IMPLANTAÇÃO DE MECANISMOS DE SEGURANÇA DA INFORMAÇÃO EM PREFEITURA MUNICIPAL

Betânia dos Santos Rossi[1]; Isabela Garcia Santos Vieira[2]; Luiz Fernando Ribeiro de Paiva[3]
[1,2,3] Universidade de Uberaba – UNIUBE, Uberaba – Minas Gerais
betaniarossi@gmail.com; isabelagsv@gmail.com; luiz.paiva@uniube.br

Resumo

A segurança da informação se configura como uma das principais preocupações dos gestores de todos os tipos de organizações que utilizam sistemas informatizados, sejam eles de instalações próprias ou de empresas terceirizadas. É necessário garantir a integridade dos dados e sua proteção contra roubo e qualquer outro tipo de acesso indevido.

O presente trabalho tem como objetivo propor a implantação de políticas de segurança da informação em uma prefeitura municipal brasileira. Por meio do estudo realizado na referida prefeitura, percebeu-se que as atuais técnicas e sistemas de segurança da informação podem ser melhoradas, adotando-se padrões e políticas mais eficientes. O setor de Tecnologia da Informação (TI) desta prefeitura adota, já há alguns anos, uma série de procedimentos de segurança da informação como, por exemplo, o armazenamento dos *backups*[1] de dados em mais de um local físico. Existe, no entanto, a necessidade de se buscar outras formas para garantir a segurança da informação, como implantar ferramentas avançadas de proteção de dados, oferecer orientações aos usuários, implantar determinadas técnicas e procedimentos de segurança, e até mesmo oferecer treinamentos e cursos de capacitação aos profissionais de TI.

A partir do estudo realizado, propõe-se a implantação de uma Política de Segurança da Informação (PSI)[2] na Prefeitura Municipal que é alvo do presente estudo, buscando conscientizar gestores, diretores, chefes de departamentos e demais envolvidos com informações organizacionais sobre a importância do processo que está sendo proposto.

Será preciso garantir que sejam seguidas as normas impostas pela PSI e esta dependerá de constantes revisões e atualizações, para que se obtenham bons resultados com sua implementação.

Há também a preocupação em deixar claro, no ambiente pesquisado, que a PSI não é apenas uma forma de se estabelecer a proteção de dados, mas, também, de conscientizar a todos na organização de que as informações são um precioso bem que a prefeitura municipal processa em favor da comunidade.

Palavras–chave: Proteção de dados, Política de Segurança da Informação, Ataques cibernéticos.

Introdução

A segurança da informação é tida como um ponto crucial na busca pelo sucesso das organizações diante de seus objetivos, considerando que na atualidade as informações que a empresa armazena e processa, sendo este, portanto, um recurso patrimonial de extrema importância. No que se refere a lidar com dados organizacionais, é necessário estar atento quanto a alguns aspectos, como

[1] Cópia de Segurança dos dados que é feita com determinada periodicidade.

[2] Registro documentado de mecanismos de segurança a serem adotados, sendo definidos segundo determinadas normas, como as da ABNT (Associação Brasileira de Normas Técnicas).

confidencialidade, integridade e autenticidade, aspectos essenciais à segurança da informação que são citados no guia "Boas práticas em segurança da informação" do Tribunal de Contas da União (TCU):

> A segurança de informações visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas pela instituição. (BRASÍLIA, 2012, p. 9).

Na esfera pública há que se preocupar, ainda, com as questões legais e sociais, observando aspectos como o da disponibilidade e da transparência.

As instituições são responsáveis por guardar e proteger as informações que processam e devem ser capazes de cuidar da questão da autenticidade dos dados. Na PSI, devem estar contempladas as políticas de acesso às informações e relativas ao uso de recursos computacionais necessários para seu processamento e proteção.

O objetivo do presente trabalho é propor a implantação de políticas de segurança da informação em uma prefeitura municipal brasileira, que não será identificada por motivos de segurança.

Deve ser salientado o fato de que vários dos aspectos de segurança da informação que são considerados para órgãos públicos, quando se planeja implementar políticas de segurança, também se adequam às necessidades de empresas privadas e outras instituições. Em ambos os contextos, é necessário que os usuários estejam devidamente orientados no sentido de seguir as diretrizes de segurança para manter protegidas as informações que estejam sob sua responsabilidade. Cabe ao gerente de Tecnologia da Informação (TI) cuidar para que a socialização das regras e políticas seja efetiva.

Conforme consta do texto "Boas Práticas em Segurança da Informação" do TCU (BRASÍLIA, 2012), existem controles de acessos lógicos a serem implementados para impedir acessos não autorizados a dados, programas e sistemas, sendo que, em termos da proteção de recursos computacionais, deve haver a proteção de aplicativos, arquivos de dados, utilitários e do sistema operacional.

Assim, as empresas devem investir em sistemas de segurança da informação – *hardware* e *software* – de forma a prevenir e impedir todos os tipos de ataques cibernéticos e as contaminações por códigos maliciosos (*malwares*), pois a perda de dados, o roubo de informações e a paralização de sistemas, dentre outros problemas, podem trazer grandes prejuízos.

1. Investimentos e Treinamentos

Para que se possam prevenir ocorrências indesejáveis ou falhas de segurança da informação, devem ser realizados os investimentos necessários em sistemas de segurança e em treinamento/certificação de equipes. Também se aplicam, em alguns casos, a terceirização de alguns serviços.

Todos esses itens, no entanto, são definidos a partir de um planejamento prévio, um projeto de implantação ou readequação dos mecanismos e políticas de segurança de sistemas e dados da organização.

Durante a realização do presente estudo, foi possível verificar que, em determinados setores da prefeitura visitada, os equipamentos de informática são antigos e que brevemente eles não atenderão à crescente demanda de processamento e armazenamento de dados da instituição. Considere-se, também, o crescente tráfego de dados em rede.

No que se refere ao momento em que se decide pela compra de novos equipamentos e pela contratação dos serviços de manutenção, vários aspectos devem ser considerados, já que

> com relação à escolha das marcas dos produtos, é aconselhável buscar

> informações técnicas completas, bem como a realização de pesquisa de satisfação de usuários dos equipamentos pretendidos. (SEGURANÇA, 2014, p. 11).

É preciso considerar que, por vários motivos, equipamentos antigos tornam as organizações mais vulneráveis quanto aos problemas de segurança da informação. Um desses motivos se refere aos sistemas de *software* que estão instalados nos equipamentos. Sistemas desatualizados se tornam vulneráveis diante de novas ameaças de contaminação e invasão de sistemas.

2. Ameaças à segurança de dados e sistema

Os sistemas de informação de uma prefeitura municipal devem ser protegidos de modo a não haver pontos vulneráveis e riscos. Servidores de páginas, servidores de bancos de dados e servidores de arquivos, por exemplo, podem sofrer diferentes tipos de ataques por meio das redes, se não houver mecanismos de proteção adequados.

A proteção no perímetro da rede da organização contra a transferência indevida de dados entre a Internet e a rede interna deve se dar pelo uso do *Firewall*[3] e de outros sistemas, como o IDS (*Intrusion Detection System*) e o IPS (*Intrusion Prevention System*), que fazem a verificação dos dados que chegam à rede em busca de possíveis ameaças. Todos esses sistemas e outros podem estar reunidos em uma solução de segurança sofisticada que reúne *software* e *hardware* e que é chamada *Appliance UTM*[4].

Existem, ainda, outros tipos de perigos e ameaças aos sistemas de informação para os quais as organizações devem voltar sua atenção. Como perigos relativos à segurança física, podem ser destacados incêndios e inundações, instalações inadequadas para equipamentos e falta de controle de acesso de pessoas, dentre outros. Como segurança lógica, há que se considerar questões como *softwares* e sistemas desatualizados ou defeituosos, os ataques cibernéticos e a contaminação por *softwares* maliciosos (*malwares*), como vírus[5], *worms*[6], *spywares*[7], *keyloggers* [8], *ransomware* [9], dentre outros. Existem, ainda, as ameaças decorrentes da ação humana, como sabotagem, inobservância de regras e fraudes.

3. Segurança da Informação no Ambiente de Trabalho

Na prática, a segurança da informação visa proteger as instituições e as pessoas contra as possíveis ameaças cibernéticas. Por exemplo, no que tange à confidencialidade, as políticas de segurança definidas devem garantir o acesso restrito aos sistemas e dados, portanto, o acesso se dará somente por pessoas autorizadas devidamente cadastradas e identificadas. Na sequência, seguem alguns recursos e políticas aplicáveis para o estabelecimento da segurança de dados nas organizações:

[3] Sistema que, por meio de regras pré-definidas, controla o tráfego entre redes distintas ou em um determinado computador, de modo que somente o tráfego autorizado prevaleça.
[4] UTM (*Unified Trheat Management*) Unified Threat Management – Central Unificada de Gerenciamento de Ameaças.
[5] *Software* malicioso que pode infectar programas para realizar ações indesejáveis e de risco para o usuário. Podem se propagar de diversas formas, como pelas redes.
[6] *Malware* que é capaz de se propagar através das redes.
[7] *Software* utilizado para coletar informações sobre o usuário em determinado computador e enviá-las para um destinatário por meio das redes, sem que o usuário tenha conhecimento.
[8] Programa que registra o que o usuário digita.
[9] *Software* instalado por criminosos em um computador para bloqueá-lo até que se pague um "resgate".

3.1 Controles Aplicáveis

Para controle o de acessos, as organizações devem exigir o uso de crachás, instalar catracas e usar outros recursos para garantir que somente pessoas autorizadas possam entrar em locais restritos, inclusive as áreas de TI.

Ao contratar funcionários, o setor de RH deve observar todas as questões relativas ao histórico e perfil dos candidatos, como antecedentes criminais e outros itens.

3.2 Firewall

O *firewall* é um sistema de controle essencial nas organizações. Este sistema, que pode ser construído na forma de *software* ou de um equipamento dedicado, implementa a segurança utilizando regras e controles sobre os dados que podem passar de uma rede a outra e determina que conexões podem ser estabelecidas. Em um computador comum ou em um servidor, controla também que dados podem entrar e sair.

3.3 Antivírus

Os sistemas antivírus têm como objetivo detectar e destruir os *malwares* que possam infectar determinadas máquinas. Para a proteção contra esse tipo de *software*, é preciso utilizar sistemas antivírus. Dentre os sistemas de proteção disponíveis no mercado, podem ser citados o Bitdefender <www.bitdefender.com.br>, McAfee <http://www.mcafee.com/br/index.html>, Norton <http://br.norton.com/>, AVG <http://www.avg.com/>, dentre inúmeros outros.

4. Política de Segurança da Informação

Para assegurar a segurança da informação nas empresas, torna-se essencial a elaboração da PSI que, segundo Beal (2008), é um documento que registra os princípios e as diretrizes de segurança adotados pela organização. Para a implantação de uma PSI é fundamental que haja a aprovação da direção do órgão ou empresa, que deverá apoiar totalmente o projeto.

Ao se identificarem os riscos para a segurança da informação, em determinado contexto, é necessário determinar quais medidas de segurança serão implantadas, para que haja uma diminuição desses riscos. Na PSI, portanto, essas questões deverão estar contempladas. É necessário designar um gestor para cuidar da implantação da PSI e para realizar a gerência da segurança. Nesse contexto, Beal (2008, p. 47) ressalta

> o item 3.1.2 da ISO 17799 recomenda a designação de um gestor responsável pela manutenção e análise crítica da política de segurança, de modo a garantir que qualquer mudança que venha a afetar a avaliação de risco original dispare uma nova análise crítica do documento.

Há que se considerar, na elaboração da PSI, os aspectos de conformidade legal, o atendimento a padrões vigentes e a adequação à realidade da organização. A conformidade legal está relacionada a estabelecer procedimentos segundo leis, normas e requisitos de segurança, lembrando, ainda, que

> políticas, padrões e procedimentos são criados para garantir que a organização atenda aos requisitos legais e às obrigações contratuais para com seus clientes, acionistas, funcionários e demais colaboradores (FONTES, 2012, p. 08).

O setor responsável pela implantação da segurança no âmbito de qualquer tipo de organização prestará conta de suas ações à gerência ou diretoria a que está subordinado hierarquicamente, considerando o organograma vigente.

Nesse cenário, o uso adequado de formulários, relatórios e demais documentos

torna-se essencial, inclusive para que pesquisas regulares sobre o andamento e o progresso das ações voltadas para a segurança possam contribuir para a obtenção de bons resultados organizacionais.

5. *Análise do ambiente informatizado da prefeitura*

Na prefeitura na qual se desenvolveu a pesquisa correspondente ao presente estudo, foi realizado o levantamento de informações, através de entrevistas, que foram realizadas com os responsáveis pelo Departamento de Planejamento e Informática. Durante a pesquisa, foi possível verificar qual é atual situação do setor de TI daquela instituição no que se refere aos sistemas de segurança. Verificou-se que os recursos existentes são primários em se tratando de segurança de dados e informações. Como exemplo, tem-se o fato de que os sistemas de proteção contra vírus são todos gratuitos, sem as características e funcionalidades de sistemas corporativos.

Em termos da infraestrutura de TI da prefeitura, verificou-se a existência de uma rede local com cabos de rede de par trançado, categoria 5, uma suíte[10] e uma rede sem fio (*wireless*) com segurança implementada no roteador[11] por criptografia de dados[12]. Essa última atende a uma área específica da prefeitura, o Gabinete Municipal. O departamento de informática conta com um servidor de arquivos[13] e um servidor de banco de dados. São cinquenta as máquinas de usuários e doze impressoras em rede. Há também um servidor de nota fiscal eletrônica, um servidor de controle de acesso à Internet, com *firewall* implementado na forma de *software*, e um servidor de monitoramento e segurança audiovisual.

Estão disponíveis, na prefeitura, dois *links* de Internet dedicados de 10 Mbps e um servidor de *Proxy* com gerenciamento de endereço físico das máquinas para o controle do acesso à Internet.

São utilizadas plataformas de sistema operacional Windows 2008 nos servidores Server e Windows 7 Professional nas máquinas clientes. Nos servidores, há um sistema de *backup* que destina os dados copiados para três unidades de discos separadas, de locais físicos distintos. A prefeitura possui *firewall*, IDS e IPS implementados na forma de *software* em um servidor dedicado.

6. *Proposta de Implantação de Sistemas de Segurança na Prefeitura*

Como primeira proposta de melhoria da segurança de dados e sistemas apresentada à administração da prefeitura municipal visitada especificou-se um equipamento de proteção do tipo Appliance UTM, sendo que o seu dimensionamento será feito em fase futura do presente projeto. A partir desse dimensionamento, a prefeitura poderá iniciar a elaboração de um edital para, posteriormente, realizar um processo de licitação.

Para que o projeto de reestruturação da segurança de dados na prefeitura municipal seja eficientemente implantado, será necessário o envolvimento de todos os setores daquele órgão. Todos devem estar comprometidos com a PSI que será implantada.

[10] Equipamento que interconecta os computadores de uma rede.

[11] Equipamento que interliga diferentes redes.

[12] Codificação de dados feita para que apenas o emissor e o receptor da informação possam decifrá-la.

[13] Nele ficam armazenados os dados dos usuários e da empresa. Por esse servidor, cada usuário é identificado para o uso dos sistemas.

UNIUBE
UBERABA Campus Centro - Av.Guilherme Ferreira, 217 - Bairro Centro - CEP: 38.010-200 - Telefone: (34) 3319-6600
Campus Aeroporto - Av.Nenê Sabino, 1801 - Bairro Universitário - CEP: 38.055-500 - Telefone: (34) 3319-8800
UBERLÂNDIA Campus Rondon - Av.Rondon Pacheco, 2000 - Bairro Lídice - CEP: 38.408-015 - Telefone: (34) 3292-5600
ARAXÁ Unidade Araxá - Av.Amazonas, 295 - Bairro São Geraldo - CEP: 38.180-084 - Telefone (34) 3612-6840

A prefeitura deverá criar, ainda, o cargo ou a função de *Security Officer* [14], que será assumido por aquele que ficará responsável pelo departamento da segurança da informação.

Deverão ser realizados treinamentos com as equipes do setor de TI que serão responsáveis pela segurança, a serem ministrados por especialistas.

Para a segurança nas máquinas dos usuários deverá ser adquirido um sistema de antivírus corporativo, para que todas as estações sejam devidamente protegidas contra a contaminação e a ação dos *malwares*.

A implementação de aplicativos para a automatização de *backups* de dados também será feita com o objetivo de diminuir o risco da perda de dados e de paralisação de algum setor da prefeitura por falha dos sistemas de informação.

7. Considerações finais

A prefeitura municipal na qual se realizou o estudo está apoiando o projeto de reestruturação da segurança, tanto no que se refere à PSI quanto ao investimento em recursos de segurança adequados. Assim, passou a priorizar os investimentos necessários e a formação de equipes, visando garantir segurança aos sistemas de informação. Há que se garantir, portanto, o atendimento aos padrões de segurança adotados, inclusive para que os responsáveis pela área de TI e a gestão municipal estejam devidamente resguardados.

Referências

BEAL, Adriana. **Segurança da Informação:** Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas S.A., 2008. 175 p.

BRASÍLIA. Benjamim Zmyler. Secretaria de Fiscalização de Tecnologia da Informação (Ed.). **Boas Práticas em Segurança da Informação.** 4. ed. Brasília: Tribunal de Contas da União, 2012. 108 p. Disponível em: <http://security.ufpb.br/menu-de-relevancia/boaspraticassi.pdf/@@download/file/boaspraticassi.pdf>. Acesso em: 24 de abr. 2016.

FONTES, Edison. **Políticas e normas para a segurança da informação.** Rio de Janeiro: Brasport, 2012. 288 p.

SEGURANÇA da **Informação para Empresas:** soluções simples e grandes resultados**. FECOMERCIO.** São Paulo: Fischer2, 2014. 48 p. Disponível em: <http://www.coaliza.org.br/wp-content/uploads/2014/05/Cartilha-Segurança-da-Informação-para-pequenas-empresas.pdf>. Acesso em: 20 de mai. 2016.

SILVA, Raquel Fonseca da; PEREIRA, Júlio César. **Identificando vulnerabilidades de segurança computacional.** 2013. 5 f. TCC (Graduação) - Curso de Sistemas de Informação, Universidade Paranaense, Paranavaí, 2013. Disponível em: <http://web.unipar.br/~seinpar/2013/artigos/Raquel Fonseca da Silva.pdf>. Acesso em: 15 maio 2016.

[14] Profissional responsável por administrar a política de segurança que será aplicada ao sistema.