IMPORTÂNCIA DA POLITÍCA DE SEGURANÇA E AS TÉCNICAS DE PROTEÇÃO AOS SISTEMAS DE INFORMAÇÃO

Keilamar Vieira Soares Silva[1]

Danilo Marques Oliveira[2]

RESUMO: Este artigo tem como objetivo abordar a importância de uma boa politica de segurança nas pequenas e médias empresas, e mostrar como estas aderem a essa politíca, pois lidam com grande quantidade de informação de clientes, funcionarios entre outros. De acordo com a literatura e a norma brasileira de segurança da informação existem tecnicas e ferramentas para uma boa politica de segurança. Deve-se observar que a maior preocupação deveria girar em torno do pessoal, pois são elas que lidam com as informações, e existe uma certa falta de atenção das empresas nesse quesito. O principal motivo para se ter uma politica de seguraça e evitar perdas financeiras, documentos, sejam estes de clientes e/ou fornecedores, além de influenciar diretamente na imagem da organização. Mas apesar de muitas empresas se preocuparem com a segurança, outras não investem nessa área, muitas vezes, por falta de conhecimento, questão de custos, cultura organizacional e preocupação com treinamentos. O fato importante que deve ser levantado é a resistência por parte dos usuários na organização, que tendem a rejeitar certas mudançasno seu ambiente de trabalho, para que isto não ocorra o mesmo deve ser realizado de forma gradativa.

Palavra-chave: Integração. ISO/IEC 27002. Planejamento. Segurança. Tecnologia da Informação.

INTRODUÇÃO

Com o aumento da utilização de computadores dentro das organizações, as informações estão sendo concentradas em um único ambiente com um grande volume de informações, no caso os servidores, então passou a ser um grande problema para segurança, administrar e prever ataques ciberneticos e roubos de informações. Sendo assim, como as informações estão armazenadas em computadores, as empresas dependem da confiança de seus sistemas que são baseados em TI. Para as empresas de pequeno e médio porte, se tornam um grande problema a questão da segurança, pois muitas das vezes, estas não possuem recursos necessários para o investimento na gestão de uma boa segurança da informação ou pensam que por ser uma pequena empresa, não seja necessário.

[1] Discente do Curso de Sistemas de Informação, UNIFIMES. keilamargt@hotmail.com

[2] Docente do Curso de Sistemas de Informação do Centro Universitário de Mineiros – UNIFIMES. danilo@fimes.edu.br

De acordo com o Beal (2005), uma política de segurança é um processo de proteção às informações contra ameaças a sua integridade, disponibilidade e confiabilidade. Para as empresas aderirem a essa política, faz-se necessário que os gestores tenham uma visão clara das ameaças e da importância dessa adoção, e ainda, que as consequências caso não adote uma proteção, podem ser piores.

Dessa maneira, as empresas precisam adotar medidas de segurança e medidas de proteção que abranjam uma grande diversidade de iniciativas que sejam capazes de proteger dados e informações, levando em conta os riscos reais (BEAL, 2005).

DESENVOLVIMENTO

Segundo Ferreira (2017) para que a política de segurança se consolide, é feito um documento ou um protocolo escrito com ações preventivas e descrito algumas medidas em caso de invasão ao sistema ou alguma perda de informações, e também, deve-se deixar a empresa com os melhores e mais modernos métodos de segurança.

Para de fato acontecer essa implantação, é necessário que todos os níveis hierárquicos dentro da empresa, tenham uma visão ampliada dos riscos que podem afetar ás informações, e quais medidas a serem tomadas em casos criticos.

No período de implantação é de suma importância uma equipe qualificada, para atender e tirar dúvidas de seus colaboradores.

Para a orientação quanto a implantação da política de segurança, tem-se algumas normas que auxiliam. Segundo a norma NBR ISO/IEC 27002 (2005):

> A segurança da informação é obtida a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessários, para garantir que os objetivos de negócio e de segurança da organização sejam atendidos. (ABNT, 2005, p s/p).

Dadas algumas definições, veremos agora os primeiros passos para a implantação. De acordo com o Ferreira (2017), primeiro vem-se o planejamento, os gestores e a equipe técnica se reúnem para fazer um levantamento de informações que são gerados pela própria organização e seus funcionários. Vale ressaltar que, caso a empresa já tenha uma política de segurança estabelecida, é importante observar se existem pontos falhos, e com isso melhorar ainda mais a segurança.

A reunião com os gestores é de suma importância, pois caso as mudanças ocorram desde o topo da pirâmide organizacional, há mais chances de ocorrência de acerto, e ainda, serve como um incentivo aos demais departamentos, explanando assim, a importância de uma política de segurança ser adotada.

Após planejamento, é a hora da equipe técnica começar a parte prática, colocando em prática, regras, definindo limites para uso de softwares, acesso à internet, e ainda, criando senhas mais fortes, criptografando e-mails, verificando a necessidade ou não de pendrives, a utilização dos computadores apenas para trabalho, e definindo uma estrutura de redes mais segura. Isto são apenas algumas regras que devem ser modeladas de acordo com a necessidade de sua organização.

Após a criação de todo o documento com a política de segurança, a mesma passa por uma avaliação com gestores afim de ser aprovada ou não. Assim que os gestores analisarem e aprovarem, é o momento de começar os treinamentos e a capacitação do pessoal, pois estes terão total envolvimento com essas regras estabelecidas. E sempre que necessário, realizar uma avaliação periódica, afim de verificar se a política de segurança não está ultrapassada, tentar sempre manter-se atualizado as novas tecnologias e formas inovadoras de segurança.

A implantação da política de segurança em pequenas empresas se torna mais fácil, pois há um envolvimento menor com pessoal e menos dados a serem manipulados. Já as grandes empresas, lidam com mais pessoal e as informações geradas são mais complexas, e assim, se tomam mais difíceis de se lidar quanto a segurança.

DISCUSSÃO

Para Ferreira (2006), o ganho da empresa com a política pode ser visto nos primeiros meses de aplicação, a curto prazo, podemos analisar a formalização de documentos, a restrição de acesso as pessoas sem autorização e maior segurança nos processos de negócio.

Em longo prazo, a implementação da política de segurança na empresa, resulta na confiança do cliente em adquirir um serviço, o planejamento e gerenciamento das informações ficam mais compactados, os investidores se sentem mais confiantes em investir em empresas que se preocupam com segurança, além da diminuição de problemas.

Outro resultado bastante interessante ao elaborar a segurança da informação, deve estar intimamente ligado as estratégias de negócio, conseguindo manter uma continuidade de negócio e uma excelência operacional. A continuidade de negócio de acordo (ABNT, 2005) ISO/IEC 27002 é um dos principais objetivos da gestão de segurança da informação, para se

ter uma continuidade de negócio precisa de decisões adequadas, que por sua vez as informações precisam estar corretas, e para isso é feita uma auditoria que assegura a integridade da informação.

A política de segurança disponibiliza algumas técnicas que chamamos de ferramentas de segurança da informação, que é, um conjunto de software, hardware e técnicas que tem como principal objetivo combater os ataques (CHESWICK, 2005, p 143). Estas, são encontradas em diversos sistemas operacionais, como Windows Server e Linux.

A seguir algumas técnicas que podem ser implantadas nas organizações:

- **Proxy:** tem a finalidade de filtrar os pacotes na rede interna da organização, e impede a conexão com outros servidores externos que são prejudiciais para o sistema. As redes de compartilhamento de arquivos oferecem ameaças como trojans, vírus que muitas vezes se disfarçam com extensões mp3, JPEG, um exemplo bem conhecido é o Squid, que é um pacote que vem nas distribuições Linux;
- **Firewall pessoal:** intercepta conexões de entrada e saída do computador, baseando em regras já definidas ou regras padronizadas, que decide quais conexões podem ou não ser aceitas. Podemos citar o Sygate como um exemplo;
- **Criptografia:** é uma técnica para cifrar uma informação, tornando-a incompreensível, exceto para o destinatário e o transmissor, que sabem como decifra-la (KUROSE, 2003, p. 605). A criptografia é importante em casos de operações bancárias, compras online, troca e-mails, coisas simples, mais que fazem uma diferença muito grande;
- **Hash:** é uma função matemática aplicada em algoritmos que utilizam mensagens de texto para a criação de outro texto (STALLINGS, 1999). A função de hash é muito importante quando, aplicada em arquivos, pois significa a execução de um algoritmo de cálculo sobre o arquivo para a geração de um número como resultado, toda alteração pode produzir mudança no resultado calculado, possibilitando saber se o arquivo foi alterado ou até mesmo verificar se os arquivos estão infectados. (FITZGERALD, 2005).

Estas são algumas técnicas que podem auxiliar para a proteção das informações, onde se percebe que a política de segurança que foi feita começa a surgir efeito. Contudo, para que as técnicas de segurança da informação continuem funcionando perfeitamente é necessário

fazer manutenção, ou seja, definir níveis de segurança. E após uma série de melhorias, é necessário ainda mudar de patamar.

Por exemplo, o caso de autenticação dos usuários que normalmente é realizado através de senhas criadas por eles próprios. Para avançar no quesito segurança, faz-se necessário a autenticação feita por biometria, isso mostra que existem recursos melhorados na hora da autenticação. Mas vale lembrar que cada organização define o patamar de segurança de acordo com suas necessidades. Para uma empresa pequena por exemplo, não se faz necessário uma autenticação por biometria, são poucos funcionários, e além de tudo, um alto investimento. Já em casos de organizações multinacionais, o investimento já é um caso a ser pensado. Independentemente de como você rotule sua política de segurança, nunca deixe de fazê-la.

CONCLUSÃO

Conclui-se através desse trabalho que para uma segurança da informação são necessárias etapas a serem seguidas, pois somente assim, consegue-se uma boa política de segurança, a qual envolve questões normativas e tecnológicas.

O mercado busca desenvolver técnicas de segurança que as empresas possam adquirir e implantarem em seus sistemas, para assim alcançarem uma boa segurança em relação às suas informações, bem como a diminuição dos riscos em sistemas vulneráveis, além é claro, de uma melhor excelência operacional. Sendo assim, é de grande importância a segurança das informações, então, não hesite em implantá-la.

REFERÊNCIAS

ABNT.NBR.ISO/IEC27002. **Tecnologia da informação-técnicas de segurança-Sistemas de gestão de segurança da informação**-Requisitos. Rio de Janeiro, ABNT, 2005.

BEAL, Adriana. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações – São Paulo: Atlas, 2005.

CHESWICK, W. BELLOVIN, S.M, RUBIN. A. D. **Firewalls e segurança na internet**. 2. ed. Rio Grande do Sul. Bokiman.2005.

FERREIRA, André L.R. **Como implantar uma politica de segurança da informação na sua empresa.** 2017. Disponivel em:<http://www.netdeep.com.br/blog/geral/como-implantar-uma-politica-de-seguranca-da-informacao-na-sua-empresa.html>. Acesso em: 27 set. 2017.

FERREIRA, Fernando Nicolau Freitas; ARAUJO, Marcio Tadeu. **Política de segurança da informação**. Rio de Janeiro: Ciência Moderna, 2006.

FITZGERALD, Jerry, DENNIS, Alan**. Comunicação e dados empresarias e redes**. Rio de Janeiro: LTC, 2005.

KUROSE. J. F.; ROSS, K. W. **Redes de computadores e a internet**. São Paulo. Addison Wesley. 2003.

SQUID. Version 2.6: **Squid.** Org. 2008. Disponível em: <http://www.Squid-cache.org/>. Acesso em: 27 set.2017.

STALLINGS. Willian**. Criptography and Network Security:** Principles and Practice, Third Edition. Prentice-Hall, 2003.

SYGATE. **Symantec**. 2007. Disponível em: <http://www.symantec.com/>. Acesso em: 27 set. 2017.