Segurança em rede: Um estudo do seu benefício em pequenas empresas

AUTORES

Murilo Merighi FERNANDES

Rafael Augusto Lessa FÉLIX

Discentes da União das Faculdades dos Grandes Lagos - UNILAGO

Mariangela Catelani SOUZA

Docente da União das Faculdades dos Grandes Lagos – UNILAGO

RESUMO

Nos dias atuais, o compartilhamento de dados e informações está cada vez mais frequente em nosso mundo. Desta forma, métodos que trazem e visam garantir uma segurança para as informações estão sendo adotadas por vários empreendimentos. Computadores e servidores de organizações também são alvos de ataques repentinos, obrigando a empresa tomarem medidas cabíveis para este tipo de situação. Para o pequeno empreendedor, adquirir uma gestão de Segurança da Informação dentro de sua organização não é uma tarefa fácil, pois há necessidade de investimentos altos e um setor especializado para desenvolvê-lo, porém, pontos positivos podem ser alcançados com este método alinhado, proporcionando aumento de continuidade, melhoria nos controles e melhoria de compreensão das funções produtivas. Portanto, o trabalho tem como objetivo abordar conceitos de Segurança de Redes em pequenas empresas, ajudando e orientando-as à como se portar mediante a ataques e/ou infiltrações ilegais em seus servidores, para segurança de sua organização.

PALAVRAS - CHAVE

Empresa; Rede; Segurança.

1 INTRODUÇÃO

No mundo contemporâneo, a sociedade está cada vez mais dependente de informações compartilhadas através da rede mundial de computadores, deve-se isto à rápida evolução digital na sociedade e pela própria facilidade que este meio proporciona. Porém, com esta desenfreada ascensão surge o problema que já é uma das principais preocupações mundial, a segurança. A sociedade depende das informações armazenadas nos sistemas computacionais para a tomada de decisão em empresas, órgão do governo, entre outros contextos organizacionais (COELHO; ARAÚJO; BEZERRA, 2014).

Com isso, há a necessidade de se recorrer a métodos que visem garantir a segurança das informações compartilhadas na internet pelas mais diversas organizações, segundo Cazemier, Overbeek e Peters (2000), ao longo dos anos, a segurança tem se tornado uma grande preocupação para empresas que investem em uma complexa infraestrutura para realizarem transações comerciais. Investimentos estes que se justificam frente ao volume financeiro desempenhado por grandes instituições de todo o mundo, garantindo assim não apenas a segurança da organização, mas também a segurança de qualquer usuário que utilize as vias de comunicação das mesmas.

É válido afirmar que segurança não depende apenas dos recursos materiais investidos, mas também é necessário o treinamento e aperfeiçoamento dos indivíduos que utilizam esse meio de comunicação. De acordo com Fontes (2012) deve-se considerar todo o tipo de usuário que utilizará a informação da organização. Logo, todos os operadores envolvidos neste processo de troca de dados necessitam ter o conhecimento necessário para não colocar a segurança de toda a informação em risco.

Por outro lado, o problema de segurança é existente no meio empresarial, causando destruição, modificação ou deturpação e até mesmo roubo, remoção ou perda de informação. Por esse motivo, precisam adotar-se estratégias para evitar tais acontecimentos. Com o crescimento de irregularidades por inexistência de segurança, as empresas devem se concentrar em empregar, investimentos estratégicos, a fim de impedir problemas que podem comprometer a organização (OLIVEIRA, 2003).

Segundo Costa, Silva e Cruz (2012), com a falta de regras de segurança para a proteção dos dados, permite-se que categorias de controle e acesso possam ser explorados por usuários externos ou internos ao sistema de computação, obtendo acesso não autorizado. Essas falhas no sistema podem ser motivadas por impactos de diferentes níveis e permitir desde uma simples ameaça, ou uma ação que comprometa a imagem corporativa, até as perdas financeiras e de mercado ao longo prazo.

O conteúdo deste artigo visa expor um breve conceito sobre a segurança da informação, os temas neste citado terão como objetivo esclarecer em linguagem simples os princípios essenciais para uma boa política de segurança nos meios eletrônicos das organizações, assim como orientar os usuários frente aos mais diversos tipos de ameaças que possam vir a comprometer quaisquer aspectos de suas vidas integrados à internet.

2 DESENVOLVIMENTO

2.1 Tipos de redes

A primeira rede formada para o intercâmbio de dados entre computadores surgiu na década de 60 batizada como ARPANET, este projeto tinha como objetivo interligar base militares e centros de pesquisas nos EUA (COMER, 2016).

Desde então, o processo de comunicação entre computadores tem se tornado maior e mais eficiente a ponto de ser considerado por muitos como indispensável nos dias atuais, porém, assim como qualquer tipo de comunicação existe risco de determinada informação ser extraviada podendo causar danos irreparáveis para os envolvidos. Este artigo discorrerá sobre quais os meios, benefícios e cuidados que envolvem a utilização de redes para o compartilhamento de informações (COMER, 2016).

A internet, segundo Castells (2003), tem sido considerada a maior invenção tecnológica dos últimos tempos em virtude do seu poder de alcance, da compressão espaço-tempo, das informações em tempo real e principalmente na sua capacidade de conectar pessoas do mundo todo nas mais variadas ocasiões.

É através da internet que inúmeras redes se interligam criando um enorme aglomerado de informações que são transmitidas instantaneamente e quase sem restrições para todas as partes do mundo. Qualquer pessoa que possua um aparelho com acesso à internet pode compartilhar informações, considerando que ela está em um meio de comunicação pública, porém, por vezes há uma necessidade de que apenas um seleto grupo de pessoas recebam e transmitam determinados dados, é então que surge a necessidade de redes fechadas a qual é possível determinar quais dados serão transmitidos e quem poderá visualizá-los (COMER, 2016).

No meio empresarial, estas redes restritas são chamadas de intranet e extranet, embora sejam baseadas no mesmo modelo da internet, Protocolo TCP/IP, elas possuem um caráter mais restritivo que impossibilita o acesso de indivíduos não autorizados à rede. De acordo com Assis (2009), a intranet é uma rede interna, fechada e exclusiva, com acesso somente para os funcionários de uma determinada empresa e muitas vezes liberado somente no ambiente de trabalho e em computadores registrados na rede, ou seja, a intranet pode ser entendida como uma rede de espaço físico definido onde apenas os aparelhos credenciados à rede podem acessar as informações ali contidas.

Já na extranet, o acesso deixa de ser restrito a uma determinada área física, porém, a restrição de usuários que podem acessar a rede se mantém, a rede pode ser acessada por fornecedores, clientes ou até mesmo funcionários que não estejam em seu local de trabalho, existem dois meios de estabelecer a conexão; via login e senha, neste caso o utilizador receberá do administrador da rede um usuário e uma senha para acessar o sistema por um link disponível na internet, ou então o acesso poderá ser realizado por uma Rede Particular Virtual (VPN), neste caso, há um tunelamento entre os dois computadores onde os dados serão criptografados de modo que os informações fiquem restritas apenas entre estes dois computadores (ASSIS, 2009).

2.2 Segurança da informação

Teoricamente, os dados que compõe a intranet e extranet estão disponíveis apenas para os usuários autorizados pelo administrador da rede, estes dados contêm informações importantes sobre a organização, como; registros de fornecedores e clientes, pesquisas, dados operacionais, dados financeiros, entre outros. Porém, apenas pelo fato da rede em questão ser restrita onde cada usuário tem um acesso definido para cada área não significa que outras pessoas não poderão ter acesso a ela (ASSIS, 2009).

A partir disto, é necessário começar a se pensar sobre a segurança das informações contidas nas redes, para Nakamura e Geus (2007), A confiabilidade, integridade e disponibilidade dessa estrutura de rede passam, assim, as ser essenciais para o bom andamento das organizações, fazendo com que elas precisem ser protegidas. Ainda, segundo os autores, a informação deve chegar aos receptores de forma íntegra e confiável, para isso é necessário que todos os elementos de rede nos quais a informação flui estejam disponíveis, oferecendo integridade e sigilo aos dados.

A Segurança da informação consiste em proteger todos os dados da organização e manter sua integridade. A segurança da informação não é apenas a segurança de dados, mas também dos bens de uma empresa como um todo (CASTRO, 2011).

Para oferecer a proteção das informações empresariais, é fundamental que exista um Sistema de Gestão de Segurança da Informação (SGSI), pela definição de Palma (2016); o SGSI inclui estratégias, planos, políticas, medidas, controles e diversos instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

Para implantar o SGSI existem diretrizes definidas pela Organização Internacional de Normalização, neste caso em específico de implementação em empresas o certificado é o ISO/IEC 27001, esta norma encoraja que os seus usuários enfatizem a importância do entendimento dos requisitos e da necessidade de uma política para a segurança da informação, cria e opera controles para gerenciar os riscos da segurança da informação, monitora e faz uma análise crítica do desempenho e eficácia do SGSI e promove a melhoria contínua baseada nas medições objetivas (FONTES, 2012).

Entre os principais benefícios pode se destacar; expressa o compromisso dos gestores com a segurança da informação, aumento da fiabilidade e segurança das informações e do sistema, investimentos conscientes e mais eficientes, aumenta o nível de participação, sensibilidade e motivação dos colaboradores, identifica oportunidades e propicia melhorias de forma contínua, aumenta a confiança perante os clientes e parceiros, melhoramento do desempenho operacional proveniente de normas e análise de risco e implanta um sistema de controle da gestão, aumentando a eficácia da empresa. As normas ISO/IEC 27001 estão vinculadas à família ISO 27000 que possui 36 normas publicadas oficialmente, até a data deste artigo (PANDINI, 2015).

O modelo é resultado do consenso entre especialistas, sendo considerado o estado da arte no que tange padronização para o segmento de segurança da informação, e tem o objetivo de apresentar um apanhando geral sobre o sistema de gestão de segurança da informação e ambientalizar os leitores sobre termos técnicos utilizados durante o processo de padronização (PANDINI, 2015).

2.3 A Pequena Empresa e o Uso da Tecnologia de Informação

Para Solomon (1986), uma certa tecnologia pode ser boa ou ruim para a pequena empresa. Na verdade isso depende da forma de como ela é utilizada. Eficiência, precisão, recursos, atividades e maior eficácia em adquirir resultados são garantidas por esse auxílio em informações de sistemas com uma boa administração de processos.

2.4 Aplicação da tecnologia de informação na pequena empresa

A inclusão de um sistema de segurança em uma pequena empresa pode fazer toda a diferença em seu desempenho, mas é preciso tratá-lo com muito cuidado, pois qualquer erro pode acarretar sérios problemas que comprometerão toda a empresa. A maior dificuldade das pequenas empresas é não possuir sistemas de controles informatizados, porém o baixo custo e difusão dessa tecnologia as incentiva a investir nesse tipo de gestão, com o objetivo de melhorar seu desempenho em relação à concorrência (PANDINI, 2015).

Ainda que pareça positivo, esse tipo de investimento pode trazer prejuízos para a organização se não houverem pessoas capacitadas para utilizar adequadamente esta tecnologia. Sendo assim é necessário que se faça uma criteriosa avaliação da real necessidade e custo benefício da implantação de um sistema de informação para que todos os aspectos empresariais sejam influenciados (PANDINI, 2015).

2.5 Benefícios da segurança de rede em pequenas empresas

Segundo Oliveira (1998), pode-se medir a eficiência da tecnologia comparando o custo para seu desenvolvimento com o beneficio alcançado com seu uso. Esse custo inclui a produção, coleta, processamento e distribuição do sistema. Com uma gestão mais aprofundada, a utilização deste mecanismo possibilita desenvolver uma determinada função com mais rendimento diário, levando ao usuário a ter um aumento satisfatório, facilitando seu trabalho.

Aumento de continuidade: Ajuda na integridade mecânica, maior rendimento operacional e traz uma satisfação no ambiente de processos. Melhoria dos controles: Concede baixos custos de operação, facilita a infiltração de informações, baixa repetição da função, amplia a visão estratégica e da segurança nas decisões da empresa. Melhoria de compreensão das funções produtivas: Definição apurada das visões e valores da organização, rendimento satisfatório dos trabalhadores engajados no setor, amplia a visão de investimentos, ajuda manter todos os setores interligados aumentando a qualidade de serviço (PANDINI, 2015).

2.6 Importância da TI nas Organizações

Os sistemas que dão informação ao administrador são extremamente importantes para o desenvolvimento das funções de organização, planejamento, liderança e controle. Para Stoner (1999), toda a estratégia de uma empresa se faz concreta a partir da obtenção de informações precisas e pontuais. Um dos perigos atuais e que mais tem acontecido são os ataques hackers, que acessam e roubam as informações com o objetivo de cobrar para devolvê-las. Todos os processos tecnológicos de uma organização possuem brechas na segurança, que possibilitam o ataque. É de suma importância considerar que todo o sistema esteja apto e preparado para este tipo de investidas (SÊMOLA, 2003).

Para Schneier (2001), “as ameaças do mundo digital espelham as ameaças no mundo físico. Se o desfalque é uma ameaça, o desfalque digital também é uma ameaça. Se os bancos físicos são roubados, então os bancos digitais serão roubados”.

Para Sêmola (2003), existem três aspectos a serem considerados quando se trata de segurança da informação: tecnológicos, físicos e humanos. A rede tecnológica é a mais preocupante para as empresas, porém os aspectos físicos e humanos também são de suma importância para a segurança dos dados (SÊMOLA, 2003).

2.7 Camada Física

A camada física diz respeito ao ambiente onde estão os computadores, servidores e meios de comunicação. Em geral, as pequenas e médias organizações têm seus dados mantidos em servidores, proporcionando a entrada de intrusos na rede. Entretanto, nas médias empresas esse problema é minimizado por meio da conscientização dos servidores quanto aos procedimentos de segurança da informação. Formas consideráveis para obtenção de proteção nesta camada são: firewalls e recursos para manter uma estabilidade de energia (SÊMOLA, 2003).

2.8 Camada tecnológica

A camada tecnológica diz respeito ao uso de softwares, que colaboram com todo o processo funcional de informações, dados e transações. Segundo Adachi (2004), é na camada tecnológica que estão “regras, normas,

protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas". A melhor forma de manter a segurança dos softwares é atualiza-los com frequência, de acordo com a mais recente correção de segurança do fabricante (SÊMOLA, 2003).

2.9 Camada Humana

Como o nome diz, esta camada é composta pelos indivíduos que exercem suas funções dentro da empresa. Os principais aspectos a serem considerados nesta camada são: a conscientização quanto aos riscos, a familiaridade com o uso da tecnologia da informação, o risco dos invasores e a engenharia social (ADACHI, 2004). Por se tratar do fator humano, que envolve os aspectos emocionais, psicológicos e sócio-culturais, a camada humana é a de mais difícil gerenciamento (SCHNEIER, 2001).

3 ANÁLISES E IMPORTÂNCIA DOS SISTEMAS

Os sistemas são voltados para auxiliar nas rotinas administrativas e operacionais dos clientes e por possuir clientes de diferentes portes as medidas oferecidas para que esses protejam seus dados e o suporte a segurança de seus dados varia de acordo com o seu contrato.

O acesso dos produtos é limitado a usuários cadastrados, de modo que sem o conhecimento desse par de segurança o sistema não é executado. Por sua vez, em nível de dados, as informações são criptografadas impedindo a leitura de dados sigilosos. Para evitar a perda das informações dos sistemas em caso de problemas no hardware o backup dos dados é realizado diariamente, podendo ser realizado em nuvem, mídia física ou ambos.

Quando o cliente possui uma estrutura na qual serão necessárias um número maior de conexões simultâneas recomenda-se a utilização de servidores dedicados, os quais são protegidos por softwares de firewall, antivírus e anti-malware/spy-ware. Além disso, a empresa oferece o serviço de gestão de rede utilizando MicroTik para administrar as conexões, evitando conexões não autorizada e navegação para páginas potencialmente perigosas.

O servidor geralmente fica localizado nas dependências do cliente, por isso para evitar picos de energia no servidor, é recomendável a utilização de estabilizadores de energia e no-break no servidor, além de posicioná-lo em local preferencialmente climatizado. Por fim, ela oferece serviços de manutenção e suporte operacional de segunda a sábado em horário comercial.

4.CONCLUSÃO

Nos dias atuais, a utilização de meios digitais pelas empresas deixou de ser um diferencial e se tornou quase que obrigatória para aquelas que almejam crescer e se destacar no mercado. Por isso, a necessidade de se manter informado e buscar quaisquer meios para o desenvolvimento da tecnologia da informação é importante, se trata de uma área muito dinâmica onde sempre surgem novas oportunidades e com elas também novas ameaças.

Assim como os bancos mantém seu dinheiro dentro de cofres enormes e quase impenetráveis, as empresas também precisam proteger a sua riqueza, de nada adianta uma empresa manter um grande e bem estruturado sistema de informação se não houver segurança para ele. Não se deve menosprezar a segurança, por ser algo que não é perceptível no dia a dia é possível que não haja a devida atenção para a sua manutenção, isso

permite que falhas no sistema, falhas estas que são as responsáveis por violações de terceiros e possíveis perdas de dados do sistema.

O Sistema de segurança da informação é algo que merece uma atenção especial, não apenas de recursos materiais, mas também de recursos humanos. É necessário que a empresa possua uma política clara e que englobe todos os departamentos para que todos os colaboradores sejam adeptos ao sistema, é de extrema importância que todos os funcionários estejam em contato continuo com o setor de TI para que as instruções sejam bem executadas prevenindo assim ao máximo brechas que possam prejudicar todo o sistema.

O custo para a aplicação e monitoramento de um sistema de segurança pode ser um empecilho para as pequenas empresas, já que, é necessário que haja uma estrutura juntamente com um profissional adequado para acompanhar o desenvolvimento do sistema. Para tornar todo este processo viável, a empresa pode recorrer aos profissionais liberais que executem esse tipo de trabalho, há também a possibilidade de contratar uma empresa, já que, hoje em dia existem empresas especializadas que oferecem produtos e serviços para todo o sistema de informação.

5.REFERÊNCIAS

OLIVEIRA, Wilson. **Técnicas para Hackers - Solução para Segurança**. Lisboa: Centro Atlântico, 2003

ARAUJO, Luiz. G. S.; BEZERRA, Edson. K.; COELHO, Flávia. E. **Gestão da Segurança da Informação**. Rio de Janeiro: Rede Nacional de Ensino e Pesquisa, 2014

CAZEMIER, Jacques. A.; OVERBEEK, Paul. L.; PETERS, Louk. M. C. **Security Management**. Londres: The Stationery Office, 2000.

J. da S. Costa, J. da Silva, M. A. P. da Cruz. **Revista Inova Ação**. Teresina, v. 1, n. 2, art. 6, p. 77-88, jul./dez. 2012.

ASSIS, Pablo. **O que é intranet e extranet?.** Disponível em: <https://www.tecmundo.com.br/conexao/1955-o-que-e-intranet-e-extranet-.htm>. Acesso em: 21 ago. 2018.

CASTELLS, Manuel. **A Galáxia da Internet:** reflexões sobre a Internet os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Editor, 2003.

CASTRO, Rita C. C; SOUSA, Verônica L. P. **Segurança em Cloud Computing:** Governança e Gerenciamento de Riscos de Segurança. Disponível em: <http://www.academia.edu/7520311/Seguran%C3%A7a_em_Cloud_Computing_Governan%C3%A7a_e_Gerenciamento_de_Riscos_de_Seguran%C3%A7a >. Acesso em: 25 ago. 2018.

COMER, Douglas. **Redes de Computadores e Internet**. 6 ed. Porto Alegre: Bookman Companhia Editora, 2016.

FONTES, Edson. **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 Livros e Multimídia, 2012.

NAKAMURA, Emilio T.; GEUS, Paulo L. **Segurança de Redes em Ambientes Cooperativos**. São Paulo: Novatec Editora, 2007.

NETO, José A. M. **A computação em nuvem para as MPEs**. Disponível em: <http://www.administradores.com.br/informe-se/artigos/a-computacao-emnuvem-para-as-mpes/51444/>. Acesso em: 06 set. 2018.

OLIVEIRA, Antonio C. M. **Tecnologia de informação:** competitividade e políticas públicas. Revista de Administração de Empresas, São Paulo, v. 36, n. 2, p. 34-43, 1996.

OLIVEIRA, M. M**. A vitalidade das pequenas. Pequenas Empresas Grandes Negócios**, n.110, ano X, março de 1998.

PALMA, Fernando**. Sistema de Gestão de Segurança da Informação (SGSI).** Disponível em: <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em: 18 ago. 2018.

PANDINI, Willian. **ISO 27000, primeiros passos com a norma.** Disponível em: <https://ostec.blog/padronizacao-seguranca/primeiros-passos-iso-27000>. Acesso em: 14 ago. 2018.

SANTOS, Raimundo N. M. **Sistemas de informações estratégicas para a vitalidade da empresa.** Ciência da Informação, Brasília, v.25, n.1, p.12-14, jan/abr de 1996.

SOLOMON, Steven. **A grande importância da pequena empresa:** a pequena empresa nos Estados Unidos no Brasil e no mundo. Rio de Janeiro. Editorial Nórdica, 1986.

SCHNEIER, Bruce. **Segurança.com:** Segredos e mentiras sobre a proteção digital. Rio de Janeiro: Campus, 2001

SÊMOLA, Marcos. **Gestão de Segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus, 2003

ADACHI, Tomi. **Gestão e Segurança em Internet Banking**. São Paulo: FGV,2004

STONER, James A.F.; Freeman, R. Edward**. Administração**. 5 ed. Rio de Janeiro: LTC, 1990