ESTUDO DE CASO: PRINCIPAIS PILARES DA SEGURANÇA DA INFORMAÇÃO NAS ORGANIZAÇÕES

MATEUS MICAEL COUTINHO, ROBSON NUNES DOS SANTOS, VITOR HENRIQUE DA SILVA CUSTODIO, ELIANE CRISTINA AMARAL, ELINEY SABINO, NARUMI ABE

Resumo

Este artigo apresenta um estudo de caso sobre a Segurança da Informação em uma empresa de pequeno porte, onde foram analisados a existência de uma Política de Segurança e os princípios básicos (Confidencialidade, Integridade e Disponibilidade) da Segurança da Informação implementados na organização. As informações foram coletadas através de entrevista no local e questionário aplicado ao Sócio e Gestor de Tecnologia da Informação da empresa. A Informação é muito importante e deve ser tratada como principal ativo de uma empresa que deseja se manter em um alto nível de competição no mercado. Seja uma empresa de pequeno, médio ou grande porte, todas têm informações sigilosas, que se forem perdidas ou roubadas, podem comprometer as atividades da empresa, como suas operações e funcionamento. Com o avanço da tecnologia e o aumento do uso dessas tecnologias nas empresas, a preocupação com os riscos na Segurança das Informações tem se tornado maior por parte de muitos empresários, embora muitos dos empresários ainda não dão muita importância para a Segurança das Informações e não tratam a informação como um dos principais patrimônios da empresa, e não calculam as consequências da perda ou roubo das mesmas. As análises feitas no estudo de caso deste artigo, apresentam avaliações em conformidade com a norma ABNT NBR ISO/IEC 27002:2005, onde são exibidos os problemas encontrados na empresa, e por fim, apresenta sugestões elaboradas para os pontos problemáticos encontrados.

Palavras-chaves: Tecnologia da Informação, Confidencialidade, Integridade, Disponibilidade, Tecnologia, Segurança da Informação, Política de Segurança

Abstract

This article presents a case study on Information Security in a small company, where it was analyzed the existence of Security Policy and basic principles (Confidentiality, Integrity and

Availability) of Information Security implemented in the organization. As information was collected through on-site interview and questionnaire applied to the Partner and Information Technology Manager of the company. Information is very important and should be treated as the main asset of a company in which it is in conformity with a level of competition in the market. Whether it is a small business, something or large, all sensitive information, which can be lost or stolen, can compromise as company activities, such as its operations and operation. With the advancement of technology and the increased use of technologies in companies, a concern about the risks in Information Security on the issue made greater by many entrepreneurs, although many of the entrepreneurs are still not important to Information Security and not Treat information as one of the principal assets of the company, and is not calculated as a consequence of the loss or theft of your subtitles. The analyzes made in the case study of this article are evaluated in accordance with the ISO / IEC 27002: 2005 standard, where the problems encountered in the company are presented, and finally, it presents elaborated suggestions for the problem points encountered.

Keywords: Information Technology, Confidentiality, Integrity, Availability, Technology, Information Security, Security Policy

Introdução

A Segurança da Informação é um assunto que deve estar sempre presente em todas as organizações que desejam manter informações protegidas. As informações são um dos bens mais importantes das organizações. Ao mesmo tempo, essas informações estão sempre sob risco. A perda ou vazamento de informações podem acarretar em grandes prejuízos para as organizações. Na atual era digital, a segurança da informação tem sido preocupante para as empresas, pois informações relevantes que antigamente eram guardadas dentro de gavetas, hoje estão guardadas em ambientes virtuais.

Este artigo tem como objetivo identificar possíveis falhas que envolvam os três principais pilares da Segurança da Informação com a análise de um estudo de caso feito a partir de uma entrevista com uma empresa do setor de comércio varejista da cidade de Registro, interior de São Paulo.

A fim de identificar as principais falhas de segurança de dados e informações, com os dados obtidos através de entrevista, procuramos citar algumas soluções envolvendo os três principais pilares da segurança da informação. Tendo em vista as falhas apresentadas, o trabalho alerta aos profissionais de tecnologia da informação e gestores de empresas aos fatores de riscos sobre a perda e vazamento de informações. Com tudo isso o artigo tem como objetivo conscientizar para que se possa melhorar o cenário atual do nível de segurança das informações nas empresas

A maioria das empresas de pequeno e médio porte no Brasil, não se preocupam com a Segurança da Informação, pois os gestores acham que suas empresas não são tão importantes para serem alvo de criminosos. Com isso adotaram-se as seguintes questões:

- A empresa possui uma política de informação?

- A empresa aplica a segurança básica das informações?

A justificativa desse artigo vem da necessidade e da importância de analisar se estão implementados os princípios básicos da Segurança da Informação pelo grande valor que as informações possuem dentro de uma empresa.

Este artigo contribui para uma conscientização da importância da Segurança da Informação na empresa estudada, que antes não considerava muito importante a informação e não via a informação como o principal ativo da empresa.

Ambiente de Segurança da Informação

A informação está presente em todo nosso cotidiano, para VANCIM (2016), seja no ambiente pessoal ou profissional. No contexto profissional, mais especificamente em organizações as informações são de extrema importância e tem impacto direto nas tomadas de decisões.

Atualmente, as informações representam o bem de maior valor para as organizações. A evolução da tecnologia da informação e das redes de comunicação exibe um novo cenário. A maioria dessas informações estão hoje informatizadas, possuindo formas diferentes de objetos reais, porém, tendo o mesmo valor de objetos reais e, em diversos casos, tendo um valor maior. Por isso, a informação é um assunto muito importante, pois atinge todos os indivíduos e os negócios de uma organização.

> A informação possui um ciclo de vida. Ela nasce com a produção, tem um tempo de vida útil, na qual é manuseada, utilizada interna e externamente, transportada por diversos meios, armazenada, e morre com a sua destruição (DANTAS, 2011, p.19).

As vulnerabilidades das informações são pontos frágeis, que DANTAS (2011), podem ser explorados por uma ou diversas ameaças que podem ocasionar danos.

As vulnerabilidades podem estar presentes em diversos lugares, como por exemplo: instalações físicas desprotegidas contra inundações, incêndios e outros desastres naturais; falta de políticas de segurança; falta de controles de acessos e utilização de materiais da empresa; equipamentos sem restrição para sua utilização.

Para DANTAS (2011), a política da segurança da informação são objetivos documentados e transformados em valores, princípios e requisitos para se obter um padrão de proteção para as informações. Seguindo essa linha de raciocínio, pode-se definir a política de segurança da informação como: um documento que determina princípios, valores, compromissos e requisitos para a segurança da informação.

A elaboração do escopo da segurança da informação está relacionada com as atividades da organização e do nível de segurança que se pretende obter. As normas elaboradas na política de segurança devem ser comunicadas a todos os funcionários da organização, de forma relevante, acessível e de fácil compreensão. A política de segurança, conforme SILVA, CARVALHO e TORRES (2003), é

um conjunto de regras elaboradas que definem o que é considerado pela organização como aceitável ou inaceitável, envolvendo as medidas a impor aos infratores.

A informação é um bem muito importante para as organizações. Antigamente FONTES (2008), todas informações críticas de uma empresa eram armazenadas em papéis dentro de gavetas sem muita segurança. Atualmente a maioria das informações independentemente do nível de tecnológico, devem ser de relevância preocupação dos empresários.

A segurança da informação tem o objetivo de estabelecer técnicas para disfunções não técnicas dentro das organizações. De acordo com Moreira e Cordeiro (2002), pode-se gastar muito tempo, dinheiro e esforço em segurança de informações, porém sempre ocorrerá problemas de perda de dados ou interrupções de suas atividades de forma acidental, devido a bugs de software, mau uso, hackers, entre outros motivos.

Segundo VANCIM (2016), todo processo dentro de uma organização requer informação. A comunicação é necessária para que as informações trafeguem de forma segura entre responsáveis por essas tarefas. Essas informações são um dos ativos mais importantes e fundamentais nos processos organizacionais. Sendo assim é possível afirmar que as informações são muito importantes para um bom resultado das negociações.

A Segurança da Informação, para DANTAS (2011), abrange ações para proteger informações contra ameaças, com a intuito de garantir a continuação das atividades de uma organização. Esse conceito para a segurança da informação é estabelecido pela norma ISO/IEC 27002:2005, que diz que deve haver preservação da confidencialidade, da integridade e da disponibilidade da informação.

A segurança da informação FONTES (2008), foi criada para que organizações operem as informações essenciais para as atividades estratégicas, táticas e operacionais de maneira confiável.

Segurança da informação, conforme BEAL (2005), tem como objetivo proteger as informações de ameaças a confidencialidade, integridade e disponibilidade.

> A segurança da informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (NBR ISSO/IEC 27002:2005) (DANTAS, 2011, p.11)

O Processo da segurança da informação, para FONTES (2008), nas organizações deve considerar as informações que envolvam ou não tecnologia. As informações no ambiente, nos papéis e nas mentes dos indivíduos devem ser considerados no processo de segurança da informação.

> A informação é o elemento fundamental para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor, podendo levar a organização do sucesso ao fracasso, em função de impactos financeiros, operacionais ou de imagem, ocasionados por falhas, erros ou fraudes no uso da informação (FONTES, 2011, p. 2)

A administração da uma empresa e os funcionários envolvidos, de acordo com SILVA, CARVALHO e TORRES (2003), são os proprietários das informações usadas na organização no relacionamento com os clientes e na comercialização de seus bens. É ela que define o que será feito e o que ocasionará reflexões na segurança, como a utilização dessas informações pelos utilizadores.

A informação deve garantir três requisitos fundamentais, segundo DANTAS (2011), são eles: a confidencialidade, a integridade e a disponibilidade, requisitos estes, que devem ser mantidos, pois são os princípios da segurança da informação.

A conservação da confidencialidade, integridade e disponibilidade de informações utilizadas nos sistemas de informações, conforme SILVA, CARVALHO e TORRES (2003), exigem medidas de segurança, que são utilizadas também para garantir a autenticidade e a irretratabilidade.

Todas as medidas utilizadas, independente do objetivo, precisam ser colocadas em prática antes da efetivação dos riscos. Tais medidas podem ser classificadas de acordo com os tipos de riscos, em duas categorias: proteção e prevenção.

A prevenção tem como objetivo as medidas que buscam conter as ameaças existentes. Essas medidas acabam quando uma ameaça passa a ser um incidente.

Segundo SILVA, CARVALHO e TORRES (2003), a proteção tem como objetivo as medidas que visam implantar um sistema de informação, com requisitos de inspecionar e detectar as ameaças para reduzir o impacto causado quando essas se efetivam:

- Confidencialidade: Atualmente a competitividade das empresas estão nas informações que elas detêm. Para isso, existem métodos que garantem a confidencialidade das informações e que não impedem o acesso delas por pessoas autorizadas. Os requisitos de

confiabilidade são manipulados pelo nível das informações.

- Integridade: A integridade é um requisito vital para garantir os dados e informações processadas, transmitidas pelos sistemas de informação. O valor de uma informação está na fiabilidade. Qualquer alteração, por menor que seja, pode comprometer a integridade de um grande volume de dados e informações, assim podendo causar enormes prejuízos. Para isso são necessários sistemas de validação, que podem ser automáticos ou manuais, de acordo com o grau de importância das informações. Um exemplo, podem ser aplicados processos de revisão, por amostras, da integridade dos dados. A integridade é de suma importância para a recuperação de informações perdidas.

- Disponibilidade: O acesso a informação por pessoas permitidas é essencial para o prosseguimento das atividades da empresa. Obter a informação, mas não puder acessá-la no momento que se precisa dela, é igualmente a não ter nenhuma informação. As medidas de segurança dos dados e informações devem possuir aspectos que permitam o acesso aos mesmos no momento necessário. É muito importante empregar o acesso a informação juntamente com a conservação da confidencialidade da mesma. As formas de segurança utilizadas não poderão exibir os dados para o acesso por pessoas não autorizadas e não deverão restringir o acesso pelos permitidos.

Estudo de caso

Analisaremos através de um estudo de caso, conforme indicado por Gomes (2006), refere-se à investigação de situações envolvidas em um determinado ambiente. Diversos fatores são observados em busca de evidências que descrevam uma determinada situação.

Em uma entrevista realizada com um sócio e gestor de Tecnologia da Informação de uma empresa do setor de comércio varejista com aproximadamente 35 funcionários, da cidade de Registro/SP, na qual o nome não será citado nesse artigo por questões éticas. Sendo assim foi denominada como Empresa X para o uso nesse artigo para não serem expostas vulnerabilidades, informações confidenciais, entre outras informações sigilosas da organização.

Nessa entrevista, foram vistas as necessidades da implementação básica da segurança das informações na organização com base nas pesquisas citadas, neste artigo, para garantirem possivelmente mais segurança nas atividades da empresa e os objetivos do negócio.

O objetivo primordial, desse estudo de caso, é fazer uma análise da situação atual da segurança da informação em uma empresa do mundo real e identificar as ameaças e as vulnerabilidades relacionando os principais requisitos básicos da segurança da informação, segundo DANTAS (2011), são eles, a confidencialidade, a integridade e a disponibilidade das informações.

Na Empresa X, em seu âmbito, utiliza Tecnologia da Informação dentro da organização, onde possui dois servidores, um deles operando com o Sistema Operacional Windows Server 2003 e outro com Windows Server 2008, onde o servidor com Windows Server 2003 é utilizado para armazenamento de arquivos e o outro com Windows Server 2008 para rodar a aplicação do *Enterprise Resource Planning* (ERP), em português, Gestão Empresarial. A empresa também possui vinte e duas estações de trabalho.

No servidor de arquivos, os funcionários têm usuário e senha de acesso, porém a senha é padrão para todos os funcionários e todos possuem o mesmo acesso. O acesso ao servidor de aplicativos, onde todos os funcionários utilizam para acessar o sistema ERP, são necessários usuários e senhas de acesso, e nesse caso todos possuem o seu próprio.

Para acessos à internet, os funcionários não possuem nenhuma restrição nas estações de trabalho quanto ao uso e a quais endereços virtuais podem ou não podem ser acessados, e todos os funcionários utilizam a rede WIFI da empresa.

O uso da internet em horário de trabalho tem apenas proibição de cunho ético-moral, feito de maneira oral, ou seja, verbal, não estabelecendo regras escritas ou documentadas para os funcionários da instituição.

A rede possui um servidor firewall, Brazil Firewall (BFW), fazendo apenas o balanceamento entre duas conexões de internet, os servidores não possuem antivírus, apenas nas estações clientes é utilizado uma versão gratuita de antivírus. A Empresa X, no momento não possui nenhum plano de implantação de uma política de segurança das informações.

Essas informações foram fornecidas pelo sócio e gestor de TI, juntamente com as questões abaixo respondidas, que haviam sido aplicadas para que houvesse um melhor entendimento da situação da Empresa X.

Questionário:

1. Na empresa é utilizado Tecnologia da Informação para guardar informações?
(X) SIM ( ) NÃO

2. A empresa possui uma política de Segurança da Informação?
( ) SIM (X) NÃO

3. A empresa tem objetivo de implantar uma Política de Segurança das Informações?
( ) SIM (X) NÃO

4. A empresa protege as informações computadorizadas, contra acessos indevidos?
( ) SIM (X) NÃO

5. As informações da empresa estão sempre disponíveis quando o proprietário ou pessoas autorizadas ao acesso dessas informações necessitam?
(X) SIM ( ) NÃO

6. A empresa cuida da integridade das informações, possuindo algum controle para que as informações não sejam manipuladas indevidamente?
( ) SIM (X) NÃO

Análise do Estudo de Caso

De acordo, com os estudos apresentados neste artigo, a Empresa X apresenta um nível baixo de maturidade em relação a segurança das informações. A Empresa X não cuida de diversos riscos aos quais está exposta, ignorando a conservação da confidencialidade, integridade e disponibilidade das informações, conforme indicado por SILVA, CARVALHO e TORRES (2003) e DANTAS (2011), além de não existir preocupação por parte de todos os envolvidos nas atividades da empresa. Com a descrição do estudo de caso e as questões respondidas pela Empresa X relatados acima, foram destacados os seguintes problemas encontrados: ausência de política de segurança da informação

> Um estudo de caso é uma investigação empírica que:
> - Investiga um fenômeno contemporâneo dentro de seu contexto na vida real, especialmente quando os limites entre o fenômeno e o contexto não estão claramente definidos; (...)
> - Enfrenta uma situação tecnicamente única em que haverá muito mais variáveis de interesse do que pontos de dados, e, como resultado;
> - Baseia-se em várias fontes de evidências necessitando de uma triangulação para a convergência dos dados;
> - Beneficia-se do desenvolvimento de proposições teóricas prévias para conduzir a coleta e a análise dos dados. ” (YIN, 2001, pág. 32).

Para este problema sugere-se a criação de um documento estabelecendo políticas da segurança dentro da empresa, pois afirma SILVA, CARVALHO e TORRES (2003), que estes elementos formais definem os objetivos da organização em relação a segurança da informação, bem como as atitudes de empreender com vista a concretização dos mesmos:

- Falta de controle dos acessos aos arquivos na rede computadorizada

Como citado no estudo de caso, pode-se compreender que os arquivos armazenados no servidor de arquivos, podem ser acessados por todos os funcionários da empresa, existindo então a falta de proteção adequada aos arquivos e não garantindo a confidencialidade e integridade das informações. Com base nisso, propõe-se a implementação de métodos que controlem os acessos aos arquivos apenas pelas pessoas autorizadas e que garantam a integridade das informações, pois segundo SILVA, CARVALHO e TORRES (2003), existem métodos que garantem a confidencialidade e não impedem o acesso delas por pessoas autorizadas e a integridade é um requisito vital para garantir a fiabilidade das informações:

- Falta de regras mais definidas em relação aos acessos e usos da internet.

Este problema é tão importante quanto os demais, tendo em vista que as faltas de controle de acessos a determinados endereços na internet, de acordo com DANTAS (2011), podem abrir uma porta para vulnerabilidades e o acesso sem controle da rede WIFI, por meio de dispositivos móveis podem

comprometer a disponibilidade das informações, pois conforme SILVA, CARVALHO e TORRES (2003), obter a informação, mas não puder acessá-la no momento que se precisa dela, é igual a não ter informação nenhuma.

Para estes problemas recomenda-se a inclusão também de políticas sobre o uso da internet e sobre quem pode ou não acessar a internet por meio de dispositivos móveis através da rede WIFI.

Considerações Finais

Este artigo teve como propósito apresentar uma visão básica definida por autores, sobre a Segurança da Informação, com destaque aos princípios básicos, que são eles: A confidencialidade, a integridade e a disponibilidade, que auxiliam na Gestão da Segurança da Informação. Neste artigo também foi apresentado também um estudo de caso de uma empresa com situações precárias em relação ao nível de segurança da informação, para que houvesse um melhor entendimento da aplicação dos princípios básicos da Segurança da Informação, com as possíveis soluções apresentadas por este artigo, aos problemas encontrados nessa empresa.

A informação é um fator de preciosidade para as pessoas. Dentro de uma empresa, as informações devem ser tratadas com uma maior importância e devem ser vistas como um ativo essencial para o negócio, e que necessariamente precisa ser protegida.

As informações aqui apresentadas incitam uma reflexão sobre os cuidados que devem ser tomados com a segurança de informações.

De modo geral, este artigo contribuiu para que houvesse na empresa, uma conscientização da importância da Segurança da Informação, que antes era considerado um fator técnico pela Empresa X, e não como uma estratégia de negócios.

Referências bibliográficas

BEAL, A. Segurança da informação. São Paulo. Atlas, 2005.

DANTAS, L.M. Segurança da Informação - Uma Abordagem Focada em gestão de Riscos. Olinda. Livro Rapido, 2011.

FONTES, E. Políticas e Normas para a Segurança da Informação- Como desenvolver, implantar, e manter regulamentos para a proteção da Informação nas Organizações. Rio de Janeiro; Brasport, 2012.

FONTES, E. Praticando a Segurança da Informação. 1. ed. Rio Janeiro; Brasport, 2008.

GOMES, J.S. O Método de Estudo de Caso Aplicado à Gestão de Negócios. 1.ed. São Paulo; Atlas,2006.

SILVA T.P; CARVALHO H; TORRES B.C. Segurança dos Sistemas de Informação - Gestão Estratégica da Segurança Empresarial. Portugal. Atlántico, 2003.

VANCIM, F.F.N. Gestão de Segurança da Informação. Rio de Janeiro; SESES, 2016.

YIN, R.K. Estudo de caso - Planejamento e Métodos. 2.ed. Rio de Janeiro; Bookman, 2001.