Proposta de Consultoria na área de TI ASSERTIVA

Bruno Seiti, Felipe Leitão, João Pedro Libonati

Nós somos da Hentai Lab Corp. East e foi efetuada uma análise do documento sobre a Assertiva enviado a nós. Foi identificado alguns pontos que podem ser melhorados na área de TI da empresa, principalmente de segurança da informação.

**1) O que é Segurança da Informação e sua importância.**

Segurança da Informação é a prática de garantir Confidencialidade, Integridade e Disponibilidade. A segurança máxima não existe, porque conforme o cohecimento sobre a técnologia evolui, novas falhas de segurança vão sendo descobertas. Além disso, não há retorno na Segurança da Informação, mesmo com isso, é importante para qualquer empresa,pois nformação é um ativo, assim, tem que existir processos, uma estrutura (tanto de Infraestrutura quanto de sistemas), concientização dos funcionários para evitar falsificação e vazamento de dados ao máximo, com isso, mitigando perdas financeiras e de imagem.

**2) Segurança da Informação em relação à Assertiva.**

Pelo negócio da Assertiva ser de lidar com dados vaviávies, as informações da Assertiva são o maior ativo da empresa, o que resulta em que se esses dados ficarem comprometidos, seja por vazamento ou pelos dados não estarem de acordo com a realidade, teremos sérios problemas.

Por exemplo, vamos imaginar que um boleto de uns dos clientes se torne público por uma falha da assertiva, isso acarretaria um sério processo judicial para a acertiva, onde nós perderiamos muito por processos e provavelmente também perderiamos o cliente. Agora vamos imaginar se isso ocorreçe para os dados de todos os clientes dos clientes, isso poderia ser o fim da assertiva.

Então é muito importante que haja um plano de segurança da informação para a Assertiva.

Para isso, fizemos uma análise que contempla os três pilares da segurança da informação (Confidencialidade, Integridade e Disponibilidade) e dividimos em 5 temas: setor, ambiente, pessoas responsáveis pelo setor e pelo ambiente, processos empregados e as tecnologias empregadas.

**3) Problemas encontrados, com relação:**

# 3.1) 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.

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 ou por conta de um um funcionário acabe passando informações sem a intenção de danificar a empresa.

As políticas de segurança e de senhas não são citadas, então levamos em consideração que não há, e isso é um problema, uma vez que senhas são usadas para acessar e modificar informações confidenciais e até gerenciar o sistema, em alguns casos.

# 3.2) ao ambiente

Há diversos equipamentos e software listados no documento que dá uma noção de obsolecência, o que é ruim porque não há suporte de segurança para várias dessas tecnologias.

Como os softwares instalados nos computadores são antigos, é possível que os computadores sejam de modelos antigos também. Assim, as máquinas podem não ser compatíveis ou não ter performace suficiente para usar softwares mais recentes.

Topologia: todos conectados à mesma rede 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.

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.

Nada é dito sobre a localização dos servidores. Eles devem estar alocados em um local confidencial, para dar segurança ao funcionamento.

# 3.3) 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 TI, impactando na empresa diretamente, 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 na área para prevenir novas ameaças e obsolescência de certas práticas.

Não há alguém responsável pelo ambiente de TI, assim o ambiente pode ficar desorganizado e não eficaz.

Falta de engajamento, o que faz com que a TI, que está sempre em mudança, se torne frágil e sem rumo.

Os papéis e as responsabilidades não estão bem definidos.

# 3.4) aos processos empregados

Falta de documentação, formalidade e definição dos processos empregados. Isso faz com que todo o trabalho e as operações da empresa que são envolvidas com a TI acabam ficando desorganizadas.

Os chamados recebidos são anotados em fichas eletrônicas, os quais podem 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.

# 3.5) as tecnologias empregadas

Windows 7 (OS sem suporte), Microsoft office 2003 (Pacote de Softwares sem suporte), aplicativos internos desenvolvidos em Visual Basic 4 (versão desatualizada) são alguns exemplos de tecnologias obsoletas. O sistema operacional do servidor é o Debian Jessie (Linux desatualizado).

**4) Possibilidades de melhoria, com relação:**

# 4.1) 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.

3. Políticas de segurança da infromação e uso dos recursos de TI: é preciso que tenha políticas de segurança para impedir que hackers façam engenharia social ou algo similar. Também, concientizar os funcionários sobre a importância da segurança da informação e como garantí-la.

4. Colocar regras para o uso das máquinas porque alguém poderia pedir senhas se passando por alguém de confiança e “roubar” informação ou danificar computadores e equipamentos.

# 4.2) ao ambiente

1. Separar a rede em 3 rotas: rede do servidor, rede corporativa e outra rede para usar o Wi-Fi.
2. Os backups devem ser alocados em uma sala confidencial na empresa e/ou duplicados alocados em nuvem (se for possível, por questões legais). A ideia é possuir alguns locais de backup, podendo até serem espalhados em alguns sites pelo Brasil, assim, caso ocorra algo a algum backup haverá outro seguro.
3. Os servidores devem, também, estar em local confidencial.
4. Verificar a potência dos computadores. E se não forem muito recentes, recomenda-se investir em equipamentos novos.

# 4.3) às pessoas responsáveis pelo setor e pelo ambiente

1. Treinar ou contratar pessoal. É importante que as pessoas responsáveis por TI estejam em um nível alto de conhecimento sobre os temas principais de tecnologia e que esteja sempre se atualizando.

# 4.4) aos processos empregados

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

2. Criar um processo para desligar Wi-Fi fora do horário comercial, para dificultar “roubo” de dados.

3. Criar um processo para fazer backups toda semana, ou todos os dias. É muito importante fazer backups rotineiros para possuir sempre a versão mais atualizada possível de um backup.

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. Assim, deve ter um processo para tomada de decisão feito por algum responsável para as compras do setor de TI.

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

# 4.5) as tecnologias empregadas

1. Padronizar as tecnologias usadas para simplificar a instalação e o gerenciamento dos softwares instalados.
2. Verificar, realizando testes, a possibilidade de atualização para Windows 10 e outros softwares nas máquinas.

Com isso, finalizamos nosso resultado de análise. Esperamos ter ajudado e estamos à disposição.