *whitelist*, será negada;

- Funciona em três modos:

- **permitir** – a transação solicitada, por estar presente na *whitelist* é repassada ao SGBD e lá é executada, de acordo com as regras internas do SQL e do controle de acesso;

- **negar** – a transação solicitada, por estar ausente da *whitelist*, é descartada;

- **detectar** – a transação solicitada, por estar ausente da *whitelist*, é repassada ao SGBD e, ao mesmo tempo, é reportada aos administradores com os motivos da violação das políticas vigentes, deixando a esses administradores a decisão pela ação a tomar.

Bancos de dados comerciais: criptografia

Segundo Microsoft (2016), a criptografia é o processo de se esconder o significado de dados ou informações por meio de uma chave ou senha. Esse mecanismo torna os dados ilegíveis para quem não tem a chave para decifrá-los, o que aumenta a segurança

mesmo quando alguma entidade não autorizada ganhar acesso físico ao servidor. Em casos assim, os dados estarão protegidos, pois apenas os usuários autorizados terão as chaves para decifrar os dados, tornando-os inúteis para os invasores (MICROSOFT, 2016).

A criptografia é um mecanismo que pode — e deve! — ser utilizado para todos os tipos de comunicações e transações em que as informações tenham valor (e não precisam ser apenas informações financeiras para terem valor). É fato que a criptografia gera maior processamento tanto do lado do servidor como do lado do cliente, além de gerar maior tráfego na rede. Contudo, com as velocidades de processamento e de transmissão que temos à nossa disposição nos dias de hoje, esses *overheads* são desprezíveis. O ganho em segurança é de ordem de grandeza maior que a perda em desempenho (que, novamente, é desprezível).

Vejamos alguns exemplos de soluções:

- **soluções de criptografia de dados armazenados** – são módulos dos SGBD comerciais especificamente desenvolvidos para proteger os dados quando estão em seu armazenamento. Visam evitar que indivíduos não autorizados que ganhem acesso ao sistema (invadindo o sistema operacional, por exemplo) tenham acesso aos dados em disco, pois estarão cifrados. Essas soluções complementam as soluções de tunelamento disponíveis para proteger os dados enquanto estão sendo transportados (ORACLE, 2016).

- Características

- **gerenciamento de chaves e certificados digitais** – soluções gerenciam chaves de criptografia, integrando-as com as chaves do sistema de tunelamento e gerenciando os usuários para manter consistência nas chaves;

- **criptografia total ou parcial** – os dados podem estar totalmente criptografados, ou pode-se configurar o sistema para que limite a criptografia por usuário, por bancos de dados ou até mesmo por colunas dos bancos de dados (tipos de registro).

- **soluções de tunelamento** – soluções para cifragem dos dados durante o transporte, garantindo-lhes a segurança mesmo enquanto estão sendo transportados e, nessa situação, estão fora do controle do SGBD ou da aplicação que requisita a transação (MICROSOFT, 2016).

- Características

- **criptografia total ou parcial** – permite tunelamento parcial (apenas dos processos de autenticação e autorização, não recomendado) ou total (cifragem de toda a comunicação, desde seu início, até a desconexão do usuário);

- **criptografia hierarquizada** – exige de chaves privadas, chaves púbicas

combinadas a chaves privadas ou certificados associados a chaves públicas e privadas, dependendo da criticidade da comunicação. Cada nível hierárquico oferece maior segurança que o nível anterior, mas também consome mais recursos de processamento e memória do sistema.

Bancos de dados comerciais: auditorias de *logs* e eventos

Uma das grandes vantagens dos SGBDs modernos é a manutenção de "*logs*", que são registros que armazenam informações sobre tudo o que ocorre no sistema. Hingarh e Ahmed (2013) definem o armazenamento de informações sobre o sistema como uma necessidade fundamental para os sistemas corporativos nos dias de hoje, e os *logs* são a principal ferramenta à disposição da administração de TI para esse fim.

Por meio dos *logs* podem ser estabelecidas as trilhas de auditoria, que são registros de atividades que podem ser utilizados para reconstruir o caminho completo e todas as características de uma ação executada (ou de um conjunto de ações executadas) no sistema (HINGARH; AHMED, 2013).

Os SGBDs comerciais contêm em seu código módulos de auditoria, uma vez que no Brasil o Ministério do Planejamento, por meio da Secretaria de Logística e Tecnologia da Informação, a auditoria de sistemas é regulamentada. Os sistemas de informação que interagem com sistemas do governo brasileiro, nas esferas federal, estadual e municipal, devem ser auditáveis, com regras específicas e formais para cada sistema (ARAÚJO et al., 2015). Ocorre que, por exemplo, os sistemas que são utilizados em bancos e outras instituições financeiras devem periodicamente fornecer informações para o Banco Central, para a Receita Federal e outros órgãos reguladores e, portanto, os SGBDs utilizados nessas instituições devem ser passíveis de auditorias formais. Como todos os fornecedores comerciais de soluções de bancos de dados visam atender ao mercado financeiro, todos os SGBDs de mercado devem contemplar módulos de auditoria.

Exemplificando

O ato Sarbanes-Oxley (também conhecido como SARBOX) é uma lei federal norte-americana aprovada em 2002, que foi adotada internacionalmente por países que participam de ações de comércio com os EUA e com o Mercado Comum Europeu. O ato foi criado em reação ao escândalo da Enron, em que a empresa maquiou suas contas por anos a fio, gerando centenas de bilhões de dólares de prejuízo quando o caso veio à tona em 2001.

A SARBOX estabelece processos rígidos para auditoria com base em trilhas formais e relatórios oficiais periódicos sendo avaliados por consultorias

independentes. É o melhor exemplo mundial de gestão de sistemas por meio de trilhas de auditoria (PORTAL DE AUDITORIA, s. d.).

Vejamos as características demandadas por esses módulos de auditoria no que concerne a segurança dos sistemas (ARAÚJO et al., 2015, p. 22):

> **A auditoria de segurança abrange o reconhecimento, o registro, o armazenamento e a análise de informações relevantes relacionadas à segurança. Por meio destes requisitos os registros de auditoria podem ser examinados para a determinação de quais atividades relevantes para a segurança ocorreram e qual usuário foi responsável pelas ações.**

Pesquise mais

O conjunto de características, critério, condições mínimas e medidas para auditoria de segurança da informação e programas e equipamentos é uma norma publicada pelo Governo Federal determinando os critérios para auditoria de segurança da informação. Disponível em: <http://www.governoeletronico.gov.br/documentos-e-arquivos/GT8135%20-%20CriteriosAuditoriaSeguranca%20V%2004_08_15.pdf>. Acesso em: 16 dez. 2016.

É fundamental, portanto, que os SGBDs de mercado forneçam, no tocante às informações ditas relevantes para a segurança da informação, ferramentas para:

- **reconhecimento** – formas de se identificar e buscar informações do sistema relevantes para a manutenção da segurança;
- **registro** – mecanismos formais de registro de informações relevantes para a segurança do sistema (*logs* e relatórios dos sistemas);
- **armazenamento** – mecanismos formais de armazenamento, seja em forma de arquivos simples, lineares e em formato aberto — desde que armazenados de forma adequada em repositórios bem definidos e protegidos — até bancos de dados especiais, definidos para esse propósito;
- **análise** – mecanismos formais para analisar os dados armazenados, colhendo informações que permitam a tomada de decisão no sentido de manter a segurança do ambiente.

Bancos de dados comerciais: controle e análise de privilégios

Como o SQL é padronizado em todos os SGBD de mercado no que tange o controle de acesso (comandos GRANT e REVOKE), os módulos guardam semelhança entre si. Esse assunto já foi extensamente coberto na unidade 2 desta disciplina.

No que concerne à análise de privilégios, Oracle (2016) aponta que se trata do processo de analisar os privilégios utilizados por um usuário em suas operações diárias contra os privilégios a ele atribuídos. As análises permitem a geração de relatórios que, por sua vez, auxiliam na adequação dos privilégios às necessidades do usuário.

Privilégios que ficam sem uso por períodos definidos pela administração do sistema podem ser revogados sem prejuízo para as atividades do cliente. Além disso, privilégios recém-concedidos podem ser averiguados quanto à sua necessidade nos períodos subsequentes à concessão, permitindo sua manutenção ou remoção, de acordo com o que for coletado pelo módulo de análise de privilégios.

A análise de privilégios permite:

- coleta de atividades e exercícios de privilégios em tempo integral;
- geração de relatórios com recomendações;
- recomendações podem incluir até mesmo a criação de novos perfis ou readequação de perfis existentes.

Reflita

Se o usuário já justificou suas necessidades de privilégio, não seria desperdício de recursos de processamento, memória e rede executar de forma permanente um módulo que analisa privilégios de acesso? O que justifica a existência e a execução perene desse módulo?

Sem medo de errar

Para explicar a Talínia sobre os principais módulos de proteção e segurança em um sistema de bancos de dados de mercado, você pode dividir o assunto em 4 partes, a saber:

1. Firewall;

a. Mostre a Talínia que existem dois tipos de firewalls:

i. os firewalls específicos, voltados ao controle de aplicações, que quando

aplicados a bancos de dados permitem ou negam a passagem das requisições com base em uma tabela de regras que basicamente analisa a origem e o destino dos pacotes, sem analisar-lhes o conteúdo;

ii. os firewalls genéricos, que funcionam com vários bancos de dados, e que de fato atuam como pacotes de IDS/IPS específicos para firewalls. Esses pacotes de fato abrem o conteúdo das requisições de transação e os analisam, deixando passar apenas aqueles com requisitos adequados e que não ponham os dados, os usuários e o sistema em risco.

b. Faça uma busca na internet pelas soluções de mercado para firewalls de bancos de dados e apresente uma lista com as vantagens e desvantagens de cada um.

2. Criptografia;

a. Descreva os pacotes de tunelamento de comunicações, enfatizando a necessidade de que esse tunelamento englobe toda a comunicação, não se restringindo aos processos de autenticação e autorização;

b. Descreva os pacotes de criptografia de dados armazenados, que complementam a criptografia de comunicação, protegendo os dados nos repositórios do sistema.

3. Auditoria e *logs;*

a. Mostre à Talínia a importância dos *logs* para a manutenção de informações sobre as ações que corriqueiramente são realizadas no sistema;

b. Explique para a empreendedora o que são trilhas de auditoria e para que servem, enfatizando sua importância nos processos de auditoria;

c. Mostre à Talínia que a questão da auditoria não é só uma boa ideia, mas uma regulamentação governamental.

4. Controle e análise de privilégios.

a. Mostre à Talínia que a gestão dos privilégios não termina com a atribuição destes, mas, sim, se estende por todo o período em que o usuário efetivamente tem acesso ao sistema;

b. Mostre à empreendedora como funciona o processo de análise de privilégios, confrontando periodicamente os privilégios utilizados com os privilégios atribuídos ao usuário.

Avançando na prática

Auxiliando a manter os dados seguros

Descrição da situação-problema

Salete, uma jovem executiva do setor de energia, procura você, consultor de segurança, com uma dúvida importante. A executiva trabalha o tempo todo com dados sensíveis, que precisa ter à disposição, e que comunica com outras partes, sejam executivos ou servidores remotos. Sabendo da sensibilidade das comunicações que efetua a todo o momento, Salete adotou uma solução de tunelamento que engloba todo o ciclo de vida das comunicações. Porém, recentemente Salete tem tido a seguinte preocupação: e se, ao invés de grampear as comunicações (um ato inútil, uma vez que estão protegidas pelo túnel criptográfico), os bandidos tiverem acesso aos dados em seu notebook? Salete já tem uma solução robusta de antivírus na máquina e uma senha não trivial para entrar no sistema, e até julgava que estava protegida. Contudo, um colega de empresa teve dados sob sua guarda expostos, o que lhe gerou o desligamento imediato da empresa e um processo judicial. Salete agora está com medo.

Sua tarefa é auxiliar Salete a proteger-se também nesse aspecto. Como você a ajudaria? Que medidas podem ser tomadas para proteger os dados que não estão sendo comunicados?

Resolução da situação-problema

A senha de acesso robusta e o antivírus certamente auxiliam, mas não são suficientes, como o colega de Salete pode constatar "na pele". Precisamos ajudar a aumentar a robustez do sistema de Salete. Nesse sentido, três atitudes podem ser de grande auxílio:

1. Instalação e configuração de um firewall pessoal para a rede e também de um firewall pessoal para as aplicações e transações, de preferência um que interprete as transações requisitadas ao notebook de Salete: identifique e imediatamente interrompa aqueles que são considerados maliciosos.

2. Instalação de um sistema de criptografia de disco para que os dados armazenados estejam também protegidos, no caso de um ladrão não se preocupar em invadir o notebook e decidir levá-lo embora. Neste caso o ladrão não vai ter qualquer tipo de acesso aos dados, a menos que saiba a senha, o que demanda que a senha escolhida seja robusta.

3. Implantação de um sistema de manutenção de *logs* e estabelecimento

de trilhas de auditoria no notebook, de forma que possam ser acompanhadas as transações e obtidas informações de uso para melhoria contínua da segurança do dispositivo, por meio da análise dos dados coletados.

Faça valer a pena

1. O termo firewall, que em inglês que significa (em tradução livre) "porta corta fogo", foi criado para definir um tipo de dispositivo que se posta entre a rede externa (internet) e a rede interna de uma organização, permitindo a passagem apenas de tráfego autorizado (NAKAMURA e GEUS, 2007). Esses dispositivos que, em seu nascimento, foram direcionados a proteger a rede, tiveram seu conceito expandido para outros níveis da comunicação. Podemos pensar em um firewall como uma barreira lógica que permite apenas a passagem de elementos autorizados.

Observe a sentença a seguir, que concerne um firewall tradicional de bancos de dados:

As regras de firewall de bancos de dados são simples, pois o que é analisado é _____ do comando e _____.

Assinale a alternativa que completa a sentença sem prejuízos ao conceito apresentado:

a) o objetivo; o valor da transação.

b) a criptografia; o valor da transação.

c) a sintaxe gramatical; quem autorizou a transação.

d) a origem; o subsistema a que se destina.

e) o objetivo; o valor da transação.

2. Segundo Microsoft (2016), a criptografia é o processo de se esconder o significado de dados ou informações por meio de uma chave ou senha. Esse mecanismo torna os dados ilegíveis para que não tenha a chave para decifrá-los, o que aumenta a segurança mesmo quando alguma entidade não autorizada ganhar acesso físico ao servidor.

Analise as asserções a seguir:

I. É fato que a criptografia gera maior processamento tanto do lado do servidor como do lado do cliente, também é fato que gera maior tráfego na rede.

PORQUE

II. Com as velocidades de processamento e de transmissão que temos à nossa disposição nos dias de hoje, esses *overheads* são desprezíveis.

Analisando-se as asserções acima, conclui-se que:

a) As duas afirmações são verdadeiras e a segunda justifica a primeira.

b) As duas afirmações são verdadeiras e a segunda não justifica a primeira.

c) A primeira afirmação é verdadeira e a segunda é falsa.

d) A primeira afirmação é falsa e a segunda é verdadeira.

e) As duas afirmações são falsas.

3. Uma das grandes vantagens dos SGBDs modernos é a manutenção de "*logs*", que são registros que armazenam informações sobre tudo o que ocorre no sistema. Hingarh e Ahmed (2013) definem o armazenamento de informações sobre o sistema como uma necessidade fundamental para os sistemas corporativos nos dias de hoje, e os *logs* são a principal ferramenta à disposição da administração de TI para esse fim.

Sobre as trilhas de auditoria em sistemas comerciais de bancos de dados, podemos afirmar o seguinte:

a) São prejudiciais, pois expõem os dados a ataques de hackers e vírus.

b) São desnecessárias na presença de criptografia forte do sistema.

c) Estão presentes nos sistemas por regulamentação governamental.

d) São fundamentais para o funcionamento do SGBD, pois, sem elas, o sistema para.

e) São parte fundamental do tunelamento de dados durante a comunicação.

Referências

ARAÚJO, A. S. et al. **Conjunto de características, critério, e condições mínimas e medidas para auditoria de segurança da informação e programas e equipamentos**. Brasília: Imprensa Oficial, 2015.

BACA, M. **Introduction to Metadata**. Los Angeles: Getty Institute, 2008.

CHAPPIE, M. **Metadata security and preventing leakage of sensitive information**. Site TechTarget, publicado em: 18 nov. 2013. Disponível em: <http://searchsecurity.techtarget.com/tip/Metadata-security-and-preventing-leakage-of-sensitive-information>. Acesso em: 16 dez. 2016.

CHIECO, B. **Estratégia de BYOD é essencial para bom rendimento dentro da empresa, diz IBM**. Site Convergence.com.br. Publicado em: 24 set. 2013. Disponível em: <http://convergecom.com.br/tiinside/24/09/2013/estrategia-byod-essencial-rendimento-empresa-ibm/>. Acesso em: 15 dez. 2016.

DIAZ, J. **These breasts nailed a hacker for the FBI**, site Gizmodo, publicado em: 12 abr. 2012. Disponível em: <http://gizmodo.com/5901430/these-breasts-nailed-anonymous-hacker-in-fbi-case>. Acesso em: 16 dez. 2016.

GHORBANZADEH, P. et al. **A Survey of Mobile Database Security Threats and Solutions for It**. 3rd International Conference on Information Sciences and Interaction Sciences (ICIS), 23-25 jun. 2010, Chengdu, China, p. 676-682

GUERBER, C. **Redes de Computadores – TCP/IP**. Site Universidade do Contestado, publicado em: 14 nov. 2007. Disponível em: <http://www.mfa.unc.br/info/carlosrafael/rco/aula17-1.pdf>. Acesso em: 16 dez. 2016.

HANSEN, J. **What's different about mobile security?**. Site Breezy.com. Publicado em: 21 out. 2014. Disponível em: <http://www.breezy.com/blog/2014-10-21-whats-different-about-mobile-security.html>. Acesso em: 15 dez. 2016.

HINGARH, V.; AHMED, A. **Understanding and conducting information systems auditing**. Singapura: Wiley, 2013.

HORN, L. **The 20 mors common PINs are painfully obvious**. Site Gizmodo.com. Publicado em: 26 set. 2012. Disponível em: <http://gizmodo.com/5946582/the-20-most-common-pins-are-painfully-obvious>. Acesso em: 15 dez. 2016.

KIPP, S. **Exponential bandwidth growth and cost declines**. Site Network World, publicado em: 10 abr. 2012. Disponível em: <http://www.networkworld.com/article/2187538/

tech-primers/exponential-bandwidth-growth-and-cost-declines.html>. Acesso em: 16 dez. 2016.

LEMOS, R. **Metadata Poses Both Risks And Rewards**, site Dark Reading, publicado em: 19 mar. 2014. Disponível em: <http://www.darkreading.com/document.asp?doc_id=1251053&>. Acesso em: 16 dez. 2016.

LUGO, I.; PARKER, D. **Software Firewalls: Made of Straw?**. Site Symantec, publicado em: 2 nov. 2010. Disponível em: <https://www.symantec.com/connect/articles/software-firewalls-made-straw-part-1-2>. Acesso em: 16 dez. 2016.

MATTHEWS, A.; GLISER, S. **Creating Mobile Apps with JQuery**, Birmingham: Packt Publishing, 2015.

MICROSOFT. **SQL Server Encryption**. Site Microsoft, publicado em: 3 maio 2016. Disponível em: <https://msdn.microsoft.com/en-us/library/bb510663.aspx>. Acesso em: 16 dez. 2016.

MOBILEIIRON. **Mobile Security: Threats and Countermeasures**. Site MobileIron.com. Publicado em: 28 nov. 2014. Disponível em: <http://info.mobileiron.com/rs/mobileiron/images/Mobile-Security-Threats-and-Countermeasures-WP-MKT-6361%5B1%5D.pdf>. Acesso em: 15 dez. 2016.

MYSQL. **MySQL Enterrise Firewall**. Site MySQL.com, publicado em: 2016. Disponível em: <https://www.mysql.com/products/enterprise/firewall.html>. Acesso em: 16 dez. 2016.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec, 2007.

NISO, National Information Standards Organization. **Understanding Metadata**. Site NISO.org, 2004. Disponível em: <http://www.niso.org/publications/press/UnderstandingMetadata.pdf>. Acesso em: 16 dez. 2016.

ORACLE Systems. **Oracle Audit Vault and Database Firewalll – White Paper**. Site Oracle.com, publicado em dezembro de 2015. Disponível em: <http://www.oracle.com/technetwork/database/database-technologies/audit-vault-and-database-firewall/downloads/owp-audit-vault-db-firewall-122-2844505.pdf>. Acesso em: 16 dez. 2016.

OWASP. Open Web Application Security Project – **OWASP Mobile Security Project**. Site OWASP.org, publicado em 2014. Disponível em: <https://www.owasp.org/index.php/OWASP_Mobile_Security_Project#Top_Ten_Mobile_Risks>. Acesso em: 16 dez. 2016.

PORTAL DE AUDITORIA. **Introdução à Lei Sarbanes-Oxley**. Site Portal de Auditoria. Disponível em: <http://www.portaldeauditoria.com.br/auditoria-interna/Introducao-a-lei-Sarbanes-Oxley-SOx.asp>. Acesso em: 16 dez. 2016.

RAHIMI, S. K.; HAUG, F. S. **Distributed Database Management Systems** – A practical approach. Nova York: Wiley, 2010.

SHELDON, R. **Wireless carrier security risks**: Keeping enterprise data safe, site Techtarget,

publicado em: abril de 2012. Disponível em: <http://searchmobilecomputing.techtarget.com/tip/Wireless-carrier-security-risks-Keeping-enterprise-data-safe>. Acesso em: 16 dez. 2016.

SHETTY, K.; HANNA, G. **Oracle Audit Vault and Database Firewall Concepts Guide**. San Francisco: Oracle Press, 2016.

SOUZA, T. B.; CATARINO, M. E.; SANTOS, P. C. Metadados – catalogando dados na Internet. **Revista Transformação**, v. 9, n. 2, p. 93-105, maio-agosto, 1997.

Segurança em servidores de banco de dados

Convite ao estudo

Chegamos à unidade final de nossos estudos sobre segurança de sistemas de bancos de dados.

Já que vimos vários aspectos ligados aos dispositivos, isto é, aos clientes de bancos de dados. Agora é hora de entendermos como proteger o cerne de um ambiente típico de bancos de dados: o servidor. E essa proteção vai desde prevenir os ataques diretos, via SQL Injection, até atitudes mais amplas, como no caso da adoção de políticas de segurança.

Com esta unidade, damos sequência ao desenvolvimento da competência geral da disciplina, que é conhecer e ser capaz de definir políticas de segurança lógica e física de dados. Desenvolveremos também a competência específica que é conhecer e ser capaz de utilizar técnicas para segurança de bancos de dados e seus servidores.

Os objetivos de aprendizagem desta unidade são:

• Conhecer e compreender o que é SQL Injection, suas técnicas, prevenções e efeitos;

• Conhecer os aspectos fundamentais da proteção e do controle de acesso a servidores de bancos de dados e a recursos estratégicos para a organização;

• Compreender para que serve e quais os pontos principais de uma política de segurança de bancos de dados.

O empresário Gilberto é o proprietário da Imobiliária R#R2 e está com um problema que lhe dá a maior dor de cabeça: os imóveis que ele capta para vender e/ou alugar e anuncia em seu site estão aparecendo, alguns

dias depois, no website de sua maior concorrente: a imobiliária X@X2. Um amigo de Gilberto, que já trabalhou em uma empresa que teve problemas semelhantes, aconselhou o empresário a verificar o problema com auxílio profissional, e por isso você foi contratado. Gilberto não entende nada sobre o assunto, pois sua especialidade é vender imóveis; vai precisar, então, entender do que se trata e ao mesmo tempo ser auxiliado a resolver o problema. Como ajudar Gilberto?

Na primeira seção desta unidade, entenderemos o que é SQL Injection e conheceremos o histórico desse ataque. Na Seção 4.2, conheceremos um pouco mais sobre as técnicas empregadas nesse ataque. Na Seção 4.3, vamos conhecer formas de prevenção contra o SQL Injection. Por fim, na Seção 4.4, conheceremos exemplos reais de ataques de SQL Injection e os impactos que causaram.

Seção 4.1

Introdução ao SQL Inject

Diálogo aberto

Uma coisa que todo profissional de segurança e todo administrador de bancos de dados aprende logo no início da carreira é que nem toda requisição ao banco de dados é válida só porque vem de uma origem autorizada. Um ataque insidioso disfarçado de uma sequência de requisições SQL pode estar contido nos pacotes. Entender que tipo de ataque é este e como ele veio a ser disseminado é fundamental para que possamos evitá-lo nos ambientes sob nossa responsabilidade.

Nesta etapa do projeto para o qual você foi contratado por Gilberto, o empresário do setor imobiliário, você deverá ajudá-lo a resolver o problema mais prioritário de evasão de informações, que você desconfia ser um caso de SQL Injection. Para tanto, você deve mostrar a Gilberto do que trata esse ataque, como ele ocorre, como é possível prevenir, atuando diretamente sobre o ambiente do site de Gilberto para corrigir o que estiver errado nesse sentido, e mostrar ao empresário que o problema, de fato, é sério e precisa de vigilância constante.

Nesta seção, conheceremos o que é SQL Injection e o histórico desse ataque, veremos quais são as técnicas empregadas nesse ataque, como preveni-lo e conheceremos também alguns de seus casos mais famosos e os impactos que causaram.

Não pode faltar

A partir de agora, vamos entender o que é o ataque de SQL Injection, que tem o potencial de ser um dos mais devastadores contra bancos de dados na atualidade, apesar de já ter quase vinte anos de idade.

O que é SQL Injection – histórico

Segundo Clarke (2012), SQL Injection é o ataque que ocorre quando o atacante a

possibilidade de criar uma *query* SQL (um comando SQL) com elementos inválidos na sintaxe (caracteres de controle, tais como aspas e outros) mal posicionados, com o servidor respondendo a estas *queries* mal formatadas de maneira inesperada, potencialmente danosa.

Obviamente que essas *queries* não geram respostas válidas, pois não configuram transações válidas. No entanto, se o sistema não estiver protegido adequadamente, gerarão, sim, respostas, ao invés de serem descartadas, o que pode permitir acesso não autorizado aos bancos de dados, coleta de informações por parte dos bandidos e até mesmo causar dano no sistema, apagando ou corrompendo dados e informações armazenadas (CLARKE, 2012).

É interessante observar que o nome "SQL Injection" se refere à inserção de códigos (não especificados na sintaxe) em comandos e *queries* SQL. Este foi o primeiro tipo de ataque de injeção de código, mas hoje nem de longe é o único. No mais das vezes, quando mencionamos "SQL Injection", podemos estar nos referindo a vários ataques da mesma natureza, em que códigos não adequados à sintaxe de uma linguagem qualquer permitem a interação dos bandidos com o sistema, obtendo informações e acessos não autorizados (OWASP, 2013). Em sua lista Top-10, de 2013, para ataques cibernéticos, a OWASP (Open Web Application Security Project) cita que várias linguagens são passíveis de ataques de injeção de código, entre elas:

• SQL – Structured Query Language, a linguagem de interação com bancos de dados, permite consultas e é o alvo principal dos esforços de segurança de bancos de dados;

• LDAP – Lightweight Directory Access Protocol, um protocolo bastante usado para controle de acesso a sistemas e aplicações;

• XML – Extensible Markup Language, uma linguagem interpretada que estende as funcionalidades do HTML;

• SMTP – Simple Mail Transport Protocol, o protocolo de envio e recebimento de mensagens de e-mail. tem

Assimile

SQL Injection é uma particularidade de um ataque mais amplo conhecido como injeção de código.

Em que pese apenas o primeiro exemplo citado acima (SQL) ser uma linguagem adequada para receber o nome "SQL Injection", a indústria de segurança da informação tradicionalmente chama de "SQL Injection" qualquer ataque de injeção de código, independentemente da linguagem envolvida (CLARKE, 2012).

É importante observar que os ataques de SQL Injection são conhecidos há bastante tempo, como veremos a seguir, e as vulnerabilidades que os geram têm sido resolvidas paulatinamente à medida que novas versões de software são lançadas. Os ataques mais frequentes, portanto, dependem, na maioria dos casos, da presença de código legado, não atualizado, para que possam ocorrer (OWASP, 2013).

Os ataques de SQL Injection não são novos. Segundo Phrack (1998), o hacker conhecido como "rain.forest.puppy" (conhecido pelas iniciais RFP, jamais identificado, mas com mais de duas décadas de serviços prestados à comunidade de segurança da informação) identificou esse ataque em 1998, publicando um artigo seminal sobre o assunto no Natal daquele ano.

RFP descobriu que conseguiria acesso a informações sobre a árvore de diretórios de um sistema Windows NT (bastante comum na época) rodando o servidor Web IIS, da Microsoft, com base em um comando malformado (PHRACK, 1998):

```
%documentroot%\<NOME_FALSO>.idc.
```

Ocorre que, no comando acima, o identificador %documentroot% é usado no lugar do caminho completo de diretório, que é uma informação sensível e não divulgada pelos servidores Web, por ser potencialmente danosa. Ocorre, também, que a terminação ".idc" designa procedimentos de bancos de dados que são enviados ao módulo SQL e são executados, com base nas permissões disponíveis. Infelizmente, antes de checar as permissões, o sistema identificava a presença (ou não) do procedimento IDC cuja execução estava sendo solicitada. No caso de um procedimento falso de nome, por exemplo, "PROC_FALSO" ser acionado, a resposta do sistema era (PHRACK, 1998):

```
"Cannot open c:\inetpub\wwwroot\PROC_FALSO.idc"
```

O problema com essa resposta é de fácil observação: o sistema acaba de revelar ao atacante o diretório raiz dos documentos armazenados no diretório "C:\inetpub\wwwroot\", que é uma informação bastante sensível, a qual deveria ser mantida em sigilo pelo sistema. Sabendo o ponto a partir do qual todos os arquivos estão armazenados, o atacante tem seu trabalho bastante facilitado (PHRACK, 1998).

Essa é a principal característica dos ataques de SQL Injection (e da grande maioria dos ataques de Code Injection também): ao criar sentenças inválidas sob o ponto de vista da sintaxe da linguagem em questão (SQL, no caso do SQL Injection), mas que não são rejeitadas pelo sistema, o atacante consegue acesso a informações que deveriam ser mantidas longe dos olhos de qualquer indivíduo não autorizado.

As portas abertas pelo hacker RFP em seu artigo foram exploradas por inúmeros interessados pelo mundo afora, e em pouco tempo as falhas ganhavam o nome de "SQL Injection". Nestas quase duas décadas em que o ataque existe, tornou-se um dos mais explorados, uma vez que os pacotes contendo essas transações maliciosas

passam facilmente pelos firewalls e antivírus, pois esses ataques não são direcionados à rede, mas sim às aplicações (CLARKE, 2012).

Técnicas de SQL Injection

Para entendermos como funciona o ataque de SQL Injection na prática, é importante, antes, entendermos como ocorre a passagem de parâmetros para uma aplicação Web. Quando estamos navegando, digamos, em um site de compra e desejamos ver todos os itens que custam menos de R$100,00 (clicando em um botão com esse valor ou explicitando-o em uma caixa de diálogo), o código em nosso navegador vai enviar ao sistema uma URL com um formato semelhante a este (CLARKE, 2012):

```
http://www.site-de-compras.com/produtos.php?valor_max=100
```

Neste exemplo, o site encontra-se no endereço http://www.site-de-compras.com, o aplicativo interno sendo acionado (sem que o usuário precise se preocupar com isso) chama-se produtos.php, e há um parâmetro passado na variável valor_max, sendo que esse valor é 100 (representando R$100,00). A interface web que o usuário tem à disposição cuida de criar a URL enviada com os dados escolhidos, e tudo isso ocorre sem que ele precise se preocupar.

Do lado do servidor, a variável valor_max terá seu valor extraído, e uma *query* SQL será montada, gerando algo semelhante a:

```
"SELECT *

FROM Produtos

WHERE Preco < '100,00'

ORDER BY DescricaoProdutos;"
```

É importante observar ques na construção do comando acimas a vírgula e os dígitos de centavos, bem como as aspas simples no número "100", são adicionadas pelo sistema, que cria a sintaxe adequada para que o comando SQL seja aceito.

Vejamos agora um ataque simples que pode ser feito com esse mecanismo. Se o atacante cria sua própria URL e o faz da seguinte forma, teremos um comportamento diferente por parte do sistema:

```
http://www.site-de-compras.com/produtos.php?valor_max=100' OR '1' = '1
```

Essa URL, que jamais seria criada pela interface à disposição do usuário, contém um conjunto de caracteres que não faz sentido, logo depois do número 100. Contudo, o valor de valor_max agora é "100' OR '1' = '1". Observemos como esse valor vai ser

adicionado pelo sistema ao comando SQL:

```
"SELECT *

FROM Produtos

WHERE Preco < '100,00' OR '1' = '1'

ORDER BY DescricaoProdutos;"
```

A *query* montada agora tem um significado diferente: os registros serão exibidos em dois casos:

• Caso 1: a variável "Preco" do registro em questão tem valor inferior a 100;

• O valor '1' seja igual ao valor '1'.

Obviamente que a segunda condição sempre será verdadeira, e, nesse caso, todos os registros do banco de dados serão expostos. Ou seja, o valor supostamente sem sentido atribuído à variável valor_max gerou uma *query* sintaticamente válida, que gera um resultado inesperado para quem criou a aplicação: expõe, sem filtro, todo o conteúdo do banco de dados de produtos, mesmo aqueles que porventura o dono do banco de dados não queira que sejam vistos.

Essa "injeção" de código não adequado para formar uma *query* SQL está na base de todos os ataques SQL (OWASP, 2013).

Segundo OWASP (2013), são várias as técnicas derivadas da técnica clássica, que também configuram ataques de SQL Injection:

• Filtragem inadequada (ou ausente) de caracteres de controle – é o nome formal e genérico da técnica clássica de SQL Injection. Um ou mais caracteres de controle passados como parâmetros. Como não são filtrados (ou descartados como ilegais), um ou mais caracteres de controle passados como parâmetros terminam por compor uma *query* SQL, que, por sua vez, gera resultados não autorizados pelo sistema;

• Manipulação incorreta de tipos – ocorre quando o interpretador dos comandos não está preparado para identificar e tratar adequadamente os tipos passados nas variáveis, gerando comandos SQL que podem gerar resultados inesperados e indesejáveis;

Exemplificando

```
Comando_Criado :=   SELECT *
                    FROM Tabela
                    WHERE Login = "+ Vari + ";"
```

Nesse caso, espera-se que a variável seja um número, mas se for uma *string* (cadeia de caracteres), o sistema também a aceitará caso não haja mecanismos internos para descartar tudo o que não for número. Nesse caso, uma cadeia de caracteres do tipo "1;DROP TABEL Usuarios" pode provocar a remoção de toda a tabela chamada "Usuarios".

• **Injeção SQL às cegas** – ocorre quando o sistema não apresenta respostas diretas, tais como apresentação de tabelas e registros SQL. Nesse caso, as respostas vêm oblíquas, em muitos casos sob forma de mensagens de erro ou de avisos, que por não estarem adequadamente ajustadas, dão mais informações ao atacante do que o sistema deveria dar;

• **Exemplo** – o ataque descoberto por RFP em 1998 que descobria a árvore de diretórios de um servidor Web.

• **Injeção SQL de segunda ordem** – no caso, a expressão "segunda ordem" implica em comandos SQL mal-intencionados (como nos casos descritos acima) serem enviados como parâmetro a um sistema que os reenvia a outro sistema, sendo que este segundo sistema executa os comandos, tendo maiores privilégios para tanto.

Reflita

Há algum valor possível em se enviar um comando SQL às cegas, isto é, sem que seja possível colher o resultado do comando e com acesso apenas às mensagens de erro que daí provêm?

Prevenção contra SQL Injection

Em que pese um ataque de SQL Injection, quando realizado, poder ser bastante nocivo ao ambiente, prevenir contra esse tipo de problema não é tarefa complicada para o administrador do ambiente. Clarke (2012) recomenda que as técnicas para prevenir o SQL Injection sejam adotadas em conjunto, ao invés de separadamente. Alguns passos simples e importantes na proteção, segundo o autor, são:

• **Manter o software sempre atualizado** – SQL Injection é um tipo de ataque que incide sobre sistemas que não estão preparados para lidar com requisições mal formatadas. Ocorre que os fabricantes de sistemas operacionais, servidores Web, servidores de SGBD e de demais softwares que de alguma forma participam do processo de interpretação de comandos já se preocupam ininterruptamente em atualizar os pacotes toda vez que alguma impropriedade é descoberta. A vasta maioria dos ataques pode ser impedida, nos dias de hoje, simplesmente mantendo o software atualizado;

• **Segurança dirigida ao/pelo domínio (DDS – Domain Driven Security)** – técnica

que consiste em pensar todo o domínio por onde passa uma transação como sendo um todo que precisa ser unificado em termos de segurança. Neste sentido, o DDS demanda que a transação seja pensada do começo ao fim pelos responsáveis e desenvolvedores de todos os módulos e aplicativos, pelos quais a transação e os dados passam e/ou são interpretados. Demanda:

• Linguagem normatizada – termos, requisitos, entidades de processamento iguais em todos os níveis, entre outros;

• Elementos técnicos normatizados – tipos de variáveis, tratamento de erros, passagem de parâmetros, restrições quanto aos dados, entre outros;

• Integração dos módulos regida pelo design de segurança obtido em conjunto;

• Testes sistêmicos extensivos dos módulos integrados.

• **Comandos parametrizados** – Ao invés de permitir a construção dinâmica de comandos, as aplicações – assim como a interface Web — podem trabalhar com alternativas fixas, pré-determinadas pelo sistema como um todo, evitando que comandos sejam criados em tempo real. Os comandos são, ao invés disso, montados como se fossem um quebra-cabeça, com as peças já prontas para serem usadas. Dessa forma não é possível passar parâmetros errôneos por meio de um comando;

• **Validação de entrada** – consiste na inserção de um módulo de interpretação e análise dos comandos, enviando ao sistema apenas aqueles que forem congruentes e possam ser passados adiante. Dessa forma, comandos mal formatados ou abertamente maliciosos são identificados e geram apenas uma mensagem de erro de sintaxe. Alternativamente, os módulos individuais podem realizar o processo de validação das entradas a cada estágio da tramitação da transação pelos vários módulos do sistema. Esse segundo método de validação de entrada tem a vantagem de ser mais efetivo, pois há uma análise na "porta de entrada" de cada módulo, porém há maior consumo de recursos do sistema;

• **Whitelisting/Blacklisting** – são módulos de controle de acesso de entrada das transações no sistema. As transações oriundas de locais (usuários, aplicativos e sistemas) presentes em whitelists (listas autorizadas) podem entrar, pois são confiáveis. Aquelas contidas em blackists (listas de negação) são marcadas como oriundas de fontes nocivas e são descartadas sem maior cerimônia. Os demais (não contidos nem em whitelists ou blacklists) passam pelo processo de validação de entrada e devem ser autorizados por algum responsável pelo sistema.

Pesquise mais

Um interessante artigo da revista SQL Magazine exemplifica com detalhes um ataque de SQL Injection, mostrando o mecanismo e ensinando uma

técnica simples para prevenção. O artigo chama-se *SQL Injection: o que é, por que funciona e como prevenir* e traz bastante valor para a discussão acerca do SQL Injection.

MATHEUS, C., **SQL Injection: o que é, por que funciona e como prevenir**, Revista SQL Magazine, Vol. 2, n. 23, 27 jul. 2007, disponível em: <http://www.devmedia.com.br/sql-injection-o-que-e-por-que-funciona-e-como-prevenir-sql-magazine-23/6102>. Acesso em: 21 fev. 2017.

Exemplos e impactos de SQL Injection

Infelizmente, por mais simples que seja evitar os ataques de SQL Injection, com soluções e técnicas disponíveis desde antes do ano 2000 (CLARKE, 2012), temos vários casos ao longo das últimas duas décadas em que esses ataques foram registrados. Vejamos alguns dos mais interessantes:

• **Guess, 2002** – O jovem de 19 anos Jeremiah Jacks conseguiu, em poucas horas, encontrar um nó nos servidores da Guess o que lhe permitiu emitir um comando SQL cujo resultado foi a exibição de registros de bancos de dados contendo nome, número, data de expiração e código de segurança de 200.000 cartões de crédito de clientes da empresa. Pior: Jacks tentou durante dias avisar a Guess da vulnerabilidade, mas não teve sucesso algum. Apenas quando ele procurou a empresa SecurityFocus e contou sobre seu ataque que obteve sucesso, pois a própria SecurityFocus alertou a Guess (POULSEN, 2002);

• **Lições a aprender** – Quando a empresa recebe um alerta de segurança, por mais que possa parecer absurdo este alerta, não é uma prática aceitável ignorá-lo.

• **PetCo, 2003** – O mesmo Jeremiah Jacks, usando o mesmo mecanismo viria a expor dados de cartão de crédito da PetCo, em 2003, com duas diferenças: dessa vez foram 500.000 números expostos e dessa vez o jovem demorou menos de 1 minuto para acessar os dados. Felizmente a PetCo foi mais inteligente que a Guess e aceitou o aviso de Jacks quando ele ligou para avisar do caso. Isso porque o caso da Guess havia sido amplamente divulgado, e a PetCo não quis correr riscos;

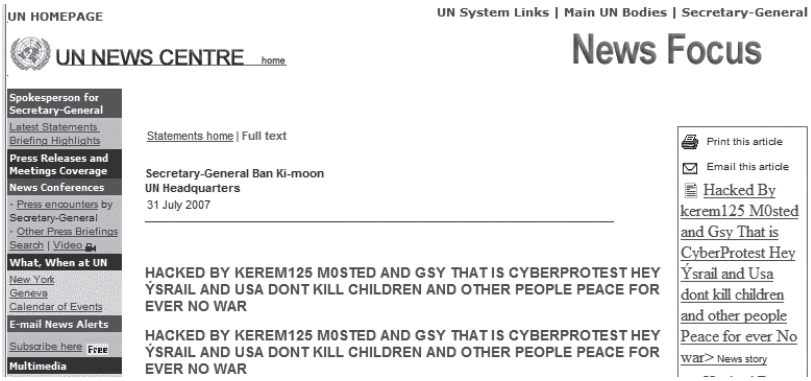
• **Lições a aprender** – Dar ouvidos a um alerta de segurança é bom, mas melhor ainda será ouvir um caso de violação de segurança no mercado e fazer um teste de penetração usando a mesma técnica para ver se nosso ambiente não contém a mesma vulnerabilidade. Afinal de contas, a PetCo poderia ter ficado sabendo da falha não pela boca do bom samaritano Jeremiah Jacks, mas em uma manchete de jornal anunciando o roubo de meio milhão de números de cartões de crédito.

• **Site das Nações Unidas, 2007** – No fim de semana de 11 e 12 de agosto de 2007, os hackers "kerem125", M0sted e "Gsy That" usaram um comando mal formatado de SQL para obter informações que lhes permitiram invadir o site da ONU, onde trocaram

a página do então Secretário Geral Ban Ki-Moon por mensagens contra Israel e os EUA, pelas mortes de crianças em suas invasões militares;

• **Lições a aprender** – Não é porque a organização é sem fins lucrativos ou mesmo de utilidade pública que se pode baixar a guarda no que concerne à segurança de bancos de dados. E não é porque se trata de uma organização de alcance mundial que a infraestrutura não terá vulnerabilidades. É fundamental ficar atento para a segurança independentemente do porte ou da natureza da instituição.

Figura 4.1 | Página do Secretário Geral da ONU Ban Ki-Moon após o ataque via SQL Injection



Fonte: <https://hackademix.net/wp-content/uploads/2007/08/un-ss2.png>. Acesso em: 21 fev. 2017.

• **Site da cantora Lady Gaga, 2011** – O grupo SwagSec atacou o site da cantora Lady Gaga, levando milhares de registros com informações de fãs da artista, bem como todo um diretório de e-mails. O grupo usou uma falha no código para perpetrar o ataque de SQL Injection, valendo-se do fato de que apesar de a vulnerabilidade ser de conhecimento público havia meses, e as correções estarem disponíveis, foram aplicadas no site de Lady Gaga apenas depois do ataque.

• **Lições a aprender** – é uma temeridade sem tamanho não aplicar correções para uma vulnerabilidade de conhecimento público, e nada justifica isso.

Exemplificando

Em maio de 2011, o grupo de hackers LulzSec invadiu vários sites da Sony, usando para tanto uma técnica de SQL Injection cego, comprometendo milhares de senhas, bem como dados pessoais de clientes (nomes, endereços e documentos), além de roubar 3,5 milhões de cupons "vale-música" (CLARKE, 2012).

Sem medo de errar

Desconfiado que, no caso do empresário Gilberto, o que está ocorrendo para que informações sobre imóveis à venda e para alugar, captados por sua imobiliária, apareçam no site da concorrência seja um caso típico de SQL Injection, você toma as ações que vão auxiliar na resolução do problema.

Um curso de ação válido neste caso é o seguinte:

1. Explicar, em termos simples e compreensíveis, o que é SQL Injection, de forma que Gilberto saiba do que se trata o problema.

2. Realizar um teste de penetração no ambiente da imobiliária de Gilberto, utilizando as principais técnicas de SQL Injection, determinando, assim, como os bandidos estão roubando as informações do site do empresário.

3. Identificar, no ambiente de TI da imobiliária, quais pacotes de software precisam de atualização, implantando e testando essas atualizações. É importante observar que as atualizações podem (e devem) ser realizadas mesmo antes da análise das vulnerabilidades, uma vez que, por si só, já resolvem vários problemas potenciais que possam estar presentes no ambiente.

4. Realizar uma avaliação detalhada no código do site e em todas as aplicações pelas quais as transações passam, determinando aquelas que se apresentam vulneráveis aos ataques de SQL Injection.

5. Aplicar as técnicas de correção, eliminando as possibilidades de SQL Injection identificadas.

6. Criar um mecanismo de avaliação periódica do ambiente, designando um profissional para cuidar desse aspecto, que busque periodicamente informações sobre o assunto e mantenha o ambiente sempre em dia, e sempre testado.

Dessa forma, essa questão apresentada por Gilberto tende a ser resolvida e as chances de o problema não se repetir são grandes.

Avançando na prática

Convencendo o empresário a se proteger

Descrição da situação-problema

Hermes Gerums é um empresário do setor de compra e venda de tecidos por atacado. Esse não é um setor com alto grau de automatização ou de informatização, mas Hermes descobriu que um site que exponha seus produtos pode aumentar as

vendas e, como ele é bastante interessado (e não gosta muito de gastar dinheiro), decidiu aprender e implantar o site ele mesmo. Para isso, conseguiu uma antiga cópia do ambiente de comércio eletrônico que um amigo seu implantou oito anos atrás e, depois de muito sacrifício, colocou o ambiente para funcionar e o configurou para sua empresa e seus produtos.

Quando Hermes mostra o ambiente para você, seu amigo e especialista em segurança de sistemas de bancos de dados, você percebe que além dos produtos e preços para o usuário final, a interface com o usuário disponibiliza o sistema interno — que só poderia ser visto pelos funcionários da empresa — e a qual também contém informações sobre fornecedores e preços cobrados da empresa de Hermes.

Essas informações são bastante sensíveis e estão armazenadas em um sistema que não é atualizado há oito anos. Hermes não quer mexer nisso, uma vez que deu um trabalhão fazer funcionar, e ele é partidário da opinião de que "em time que está ganhando, não se mexe".

Em sua opinião, há alguma coisa de errado com esse quadro? Se sim, como ajudar Hermes?

Resolução da situação-problema

Qualquer profissional de segurança sabe que uma das principais fontes de problemas para um ambiente informatizado é a falta de atualização do software. No caso do ambiente de Hermes, oito anos é um tempo absolutamente inaceitável, e, mesmo que haja risco de provocar interrupções nos serviços, o ambiente deve ser atualizado com urgência. Neste período de oito anos, várias vulnerabilidades foram descobertas em sistemas operacionais, bancos de dados, sistemas de autenticação, servidores Web e vários outros sistemas que o ambiente de Hermes pode fazer uso.

Não há, em outras palavras, uma justificativa viável para não atualizar o ambiente.

Você pode ajudar Hermes apresentando-lhe um plano para replicar o ambiente em laboratório (um ambiente separado, simulando o ambiente real), realizar as atualizações ali, acertando-as até que funcionem, e depois transportar as soluções e atualizações para o ambiente real, minimizando, assim, os transtornos.

Faça valer a pena

1. SQL Injection é o ataque que ocorre quando o atacante tem a possibilidade de criar uma *query* SQL (um comando SQL) com elementos inválidos na sintaxe (caracteres de controle, tais como aspas e outros) mal posicionados, com o servidor respondendo a essas *queries* mal formatadas de maneira inesperada, potencialmente danosa.

No que concerne o ataque conhecido pelo nome de SQL Injection, é correto afirmar que:

a) É um vírus bastante perigoso que ataca bancos de dados em ambientes financeiros.

b) É uma negação de serviço que ocorre em função da violação de integridade.

c) Não é um problema de segurança, mas sim uma característica dos bancos de dados.

d) É um caso especial de um ataque mais genérico: o ataque de inserção de código.

e) É exclusivo aos ambientes hospitalares, clínicas e farmácias.

2. De maneira geral, os ataques de SQL Injection ocorrem quando um código estranho à sintaxe de um comando SQL é injetado neste comando, gerando um código que não cumpre com um propósito válido e previsto pela aplicação, mas que ainda assim é interpretado e executado pelo sistema a que se destina, produzindo efeitos indesejáveis neste sistema.

A filtragem inadequada (ou ausente) de caracteres de controle ocorre quando:

a) Um ou mais caracteres de controle são passados como parâmetros e, por não serem filtrados (descartados como ilegais), terminam por compor uma *query* SQL, que, por sua vez, gera resultados não autorizados pelo sistema.

b) O interpretador dos comandos não está preparado para identificar e tratar adequadamente os tipos passados nas variáveis, gerando comandos SQL que podem gerar resultados inesperados e indesejáveis.

c) O sistema não apresenta respostas diretas, tais como apresentação de tabelas e registros SQL e, nesse caso, as respostas vêm oblíquas, em muitos casos sob forma de mensagens de erro ou de avisos, que, por não estarem adequadamente ajustados, dão mais informações ao atacante do que o sistema deveria dar.

d) Os comandos SQL mal-intencionados são enviados como parâmetro a um sistema que os reenvia a outro sistema, sendo que este segundo

sistema executa os comandos, tendo maiores privilégios para tanto.

e) Os comandos SQL são traduzidos para outra linguagem de programação orientada a objetos e passados como parâmetros por um sistema de autenticação, que filtra o código malicioso e o executa diretamente no sistema operacional.

3. Em que pese um ataque de SQL Injection, quando realizado, poder ser bastante nocivo ao ambiente, prevenir-se contra este tipo de problema não é tarefa complicada para o administrador do ambiente. Clarke (2012) recomenda que as técnicas para prevenir o SQL Injection sejam adotadas em conjunto, ao invés de separadamente.

Manter o software de um ambiente de bancos de dados é uma medida efetiva contra o SQL Injection? Por quê?

a) Não, pois não auxilia na identificação do que está errado com o comando criado para o ataque.

b) Sim, pois não há ataque de negação de serviços que resista a uma atualização de software.

c) Sim, pois a atualização de software corrige a consistência dos dados armazenados nos bancos de dados, impedindo sua deterioração.

d) Não, pois atualização de software não previne contra vírus.

e) Sim, pois a vasta maioria das vulnerabilidades que permitem esse ataque já foi descoberta e corrigida pelas atualizações de software.

Seção 4.2

Controle de acesso não autorizado

Diálogo aberto

Olá! Vamos dar sequência aos nossos estudos?

Os servidores de uma organização são o ponto mais delicado da estrutura de TI. É ali que residem os dados, a inteligência e os diferenciais de informação da organização. Devem ser protegidos a todo custo. Nesse sentido, proteções físicas — implementadas para proteger os dispositivos em si —, bem como proteções lógicas — implementadas para proteger as informações e os dados contidos nos dispositivos — são fundamentais para que a organização se mantenha com chances de sucesso em suas ações.

Ao tentar ajudar o empresário Gilberto, você buscou, identificou e ajudou a resolver ataques de SQL Injection no ambiente de TI. Contudo, apenas algumas semanas depois, você foi chamado de volta, pois, apesar de não haver evidência de novos ataques de SQL Injection, a imobiliária rival X@X2 continua recebendo informações confidenciais da R#R2 (empresa). Você está desconfiado de que um ataque não tecnológico possa acontecer: o ataque de engenharia social. Que passos podem ser realizados para identificar e prevenir esse tipo de ataque no ambiente de TI da R#R2?

O objetivo desta seção é fornecer ao aluno elementos que lhe permitam entender aspectos fundamentais da proteção e do controle de acesso a servidores de bancos de dados e a recursos estratégicos, para a organização.

Os conteúdos a serem vistos nesta seção, que o auxiliarão a resolver a situação-problema, são os seguintes:

- Engenharia social;
- Aumento não autorizado de privilégios de acesso;
- Controle de acesso físico;
- Compartilhamento de senhas.

Vamos, então, acompanhar mais este caso.

Não pode faltar

Nem todos os ataques a ambientes informatizados utilizam a tecnologia como ferramenta. Alguns deles se utilizam de um elemento bem mais passível de violação, por ser muito mais complexo, e de controle muito mais difícil: o ser humano. Muitos dos problemas de segurança que enfrentamos "desde sempre" se devem à incapacidade de o indivíduo agir corretamente no quesito segurança, nas situações que enfrenta em seu dia a dia.

Veremos, a seguir, alguns desses ataques, voltados a violar a segurança de servidores e de ambientes de TI em geral.

Engenharia social

Segundo Watson, Mason e Ackroyd (2014), a expressão "engenharia social" tem muitas definições, dependendo do campo de estudo a que nos referimos. Uma das definições mais clássicas mencionadas pelos autores é: "a aplicação de princípios sociológicos a problemas sociais específicos" (WATSON; MASON; ACKYORD, 2012, p. 2). Essa definição exemplifica como devemos olhar para a expressão sob os olhos da segurança da informação.

Uma definição dos autores que se aproxima um pouco mais dos interesses da Segurança da Informação é: "a arte de se intencionalmente manipular o comportamento, utilizando-se para tanto, de mecanismos de comunicação especificamente construídos para este fim" (WATSON; MASON; ACKROYD, 2014, p. 2.). Com essa definição, já conseguimos vislumbrar o que a engenharia social usa como ferramenta no campo da segurança: a manipulação do comportamento do indivíduo. Alguns exemplos desse tipo de manipulação:

• O vendedor explica as características de um produto e em seguida pergunta: "quantos você quer comprar?" Ao invés de perguntar se o cliente potencial tem interesse em efetuar a compra, o vendedor assume que sim e já tenta induzi-lo a pensar não mais no se quer comprar, mas sim em quantos quer comprar;

• O consultor, tentando marcar uma reunião presencial com o cliente potencial pergunta: "segunda-feira às 14 horas para você está bom ou você tem preferência por outro horário?" Ao invés de perguntar se o cliente potencial está disponível para uma reunião, o consultor assume que sim e tenta impor um dia e uma hora, dando a opção explícita de o cliente mudar apenas a hora;

• O amigo, tentando influenciar alguém sobre uma opinião política qualquer pergunta: "concorda comigo que Fulano de Tal, ao ter cometido tal ação, não merece o nosso voto?" Aqui, temos várias tentativas de manipulação, começando pelo

"concorda comigo?", uma vez que nosso senso de empatia nos facilita dizer "sim". Temos também a afirmação de que Fulano de tal cometeu a ação, que pode não ser um fato, mas uma opinião pessoal. Por fim, a tentativa de manipulação para a ação a ser tomada, com a negação do voto, nesse caso.

Assimile

A engenharia social é uma estratégia de ataque que não depende de tecnologia, mas sim da exploração de vulnerabilidades psicológicas inerentes à natureza humana.

Todos esses são exemplos clássicos de tentativa de manipulação, e, segundo os autores, técnicas como essas têm um grau de eficiência comprovada muito maior do que gostaríamos que tivessem.

Ainda que a definição acima seja mais próxima, ela é genérica demais, no sentido de que se aplica a qualquer tipo de tentativa de manipulação. Para se aproximar ainda mais do que é a engenharia social quando aplicada à segurança da informação, Watson, Mason e Ackroyd (2014, p. 3) oferecem ainda outra definição, desta vez do SANS Institute: "engenharia social é a 'arte' de se utilizar o comportamento humano para se violar a segurança, sem que o participante (ou vítima) sequer perceba que foi manipulado". Ou seja, a engenharia social é um tipo de ataque que se alicerça não nas vulnerabilidades da tecnologia, mas sim nas vulnerabilidades da natureza humana.

Por que somos tão suscetíveis a ataques de engenharia social? A resposta está em nossa natureza. Metvivier (2016) aponta 5 características comuns na psique humana que facilitam a ação dos engenheiros sociais:

1. Respeito à autoridade – Tendemos a respeitar aquilo que se apresenta como oficial, uma vez que a suposta posição oficial confere autoridade a quem a detém.

Exemplo: Um indivíduo que se apresenta por telefone como sendo da área de suporte da empresa, fazendo testes em seu ambiente, e que, entre outras informações aparentemente inócuas, solicita sua senha.

2. Busca por oportunidades de gratificação – Estamos sempre em busca de oportunidade de ganhos, por exemplo: estando atentos a descontos em produtos e serviços de nosso interesse. O engenheiro social usa essa característica em seu favor, por exemplo: quando afirma que haverá alguma chance de ganho pessoal caso a vítima realize alguma ação.

Exemplo: Muitos golpes de *phishing* (coleta de informações sigilosas com falsas premissas) se apoiam em falsas promessas de produtos a baixos preços ou mesmo de graça. A vítima preenche o formulário, dá suas informações e não recebe nada em troca a não ser mais um golpe em seu futuro.

3. Dever moral – Em muitas situações, nosso senso moral nos impele a agir desta ou daquela forma, e o engenheiro social abusa dessa característica.

Exemplo: Em muitos casos, tragédias ou acontecimentos de alcance nacional elevam nosso senso moral, e somos compelidos a ajudar. Engenheiros sociais, sabendo dessa determinação pessoal que é comum em muitos de nós, criam falsas instituições de apoio e caridade, arrecadando fundos e mantimentos para supostamente auxiliar os necessitados, ficando com as doações para si.

4. Culpa – Os engenheiros sociais muitas vezes abusam de nosso senso de culpa por situações sociais inaceitáveis, e a taxa de sucesso é alta nesses casos.

Exemplo: Casos de falsa mendicância, por exemplo, são comuns e mostram como o engenheiro social (e um falso mendigo nada mais é que um engenheiro social) abusa de nosso senso de culpa.

5. Desejo de agradar – Subliminarmente, estamos sempre em busca de autoestima, e uma maneira de aumentarmos nossa percepção de autoestima é agradando a quem nos pede um favor. Os engenheiros sociais estão bastante cientes dessa fraqueza.

Exemplo: O engenheiro social, buscando acesso a um prédio para o qual não tem autorização, chega com os braços cheios de pacotes e espera na porta, por alguém que lhe faça a "gentileza" de abrir a porta.

Os casos são inúmeros, mas as ferramentas para combater a engenharia social são poucas e — desde que bem utilizadas — efetivas. Kevin Mitnick, o engenheiro social que se transformou em consultor de segurança (depois de ser capturado pelo FBI e de ter passado cinco anos na prisão), mostra que são simples as soluções (BARWICK, 2015):

• **Treinamento** – esse é o controle mais efetivo contra engenharia social. Os colaboradores de uma organização devem ser constantemente treinados a identificar potenciais situações de engenharia social, sendo instruídos sobre como agir em cada caso;

• **Controle de tráfego de saída** – os firewalls anti-malwares e sistemas de detecção de intrusos são excelentes para identificar tentativas de entrada de dados e processos não autorizados. Contudo, esses mesmos elementos são notoriamente falhos em identificar tráfego de saída, ou seja, tráfego gerado quando algum elemento já penetrou o ambiente. A engenharia social visa, em muitos casos, a inserção destes elementos no ambiente, sobrepujando as barreiras cibernéticas. É fundamental que o tráfego de saída seja tão examinado e avaliado quanto o tráfego de entrada;

• **Testes constantes de senhas** – senhas fracas são facilmente quebradas por mecanismos de força bruta. Os administradores devem ser os primeiros a saber se há senhas fracas de acesso em seu ambiente, pois, quando descobrem estas senhas, exigem que os usuários as alterem. Caso as mesmas senhas fracas sejam descobertas

por cyber-bandidos, eles não agirão com o mesmo senso de responsabilidade;

• **Testes de penetração por meio de engenharia social** – os administradores do ambiente podem também executar ataques simulados de engenharia social para averiguar o quanto seus colaboradores são suscetíveis a cair em ataques semelhantes. Mais uma vez, é prudente que as vulnerabilidades sejam identificadas pelos administradores, pois, se existirem e forem identificadas pelos cyber-bandidos, estes não agirão com os interesses da organização em mente;

• **Adoção de identificação biométrica eficiente** – senhas são violáveis e *tokens* (dispositivos de identificação, tais como crachás magnéticos) são passíveis de roubo. Mas características biométricas não são transferíveis, pois são únicas para cada indivíduo. Devem ser adotadas sempre que possível.

Exemplificando

Kevin Mitnick, o mais bem-sucedido engenheiro social dos anos 1980 e 1990, abusava do respeito que nutrimos pela autoridade: em mais de uma ocasião ele se apresentou como parte do time de segurança da empresa, em uma tarefa de coletar os crachás dos funcionários (inclusive dos guardas de segurança), como parte de um processo para troca destas identidades, prometendo que as novas viriam mais tarde.

O vídeo relatando exatamente esse ocorrido está disponível em: <https://www.cnet.com/news/social-engineering-101-mitnick-and-other-hackers-show-how-its-done/>. Acesso em: 22 fev. 2017.

Aumento não autorizado de privilégios de acesso

Um dos principais alvos dos engenheiros sociais é, uma vez ganhando acesso a um sistema qualquer, aumentar seus privilégios de acesso com vistas ao roubo de informações, ou também com vistas a ganhar, a partir desse primeiro sistema comprometido, acesso a outros sistemas do ambiente. Segundo Watson, Mason e Ackroyd (2014, p. 23): "quanto maiores os privilégios designados a um usuário, maior o risco que este usuário representa ao negócio". Uma interpretação dessa afirmação implica que o alvo preferencial para um ataque seria o usuário de maior privilégio, mas, como alertam os autores, esse usuário também seria alvo de maior preparo e maior treinamento contra-ataques aos seus recursos e conhecimentos. Os autores alertam para uma estratégia mais efetiva: o ataque a indivíduos com menor acesso, seguido de ações para aumentar os privilégios indevidamente, os chamados ataques de escalada de privilégios.

Rouse (2010) afirma que há dois tipos de ataques de escalada de privilégios, sendo que é da alçada dos responsáveis pela segurança do ambiente evitar e combater ambos:

• **Ataques verticais de escalada de privilégios** – o atacante aumenta seus próprios privilégios, ganhando privilégios mais sensíveis. Geralmente, esses privilégios aumentados são obtidos por meio de ataques aos sistemas de TI da empresa, em especial ao software de controle de privilégios ou ao banco de dados;

• **Ataques horizontais de escalada de privilégios** – o atacante tem um conjunto de privilégios e consegue os mesmos privilégios, mas para um usuário diferente (consegue acesso à conta de outro usuário). Este ataque é, no mais das vezes, perpetrado com técnicas de engenharia social.

Controle de acesso físico

O controle de acesso físico a uma organização — e em especial aos servidores do parque de TI dessa organização — é fundamental para se evitar perda de informações e de equipamentos.

Segundo Marcondes (2016, p. 1), "controle de acesso físico é qualquer aplicação de procedimentos e/ou equipamentos com o objetivo de administrar o acesso físico de pessoas, veículos e materiais a uma determinada área delimitada". O objetivo é gerar mais segurança para o ambiente físico, livrando-o de presenças não autorizadas.

As atividades a serem executadas por um sistema de controle de acesso físico são (MARCONDES, 2016):

• Delimitar a área onde há restrição de acesso;

• Barrar o acesso não autorizado de qualquer entidade;

• Liberar o acesso autorizado de qualquer entidade;

• Checar as permissões de acesso de uma entidade qualquer antes de garantir-lhe ou barrar-lhe o acesso;

• Relatar e registrar todas as tentativas de acesso, sejam elas autorizadas ou não autorizadas;

• Gerar relatórios de acesso quando solicitados.

Um sistema de controle de acesso deve ser composto por (MARCONDES, 2016):

1. Pelo menos uma barreira de acesso perimetral (muro ou cerca).

2. Um ponto de acesso à barreira perimetral supervisionado (por pessoal ou equipamento).

3. Tantas barreiras físicas de acesso interno quanto se façam -se para assegurar

pontos específicos do ambiente (paredes, salas-cofre).

4. Pontos de acesso controlados a cada um dos ambientes (portas, catracas, confinamentos etc.).

5. Sistema formal de identificação, preferencialmente baseado em dois níveis (crachá com foto e senha, ou crachá com foto e biometria, por exemplo), com registro em base de dados.

6. Sistema de monitoração por vídeo nos pontos de acesso, com registro em mídia permanente.

7. Política de acesso físico (parte da política de segurança da organização), versando sobre como deve ser efetivado o controle de acesso aos recursos da organização.

Por fim, um sistema de controle de acesso físico deve ter as seguintes características, impreterivelmente (MARCONDES, 2016):

• **Velocidade** – para ambientes de alta circulação, até mesmo alguns segundos por usuário podem gerar filas indesejáveis e afetar a produtividade, portanto o sistema deve ser rápido (sem prejuízo para a precisão, obviamente);

• **Baixo custo de operação e manutenção** – idealmente, um sistema deve conter o máximo de automatização possível, uma vez que a automatização reduz custos (os custos de pessoal são sempre o maior ofensor operacional);

• **Integração** – capacidade de se integrar com outros recursos informatizados da empresa, como no caso do sistema de ponto ou outros sistemas de controle de acesso em vigência na organização;

• **Controle por perfis de usuário** – o sistema deve facilitar a administração por meio de perfis de acesso, que simplificam o controle de acesso dos funcionários, dividindo-os em perfis específicos;

• **Impede duplicidade de direção** – quem entrou é impedido de "entrar" novamente, e quem saiu é impedido de "sair" novamente, com tentativas de duplicidade registradas pelo sistema;

• **Rastreabilidade** – registro de todos os eventos (bem-sucedidos ou não), armazenamento de todas as informações e geração de relatórios técnicos e gerenciais.

Reflita

Faria sentido contar com um aparato de última geração de controle de acesso físico sem que esse fosse alicerçado sobre uma robusta política de segurança? Quais seriam os efeitos indesejados (se é que haveria algum)?

Compartilhamento de senhas

Nenhuma boa política de segurança (e falaremos especificamente sobre elas na próxima seção) pode ser considerada abrangente se não tiver uma porção específica sobre o tratamento de senhas. E esse tratamento só é completo se há uma instrução específica alertando contra (ou ainda melhor: proibindo explicitamente) o compartilhamento de senhas.

Hüntermann (2013) nos fala sobre pesquisa da McAfee feita no Brasil, coletando dados sobre os resultados prejudiciais de casos pessoais de compartilhamento de senhas. Segundo a pesquisa comentada pelo autor, temos que as ações de parceiros (amigos, pares amorosos, cônjuges) que têm acesso à senha dos smartphones e sites de redes sociais dos parceiros, em muitas situações, levam a problemas. Nesses casos, os parceiros que se sentem prejudicados pelo que veem nos dispositivos e contas de seus pares muitas vezes optam por expor os dados pessoais desses pares, gerando transtornos enormes. Os motivos alegados para essas ações de exposição, segundo a pesquisa da McAfee, são (HÜNTERMANN, 2013):

1. Mentira (48%).

2. Traição (39%).

3. Publicação de foto inapropriada (33%).

4. Término de relacionamento (15%).

5. Cancelamento de casamento (13%).

6. Outros (13%).

Não é difícil entender porque o compartilhamento de senhas pessoais é problemático. Há outras razões para não compartilharmos senhas, expostas na mesma pesquisa da McAfee, sendo que a principal delas é o chamado "roubo de identidade". Segundo a pesquisa, os dados potencialmente mais danosos compartilhados — e que deveriam ser privativos de seus donos — são (HÜNTERMANN, 2013):

1. Conteúdo do celular (59%).

2. Contas de e-mail (58%).

3. Senhas (39%).

4. Números de contas bancárias não conjuntas (35%).

5. Códigos de seguro de saúde (31%).

Na cartilha de segurança para a Internet, publicada pelo Cert.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança), há uma análise bastante

coerente e importante sobre os possíveis problemas que podem surgir a partir do compartilhamento de senhas. O que um usuário que tenha sua senha pode fazer e (CERT, 2012):

- Acessar a conta de e-mail e ler e-mails, enviar e-mails no nome do dono da conta, passando-se por ele (ou mesmo SPAM em nome do dono da conta), enviar mensagens de *phishing* e outros tipos de códigos maliciosos, usar a lista de contatos para fins pessoais sem autorização, trocar senhas de outras contas cadastradas no endereço de e-mail, conseguindo acesso a elas e evitando que o dono de direito as acesse daí para frente;

- Acessar o computador e assim ter acesso a informações privativas ali armazenadas, como números de documentos e cartões de crédito ali armazenados;

- Usar o computador como ponte para ataques a outros sistemas e computadores na Internet;

- Usar a conta para realizar operações não autorizadas e potencialmente danosas para o dono das informações;

- Acessar redes sociais e se passar pela pessoa, obtendo informações sensíveis dos amigos e abusando da confiança destes.

O compartilhamento de senhas dificulta a identificação do gerador de uma ação, mas não dever ser empecilho para atribuição de responsabilidade, uma vez que o responsável deve ser sempre o dono do recurso. Se a conta pertence a "A", e "A" compartilha suas credenciais com "B", se algo sair errado o responsável deve ser "A", pois não deveria ter compartilhado as credenciais, em primeiro lugar.

A permissão de acesso a uma conta só deve ocorrer na presença do dono da conta, sem que este revele a senha à pessoa que vai fazer o uso. E, ainda assim, com a combinação expressa do que vai ser feito, acordada de antemão, e com a anuência do dono da conta, e somente nos casos explicitamente permitidos pela política de segurança da instituição (se a politica de segurança não especificar este item, deve-se assumir que não é permitido em situação alguma). Qualquer desvio desse tipo de procedimento põe os dados em risco.

Pesquise mais

Tomé, Fabri, Cunha e Zem-Lopes (2013) realizaram um excelente trabalho arregimentando e discutindo informações acerca do estado da técnica em controle de acesso físico empresarial. Vale a pena estudar mais a fundo o artigo por eles produzido.

TOMÉ, M. et al. Controle de Acesso Físico nas Empresas. FATEC,

Monografia de Conclusão de Curso, publicado em 2013. Disponível em: <http://www.fatecguaratingueta.edu.br/fateclog/artigos/Artigo_63.pdf>. Acesso em: 22 fev. 2017.

Sem medo de errar

Para ajudar o empresário Gilberto e descobrir se a Imobiliária R#R2 está sendo vítima de ataques de engenharia social, você deverá executar um plano com vários passos. O ideal é que a avaliação ocorra em várias frentes, a saber:

1. Realizar uma detalhada varredura no ambiente de TI da R#R2, bem como nos equipamentos de funcionários que se conectem a esse ambiente, em busca de malware que tenha sido instalado como resultado de algum ataque de engenharia social.

2. Fazer um backup do arquivo de senhas, demandar que todos os funcionários troquem suas senhas por senhas fortes, e, em seguida, realizar um teste no arquivo de senhas com vistas a identificar senhas fracas. Caso alguma seja encontrada, informar aos funcionários e reforçar a instrução para a adoção de senhas fortes.

3. Realizar um teste de penetração ao longo de algumas semanas, usando apenas técnicas de engenharia social, com o objetivo de identificar vulnerabilidades e suscetibilidades a esse tipo de ataque.

4. Realizar um treinamento formal contra engenharia social, envolvendo obrigatoriamente todos os funcionários da R#R2 e estendendo opcionalmente o treinamento a seus cônjuges (uma vez que esses cônjuges também podem ser alvo de ações de engenharia social).

5. Adotar medidas formais na política de segurança da empresa para evitar ataques futuros de engenharia social.

Dessa forma, Gilberto não só poderá identificar ataques que tenham ocorrido ou estejam ocorrendo, mas também poderá impedir que novos ataques baseados em técnicas de engenharia social venham a ser perpetrados no futuro.

Avançando na prática

Melhorando a segurança de um galpão

Descrição da situação-problema

Robsom é dono de um depósito que é alugado como entreposto para produtos hortifrutigranjeiros. Ele acaba de procurar você e sua empresa de segurança física em

função de uma necessidade inusitada: como seu galpão fica em um ponto estratégico, próximo ao aeroporto e à beira de uma via de acesso à capital do Estado, ele foi procurado pela DY, uma fábrica de computadores que está entrando no mercado brasileiro. A DY está em busca de parcerias para armazenagem dos computadores que traz ao Brasil, antes que esses equipamentos sejam distribuídos para as lojas e redes de revenda. Robsom foi procurado pelos executivos da empresa, pois estão interessados em um contrato de longo prazo.

Ocorre que os executivos da DY têm exigências quanto à segurança física do local de armazenamento, e, para tanto, Robsom terá que apresentar um plano para adequação do local. Quando armazenava apenas produtos hortifrutigranjeiros, a "segurança" do local era feita pela cerca e por seus cachorros da raça rottweiler, o que é insuficiente para a DY.

Como você pode ajudar Robsom? Como é sua sugestão para uma solução de segurança física para o local? Os investimentos, se aceitos, serão divididos com a DY, o que facilitará bem as coisas para Robsom. O que ele não pode é perder o contrato.

Resolução da situação-problema

Um bom projeto de segurança física deve contar com a adequação da cerca, inclusive com a instalação de câmeras e cerca elétrica em todo o perímetro. A cerca em si não impede a passagem de uma pessoa determinada e de posse de um bom alicate, mas em conjunto com as câmeras, evita que alguém por aí tente passar.

A cerca deve ser aberta apenas em uma entrada principal, que deve contar com a presença de um guarda em período integral, e também de portões com região de confinamento (dois portões, com o veículo ficando em uma região intermediária com um porão atrás e outro à frente).

Outra medida importante é a adequação das paredes do depósito, bem como das portas de entrada e saída, que devem ser resguardadas e equipadas com sensores e câmeras.

Todas as portas desobstruídas devem ter acesso com autenticação em dois níveis; sugere-se o uso de crachá e reconhecimento de íris. Os equipamentos para esse tipo de identificação são facilmente integráveis a sistemas de controle de acesso.

O sistema deve contar com duplicidade de base de dados (uma das cópias deve ficar fora do ambiente), com a capacidade de gerar relatórios e avisar os responsáveis por meio de SMS em caso de tentativas de violação.

Faça valer a pena

1. Os servidores de uma organização são o ponto mais delicado da estrutura de TI. É ali que residem os dados, a inteligência e os diferenciais de informação da organização. Devem ser protegidos a todo custo. Nesse sentido, proteções físicas — implementadas para proteger os dispositivos em si —, bem como proteções lógicas — implementadas para proteger os dados e as informações contidas nos dispositivos — são fundamentais para que a organização se mantenha com chances de sucesso em suas ações.

Podemos afirmar que a engenharia social é um tipo de ataque que se baseia em que tipo de vulnerabilidades?

a) Vulnerabilidades inerentes à engenharia.

b) Vulnerabilidades inerentes à natureza humana.

c) Vulnerabilidades inerentes às redes de computadores.

d) Vulnerabilidades inerentes aos servidores.

e) Vulnerabilidades inerentes aos desktops e smartphones.

2. Segundo Watson, Mason e Ackroyd (2014, p. 23): "quanto maiores os privilégios designados a um usuário, maior o risco que este usuário representa ao negócio". Uma interpretação dessa afirmação implica que o alvo preferencial para um ataque seria o usuário de maior privilégio, mas, como alertam os autores, esse usuário também seria alvo de maior preparo e maior treinamento contra ataques aos seus recursos e conhecimentos. Os autores alertam para uma estratégia mais efetiva: o ataque a indivíduos com menor acesso, seguido de ações para aumentar os privilégios indevidamente, o chamado _____ _____

Qual o nome do ataque que mais adequadamente completa o raciocínio expresso no parágrafo acima?

a) Ataque de negação de serviços.

b) Ataque de violação de privacidade.

c) Ataque de engenharia social.

d) Ataque de escalada de privilégios.

e) Ataque de remoção de privilégios.

3. Segundo nos informa Marcondes (2016, p. 1), "controle de acesso físico é qualquer aplicação de procedimentos e/ou equipamentos com o objetivo de administrar o acesso físico de pessoas, veículos e materiais a

uma determinada área delimitada".

Segundo o que aprendemos sobre controle de acesso físico, qual o objetivo das medidas nesse sentido? Assinale a alternativa que melhor e mais amplamente descreve esse objetivo:

a) Proteger a rede contra acesso não autorizados.

b) Proteger os servidores.

c) Proteger o prédio contra deteriorações e desastres provocados pelos elementos ou pelo homem.

d) Assegurar as informações contra malware e ataques de negação de serviço.

e) Gerar mais segurança para o ambiente físico, livrando-o de presenças não autorizadas.

Seção 4.3

Políticas de segurança para bancos de dados

Diálogo aberto

Nesta nossa última seção, vamos entender como funcionam e para que servem as políticas de segurança. Mas será mesmo que o assunto é importante?

Vejamos. Tente responder às seguintes perguntas: se um estranho te aborda no ônibus e diz: "oi, minha senha para entrar no meu webmail é 'Juquinha', qual é a sua?", você retribui a gentileza? Se você recebe um e-mail dizendo "clique aqui para ganhar mil reais", você clica? Se você acha um pendrive de 64GB próximo à entrada de sua casa, e nesse pendrive está escrito "coleção de filmes do Oscar", você coloca o pendrive diretamente em seu computador?

Se você respondeu "não" para as três questões, você já tem alguma noção do que é e da importância de uma política de segurança. Se responder "sim" para alguma delas, você precisa urgentemente entender o que é uma política de segurança e adotá-la para si.

Agora que você "limpou" o ambiente da Imobiliária R#R2, eliminando os vazamentos que teimavam em levar os imóveis anunciados na empresa para a Imobiliária X@X2, sua concorrente direta, você tem mais um desafio. O empresário Gilberto não quer mais passar pela desagradável situação de ver seus dados sendo comprometidos e pede sua ajuda mais uma vez. Ele pergunta que ferramentas de segurança deve adotar em seu parque tecnológico para resolver de vez a situação, mas você sabe que não é nas ferramentas, mas sim nos processos que se encontram as respostas. Você deve agora falar a Gilberto sobre as melhores práticas na gestão de segurança de bancos de dados e ajudá-lo a adotar uma política formal de segurança. Como explicar a ele o que são e para que servem as melhores práticas? Como auxiliá-lo a criar uma política de segurança que proteja seu ambiente, mas não seja restritiva aos negócios?

Nesta última seção, veremos os seguintes conteúdos: melhores práticas em segurança de bancos de dados, políticas de acesso físico, políticas de acesso ao servidor de bancos de dados e, por fim, políticas de acesso aos bancos de dados.

Espero que você tenha aproveitado os conteúdos dessa disciplina vistos até aqui, e que aproveite mais os dessa última seção. Espero também que esses conteúdos venham a ser bastantes úteis em sua caminhada profissional. Até a próxima!

Não pode faltar

Imagine um hospital com os melhores equipamentos, as melhores tecnologias, com tudo "de ponta". Imagine, porém, que nesse hospital os médicos e enfermeiros — todos capacitados — não tivessem uma forma coordenada de trabalhar. Ou seja: todo mundo sabe muito sobre saúde, mas não se conversa e faz as coisas como acha que deve fazer. Você se animaria de procurar serviços de saúde em um hospital assim? Vejamos: os médicos aparecem quando querem, não há protocolos para os enfermeiros para a prestação de cuidados, os medicamentos são passados aos cuidadores quando conveniente, as salas de cirurgia são ocupadas por quem chegar primeiro e assim por diante.

Por mais que os equipamentos sejam de primeira linha, e que os profissionais sejam bem capacitados, parece que falta alguma coisa, não é verdade?

E o que falta?

Falta processo. Falta um conjunto de procedimentos que coordene todas as ações. Sem esse conjunto de procedimentos — ou seja, sem esse processo — esse hospital estaria fadado ao fracasso, certamente. É disso que trataremos nos itens a seguir, e nosso assunto principal é a segurança de bancos de dados.

Melhores práticas em segurança de bancos de dados

Em que pese a tecnologia da informação, no caso mais geral, fazer parte das ciências exatas, sempre haverá questões de natureza humana a ser tratadas, o que certamente muda a forma como resolvemos certos problemas. A partir daí, já não podemos mais tratar o assunto com exatidão. Isso porque o elemento humano adiciona um componente notória e obviamente não exato, nem sempre lógico, nem sempre coerente, nem sempre consistente. Um componente humano muda todo o panorama (e o próprio nome já diz tudo).

Quando adicionamos o componente humano a uma situação qualquer, deixamos de ter um conjunto exato de regras de operação, pois o elemento humano não é exato. Nash e Ehrenfeld (1997) afirmam que, nesses casos, a adoção de melhores práticas é a forma mais adequada de condução da situação em questão. Melhores práticas são métodos ou técnicas que são amplamente usados e empiricamente aceitos como superiores, por gerarem melhores resultados que os outros métodos

ou técnicas. A consolidação de melhores práticas pode gerar padrões acreditados de gestão, como nos casos da ISO 9000 e da ISO 14001 (NASH; EHRENFELD, 1997).

Reflita

O que ocorreria se insistíssemos em reger um sistema em que o componente humano tem papel preponderante com regras determinísticas rígidas, ao invés de por meio de melhores práticas? Seria possível obtermos sucesso?

No que concerne às melhores práticas de segurança de bancos de dados, Lowans, Reed e Meunier (2015), em um artigo de recomendações do Gartner Group — grupo de consultoria de alta credibilidade no campo da tecnologia da informação — apontam para nove melhores práticas, a saber:

1. **Política de segurança** – a organização deve adotar procedimentos formais para identificar dados sensíveis, gerenciar usuários e privilégios, monitorar e gerenciar os padrões de uso dos dados, gerenciar mudanças, entre outras tarefas.

Recomendações – definir uma política de segurança que tenha na proteção das informações seu centro, e alinhar essa política de segurança à política de governança do negócio. Definir formalmente configurações, regras de acesso físico, e lógico e segregação de funções, bem como o fluxo de comunicação e de requisitos para toda a operação.

2. **Descoberta e classificação de dados** – dados devem ser identificados e delimitados e, uma vez feito isso, devem ser classificados de acordo com sua sensibilidade (ou seu valor) para a organização.

Recomendações – implantar processos e ferramentas para a identificação e delimitação automática de dados, bem como (no tocante ao processo) para sua importação nos bancos de dados da organização. Adotar um procedimento formal de classificação dos dados (públicos, confidenciais e ultra confidenciais, por exemplo) e adotar mecanismos de proteção e controle de acesso a estes, de acordo com sua classificação.

3. **Avaliação de usuários e permissões** – a inclusão de usuários e atribuição de privilégios é função específica de um sistema de gerenciamento de bancos de dados.

Recomendações – estes processos de inclusão de usuários e atribuição de privilégios devem ser realizados de acordo com parâmetros formais valendo para toda a organização, seguindo regras específicas e auditáveis, integrados com sistemas de gestão de recursos humanos.

4. **Monitoração e auditoria de usuários privilegiados** – usuários privilegiados

são aqueles que têm acesso direto ao SGBD sem precisar acessar os dados por meio de aplicações. São especiais porque podem atuar diretamente sobre o sistema, uma capacidade que, se for malversada, pode trazer prejuízos irreparáveis para a organização.

Recomendações – os usuários privilegiados devem ser monitorados individualmente e em tempo real, com alertas sendo gerados também em tempo real, em caso de atividades suspeitas. Nesses casos, o sistema de alerta deve estar integrado com outros sistemas de segurança do ambiente, permitindo ações em tempo real tanto por parte dos sistemas de segurança quanto por parte dos operadores.

5. **Monitoração e auditoria de usuários de aplicações** – usuários de aplicações são aqueles que têm acesso ao sistema por meio das aplicações, que por obrigação têm autorização para acessar os bancos de dados e supostamente já controlam o que o usuário pode e o que ele não pode fazer. Ocorre que, como os ataques de SQL Injection vistos na Seção 4.1 nos mostram, não é sempre que ese controle funciona.

Recomendações – sempre utilizar os recursos disponíveis no sistema para identificar qual usuário final realiza quais ações no sistema por meio de aplicações. De posse dessa afirmação, traçar perfis de uso para cada usuário e monitorar, identificando e averiguando eventuais desvios.

6. **Relatórios, análise e coleta de eventos** – a coleta de eventos é uma das capacidades mais comuns em sistemas de todas as naturezas, e não é diferente no caso dos SGBDs. Ações realizadas no sistema e/ou pelo sistema podem ser facilmente registradas e consultadas pelos administradores.

Recomendações – o Gartner recomenda que os sistemas de coleta e análise de *logs* sejam integrados e alimentem um sistema global de monitoração, pois eventos que isoladamente não significam nada, quando combinados a outros eventos em outras partes do ambiente, podem mostrar a ocorrência de ataques.

7. **Gerenciamento de vulnerabilidades e configurações** – a varredura, o mapeamento e a catalogação de vulnerabilidades são processos que permitem a identificação de problemas potenciais no ambiente antes que eles se tornem problemas reais.

Recomendações – este processo deve ocorrer continuamente no sistema, com atualização constante da base de conhecimentos. Os responsáveis pela segurança devem também participar de comunidades voltadas para a monitoração de vulnerabilidades, pois a inteligência coletiva gerada por essas comunidades é altamente valiosa para a organização (e daí que no mais das vezes vêm os alertas mais adiantados sobre vulnerabilidades).

8. **Prevenção e bloqueio de ataques** – processos, pessoas e ferramentas dedicados a identificar, bloquear e prevenir ataques ao sistema de bancos de dados em particular

e ao ambiente de TI em geral.

Recomendações – os administradores devem se certificar de que as partes componentes deste aparato estão sempre em pleno funcionamento: processo, pessoas e equipamento. Isso se obtém por meio de testes periódicos no próprio ambiente, criados para avaliar a efetividade de todo o conjunto.

9. **Criptografia, tokenização e mascaramento de dados** – o uso de técnicas de ofuscação de dados (criptografia), o uso de dispositivos externos para identificação de usuários autorizados (tokenização) e o uso de técnicas para "disfarçar" dados e porções sensíveis do sistema (mascaramento) são mandatórios em um sistema de bancos de dados, pois visam protegê-los contra olhares externos não autorizados.

Recomendações – utilizar ferramentas de ofuscação tanto para dados em comunicação quanto para dados em repouso, sem exceção. Considerar as técnicas mais robustas, pois, mesmo que consumam mais recursos, são recomendáveis. Isso porque o crescimento do poder de processamento e da banda passante de dados em comunicação é suficiente para lidar com o overhead gerado, sem prejuízo para o desempenho do sistema.

Essas melhores práticas são válidas para bancos de dados sendo utilizados em quaisquer tipos de organização, como reforçam Lowans, Reed e Meunier (2015).

Assimile

As melhores práticas em segurança podem ser refinadas, nada impedindo que melhorem com o passar do tempo, uma vez que são regras empíricas. O ciclo PDCA (discutido mais à frente), por exemplo, auxilia nessa melhoria contínua, com o passar do tempo, como mostra o esquema a seguir:

Figura 4.2 | Ciclo PDCA de melhoria contínua

Fonte: <https://www.salpinx.com.br/wp-content/uploads/2016/04/Ciclo_PDCA-som.png>. Acesso em: 22 fev. 2017.

Políticas de acesso físico

Ao descrever os procedimentos que devem constar em políticas de segurança, com o objetivo de que a organização esteja conforme os requisitos de várias normas vigentes, Williams (2013) menciona que o acesso físico é focado por várias normas e padrões. As normas e padrões de indústria que requerem conformidade física (no tocante à tecnologia da informação, claro), são (WILLIAMS, 2013):

- ISO/IEC 27001;
- NIST 800-53;
- HIPAA Standard;
- PCI DSS 2,0;
- AUP V5.0.

Os pontos de conformidade da segurança física a serem implementados pelas organizações que visam certificação de segurança com base nas normas acima são 18 no total, dos quais podemos citar os cinco principais (WILLIAMS, 2013):

- Descrição dos procedimentos formais que a organização desenvolveu para facilitar a implementação de controle de proteção física e ambiental;
- Descrição dos procedimentos em vigor que desempenhem auditorias periódicas de conformidade da solução de segurança física da organização;
- Descrição do uso de perímetros e/ou segurança física para proteção de áreas que contenham repositórios ou equipamentos de processamento de informações;
- Descrição dos controles existentes para aprovação, registro e supervisão de visitantes aos locais físicos da organização;
- Descrição do uso de identificação visível para funcionários, prestadores de serviços, terceiros e visitantes.

Outros pontos importantes para a certificação de segurança física tratam de:

- Medidas para prevenção de acidentes e recuperação de desastres (fogo, inundação etc.);
- Medidas de controle de acesso a recursos de TI, tais como servidores e elementos de comunicação (roteadores, modems, linhas internas e externas);
- Medidas de monitoração de movimentações físicas (pelos locais da organização) e lógicas (pelos sistemas da organização).

Exemplificando

Exemplos de medidas para prevenção de acidentes e recuperação de desastres:

- Planejamento de evacuação dos locais em caso de emergência;
- Estabelecimento de uma CIPA, com responsáveis pela prevenção de acidentes e ação em caso de acidentes;
- Estabelecimento de brigada de incêndio;
- Estabelecimento de procedimentos de backup periódico;
- Implantação de um backup site, contendo equipamentos e sistemas sobressalentes para funcionamento em regime emergencial.

A certificação em uma ou mais das normas mencionadas acima garante às demais organizações (clientes, parceiros e fornecedores) que a organização certificada adota e mantém processos rígidos de controle de acesso físico, o que é uma evidência de que dados e informações ali são tratados com a seriedade que merecem. Órgãos governamentais, para citar apenas o exemplo mais óbvio, pontuam empresas que concorrem a contratos por eles publicados em concorrências públicas, com base na conformidade com normas e padrões, facilitando que as empresas certificadas vençam essas concorrências.

Políticas de acesso ao servidor de bancos de dados

Para Denezis et al. (2014), o ponto central da segurança é manter a privacidade e proteger os dados considerados de valor, garantindo que as três dimensões da segurança (confidencialidade, integridade e disponibilidade) sejam mantidas. Para os autores, a preocupação com proteção deve começar junto com o levantamento de requisitos dos sistemas em si. Nesse sentido, quando uma organização busca atender uma necessidade de negócios por meio de um sistema informatizado, a fase de levantamento de requisitos deve, por obrigação, conter uma sessão dedicada à segurança, com questões detalhadas e específicas que tragam à tona todos os requisitos para assegurar dados e equipamentos.

Esse enfoque, ou seja, a inclusão dos requisitos de segurança já na fase de planejamento e design dos sistemas, é efetivo e tende a economizar custos e dores de cabeça quando comparados a estratégias que incluem a segurança dos sistemas em fases mais adiantadas do projeto (DENEZIS et al. 2014).

São oito as estratégias para a inclusão de requisitos de segurança no design de um sistema (DENEZIS et al. 2014):

1. **Minimizar** – a quantidade de dados sendo processados e armazenados deve ser mantida em um mínimo absolutamente necessário. Os dados devem ser selecionados antes de serem coletados, isto é, devemos raciocinar sobre o que deverá ser armazenado e processado antes de iniciar o processo de coleta de dados.

2. **Esconder** – tanto os dados quanto as relações entre os dados (que geram as informações) devem ser escondidos das vistas públicas, estando acessíveis apenas aos que de fato têm necessidades legítimas. A criptografia tem um papel preponderante nesta estratégia, obviamente, e o cuidado físico com o resguardo dos servidores, também.

3. **Separar** – os dados e as informações devem ser separados física e logicamente, em compartimentos que reflitam sua utilidade e seu valor para a organização. A segregação lógica dos dados e sistemas, bem como a segregação física dos servidores, são fatores fundamentais neste caso.

4. **Agregar** – em que pese parecer contraditória com a estratégia "separar", a estratégia "agregar" visa dificultar a identificação de dados e informações individuais, sugerindo que o processamento ocorra de forma simultânea para o máximo de dados possível. Esta estratégia adiciona um componente de anonimidade ao processamento que auxilia na manutenção da confidencialidade.

5. **Informar** – é fundamental para a manutenção da segurança de um ambiente que tudo o que ocorre no ambiente seja registrado e relatado. Essas informações devem estar à disposição dos administradores do ambiente o tempo todo, e o usuário também tem direito de saber o que ocorre com seus dados, podendo escolher se aceita os rumos dados pela organização ou se decidirá removê-los e utilizar serviços de outros provedores.

6. **Controlar** – os administradores devem ter controle total — tanto lógico quanto físico — sobre todo o ambiente, o tempo todo.

7. **Fazer cumprir** (tradução livre do termo em inglês *enforce*) – todas as normas de segurança adotadas pela organização devem ser cumpridas, e quem tem a obrigação de fazê-las cumprir (e que, portanto, deve ter as ferramentas necessárias para que de fato possa fazê-las cumprir) são os responsáveis pela administração do ambiente.

8. **Demonstrar** – os administradores do ambiente devem ser capazes de demonstrar os controles de segurança, bem como a conformidade do ambiente com as normas e padrões adotados pela organização. Dessa forma, o ambiente é passível de auditoria e certificação, trazendo tranquilidade a todos os *stakeholders* (parceiros, clientes e fornecedores) que, de alguma forma, dependem da segurança do ambiente.

As estratégias de números 2, 3 e 6 são diretamente pertinentes ao controle de acesso aos servidores de bancos de dados, tanto físico quanto lógico, ou seja, os

servidores devem ser:

• **Escondidos** – armazenados em locais especiais para tanto, longe dos olhos e do acesso público, tanto do ponto de vista físico quanto lógico. Do lado físico, devem ser assegurados, instalados em sala-cofre com climatização especial (17 °C), estrutura de combate a incêndios e monitoração por circuito interno de TV 24 horas por dia;

• **Separados** – os dados devem ser separados dos demais recursos da organização, e sugere-se, inclusive, o estabelecimento de uma DMZ (segmento de rede do tipo "zona desmilitarizada", criada por um segmento separado de um *firewall*) especial em que apenas os servidores estejam instalados, sendo controlados por conjuntos especiais de regras de acesso no *firewall*;

• **Controlados** – os servidores devem ser controlados em 100% do tempo, sendo supervisionados por meio de coletas de *logs*, que devem ser automaticamente analisados por sistemas de detecção e prevenção de ataques, bem como por *firewalls* de aplicação que identifiquem todas as requisições de transação, cuidando para que apenas as requisições legítimas sejam atendidas. As precauções costumeiras de supervisão lógica, tais como *anti-malware* e autenticação segura de acesso também deverão estar sempre (100% do tempo que o servidor estiver em serviço) ativas.

Dessa forma, os servidores terão maior chance de se manterem seguros, evitando problemas dessa natureza para a organização.

Políticas de acesso aos bancos de dados

Segundo Cardoso e Moraes (2008), a política de acesso ao banco de dados deve ser implantada de acordo com os princípios do ciclo PDCA (*Plan, Do, Check, Act*), postulados por Deming, e que direcionam as principais normas internacionais, incluindo a ISO 27001, de Segurança da Informação — o campo em que a segurança de bancos de dados se insere. Os quatro passos do PDCA, aplicados à política de acesso de bancos de dados, são (CARDOSO; MORAES, 2008):

• **Planejar (*Plan*)** – por meio de uma análise de riscos, identificar os recursos físicos (servidores) e lógicos (dados e sistemas) a serem protegidos, bem como os mecanismos necessários ao controle de acesso;

• **Realizar (*Do*)** – aplicar os mecanismos definidos para a proteção;

• **Verificar (*Check*)** – monitorar os recursos, os usos (e tentativas) e coletar todas as informações disponíveis, avaliando a efetividades dos mecanismos de proteção e o desempenho do ambiente como um todo;

• **Agir (Act)** – com base nas análises, tomar as devidas ações tanto para reforçar a

segurança do ambiente quanto para melhorar, tanto quanto possível, o desempenho geral do sistema (este segundo intento deve ser secundário à segurança, obviamente).

O PDCA deve ser encarado como um ciclo, isto é, terminados os ajustes da etapa "Agir", é necessário recomeçar com nova etapa "Planejar", garantindo assim os benefícios da melhoria contínua do processo. Sempre haverá melhorias por fazer, e sempre a aplicação do ciclo trará benefícios.

Cardoso e Moraes (2008) sugerem, ainda, uma estrutura para a política de controle de acessos aos bancos de dados, a saber:

• **Declaração** – declaração de comprometimento da direção da organização para com a política de controle de acesso aos bancos de dados, investindo a equipe de segurança da autoridade necessária para definir, implementar, controlar e garantir a aplicação desta política;

• **Definição** – escopo da política e metas a serem atingidas por esta política de controle de acesso aos bancos de dados;

• **Conformidade com a legislação** – quais leis e/ou princípios regulatórios regem os controles adotados;

• **Estrutura dos controles** – definições dos controles físicos e lógicos para controle de acesso aos bancos de dados;

• **Definição de responsabilidades** – define quem são os responsáveis por cada ativo físico e lógico do ambiente, bem como pelo cumprimento dos procedimentos adotados;

• **Gestão de continuidade de negócios** – estratégias e procedimentos para minimizar interrupções na disponibilidade dos sistemas de bancos de dados;

• **Treinamento** – plano de treinamento em segurança da informação em geral e nos pontos da política em particular;

• **Consequências das violações** – estabelece o conjunto de medidas autorizadas pela direção da organização a serem tomadas em caso de violações por parte dos colaboradores, incluindo acionamentos legais;

• **Referências** – apresenta os documentos utilizados como referências para a construção da política.

Os autores informam, ainda, que a política de controle de acesso aos bancos de dados deve ser congruente com a política de segurança da organização, e sua construção deve ser coordenada com a construção daquela.

Pesquise mais

Conheça mais sobre o controle de acesso em sistemas gerenciadores de bancos de dados nesta monografia, a qual versa em detalhes sobre o assunto. Em especial, no capítulo 3, das páginas 19 até 32, o assunto é tratado de forma simples, direta e bastante instrutiva.

SANTOS, D. Controle de Acesso em Sistemas Gerenciadores de Banco de Dados, Monografia. 50 fls. Universidade Tecnológica Federal do Paraná, Curitiba, 2014. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3588/1/CT_GESER_V_2014_1.pdf>. Acesso em: 22 fev. 2017.

Sem medo de errar

Você deve começar mostrando a Gilberto que a gestão de segurança, por ser uma tarefa que envolve pesadamente o elemento humano, deve seguir as melhores práticas de mercado. Não há uma "lei exata", uma bala de prata que resolva todos os problemas com 100% de certeza e de eficiência. Há, sim, aquelas ações que o mercado vem realizando e que dão certo, merecendo a atenção da R#R2.

E o que dizem as melhores práticas? Bem, a primeira coisa que dizem é que é necessário que a empresa adote, implemente e execute uma política de segurança. Essa política deve contemplar a segurança de toda e empresa, no âmbito geral, e se concentrar no que a R#R2 tem de maior diferencial competitivo: suas informações.

Para ajudar o empresário Gilberto a construir sua política de segurança de bancos de dados, você pode começar apresentando-lhe um formulário base de coleta de dados para criação de política, partindo então, daí, tanto para ajustar o formulário quanto para coletar as informações necessárias.

Um modelo possível de ser usado é o seguinte:

Figura 4.3 | Formulário de coleta de dados

Imobiliária R#R2 – Política de Segurança		
Responsável pelo documento		
Data de criação		
Data da última modificação		
Versão do documento		
Declaração de comprometimento		
Escopo da política de segurança de bancos de dados		
Controles	Responsáveis	Metas

Fonte: elaborada pelo autor.

O refinamento desse documento, inserindo ou modificando-o para refletir as necessidades da R#R2, bem como definindo os elementos da política e estabelecendo uma agenda para o treinamento, deverão colocar a R#R2 no caminho da segurança que a empresa tanto necessita.

Avançando na prática

Evitando novos desastres

Descrição da situação-problema

Gertrudes Galalante é uma consultora de sucesso que acaba de resolver um problema difícil: depois de um incêndio em seu escritório, ela perdeu todas as informações dos projetos dos clientes, tendo que passar meses buscando os dados em antigos e-mails e solicitando-os aos clientes. Recuperou muito do que precisava, mas não tudo: pelo menos 20% das informações se perderam em definitivo.

Gertrudes procurou você, pois, após criar um ambiente de banco de dados em que todas as informações estão armazenadas e organizadas, ela teme novas perdas. Dessa forma, solicitou um projeto para que esse tipo de perda não ocorra mais.

Como ajudar Gertrudes a preservar suas informações e suas operações em face à possibilidade de novos desastres?

Resolução da situação-problema

O ponto principal dessa questão é a continuidade de negócios, isto é, permitir que as operações da empresa de Gertrudes continuem, independentemente do que esteja acontecendo. Isso implica em dois focos de atuação:

• Prevenir problemas futuros;

• Garantir a continuidade de operações em caso de imprevistos.

Para atender às necessidades do primeiro foco de atuação, você poderá sugerir a Gertrudes:

1. Adotar um processo de backup periódico com armazenamento na nuvem do material copiado.

2. Implantar medidas de salvaguarda de equipamentos, como a instalação dos servidores em uma sala-cofre, a implantação de medidas de combate a incêndio, ou mesmo a mudança de local da empresa, caso esta esteja situada em região passível de alagamentos.

3. Implantação de medidas de salvaguarda de dados, tais como a segregação dos servidores em uma DMZ separada no *Firewall*, adoção de *firewall* de aplicações para proteger os sistemas e os bancos de dados; adotar soluções de *anti-malware* e estabelecer testes periódicos do ambiente para identificação de vulnerabilidades.

Para atender às necessidades do segundo foco de atuação, você poderá sugerir a Gertrudes:

1. Estabelecer um *backup site*, com equipamentos e sistemas rodando em paralelo, com duplicação automática dos dados, permitindo que as operações continuem de forma emergencial, mesmo diante da ocorrência de um desastre qualquer, até que o ambiente principal seja restabelecido.

2. Contratação de um seguro para o ambiente, caso a empresária ainda não o tenha feito.

3. Treinamento do pessoal da empresa para atuação antes, durante e depois da ocorrência de algum desastre (plano de evacuação, brigada de incêndio etc.).

Por fim, sugira a Gertrudes que adote e implemente uma política de segurança, que se faz necessária para a boa condução de seus negócios.

Faça valer a pena

1. Em que pese a tecnologia da informação, no caso mais geral, fazer parte das ciências exatas, sempre haverá questões de natureza humana a serem tratadas, o que certamente muda a forma como resolvemos certos problemas. A partir daí, já não podemos mais tratar o assunto com exatidão. Isso porque o elemento humano adiciona um componente notória e obviamente não exato, nem sempre lógico, nem sempre coerente, nem sempre consistente. Um componente *humano* muda todo o panorama (e o próprio nome já diz tudo).

Se o elemento humano adiciona um componente de incerteza que não mais permite que um sistema seja regido por regras exatas, o que devemos utilizar como ferramenta para tentar garantir o sucesso dos esforços de administração?

a) O instinto dos administradores.

b) A experiência dos gestores.

c) A consultoria especializada no assunto.

d) As melhores práticas disponíveis.

e) Os palpites dos curiosos.

2. Uma das estratégias de design de sistemas que incorpora a segurança especifica é a quantidade de dados sendo processados e armazenados deve ser mantida em um mínimo absolutamente necessário. Os dados devem ser selecionados antes de serem coletados, isto é, devemos raciocinar sobre o que deverá ser armazenado e processado antes de inicial o processo de coleta de dados.

De acordo com os preceitos que estabelecem a inclusão de aspectos de segurança já na fase de design de um sistema, qual é o nome da estratégia postulada acima?

a) Minimizar.

b) Esconder.

c) Separar.

d) Agregar.

e) Informar.

3. Segundo Cardoso e Moraes (2008), a política de acesso ao banco de dados deve ser implantada de acordo com os princípios _____, postulados por Deming, e que direcionam as principais normas internacionais, incluindo a ISO 27001, de Segurança

da Informação — o campo em que a segurança de bancos de dados se insere.

Assinale a alternativa que completa corretamente as lacunas da frase.

a) do Kanban.

b) do WYSIWYG (*What You See Is What You Get*).

c) da STO (*Security Through Obscurity*).

d) da PSC (Política da Segurança Corporativa).

e) do PDCA *(Plan, Do, Check, Act*).

Referências

BACIK, S. **Building an effective information security policy**. Boca Raton: CRC Press, 2008.

CARDOSO, G. B.; MORAES, R. Segurança em bancos de dado: aplicando normas e procedimentos. **Revista SQL Magazine**, n. 103, ago. 2008.

DENEZIS, G. et al. **Privacy and data protection by design – from policy to engineering**. Londres: ENISA, 2014.

LOWANS, B.; REED, B.; MEUNIER, M. Market guide for data-centric audit and protection. **Gartner Group**, 15 dez. 2015. Disponível em: <https://www.gartner.com/doc/reprints?id=1-2UJB88E&ct=151221&st=sb>. Acesso em: 22 fev. 2017.

NASH, J.; EHRENFELD, J. Codes of environmental management practice: assessing their potential as a tool for change. **Annual Review of Energy and the Environment,** v. 22, p. 487-535, 1997.

WILLIAMS, B. **Information security policy development for compliance**. Boca Raton: CRC Press, 2013.

Anotações

Anotações

Anotações

ISBN 978-85-8482-866-1