SEGURANÇA DA INFORMAÇÃO

Adrielle Fernanda Silva do Espírito Santo

Departamento de Ciência da Computação - Instituto Cuiabano de Educação (ICE)

Caixa Postal 78.065-130 – Cuiabá – MT – Brasil

adrielle.espiritosanto@gmail.com

Abstract. With the increasing number of information technology and the rapid spread of it also increased the crimes related to it and it became necessary to keep the information free of business risks and hazards that might damage it, so research on this subject is to seek more knowledge and get to understand the importance of implementing information security in enterprises. So the problem is, why bother with the data security of your company? To solve this problem we resort to consultation of bibliographical references, which we seek through analysis, ideas, suggestions and arguments that help us in this reflection.

Resumo. Com o crescente aumento das tecnologias de informação e com a rápida disseminação dela, cresceu também os crimes relacionados a ela e surgiu a necessidade de manter as informações das empresas livre de riscos e perigos que possam danificá-la; portanto pesquisar sobre este assunto é buscar maior conhecimento e assim conseguir entender a importância de implantar a segurança da informação nas empresas. Portanto o problema é, por que se preocupar com a segurança dos dados da sua empresa? Para resolver este problema recorremos a consulta de referências bibliográficas, onde por meio de análise buscamos, idéias, sugestões e argumentos que nos ajudem nesta reflexão.

Segurança da informação

Atualmente a informação é arma estratégica em qualquer empresa e também é um recurso de vital importância nas organizações. A segurança da informação é um recurso que tem por finalidade proteger e também é uma forma de gestão. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos." [BLUEPHOENIX, 2008].

A informação está em toda a parte e pode ser armazenada em papéis impressos, eletronicamente em ficheiros e banco de dados, em imagens ou vídeos e até em conversas entre os funcionários. Porém só é reconhecida a importância da informação quando é destruída, perdida ou até roubada. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" [DAVIS, 1997 APUD BLUEPHOENIX, 2008]. Custo nesta citação significa apurar o valor das perdas tanto em dinheiro quanto na reputação da organização, na confiança e em outros valores que a organização mantém como princípio de sua missão como empresa.

Para se implantar um projeto de segurança da informação em uma organização é preciso primeiramente estabelecer as diretrizes, mecanismos de segurança, políticas e procedimentos, ferramentas de proteção e autenticação, e a sua relação custo beneficio. Estabelecer o nível de segurança é fundamental. Este nível de segurança deve garantir que cada funcionário só poderá acessar o conteúdo que lhe é permitido; por exemplo um contador ele deve ter acesso apenas ao conteúdo de informação que faz parte do seu trabalho e não poderá acessar um dado que for de outro departamento que não tenha nenhuma relação com as funções na qual ele desempenha. O que este exemplo demonstra é que a informação tem que estar segura e disponível apenas a quem esteja autorizado. "Em termos organizacionais, a informação tem um papel vital no que diz respeito à gestão, à organização e subsistência das entidades. O valor que a informação representa não é mensurável e a sua perda pode resultar em paragens, produtividade, desorganização e instabilidade."[BLUEPHOENIX, 2008].

Para a montagem desta política, deve-se levar em conta:

- Riscos associados à falta de segurança;
- Benefícios;
- Custos de implementação dos mecanismos.

Os riscos associados à falta de segurança é o que pode ser perdido por exemplo com um bug em seu banco de dados, os hackers podem se beneficiar destas falhas e conseguir se infiltrarem no sistema da organização. Dentro do sistema da empresa eles tem acesso a todos a dados relacionados à empresa, bem como dados de seus clientes. Por esse fato para adotar uma política de segurança da informação deve-se levar em conta isso. Além de fatores naturais como incêndios, inundações, terremotos.

Os benefícios esperados são evitar vazamentos, fraudes, espionagem comercial, uso indevido, sabotagens e diversos outros problemas que possam prejudicar a empresa. A segurança visa também aumentar a produtividade dos funcionários através de um ambiente mais organizado e viabilizar aplicações críticas das empresas.
Os custos de implementação dos mecanismos variam de acordo com o que a organização pretende implementar.

Vulnerabilidades, Perigos e Ameaças à Segurança

As ameaças a segurança podem ser de diferentes formas como incêndios, inundações, falhas de energia, sabotagem, vandalismo, roubo, e outros. O uso da Internet nas organizações trouxe novas vulnerabilidades na rede interna. Se não bastassem as preocupações existentes com espionagem comercial, fraudes, erros e acidentes, agora as empresas também precisam se preocupar com os hackers, invasões, vírus e outras ameaças que penetram através desta nova porta de acesso. Os sistemas de informação, as redes de computadores, os bancos de dados, sistema de energia e comunicação são um dos pontos de vulnerabilidade e risco. Para obter segurança em uma aplicação para Internet ou Intranet, é preciso cuidar de quatro elementos básicos:

- Segurança na estação (cliente);
- Segurança no meio de transporte;
- Segurança no servidor e
- Segurança na Rede Interna.

Segurança na estação

No uso de Internet e Intranet, um dos elementos mais vulneráveis sem dúvida é a estação de trabalho. As estações dos usuários podem armazenar chaves privadas e informações pessoais na maioria das vezes sem proteção ou controle de acesso. Estações de trabalho estão ainda sujeitas a execução de programas desconhecidos sendo expostas a grampos de teclado e outras armadilhas de ganho de acesso.

Segurança no meio de transporte

Um método usado para garantir a privacidade e a integridade das informações enviadas pela Internet / Intranet, é a segurança no meio de transporte. A segurança nos meios de transporte faz uso de algumas tecnologias como firewalls, criptografia, e outros. A criptografia é uma ferramenta fundamental para garantir que a informação chegue ao seu destino sem que alguém sem ser o destinatário faça uso da informação. A criptografia está sendo utilizada frequentemente nas empresas para manter a segurança no correio eletrônico. A criptografia resguarda a privacidade e integridade das informações que circulam na Internet ou Intranet, além de garantir a validade e a autenticidade das mensagens, remetentes e destinatários. A criptografia transforma as informações em textos que são impossíveis de serem compreendidos enquanto a informação não chegou em seu local de destino, quando a informação está no seu destino torna compreensivo para seu remetente, por isso é uma ferramenta de alta segurança. Uma aplicação muito interessante para as empresas é a possibilidade de interligar via Internet as matrizes com suas filiais distantes. "Uma solução simples e segura para este problema é a VPN (Virtual Private Network) que utiliza encapsulamento e túneis de criptografia para trafegar informações de forma segura através de meio público (Internet).” [ISTF, 2009]. Porém a VPN é um recurso que as empresas devem tomar muito cuidado pois a ela interliga a rede interna com um funcionário que possa estar em qualquer lugar, tornando frágil o sistema da empresa.

Segurança nos servidores

O uso de Internet / Intranet exige ainda segurança nos servidores das empresas. As empresas têm conectado sua rede interna à Internet, mas, não gostariam de conectar a Internet à rede interna. Para isto, torna-se necessário o uso de firewalls que protegem o acesso através de um servidor de controle no ponto único de entrada/saída dos dados.

O uso de firewall controla os serviços e acessos permitidos, monitora o uso e tentativas de violação e protege contra invasões externas embora, exija ainda avançados conhecimentos técnicos devido a sua complexidade de uso e configuração. Um serviço bastante utilizado pelas empresas para avaliar a segurança de seus servidores são os testes de invasão. Este serviço busca normalmente identificar falhas de segurança nos servidores das empresas, informando os pontos de vulnerabilidade e recomendando ações de melhoria ou correções dos problemas. Estes testes devem ser realizados por empresas de confiança sendo fundamental o acompanhamento constante de um responsável da empresa contratada.

Segurança na Rede Interna

A segurança deve prever a proteção e controle da Rede Interna. O modelo atual para segurança das redes tem assumido que o inimigo; está do lado de fora da empresa enquanto que dentro, todos são confiáveis. Porém, sabemos que a maior parte dos problemas ocorre em função de ameaças internas. Uma solução completa abrange:

- Política de Segurança Corporativa com definição clara das diretrizes, normas, padrões e procedimentos que devem ser seguidos por todos os usuários;
- Programa de treinamento e capacitação dos técnicos e usuários;
- Recursos e ferramentas específicas para a segurança, e
- Monitoração constante da intranet; e trilhas de auditoria.

Pontos de controle de segurança

Após identificar os riscos, determinar os níveis de proteção e determinar as conseqüências que os riscos podem causar, deve-se implementar os pontos de controle para garantir que os riscos sejam reduzidos a um nível aceitável, já que não existe a total garantia de eliminação dos riscos.

Os controles podem aplicar-se a diversos pontos, na seguinte forma:

"1. Políticas de Segurança da informação;

2. Organização da Segurança da Informação;

3. Gestão e Controle de Ativos;

4. Segurança em Recursos Humanos;

5. Segurança Física e do Ambiente;

6. Gestão das Operações e Comunicações;

7. Controle de Acessos;

8. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação;

9. Gestão da Continuidade do Negócio;

10. Conformidade Legal." [BLUEPHOENIX, 2008].

As políticas de segurança da informação servem para dar suporte a todo o planejamento sobre o que vai ser implantado, sobre como deve agir cada integrante da corporação, como será abordada a política de segurança na empresa, etc. Políticas de segurança são geralmente construídas a partir das necessidades da organização e

aperfeiçoadas pala experiência do gestor de segurança da informação que deve transformar seu trabalho em algo prático, objetivo e que tenha valor corporativo. "Cada organização deve estabelecer quais políticas serão utilizadas tendo como base suas necessidades, requisitos legais, cultura interna e sistemas informatizados." [FERREIRA, ARAÚJO , 2008, 34].

Organização da segurança da informação são as medidas tomadas pelo gestor de segurança da informação na empresa, as formas pelas quais ele organiza as medidas a serem implantadas na corporação para que a empresa possa estar em segurança. "As responsabilidades pela segurança da informação são atribuídas aos funcionários e colaboradores através de ações realizadas pela área de Recursos Humanos." [SANTANDER, 2009].

"Ativo é qualquer coisa que tenha valor para a organização." [RIO DE JANEIRO, 2010]. Gestão e controle de ativos são as medidas de controle e prevenção tomadas pelo gestor de segurança da informação que visa gerir e controlar o acesso de funcionários, bem como definir o que cada profissional pode acessar de informação da empresa. Uma gestão de ativos de qualidade deve seguir essas três características:

- Deve existir um inventário de ativos;
- Para cada ativo deve ter um profissional responsável;
- Deve existir uma política de classificação da informação, ou seja, classificar em importância as informações.

Segurança em recursos humanos: "As responsabilidades pela segurança da informação são atribuídas aos funcionários e colaboradores através de ações realizadas pela área de Recursos Humanos."[SANTANDER, 2009]. O gestor de segurança da informação deve estabelecer em conjunto com o departamento de recursos humanos as seguintes diretrizes; a realização de análises de idoneidade pessoal e profissional das pessoas que pleiteiam uma vaga na empresa; definir uma política de confidencialidade ou código de ética entre trabalhadores e organização; realizar treinamentos em segurança da informação para todos os funcionários e não apenas para os profissionais de tecnologia da informação; definir uma política que dê acesso a funcionários ativos e que solicite a remoção de profissionais desligados da empresa.

Segurança física e do ambiente são os recursos que regulamentam tanto o controle de acesso, quanto a prevenção de sinistros como tempestades, furacões, terremotos, acidentes,

roubos, e outros. São medidas que previnem a empresa contra qualquer ocasião em que possa acontecer a perda, dano ou extravio de informações da empresa.

Gestão das operações e comunicações "Vale lembrar que a comunicação é um fator crítico de sucesso para a correta disseminação das políticas corporativas, já que esta provoca alteração no status quo de praticamente todos os colaboradores. Consequentemente obriga a mudanças na forma de trabalho e qualquer mudança gera resistência, sendo a comunicação a melhor maneira de reduzir os conflitos inerentes a ela."[FERREIRA, ARAÚJO, 2008, 32].

Controle de acesso são as medidas tomadas pelo gestor de segurança da informação que visam controlar o acesso por permissões tanto aos sistemas computacionais da organização quanto ao de pessoas no ambiente da empresa. " O controle de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria (accounting). Neste contexto o controle de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). Com a autenticação é possível identificar quem acessa o sistema, a autorização determina o que um usuário autenticado pode fazer, e a auditoria diz o que o usuário fez."[WIKIPEDIA,2009].

Aquisição, desenvolvimento e manutenção de sistemas de informação é a aquisição dos mecanismos fundamentais ao funcionamento do projeto, bem como a sua manutenção preventiva e frequente, além de melhorias no projeto. A manutenção da política deve ser uma orientação para o estabelecimento de um processo de revisão periódico e formal.

Gestão da continuidade do negócio é o planejamento de como será a segurança da informação nos anos seguintes da implantação e principalmente a longo prazo. Tem por finalidade permitir com que não haja interrupção das atividades da empresa e protege os processos críticos contra falhas significativas e assegura a retomada da empresa em um tempo consideravelmente rápido. Uma boa gestão de continuidade deve ter os seguintes processos:

- Realização de análises de risco no âmbito do plano de continuidade do negócio;
- Desenvolvimento, revisão e testes no mínimo anualmente no âmbito do plano de continuidade de gerenciamento de pessoas dentro da organização;
- Desenvolvimento, revisão e testes no âmbito do plano de continuidade no gerenciamento de tecnologia da informação.

Conformidade legal são controles destinados a tratar as leis, normas e requisitos de segurança. "A conformidade da organização com os requisitos legais (leis, regulamentações, estatutos, etc.) garante uma confiabilidade e o comprometimento da organização junto aos órgãos regulatórios." [SANTANDER, 2009]. Um processo de conformidade legal deve cumprir os seguintes requisitos:

- Garantir o cumprimento das leis e outras legislações vigentes;
- Zelar pelos direitos de propriedade de todos os aplicativos de informática da empresa;
- Consultar uma auditoria para verificação de pontos críticos de melhorias no ambiente da empresa.

"Tenho observado que a maioria dos problemas de segurança da informação ocorrida em organizações está relacionada a um conjunto básico de falhas na implantação e desenvolvimento do processo de segurança da informação." [SILVA, 2008].

Estão citados aqui segundo SILVA, 2008 os dez principais erros cometidos pelos gestores de segurança da informação os quais se devem prestar muita atenção para que não ocorra dentro da sua empresa.

1. A falta de políticas;
2. A falta de uma gestão de controle de acesso;
3. A falta de um gestor da informação;
4. Não cumprir os planos de continuidade;
5. Falta de registros das ações realizadas;
6. Cópias de segurança;
7. A falta de um gestor de processo de segurança;
8. A falta de uma gestão de risco;
9. A não existência de um paralelo entre a segurança e o negócio;
10. Funcionário pouco treinado e não conscientizado.

A falta de políticas de segurança da informação dentro de uma organização é um erro muito grave, pois o gestor de segurança não tem como ter controle sobre as medidas que ele está tomando dentro da empresa. A existência de uma estrutura de políticas, normas e procedimentos a serem seguidos existem para explicar como a organização deseja que o recurso informação deva ser tratado.

Uma gestão de controle de acesso para uso comum é ter controle sobre qual funcionário acessou a informação, essa medida é muito importante porque é possível controlar o acesso a informação e o descumprimento dela implica em que o sistema está falho, pois, qualquer funcionário pode ter acesso a ela sem necessidade de se identificar. Para ter controle sobre a informação deve-se colocar senhas de acessos para que somente o usuário permitido tenha disponível essa informação.

Não ter um gestor de segurança da informação torna ainda mais complicada a implantação dela, e é vital para o sucesso do processo de segurança da informação a existência de um gestor da informação. É ele o responsável por autorizar ou negar o acesso dos demais usuários da empresa àquela informação.

Não cumprir os planos de continuidade engavetando ou deixando-os desatualizados torna as metas de segurança falhas, pois, deve se manter atualizados os planos de continuidade para que a segurança possa ser eficiente e assim conseguir os objetivos que a empresa espera.

A falta de registros sobre as ações realizadas é uma falha grave, pois se deve guardar registros para possíveis investigações de auditoria onde é preciso ter arquivos para poder efetuar a auditoria. Esses registros devem ter seu tempo de duração quando forem arquivados.

As cópias de segurança devem existir para que em situações de perda possam ser recuperadas facilmente, cumprimento de requisitos legais, para ter informações sobre o histórico da empresa e para possíveis auditorias.

Um profissional especializado deve ser responsável pelo processo de segurança da informação e seu funcionamento, e outros. A falta de um gestor de processo de segurança pode pôr todo o processo de implantação da segurança da informação a perder, por isso um profissional deve ser responsável pela existência do processo de segurança da informação. Empresas de médio e grande porte podem ter um funcionário dedicado a esta função, evidentemente desde que ele tenha os pré-requisitos para a mesma.

Uma gestão que previna uma empresa sobre possíveis erros não pode ser deixada de lado, pois é de fundamental importância para o sucesso da implementação da segurança na organização.

Os princípios da segurança devem complementar com as normas já vigentes na

empresa e não competir com elas. A segurança da informação não deve atrapalhar o funcionamento da organização e deve existir um paralelo entre a segurança e o negócio para não dificultar os processos da corporação. Se a segurança da informação está atrapalhando o funcionamento da empresa deve ser revisto as diretrizes da segurança para não afetar o negócio.

As empresas devem adotar medidas para qualificar seus funcionários sobre o que vai ser implantado na organização, como será implantado e como o funcionário deve agir de acordo com as novas regras que devem ser seguidas. Por esse fato deve-se treinar e conscientizar o funcionário como será o funcionamento da organização com as normas de segurança da informação que passou a vigorar na empresa.

Conclusão

As empresas têm que estar um passo a frente das pessoas mal intencionadas e se precaver de forma que seus dados, suas informações não sejam colocadas em perigo. A segurança da informação deve ser usada como arma estratégica para as organizações, pois seguindo as normas da segurança da informação, é possível manter as informações de forma segura e idônea, reduzindo bastante os riscos de perda, extravio ou roubo de informações. Enfim vivemos na sociedade da informação, onde quem tem maior conhecimento ou mais informação sai na frente, além de que a informação é arma estratégica em todas as empresas, portanto se uma organização quer ter suas informações livre de riscos e perigos; deve se precaver usando técnicas de segurança da informação como medidas de prevenção contra possíveis ataques à empresa.

Referências

ALBERTIN,Alberto Luíz; SANCHEZ,Otávio Próspero. “Outsourcing de ti”. Rio de Janeiro : FGV, 2008.

BLUE PHOENIX. “Boas práticas de segurança”. Disponível em: www.bluephoenix.pt. Acessado em: 15/05/2010.

CARVALHO,João Antônio. “Informática – ESAF”. Rio de Janeiro : Elsevier,2007.

CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO - PRODERJ. “Diretrizes gerais de segurança da informação”. Disponível

em: http://www.proderj.rj.gov.br/Poltica%20de%20Segurana%20da%20Informa%20o.pdf. Acessado em: 20/05/2010.

“Controle de acesso”. Disponível em: http://pt.wikipedia.org/wiki/Controle_de_acesso. Acessado em: 15/05/2010.

CRASH. “Segurança da informação”. Disponível em: http://www.istf.com.br/vb/gestao-da-seguranca/4417-seguranca-da-informacao.html. Acessado em:15/05/2010.

FERREIRA, Fernando Nicolau Freitas . ARAÚJO, Márcio Tadeu de. “Políticas de segurança da informação - Guia prático para elaboração e implementação”. Rio de Janeiro: Ciência Moderna, 2008.

OLIVEIRA,Rogério Amigo de. “Informática”. Rio de Janeiro : Elsevier, 2007.

POLLONI,Enrico Giulio Franco; FEDELI,Ricardo Daniel; PERES,Fernando Eduardo. “Introdução à ciência da computação”. São Paulo : Cengage Learning, 2003.

RIBEIRO,Bruno; ALBUQUERQUE,Ricardo.” Segurança no desenvolvimento de software”. Rio de Janeiro : Campus, 2002.

SANTANDER. “Principais itens em segurança da informação”. Disponível em: http://www.santander.com.br/document/gsb/seguranca_parceiros_principais_itens.pdf. Acessado em: 25/05/2010.

SILVA, Alexandro. “Dez falhas em segurança da informação”. Disponível em: http://softwarelivre.org/alexos/blog/dez-falhas-em-seguranca-da-informacao. Acessado em: 20/05/2010.

TANAKA,Edson.” Adobe Acrobat 6.0”. Rio de Janeiro : Elsevier, 2004.