ABNT NBR ISO/IEC 17799:2005

Thiago Pelizoni

Rodrigo Z. Raminelli

André Terceiro

Emerson Navarro

Ricardo Beltrão

2012

Sumário

Resumo

Os atributos integridade, confiabilidade e disponibilidade são cruciais em um software com qualidade.

O objetivo principal da norma ISO 17799 é fornecer um conjunto de procedimentos afim de assegurar a segurança da informação, fazendo com que estes atributos possam ser alcançados.

Em julho de 2007, foi incorporada uma nova numeração, sendo atualizada para ISO 27002 [1].

Devido a característica meramente descritiva da norma, este artigo tem o intuito mostrar a qualidade de software, identificando através da norma como estes atributos podem ser implementados. Para isso, serão citados alguns serviços de computação na nuvem e de qual modo eles implementam estes atributos.

[1] ISO/IEC NBR 17799/2007 - 27002

Introdução

Dos vários atributos que um software de qualidade pode possuir, quando é necessário um nível de segurança da informação elevado, três deles se destacam:

1) Integridade: tem por principal objetivo controlar acesso ao software ou dados por pessoas não autorizadas. (1)

2) Confiabilidade: tem por principal objetivo realizar suas tarefas e manter seu funcionamento em circunstâncias rotineiras, bem como em circunstâncias hostis ou inesperadas (como por exemplo, sob um ataque).

3) Disponibilidade: tem como principal objetivo a resistência a falhas com a finalidade de manter-se disponível o maior tempo possível.

Atualmente vive-se na *"Era da Informação"*. Todos os dias há um bombardeio por uma quantidade de informação que muitas vezes não se é capaz de absorver. São redes sociais, sites de notícias em geral, mensageiros instantâneos [1], entre outras dezenas de coisas que demandam por uma segurança digital no que diz respeito ao fato de impedir um acesso não autorizado às informações sigilosas, seja a nível pessoal ou corporativo.

O uso de senhas tem sido a forma mais comum de controlar o acesso a informações privilegiadas, porém envolve dois fatores completamente diferentes: o tecnológico e o humano. Estes precisam conviver um com o outro e esta interação tem gerado inúmeros problemas. (2)

O uso de controle de acesso por níveis conhecido como ACL[2] consiste basicamente em uma lista que define qual usuário tem permissão para acessar algum determinado serviço. Isto permite ao servidor permitir ou negar acesso a uma determinada tarefa, tornando o acesso a este mais seguro.

Atualmente existem métodos mais seguros e eficazes para o controle de acesso, como por exemplo as assinaturas e certificados digitais, que consistem basicamente em utilizar criptografia assimétrica ou criptografia de chaves públicas. (3)

[1] Instant messenger

[2] Access Control List ou Lista de controle de acesso

Neste artigo será mostrado de maneira sucinta alguns procedimentos que relacionam-se à norma 17799, de modo a ser atingido um software com qualidade em termos de segurança da informação.

1 Segurança da informação

Sistemas computadorizados estão presentes em diversas atividades. Toda a economia mundial, por exemplo, é controlada por computadores. Portanto, faz-se necessário uma série de medidas para ser mantido o sigilo e a integridade que essas informações necessitam.

A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas. (4)

Independente do método com o qual a informação é armazenada ou compartilhada, faz-se necessário que ela seja protegida de maneira adequada.

A NBR ISO/IEC 17799:2005 define segurança da informação como sendo a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar seus riscos, maximizar seu retorno sobre os investimentos e as suas oportunidades. (5). Esta norma é dividida em 11 seções:

a) Política de Segurança da Informação;

b) Organizando a Segurança da Informação;

c) Gestão de Ativos;

d) Segurança em Recursos Humanos;

e) Segurança Física e do Ambiente;

f) Gestão das Operações e Comunicações;

g) Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;

h) Gestão de Incidentes de Segurança da Informação;

i) Gestão da Continuidade do Negócio;

j) Conformidade;

(6)

A segurança da informação é conseguida por intermédio de processos, políticas, procedimentos, estrutura organizacional, bem como pela utilização de softwares e hardwares.

Vale salientar que, uma gestão de negócio eficaz estabelece controles, monitoramento, além de uma análise de modo a garantir a segurança da informação.

1.1 Prejuízos

Com o advento da Internet, o acesso à informação foi facilitado, inclusive o não autorizado. Devido a uma política de segurança da informação mal implementada, corporações acabam tendo milhões ou até bilhões em prejuízo bem como, a perda de credibilidade no mercado. Softwares cujos quesitos de qualidade como integridade e confiabilidade não foram atendidos de maneira correta podem contribuir para isto.

Ocorreram alguns incidentes notórios recentes com relação a este assunto, sendo exemplificados abaixo.

PSN

[1]

Em 2010, a Playstation Network teve sua rede invadida por um grupo de hackers mundialmente conhecido, os ”Anonymous”, onde os dados de seus usuários como contas de email, senhas e números de cartões de crédito foram vazados, causando um prejuízo a empresa de aproximadamente US$ 24 bilhões (R$ 37,7 bilhões). (7)

HSBC

Em 2008, o banco HSBC perdeu um disco rígido contendo com dados de 370 mil clientes da instituição. O disco não era criptografado, porém dispunha de proteção por senha, nada que não possa ser quebrado.

Em um comunicado oficial, o banco informou que os dados incluem nomes, níveis de cobertura de seguro de vida, datas de aniversário e quais clientes eram fumantes, ou não. Não

[1] Playstation Network

haveria nada que pudesse comprometer os clientes e também não existiriam razões para supor que o disco pudesse ter caído em mãos erradas. (8)

Visa e Mastercard

Em 2010, o grupo Anonymous, através de ataques DDoS (Distributed Denial-of-Service) deixaram indisponível o sistema da Mastercard e posteriormente derrubam o site da Visa.

Os pagamentos feitos por usuários da empresa de cartões de crédito foram prejudicados.

O ataque foi realizado como uma forma de protesto pró-Wikileaks, quando esta teve suas doações bloqueadas pelas operadoras supracitadas.(9)

2 *Por onde começar?*

Primeiramente faz-se necessário um levantamento de requisitos de segurança da informação, de modo que possam ser identificados por meio de uma análise sistemática os possíveis riscos envolvidos.

Os gastos envolvidos decorrentes de falhas na segurança da informação, como nos exemplos anteriores (PSN, HSBC, Visa e Mastercard), devem ser controlados e balanceados.

A análise tem a função de direcionar e determinar quais ações gerencias são apropriadas, bem como quais as prioridades para o gerenciamento de riscos quanto à segurança da informação, onde devem ser implementados controles de modo a mitigar tais riscos.

Esta análise deve ser repetida periodicamente com intuito de identificar outros riscos decorrentes de mudanças.

Identificado os riscos e levantados os requisitos necessários, convém que seja adotada uma política adequada, de modo que os riscos sejam reduzidos a um nível aceitável.

A norma 17799 visa com suas práticas atender tais necessidades, utilizando-se das melhores práticas de segurança da informação. Convém ressaltar que a segurança da informação também depende de decisões organizacionais que, são baseadas em critérios de aceitação de riscos.

2.1 Um ponto de partida

Alguns dos controles estabelecidos na norma são considerados como princípios básicos de gestão da segurança da informação e podem ser aplicados na maioria das organizações.

Pode-se considerar como um bom ponto de partida para a implementação de segurança da informação um determinado número de controles baseados em requisitos legais e práticas de segurança da informação normalmente utilizadas.

Os controles considerados essenciais para uma organização, sob o ponto de vista legal,

incluem, dependendo da legislação aplicável:

a) Proteção de dados e privacidade de informações pessoais;

b) Proteção de registros organizacionais;

c) Direitos de propriedade intelectual;

Os controles considerados práticas para a segurança da informação incluem:

a) Documento da política de segurança da informação;

b) Atribuição de responsabilidades para a segurança da informação;

c) Conscientização, educação e treinamento em segurança da informação;

d) Processamento correto nas aplicações;

e) Gestão de vulnerabilidades técnicas;

f) Gestão da continuidade do negócio;

g) Gestão de incidentes de segurança da informação e melhorias;

(10)

3 *Estudo de caso*

A computação na nuvem[1] tem proporcionado que o acesso às informações de maneira descentralizada, ou seja, através de um computador, um tablet, um smartphone ou outro dispositivo com acesso a internet, uma pessoa pode ter acesso aos seus dados independente do local em que estiver acessando.

Desta forma, serão abordados alguns serviços disponíveis atualmente em computação na nuvem, como por exemplo: Google[2], Microsoft[3] e Facebook. Nestes casos, os atributos confiabilidade, integridade e disponibilidade são preponderantes.

[1] Cloud computing
[2] GDrive, GMail, Google Plus, Youtube
[3] SkyDrive, Hotmail e Outlook.com

4 *Proteção de dados e privacidade de informações pessoais*

De acordo com a norma, o item referente a esta sessão menciona:

”Convém que uma política de privacidade e proteção de dados da organização seja desenvolvida e implementada. Convém que esta política seja comunicada a todas as pessoas envolvidas no processamento de informações pessoais.”

”Convém que a responsabilidade pelo tratamento das informações pessoais e a garantia da conscientização dos princípios de proteção dos dados sejam tratadas de acordo com as legislações e regulamentações relevantes.”(11)

A maneira com que as empresas supracitadas implementam este item é observada por características comum entre si. São elas:

a) Existe um termo de uso circunstancial que deve ser aceito quanto ao serviço, contendo regras de utilização e segurança. Muitas vezes este termo não é lido pelos usuários;

b) Os usuários destes serviços são informados quanto a questões de segurança no uso de senhas, como não informá-la a estranhos, mantê-la em local seguro, bem como alterá-la periodicamente;

c) O dispositivo ao qual estão sendo acessadas tais informações tem que ser confiável.

5 *Identificação e autenticação de usuário*

”Convém que todos os usuários tenham um identificador único (ID de usuário) para uso pessoal e exclusivo, e convém que uma técnica adequada de autenticação seja escolhida para validar a identidade alegada por um usuário.”

”Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade.”(12)

É comum atualmente, ao efetuar um cadastro em algum serviço de internet, este possuir uma verificação de complexidade de senha. Isto se deve a muitos usuários utilizarem senhas como ”123456”, ”asdqwe”, datas de nascimento, placas de carro etc. Por este motivo, estes serviços verificam a senha digitada, mostrando um status (fraca, media, forte). Contam também com a opção de expiração de senha para um determinado período, forçando o usuário a cadastrar uma nova senha.

O Google possui uma funcionalidade chamada ”autenticação em dois passos”(13). Esta autenticação, ou verificação em duas etapas, é um recurso que adiciona uma camada extra de segurança à conta do usuário no Google. Com ele, além do nome de usuário e senha, para ter acesso à conta o usuário é obrigado a inserir um código de segurança que será enviado para seu celular (que deve ser previamente cadastrado).

Com essa funcionalidade, caso alguém roube ou adivinhe a senha de um usuário, só consigará autenticar na conta se tiver em mãos o aparelho celular cujo número está cadastrado. Isto opcionalmente pode ser configurado para execução apenas uma vez a cada 30 dias.(14).

O Facebook por sua vez possui a funcionalidade de um cadastro de confiabilidade para o dispositivo ao qual a autenticação foi efetuada, onde, a cada novo dispositivo detectado, um novo cadastro deve ser efetuado.

A Microsoft possui a mesma funcionalidade, porém isto ocorre sem intervenção do usuário, ou seja, de maneira automática. Desta forma, é possível fazer com que o computador costumei-

ramente utilizado seja confiável para uma recuperação de senha, inibindo assim os famosos ataques de recuperação de senha. Nestes ataques, sabendo um pouco da vida do usuário e respondendo perguntas muitas vezes óbvias, é possível alterar a senha e ter acesso a todas suas informações.

6 *Monitoramento*

Um sistema deve ser monitorado para que atividades não autorizadas quanto ao processamento da informação possam ser detectadas e as devidas ações possam ser tomadas.

Quando a este item, de acordo com a norma, temos:

”Convém que os sistemas sejam monitorados e eventos de segurança da informação sejam registrados.”

”Convém que registros[1] de operador e registros de falhas sejam utilizados para assegurar que os problemas de sistemas de informação são identificados.”

”Convém que as organizações estejam de acordo com todos os requisitos legais relevantes aplicáveis para suas atividades de registro e monitoramento.”

”Convém que o monitoramento do sistema seja utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso.”

Dentre as atividades referentes a esta questão que são visíveis ao usuário, um exemplo é o serviço de e-mail do Google, o Gmail, que possui a funcionalidade de exibir quando foi o último acesso, qual o endereço IP deste acesso, se este recurso, em um dado momento, está sendo acessado de outro local e qual o endereço IP deste local.

6.1 Coleta de evidências

”Nos casos em que uma ação de acompanhamento contra uma pessoa ou organização, após um incidente de segurança da informação, envolver uma ação legal (civil ou criminal), convém que evidências sejam coletadas,armazenadas e apresentadas em conformidade com as normas de armazenamento de evidências da jurisdição(ões) pertinente(s).”(15)

O Google conta com um algoritmo que analisa os acessos a sua conta, obtendo a localidade através de Geo IP. É verificado se houve algum acesso indevido através da diferença das

[1] Log

localidades, por exemplo:

Caso um usuário acesse sua conta em São Paulo, com endereço IP 201.83.226.211, e sua conta seja (ou tenha sido) acessada pelo endereço 8.12.4.8, em Kansas (Estados Unidos), o Google irá alertar este ocorrido, informando que a senha deve ser alterada, pois alguém pode ter conseguido suas credenciais e estar acessando sua conta sem autorização.

Este recurso é extremamente útil a um usuário, para monitorar quem, quando e onde acessou sua conta de maneira indevida. Caso ocorra alguma ação judicial, isto pode ser utilizado como prova de acesso indevido.

Conclusão

A segurança da informação é um fator essencial para se obter qualidade em muitos softwares e serviços. A norma ISO 17799:2005 é muito rica em informação sobre o que deve ser implementado para se obter uma boa política de segurança da informação, mas não aborda rigidamente como esta implementação deve ser feita. O objetivo deste artigo foi relacionar alguns recursos de segurança empregados nos principais serviços de computação na nuvem utilizados atualmente a tópicos abordados pela norma.

Fica evidente a predominância do fator humano para o sucesso desta implementação, onde, não haveria um resultado satisfatório em, por exemplo, obrigar um usuário a criar uma senha forte que por sua vez, devido sua complexidade, seria armazenaria em papel, podendo ser acessível a pessoas não autorizadas.

Sendo assim, pode-se concluir que, por mais que haja normas tais como a ISO 17799:2005, não existe um sistema totalmente seguro e ”impenetrável”. Todavia, a implementação das boas práticas nela descritas conseguem dificultar quaisquer possíveis ameaças ao bem mais valioso de uma corporação, suas informações.

Referências Bibliográficas

1 PRESSMAN, R. S. *Engenharia de Software Uma Abordagem Profissional*. [S.l.: s.n.], 2011. 362 p.

2 SILVA, D. R. P. da. Segurança da informação: uma reflexão sobre o componente humano. 2007. Disponível em: <http://www.cienciasecognicao.org/pdf/v10/m346130.pdf>.

3 MENKE, F. Assinaturas digitais, certificados digitais, infra-estrutura de chaves públicas brasileira e a icp alemã. 2001. Disponível em: <http://egov.ufsc.br/portal/sites/default/files/anexos/4375-4369-1-PB.pdf>.

4 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005.

5 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 9 p.

6 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 4 p.

7 IG. Prejuízo da sony com invasão da psn pode passar de r$ 37 bilhões. 2011. Disponível em: <http://economia.ig.com.br/prejuizo-da-sony-com-invasao-da-psn-pode-passar-de-r-37-bilhoes/n1300108338602.html>.

8 IDGNOW. Hsbc perde dados de 370 mil clientes. 2008. Disponível em: <http://idgnow.uol.com.br/seguranca/2008/04/07/hsbc-perde-dados-de-370-mil-clientes/>.

9 G1. Após ataque a mastercard, hackers pró-wikileaks derrubam site da visa. 2010. Disponível em: <http://g1.globo.com/tecnologia/noticia/2010/12/ataque-hacker-em-defesa-wikileaks-afeta-pagamentos-com-mastercard.html>.

10 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 11 p.

11 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 110 p.

12 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 77 p.

13 GOOGLE. As senhas e os códigos usados na verificação em duas etapas. Disponível em: <http://support.google.com/accounts/bin/answer.py?hl=pt-BR&answer=1070457&topic=1099588&ctx=topic>.

14 TECHTUDO. Por que a autenticação em dois passos é importante e como habilitá-la. 2012. Disponível em: <http://www.techtudo.com.br/artigos/noticia/2012/08/por-que-a-autenticacao-em-dois-passos-e-importante-e-como-habilita-la.html>.

15 ABNT. *ABNT NBR ISO/IEC 17799*. Rio de Janeiro - RJ: [s.n.], 2005. 102 p.