ÁREA TEMÁTICA: Inovação e Gestão Tecnológica

FRAGILIDADE NA SEGURANÇA DE INFORMAÇÃO DAS EMPRESAS DE PEQUENO PORTE

AUTORES
ANSELMO FIGUEREDO BARBAES
Faculdade Alfacastelo
anselmotubao@hotmail.com

MARCIO ROGERIO DA SILVA MELO
FACULDADE ALFACASTELO
marcio.melo@chiesibrasil.com.br

MARCOS DE OLIVEIRA MELO
Faculdade de Administração Alfa Castelo
marcosdeoliveiramelo@hotmail.com

RESUMO

O trabalho vem abordar as falhas na segurança da informação e a falta de preocupação com as informações das empresas de pequeno porte onde os gestores não se preocupam em investir recursos financeiros, humanos e tecnológicos para se obter uma estrutura confiável que traga resultados positivos ou ao menos não traga surpresas desagradáveis com perda ou roubo de informações valiosas tanto físicas como lógicas e destruição do hardware da empresa. Deixando bem aparente a falta de segurança (física, lógica e humana) na empresa, as pessoas mal intencionadas aproveitam dessa falha para fazer ataques a fim de prejudicar o bom andamento do negócio com roubo de informações para comercializá-las com os concorrentes ou apenas com a destruição de dados ou ataques a hardwares.

É apresentado também à situação de uma empresa de pequeno porte que no seu dia-a-dia deixa exposto seus dados e a pouca eficiência da troca de informações de uma infra-estrutura mal projetada e falta de especialista em segurança de informação. Buscando resolver os problemas das pequenas empresas que apresentam esse cenário é apresentada uma solução especifica para a situação da empresa apresentada, solução essa que visa à eficiência, confiabilidade dos dados com um baixo custo a fim de estar em acordo com a capacidade financeira da empresa.

Abstract (200 palavras)

The work comes to approach the imperfections in the security of the information and the lack of concern with the information and the structure in the small business companies where the managers if do not worry in investing financial resources, human and technological to get a trustworthy structure that bring resulted positive or to less does not bring ackward surprises with loss or robbery of physical valuable information as in such a way logical and destruction it the hardware of the company. Leaving well apparent the lack of security (physical, logical and human being) in the company, the badly intentioned people use to advantage of this imperfection to make attacks in order to harm the good course of the business with robbery of information to commercialize them with the competitors or only with the destruction of data or attacks hardwares. Also presented to the situation of a small business company that in its

day-by-day leaves displayed its data and to little efficiency of the exchange of information of a badly projected infrastructure and lack of specialist in information security. Searching to decide the problems of the small companies who present this scene a solution is presented specifies for the situation of the presented company, solution this that it aims at to the efficiency, trustworthiness of the data with a low cost in order to be in agreement with the financial capacity of the company.

PALAVRAS-CHAVE

Segurança, Falha, Informação.

1. INTRODUÇÃO E CONTEXTUALIZAÇÃO

A informação, que é um assunto discutido incansavelmente em várias reuniões, abordado como o principal ativo de muitas empresas, nem sempre é tratada de maneira inteligente pelos gestores, principalmente pelos gestores das pequenas empresas que geralmente ocupam todo seu tempo buscando não desaparecer do mercado. Como o foco das pequenas empresas são apenas se sustentar a cada dia para não ser superada pelos concorrentes, assuntos como investimentos tecnológicos e preocupação com a segurança da informação ficam para um segundo plano.

Há alguns anos a informação dentro de uma empresa era centralizada e poucas pessoas tinham acesso a ela, não havia automação e tinha pouco espaço para armazenagem, houve situações de empresas fecharem as portas por conta do falecimento da pessoa que detinham as informações.

Segundo o autor (SÊMOLA, 2003), hoje o compartilhamento de informações é uma prática moderna e necessária para as empresas.

Como o Sistema de informação ainda é considerado muito jovem comparando com outras áreas de conhecimento, é deixado para traz sua importância dentro das pequenas empresas. Cabe ao gestor da empresa ao perceber o assunto envolver toda a empresa e não apenas designar a tarefa da segurança da informação a pessoas especializadas e centradas no assunto.

Dentro das pequenas empresas os recursos são menores e não se tem capacidade de investimento para acompanhar a evolução da tecnologia e manter especialistas em segurança fixos na empresa, mas o mínimo necessário deve-se fazer.

Faz-se necessário fazer uma auditoria na empresa para levantar as falhas na segurança que geralmente estão explicitas aos olhos de um especialista do assunto, embora não seja visível para os gestores porque estão focados em outras áreas como, por exemplo, no Market Share (Participação de Mercado por receita ou quantidade), o mais comum feito por uma auditoria externa é seguir normas e diretrizes estabelecidas, baseadas na NBR ISO/IEC 17799.

O que vem muito ocorrendo entre as pequenas empresas que acabam se deparando com um problema de perda de dados, invasão (física e lógica) e outros tipos de falta de segurança é contratar um técnico muitas vezes não especialista em segurança da informação para aos poucos amenizar o impacto da falta da segurança na empresa, geralmente sem muito sucesso.

Para (BASILIO, 2007), a maioria dos proprietários de pequenas empresas tem uma coisa em comum, eles operam com um orçamento restrito, e freqüentemente não têm dinheiro extra para investir em um novo software.

A falta de recursos e a pouca preocupação com a segurança da informação por parte das pequenas empresas ocasionam grandes perdas, pois a vulnerabilidade exposta implica em situações desastrosas devido aos ataques diários que acontecem na internet.

2. REVISÃO BIBLIOGRÁFICA

Segundo (SÊMOLA, 2003), quando se pratica muitos erros ao pensar na segurança da informação, "provocado pela visão míope do problema e a percepção distorcida da questão", o autor faz uma analogia a um Iceberg que só é visível uma pequena parte como os problemas de segurança.

O autor complementa com alguns pecados cometidos em algumas empresas:

- Atribuir exclusivamente à área tecnológica a segurança da informação;
- Posicionar hierarquicamente a equipe de segurança abaixo da diretoria de TI;
- Definir investimentos subestimados e limitados à abrangência dessa diretoria;
- Elaborar planos de ação orientados a reatividade;
- Não perceber a interferência direta da segurança com o negócio;
- Tratar as atividades como despesa e não como investimento;
- Adotar ferramentas pontuais como medida paliativa;
- Satisfazer-se com a sensação de segurança provocada por ações isoladas;
- Não cultivar corporativamente a mentalidade de segurança;
- Tratar a segurança como um projeto e não como um processo.

Dentre as diversas características de vulnerabilidades das empresas de pequeno porte, encontram-se:

- Pouco investimento em Infra-estrutura;
- Não existe treinamento adequado para os funcionários;
- Falta de política de uso dos recursos;
- Pessoas não comprometidas.

Na visão de (MORAZ, 2006) O ambiente cibernético é palco hoje de um verdadeiro fogo cruzado entre hackers mal intencionados que buscam invadir sistemas e administradores de segurança que têm por função proteger os sistemas e que as empresas devem obter

conhecimentos sobre:

- Defesa e contra-ataque;
- Técnicas hackers de ataque;
- Administração da segurança em redes Wirelles (sem fio);
- Firewalls e segurança dos Sistemas Operacionais;
- Monitoramente e varredura de Redes;
- Segurança e proteção de websites;
- Criptografia de dados confidenciais.

Segundo (FREIRE e MACHADO) há uma grande importância em pensar em seu computador pessoal e cada usuário deve tomar cuidados básicos para evitar invasões existem várias práticas para resguardar seu computador de vírus, worms, cavalos-de-tróia, phishing e outros horrores virtuais, tais como:

Antivírus;

Firewall;

Detector de intrusos;

E outros.

3. ESTUDO DE CASO: EMPRESA "MESTRE DOS PAPÉIS COMÉRCIO DE INFORMÁTICA LTDA"

3.1 Situação Atual

Empresa (MESTRE DOS PAPÉIS COMÉRCIO DE INFORMÁTICA LDTA – Localizada na Rua das Rosas, 74 – Centro - Barueri) do Ramo de comércio varejista de materiais de informática (Hardware e Software) com pouco mais de 30 funcionários e um faturamento médio de R$ 300,000,00 por mês.

Instalada em um prédio alugado foi todo customizado para atender a estrutura da empresa, que está disposta em 3 (Três) andares, sendo 1º andar voltado para atendimento ao consumidor, faturamento e expedição, o 2º andar voltado para estoque e o 3º volta-se a Administração, Departamento Comercial, Assistência Técnica e Diretoria.

A empresa certa infra-estrutura tecnológica:

- 1 Servidor de aplicação, Sistema ERP com BD e um Web Site;
- 20 Computadores;
- Servidor P4 de configuração simples com S.O. Win 2003 Server (montado pelo próprio técnico da empresa).

O servidor da empresa é apenas acessado por pessoas conectadas fisicamente[1] a rede interna da empresa.

O Sistema ERP (Planejamento de Recursos Empresariais - é um software que executa um conjunto de atividades que atendem a necessidade de informações para a tomada de decisões, geralmente desenvolvidos em módulos. Ex: Datasul; Microsiga; SAP – (HABERKORN, 1995) batizado de RIVIERA foi desenvolvido em Visual Basic 6 por um terceiro (pessoa física), este tem o controle total do código fonte, das customizações e do banco de dados. O contrato foi firmado para que esta pessoa compareça apenas uma vez por semana na empresa para acertos e customizações.

Quanto ao Banco de dados Access, foi instalado no mesmo servidor da aplicação, isso trás diversas preocupações para a empresa já que a o software de gestão (ERP) fica todo em poder de um terceiro e em qualquer atualização muitas vezes remota deixam os dados vulneráveis, problemas com capacidade de armazenamento e manutenção também trás preocupação.

A empresa possui um site de apresentação dos produtos, mas sem características de e-commerce (Prática de comércio pela internet). O site esta hospedado em um provedor gratuito.

O sistema e o banco de dados estão instalados em um servidor disposto em um canto reservado da sala da assistência técnica em um Rack que não possui chave. Este servidor está ligado a um Nobreak de apenas 600VA (com autonomia de apenas 20 minutos).

Em relação à senha de acesso aos computadores e ao sistema, funciona da seguinte maneira. Para acesso aos computadores existe apenas uma senha que acessa todos os equipamentos e para acessar o sistema existem apenas duas senhas de acesso para cada departamento, sendo uma para o gerente da área e a outra utilizada pelos outros usuários (situação perigosa, pois torna difícil rastrear uma falha ou situação provocada intencionalmente).

3.2 Projeção Futura, Análise da Solução e Resultados a serem obtidos

O desafio é a implantação de uma solução flexível, eficiente, de baixo custo, com o objetivo de atender a demanda de pedidos por telefone, fax, e-mail, representantes externos e ainda garantir a segurança física e lógica da estrutura de informação.

O projeto desenvolvido pela TAM² (TAM² Soluções Tecnológicas Ltda – Empresa de soluções de tecnologia que atende pequenas e médias empresas) visa resolver as falhas de seguranças da empresa fornecendo soluções (softwares, hardwares, serviços de consultoria, desenvolvimento, treinamento e suporte) existentes no mercado e mudando a cultura dos colaboradores.

A empresa apresenta diversas falhas em segurança de informação tanto as por falta de infra-estrutura como por parte da gestão das informações.

---

[1] A empresa possui um Access point (ponto de acesso) wirelles (equipamento de troca de informação sem fio) apenas para uso de um dos diretores com seu note book quando estiver no prédio da empresa.

Na primeira etapa do projeto pretende-se implantar uma infra-estrutura adequada à necessidade da empresa visando à segurança da informação tanto física como lógica, a conectividade entre os representantes externos e o sistema remotamente, tudo a um baixo custo.

Configuração do acesso remoto E-tam² (Software de acesso remoto ao sistema ERP da empresa), permitindo a ligação, via VPN (Virtual Private Network - rede privativa com acesso restrito construída sobre a infra-estrutura de uma rede pública), dos notebooks dos representantes ao servidor da empresa através de qualquer ponto de acesso a Internet, fazendo que estes ao conectar estejam on-line com o sistema ERP para saber tabelas de preços, posições de estoque, entregas, efetuar pedidos, etc. E que os recursos sejam compartilhados com segurança em localidades geográficas distintas.

Numa segunda etapa do projeto, pretende-se implantar o sistema E-Guardião (solução desenvolvida pela TAM² para monitoramento de acessos e operações) com o objetivo de fornecer total segurança através de um monitoramento de servidores e serviços, assim como o sistema E-localização (solução desenvolvida pela TAM² para localização de frota) que permite clientes e fornecedores visualizar de forma segura, através da Internet, a localização exata de sua carga.

Com a aplicação da tecnologia adequada as empresas de consultoria buscam diminuir as ameaças, invasões e roubos de informações focando o trabalho na segurança física dos equipamentos, segurança da informação, transmissão das informações gerando assim aumento da produtividade, otimização dos processos e negócios e redução dos custos.

4. CONSIDERAÇÕES FINAIS

Temos situações que a informação é mais importante do que o próprio patrimônio imobilizado de uma empresa, principalmente em empresas de pequeno porte onde sua sobrevivência no mercado depende de pequenos detalhes como saber onde adquirir uma matéria-prima diferenciada, de menor custo ou ainda com maior agilidade. Sabendo disso as empresas devem cuidar um pouco mais desses recursos os tornando de maior prioridade dentro da estrutura.

O cuidado com a infra-estrutura e normas de procedimento em uma empresa como apresentado no artigo é fonte de diversos estudos e faz a diferença em um universo competitivo em que estamos nos dias de hoje, porém não se deve perder o foco do objetivo da empresa assim utilizando pessoas especializadas para a gestão da informação não deixando de incluir todos os colaboradores na função da segurança.

5. REFERÊNCIAS BIBLIOGRÁFICAS

BASILIO, Sérgio. **Pequenas Empresas: As últimas a serem protegidas**. Online. Disponível na Internet em 24 de Maio de 2007 na URL http://www.abes.org.br – acessado em 24/05/2007 ás 22:03hs. ABES – Associação Brasileira das Empresas de Software.

FREIRE, Alexandre, MACHADO, André. **Como blindar seu PC.** 1. Ed. São Paulo: Campus, 2006.

HABERKORN, Ernesto. **Teoria do ERP - Enterprise Resource Planning**. 1. Ed. São Paulo: Makron Books, 1995.

MORAZ, Eduardo. **Treinamento Profissional Anti-hacker.** 1. Ed. São Paulo: Digerati, 2006.

SÊMOLA, Marcos. **Gestão da Segurança da Informação.** 1. Ed. Rio de Janeiro: Campus, 2003.