Case ASSERTIVA

Bruno Seiti, Felipe Leitão, João Pedro Libonati

Fase I

**1. Identificar os principais problemas verificados em relação:**

**a) ao setor**

Projetos e inovações são propostos pela TIS. Setor de Tecnologia totalmente terceirizado. A Assertiva fica dependente da TIS para qualquer questão envolvida à TI, sendo que a TIS não tem nenhum compromisso em apoiar as decisões de negócio da empresa, pois o principal objetivo da TIS é com sua própria empresa, assim resultando em perca de tecnologia exclusiva da Assertiva, como aconteceu quando a TIS desenvolveu uma plataforma focada para o processo de negócio da Assertiva, porém, já que a TIS não tem como objetivo principal o sucesso da Assertiva, vendeu a plataforma para outras empresas com objetivo de seu próprio crescimento. Além disso, não há nenhum acordo formal, o que faz com que parceria dependa da confiança para o sucesso do negócio, que, como já visto, é perigoso a TIS com tanta liberdade. A TIS também é responsável pelo suporte técnico aos usuários finais, o que pode comprometer a imagem da Assertiva com seus clientes, caso a TIS preste um mal serviço.

A Assertiva não possui uma estratégia de continuidade de negócios estruturada.

**b) ao ambiente**

Servidores, computadores, celulares, etc. conectados à mesma rede junto ao Wi-Fi (funções críticas e visitantes utilizando de mesma rede), o que causa uma grande aproximação de processos críticos da empresa com uma possível pessoa desconhecida, caso essa pessoa seja uma pessoa mal-intencionada e com um mínimo de conhecimento de redes, os processos da empresa correm sérios perigos. Não possui nenhum tipo de regulamentação interna relacionada ao uso dos recursos de TI, o que pode acarretar vazamento de dados da empresa por causa de um insider, seja por mal intenção ou simplesmente descuido, pois é possível que o insider acesse links ou sites enganosos. Os backups gerados são armazenados na sala dos sócios em cada localidade ao qual pode não ser a opção mais segura de backup, mas para isso são necessárias mais informações sobre a sala dos sócios, pois é possível que dentro tenha algum planejamento de segurança, seja de incêndio, roubo, manutenção, entre outros. Como os softwares instalados nos computadores são antigos, é possível que os computadores sejam de modelos antigos também.

**c) às pessoas responsáveis pelo setor e pelo ambiente**

O gestor de TI não tem formação em TI, o que faz operações críticas para o sucesso da empresa, no caso as de TI, serem gerenciadas por uma pessoa que talvez não seja a mais qualificada para o trabalho, pois a área TI é uma área em alto crescimento, onde novas tecnologias e ameaças estão surgindo a cada momento, talvez seja necessário alguém com um amplo conhecimento da área para prevenir novas ameaças e obsolescência de certas práticas. O PDI existente está desatualizado. Equipe com falta de qualificação em TI, O qual resulta na empresa seguir cegamente as exigências da TIS em questão de recursos de TI, podendo assim com que a empresa gaste desnecessariamente com recursos que podem não agregar ao plano de negócio da empresa.

**d) aos processos empregados**

Freeware executado a cada 3 meses para armazenar arquivos na rede.

**e) às tecnologias empregadas**

Windows 7 (OS sem suporte), Microsoft office 2003 (Pacote de Softwares sem suporte), aplicativos internos desenvolvidos em Visual Basic 4 (versão desatualizada). O principal problema de utilizar sistemas e softwares desatualizados e sem suporte, é que com o passar do tempo o funcionamento do software, ou o sistema, é cada vez mais conhecido, o que resulta em descoberta de falhas, como explorar essas falhas nos sistemas e como utilizar delas de maneira mal-intencionada, assim, utilizar de sistemas desatualizados resulta em uma vulnerabilidade na segurança das informações. Também temos os dados da empresa armazenado em MySQL (banco de dados não adequado para grande armazenamento de dados). Chamados recebidos anotados em fichas eletrônicas, o qual pode resultar em falhas humanas no processo de anotações de chamadas, como, por exemplo, falha de entendimento de um valor, esquecimento no preenchimento de certas informações ou erros de digitação. Usa FTP, um protocolo para conexão com o servidor, sendo que existem opções mais seguras, além de estar em Debian Jessie (Linux desatualizado).

**2. Recomendações**

**a) ao setor**

1. Fazer formalização através de contrato jurídico legal, para evitar depender somente da confiança da TIS.

2. Desenvolver o setor de TI na empresa, para ganhar independência da TIS.

**b) ao ambiente**

1. Separar a rede em 3 rotas: rede do servidor, rede corporativa e outra rede para usar o Wi-Fi.

2. Políticas de segurança: é preciso que tenha políticas de segurança para impedir que hackers façam engenharia social ou algo do tipo. Não há regras para o uso das máquinas, assim, por exemplo, alguém poderia pedir senhas se passando por alguém de confiança e “roubar” informação ou danificar computadores e equipamentos.

3. Os backups devem ser duplicados alocados tanto em nuvem quanto em uma sala confidencial da empresa.

4. Os servidores devem, também, estar em local confidencial.

5. Verificar a potência dos computadores. E se não forem muito recentes, recomenda-se investir em equipamentos novos.

**c) às pessoas responsáveis pelo setor e pelo ambiente**

1. Atualizar o PDI, porque, com o PDI desatualizado, os funcionários perdem o potencial de se desenvolver e se tornarem mais eficientes no trabalho.

**d) aos processos empregados**

1. Fazer rotinas de atualização de software planejados fora do horário comercial ou de pico.

2. Desligar Wi-Fi fora do horário comercial, para dificultar “roubo” de dados.

3. Antes do uso do Freeware deve ser feito um escaneamento para dificultar propagação de vírus pela rede.

4. O suporte deve ser feito tanto remotamente quanto pessoalmente, dependendo do tipo de requisição.

5. Os recursos tecnológicos devem ser avaliados mais profundamente, já que é há diversas variáveis para considerar na compra de equipamento.

**e) as tecnologias empregadas**

1. Padronizar as tecnologias usadas para simplificar a instalação e o gerenciamento dos softwares instalados.

2. Verificar a possibilidade de atualização do Windows instalado na máquina, realizando testes.

3. Adotar um sistema para armazenar os chamados no banco de dados.