

UCB

MBA Gestão de Sistema de Informações

Segurança da Informação

**Política de Segurança para e-Commerce
Loja Virtual de Telecartofilia**

Prof.: Ly Freitas

Equipe: Alice Carolina M. Brito

Ana Carolina Lemos

Cristina Aparecida de Abreu

Karina Domingues Bressan Vidal

Mônica Athayde Ferreira

1º Semestre de 2002

1. Introdução

Quando se fala sobre as perspectivas comerciais das transações via Internet para as empresas são comuns projeções como a de que o comércio eletrônico pode movimentar cerca de 30 bilhões de dólares em 2005. Estimativas assim - que alardeiam montantes nada desprezíveis -, a conquista de mercados consumidores promissores, redução de custos operacionais, além da necessidade de não ficar atrás dos concorrentes, são alguns dos atrativos para empresas que apostam no mercado virtual. As inúmeras possibilidades trazidas por esse mundo sem fronteiras vieram acompanhadas de alguns entraves. Ainda falta cultura de segurança em esferas mais altas da administração e é preciso conferir credibilidade às transações de modo que os consumidores tenham mais tranquilidade ao efetuar operações pela rede.

Ataques, invasões e proliferação de novas pragas virtuais deixam os usuários mais alertas sobre questões como privacidade e o uso impróprio de informações pessoais e financeiras. No modelo de e-commerce, onde há uma estrutura de rede muito mais complexa e vulnerável, empresas e respectivos administradores devem atentar para a necessidade de garantir a segurança não somente das redes internas, mas de todos os integrantes da estrutura.

Um estudo da Revista Information Security revela que empresas integradas ao e-commerce têm o dobro de chances de ser atingidas por ataques via web server e 35% a mais de probabilidade de ser alvos de ataques do tipo denial-of-service.

Explicar os riscos que envolvem o comércio eletrônico junto aos executivos tem sido um desafio para muitos profissionais de segurança. Ao perceber a necessidade de ingressar no modelo de e-commerce, em geral são impostos prazos muito curtos para o número de questões que devem ser resolvidas, sendo a segurança muitas vezes erroneamente percebida como apoio ao negócio e não como fator essencial e prioritário ao sucesso das transações eletrônicas.

O presente trabalho tem como objetivo apresentar a política de segurança para um site de e-Commerce. Foi usado como estudo de caso o site de Telecartofilia da BrasilTelecom.

2. Descrição do Negócio

Hoje em dia as empresas estão preocupadas em facilitar a vida de seus consumidores, fazendo com que eles não precisem sair de suas casas ou local de trabalho, para realizar suas compras. Foi pensando assim que foi criada a Loja Virtual de Telecartofilia, que consiste em um site na Internet destinado a colecionadores de cartões telefônicos, onde são apresentados os últimos lançamentos, coleções, séries, e temas sobre os cartões.

O negócio foi concebido com base em pesquisas de mercado e de comportamento do público alvo (coleccionadores). A Loja Virtual de Telecartofilia tem na Internet seu principal canal de vendas, de fidelização e de comunicação, agregando valor à marca. O telecartofilista poderá comprar através da Internet e também pelo 0800 (onde as atendedoras irão fazer o pedido através da Internet);

A seguir são descritos alguns passos que ilustram o fluxo na Loja Virtual de Telecartofilia:

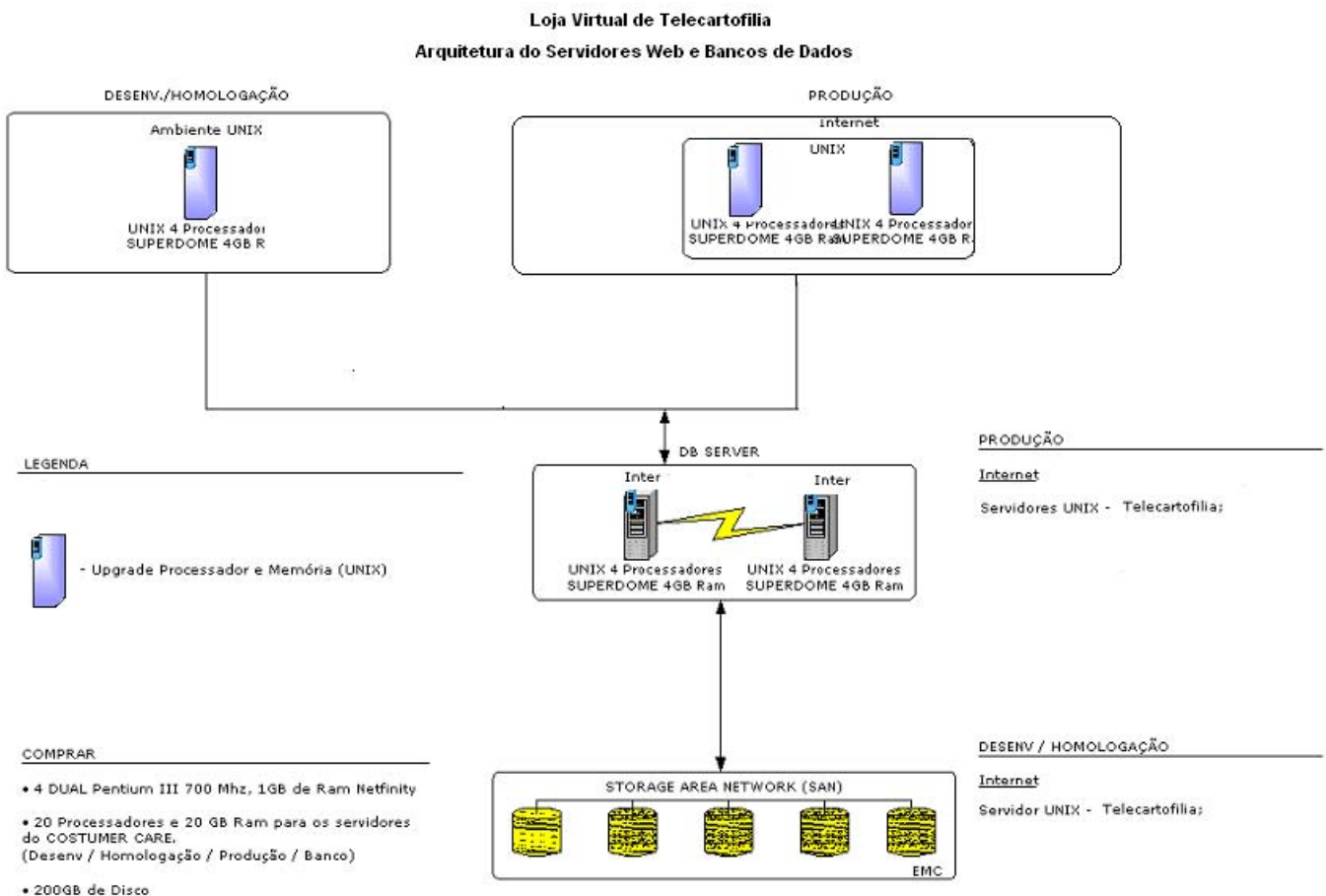
- 1) Pesquisa para visualização dos cartões que o colecionador poderá adquirir;
- 2) Visualização e seleção dos cartões que o telecartofilista queira adquirir;
- 3) Os cartões são exibidos em detalhes maximizados disponibilizando nome identificador da estampa, código, operadora, tiragem, créditos do cartão, preço unitário e demais dados necessários à compra;
- 4) Inclusão do cartão na cesta de compras, onde o telecartofilista seleciona a quantidade de cartões, o tipo do frete e o sistema informa o valor total da compra (botão “comprar”);
- 5) O telecartofilista deverá fazer o seu cadastramento ou inserir login e senha. No cadastramento, através do 0800, a atendente faz o cadastramento e encaminha o login e senha para o telecartofilista pelo correio.
- 6) As formas de pagamento serão cartão de crédito, boleto bancário e débito automático. O colecionador opta pela forma de pagamento e a compra é efetuada e transmitida para a Loja;
- 7) O processo de pagamento da compra será realizado por um sistema de e-payment (empresa de administração de pagamento on line);
- 8) O sistema emite a Nota Fiscal com todos os dados da compra e a mercadoria é encaminhada para o colecionador.

3. Arquitetura do Sistema

O Site de Telecartofilia foi desenvolvido utilizando a ferramenta de desenvolvimento Java - JavaBeans na plataforma UNIX. O servidor Web utilizado para hospedar as páginas do site é o software Apache, software adotado pela BrasilTelecom.

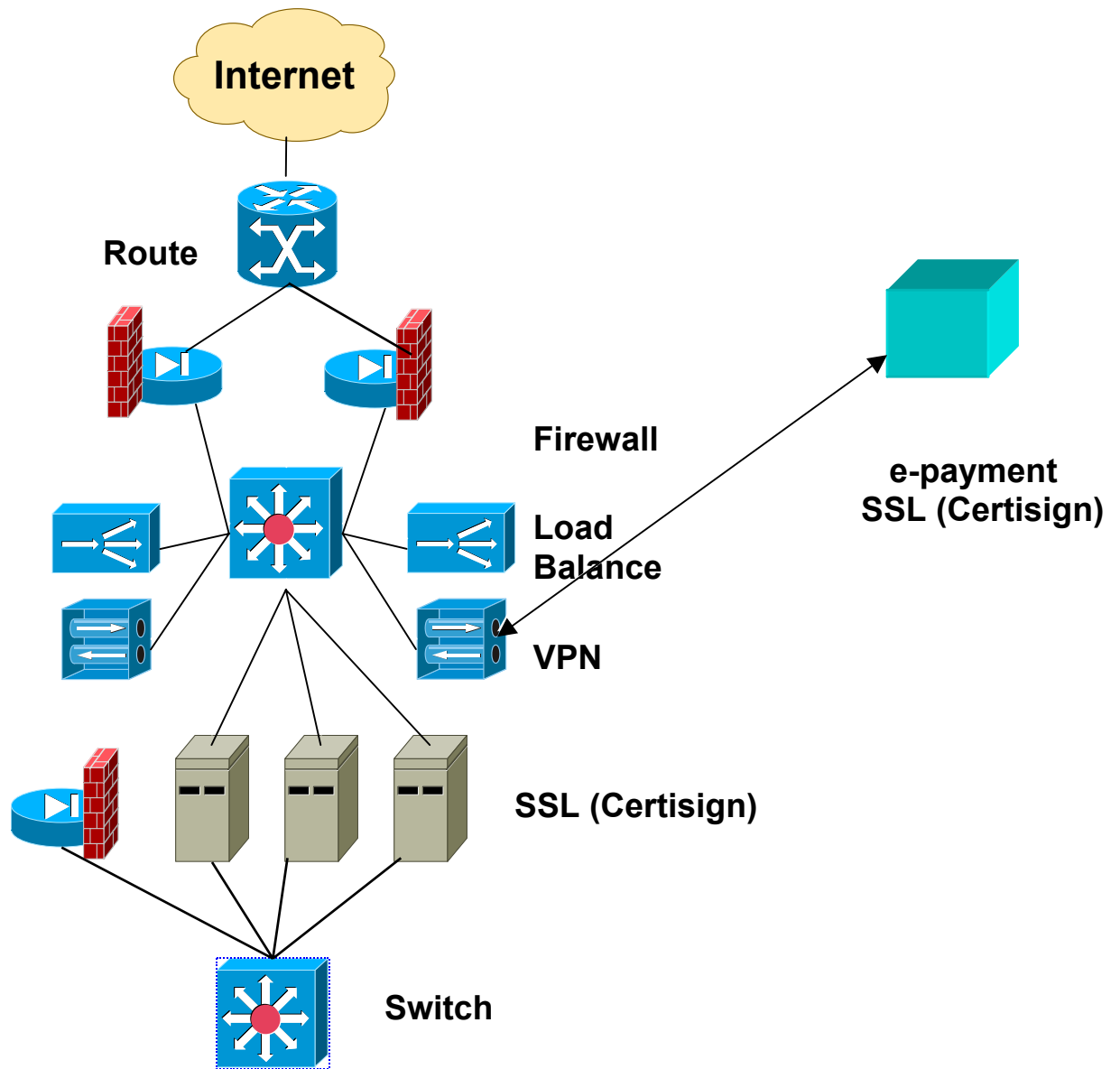
O sistema utiliza o banco de dados Oracle 8i. A aplicação conecta no Banco de Dados Oracle utilizando um driver jdbc (thin Oracle jdbc) contido no pacote classes12.zip, é necessário a instalação do Oracle Client 8.1.7.03.

Arquitetura Física



De acordo com a arquitetura física acima, a rede interna está composta dos servidores de processo Unix de BD em clustering (STF - System Tolerance to Failures) e responsáveis pelo processamento banco de dados armazenado numa arquitetura de armazenamento SAN (Storage Area Network). Dois outros servidores web estão configurados na rede interna para o ambiente de produção internet e um terceiro configurado para homologação e desenvolvimento. Essa arquitetura nos permite isolar por completo o ambiente de desenvolvimento com o de homologação.

b. Arquitectura Lógica



A rede está dividida em três segmentos, através do uso de um router e dois switches. A entrada da rede está controlada através de um router/switch conectado aos servidores de firewall e estes conectados a um switch. Ao router/switch estão ligados dois firewall balanceados (redundantes) para garantir a operação ininterrupta do sistema de segurança, duas placas de rede em cada firewall segmentam a rede interna separando-a da internet. No mesmo segmento estão dois servidores VPN, responsáveis pela criptografia das conexões extranet conectados ao switch de entrada. Os servidores estão protegidos pelo protocolo SSL (Secure Socket Layer - onde as informações transmitidas sejam codificadas para que somente o usuário e o servidor possam interpretar seu conteúdo, assegurando a privacidade da transação) que garantem a segurança das páginas nas aplicações WEB. O switch está ligado ainda a um terceiro firewall ligado através de uma segunda placa de rede a um terceiro switch, que garante separação e segurança ao ambiente de banco de dados, homologação e produção.

4. Política de Segurança

Como quaisquer outros recursos vitais para as empresas, os recursos de hardware, software, redes e dados dos sistemas de informação precisam ser protegidos por controles embutidos para garantir sua qualidade e segurança. É por isso que os controles são necessários.

Os controles eficazes propiciam a segurança dos sistemas de informação, ou seja, a precisão, integridade e segurança das atividades de recursos dos sistemas de informação. Os controles podem minimizar erros, fraude e destruição nos sistemas de informação interconectados que hoje ligam entre si usuários finais das organizações. Controles eficazes também fornecem garantia de qualidade para os sistemas de informação. Ou seja, eles podem deixar um sistema de informação computadorizado mais livre de erros e fraude e capaz de fornecer produtos de informação de qualidade mais alta do que os tipos manuais de processamento da informação. Isso pode ajudar a reduzir o impacto negativo potencial (e aumentar o impacto positivo) que a tecnologia da informação pode produzir na sobrevivência e sucesso das empresas. Entretanto, muito trabalho precisa ser feito antes que os controles adequados sejam implementados em muitas empresas. A especificação desses controles gera o documento denominado Política de Segurança da empresa.

A Política de Segurança é um mecanismo preventivo de proteção dos dados e processos importantes de uma organização que define um padrão de segurança a ser seguido pelo corpo técnico, gerencial e usuários (internos e externos). A Política de Segurança de informações deve estabelecer princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos computacionais e, conseqüentemente, as informações por eles manipuladas.

Para definir a Política de Segurança da nossa empresa, tentamos responder a algumas perguntas relativas à segurança:

- 1) O que a empresa quer proteger ?
os dados do sistema, o site (as páginas), os servidores (acesso de pessoas não autorizadas), manuais, documentos e e-mails dos projetos
- 2) Contra que ou quem ?
hackers, concorrentes, espionagem industrial, crackers, vírus, funcionários
- 3) Quais são as ameaças mais prováveis ?
desastres naturais, vírus, roubo, erro humano, mascaramento, falha de hardware / software, vazamento de informação, indisponibilidade, violação da integridade dos dados, violação autorizada, ameaças programadas
- 4) Quais as expectativas dos usuários e clientes em relação a segurança?
facilidade de acesso, precisão, acompanhar patamar tecnológico, dados não sejam

divulgados ou alterados, dados trafegados sejam protegidos (criptografados), disponibilidade (24 x 7 x 365)

5) Quais as conseqüências para a instituição se seus sistemas e informações forem corrompidos ou roubados?

a companhia que tem seu site invadido passa a imagem de incompetência, o que pode abalar ou estancar negócios junto aos clientes e parceiros, e ainda sofrer processos judiciais

Como resultado do processo de definição da Política de Segurança de nossa empresa, foi gerado o Manual de Segurança da Informação, cujos principais tópicos são descritos a seguir:

Disposições Gerais

- Para garantir o cumprimento e a disseminação das questões relativas à segurança da informação, a empresa conta com o Grupo Corporativo de Segurança da Informação e com o Administrador de Segurança da Informação.
- O Diretor da empresa é responsável por assegurar a disseminação dos conceitos de segurança da informação na empresa.

Princípios

- Toda e qualquer informação gerada, adquirida e trabalhada pela empresa é considerada de sua propriedade, devendo ser protegida de acordo com as regras do Manual de Segurança da Informação.
- É recomendado evitar que um usuário específico, tenha controle da execução de um processo em sua totalidade.
- Visando garantir a continuidade dos processos deve haver, pelo menos, mais um usuário capacitado para substituir o titular.

Norma para Técnico de Informática

- Os servidores e equipamentos de interconexão de rede devem ser preferencialmente instalados em salas específicas para este fim, sendo seu acesso controlado e restrito aos administradores do ambiente informatizado.
- Os servidores, estações cliente e equipamentos de interconexão de rede devem ser lacrados com etiqueta contra violação contendo um número de controle.
- Para garantir a integridade e bom funcionamento dos servidores e equipamentos de interconexão de rede, bem como das estações cliente, o administrador do ambiente informatizado deve providenciar a manutenção preventiva dos mesmos.

Controle de Acesso ao Recurso Informação

- O administrador do ambiente informatizado, na criação e manutenção das contas de identificação dos usuários na rede corporativa segue as regras abaixo:
 - a) verifica se a criação de contas foi autorizada pelo superior do usuário;

- b) configura os sistemas de informação de forma que o usuário:
- troque a senha no primeiro "login";
 - seja impedido de utilizar uma mesma senha por mais de 90 dias;
 - seja impedido de reutilizar as 3 (três) últimas senhas.
 - seja impedido de utilizar senhas de fácil dedução

Controle de Acesso ao Recurso Informação

- O administrador do ambiente informatizado verifica, por meio de ferramentas utilizadas para a administração do ambiente, se houve a violação das medidas de segurança.
- Para maior controle do acesso remoto à rede, o administrador do ambiente informatizado deve configurar nos equipamentos em questão, um "log" que registre, no mínimo, as seguintes informações:
 - a) endereço de origem do acesso;
 - b) endereço de destino do acesso;
 - c) informações acessadas;
 - d) identificação do usuário;
 - e) data e o horário de início e término do acesso.

Administração do ambiente informatizado

- A adoção de novas tecnologias de informática deve ser precedida de uma avaliação do impacto destas à segurança das informações.
- A administração da rede, sistemas de informação e bancos de dados deve, conforme a disponibilidade de recursos da empresa, ser feita pelos técnicos de Informática com o uso de ferramentas de segurança.
- O administrador do ambiente informatizado deve manter a data e o horário das estações cliente e servidores sincronizados, obedecendo ao fuso horário de sua localização geográfica.

Cópias de Segurança

- A realização da cópia de segurança dos servidores deve ser feita fora do horário de expediente, de forma a não prejudicar o desempenho da rede corporativa.
- A cópia de segurança dos servidores atende a seguinte periodicidade:
 - a) diária: cópia das informações armazenadas;
 - b) semanal: cópia das informações armazenadas e sistemas de informação;
 - c) mensal: cópia das informações armazenadas, sistemas de informação e sistemas operacionais.
- A cópia de segurança dos servidores deve ser gerada em 2 (duas) mídias distintas, com conteúdos idênticos, sendo armazenadas e guardadas em lugar seguro, contra danos e roubos.

Verificação do registro de acesso

- O administrador do ambiente informatizado deve:
 - a) verificar diariamente se o processo de geração de "log" está sendo executado corretamente;
 - b) manter disponível para verificação o(s) "log"(s) dos servidores por, no mínimo,

3 (três) meses;

c) pelo menos 1 (uma) vez a cada 3 (três) meses verificar o(s) "log"(s) referente(s) a este período com o objetivo de detectar possíveis falhas no processo ou acesso não autorizado ao recurso informação.

Combate a vírus

– Todas as estações cliente e servidores devem estar protegidas pelo software antivírus padrão definido pela empresa, estando este sempre ativo e atualizado.

Documentação

– Para garantir uma maior segurança das informações da empresa, é necessário que exista a documentação referente aos seguintes itens do ambiente informatizado:

a) metodologia de desenvolvimento;

b) manuais do sistema de informação;

c) manuais de utilização do sistema de informação para usuários;

d) configuração dos equipamentos de interconexão, servidores e estações cliente;

e) topologia de rede.

– Para permitir uma melhor administração da rede corporativa da empresa, sua documentação deve ser mantida atualizada pelo administrador do ambiente informatizado, sendo revisada no máximo a cada 6 (seis) meses

– A atualização da documentação das bases de dados deve ser feita mensalmente pelo administrador do banco de dados

– Todos os sistemas de informação desenvolvidos e utilizados na empresa devem ter sua documentação atualizada, pela equipe responsável (empresa ou terceiros) pelo seu desenvolvimento, sempre que houver mudança de versão

Norma para Usuário

– O acesso ao sistema e ao recurso informação disponibilizado para o usuário deve ser o estritamente necessário e indispensável ao exercício de suas atividades e deve ser solicitado pelo seu chefe imediato

– Para a liberação do acesso é necessário que o usuário assine um Termo de Sigilo e possua capacitação mínima no uso do recurso informação disponibilizado.

– O usuário é responsável pelas informações armazenadas na sua estação cliente e deve adotar as seguintes medidas para minimizar os riscos à segurança da informação:

Uso de software

– A instalação e configuração de software básico na estação cliente são feitas pela equipe de suporte técnico de informática da empresa, assim como a remoção dos mesmos.

– Só é permitido ao usuário, no ambiente de trabalho da empresa, utilizar softwares adquiridos ou desenvolvidos pela empresa.

Internet e Correio Eletrônico

- O correio eletrônico ou o acesso à internet somente deve ser utilizado pelo usuário para a execução das atividades relacionadas ao negócio da empresa.
- O usuário é responsável pelo conteúdo das mensagens enviadas via correio eletrônico sob sua identificação.

Cópia de Segurança

- O usuário é responsável pela cópia de segurança das informações armazenadas na sua estação cliente.

Identificação

- A senha para login na rede de comunicação da empresa e para acesso aos sistemas de informação é sigilosa e não pode ser compartilhada.
- Caso haja suspeita da perda de sigilo da senha, o usuário deve trocá-la imediatamente e informar a suspeita ao administrador do ambiente informatizado.
- Com o objetivo de proteger a conta do usuário contra violação, sua identificação será bloqueada caso esta tenha o acesso negado por três vezes consecutivas.

5. Plano de Contingência

O objetivo do plano de contingência é manter a integridade de dados da organização, manter operacionais os serviços de processamento de dados e prover, se necessário, serviços temporários ou com certas restrições até que os serviços normais sejam restaurados. O objetivo do plano de contingência não é dar lucro e sim evitar prejuízo.

A meta do plano de contingência é minimizar o tempo de parada dos sistemas para reduzir os impactos nos negócios e proteger as informações institucionais .

Um plano eficiente deve conter procedimentos bem detalhados e deixar o mínimo possível de decisões para serem tomadas na hora do problema.

Um plano mal elaborado ou inexistente, pode trazer conseqüências sérias para a organização tais como:

- Perda de Clientes.
- Sérios prejuízos financeiros.
- Desgaste de sua imagem.
- Perda da Credibilidade junto ao mercado.

Para garantir a disponibilidade do sistema foram adotadas medidas preventivas citadas abaixo:

- Testes de Restauração do Backup: A política de backup é um dos itens mais importantes em um plano de contingência. Para garantir que não haja falhas no backup, testes de restauração devem ser efetuados periodicamente, sempre observando o tempo esperado de recuperação dos dados.
- Sites espelhados em cidades diferentes: Essa alternativa envolve o processamento de dois sistemas idênticos nas cidades de Brasília-DF e Curitiba-PR. Os sistemas são atualizados paralelamente.
- Avaliação mínima da arquitetura técnica: Em caso de queda dos sistemas, é necessário que a arquitetura mínima necessária para o sistema funcionar esteja bem documentada.
- Monitoramento, rede, linhas de comunicação, manutenção constante: Identificar eventuais problemas de comunicação com o objetivo de minimizar os impactos.
- Política de pessoal adequada (contratação e demissão): Evitar que ex-funcionários acessem o sistema.
- Testes da aplicação na fase de homologação: Estresse da aplicação antes da mesma entrar em produção, evitando quedas de performance, erros não identificados no desenvolvimento.
- Bancos de dados e o Site em ambientes distintos: Separar o ambiente de produção do ambiente de desenvolvimento e do ambiente de homologação.
- Troca da senha do usuário de conexão com banco de dados de tempos em tempos.
- Proteção aos documentos e mídias: Os documentos devem ser protegidos contra roubo, incêndio, etc.

Como medidas corretivas foram adotadas:

- Restauração da base de dados: Apenas quando solicitado pelo técnico responsável.
- Falha de acesso ao banco de dados: Help Desk deverá ser acionado e, por sua vez, acionar o DBA de plantão ou sobreaviso para restaurar o acesso com o banco.
- Falha de conexão com o banco de dados: O Help Desk deverá ser acionado e, por sua vez, acionar o DBA de plantão ou sobreaviso para analisar e solucionar o problema.
- Falha na aplicação: Acionar o Help Desk e, por sua vez, acionar o técnico responsável da área de web.
- Falha na comunicação com a prestadora E-payment: Help Desk deverá ser acionado e, por sua vez, acionar a prestadora.
- Procedimentos de Help Desk

O Help Desk é capaz de identificar os erros através dos erros gerados pela aplicação. Todos os erros de acesso ao banco são descritos no log da aplicação.

Em caso de uma queda na comunicação via Embratel, onde todos os serviços de internet ficaram inoperantes, podemos citar duas contingências:

- O 0800 recebe as ligações por telefone dos usuários/clientes e efetua as operações solicitadas através da Internet. Para isto, basta o cliente fornecer sua conta e sua senha aos operadores.
- Loja de Telecartofilia.

6. Auditoria

Na auditoria da Tecnologia da Informação é analisado um conjunto de controles gerenciais e procedimentos que afetam todo o ambiente de informática e conseqüentemente todos os sistemas aplicativos.

Os controles organizacionais são políticas, procedimentos e estrutura organizacional estabelecidos para definir as responsabilidades de todos os envolvidos nas atividades relacionadas a área da informática.

Existe na empresa um departamento de informática com uma estrutura organizacional bem definida, com as responsabilidades de suas unidades claramente estabelecidas, documentadas e divulgadas. A política, padrões e procedimentos são estabelecidos pela alta gerência e são divulgados a todos os funcionários. Todas as alterações são aprovadas, autorizadas e documentadas pela gerência. Os funcionários tem conhecimento de suas responsabilidades e seu papel na organização.

O manual de segurança na empresa, possui diretrizes específicas sobre a segurança da informação, amplamente divulgadas a todos os usuários.

Toda documentação obedece a padrões de qualidade e confidencialidade estabelecidos pela organização.

Existe um controle de atividade dos funcionários por meio de procedimentos de operação e supervisão documentados, e políticas adequadas de seleção, treinamento, avaliação de desempenho, segregação de funções e interrupção de contratos de trabalho.

A empresa mantém contrato de terceirização com prestadoras de serviços. O contrato enfoca as cláusulas contratuais, as políticas e os procedimentos de segurança de informação da organização. Existem auditores da empresa responsáveis por auditar as instalações das prestadoras.

Os procedimentos de Controles de Mudanças são bem especificados, envolvendo mudanças de emergência e controle de versão para garantir que os funcionários utilizem a versão correta do pacote de software. A documentação é atualizada periodicamente, ou sempre que ocorre uma mudança de versão.

Há manutenção periódica de logs de atividades de mudança. O Controles de Operação de Sistemas tem como objetivo liberar os usuários de atividades repetitivas e das responsabilidades de garantir a disponibilidade dos sistemas e seu funcionamento adequado.

O Unix mantém diversos tipos de log que podem auxiliar na tarefa de auditoria do sistema, já que por meio de sua análise, pode-se identificar se o sistema está operando

normalmente ou não, e se foi utilizado por pessoas não autorizadas. O sistema Unix pode ser customizado de maneira a registrar apenas as atividades que o administrador do sistema julgar necessárias. Na empresa, deve-se registrar tudo e deve se utilizar de filtros para limitar o número de registros a serem verificados manualmente pelo administrador. Existem programas para minimizar esforços de codificação e de análise de logs. Todos os logs são revisados periodicamente pela gerência de segurança.

Para auxiliar tarefas de identificação de falhas de segurança do Unix a empresa utiliza os programas chamados security scanners, que testam o sistema em busca de brechas de segurança e fragilidade de configuração já conhecidos. Os programas são: COPS – Computer Oracle and Password System, que roda localmente e detecta senhas fáceis de serem descobertas e problemas de segurança na configuração do sistema operacional; SATAN – Security Analysis Tool for Auditing Networks e IIS – Internet Security Scanner. Estes dois últimos testam a máquina na rede em busca de falhas no software do servidor, identificando brechas de segurança e servidores de rede que tornam as máquinas vulneráveis.

7. Conclusão

Com o crescente avanço tecnológico, a popularização da Internet, a globalização e a concorrência cada vez mais acirrada, as empresas estão revendo seus antigos paradigmas e buscando mecanismos de sobrevivência, a fim de preservar o seu market share e a continuidade no negócio. Do mesmo modo que buscaram a agilidade e a capilaridade da Internet para realizar negócios, elas estão aprendendo a necessidade de olhar a segurança por outro ângulo.

A prática tem demonstrado que as empresas, de um modo geral, partem em primeiro lugar, para um trabalho de análise do nível de segurança de suas informações. Descobertas as vulnerabilidades, as empresas tratam logo de corrigi-las, implementando a segurança necessária nas várias tecnologias existentes. O comprometimento da alta gerência neste processo é fundamental.

Entre os vários benefícios de se ter uma política de segurança das informações formalizada em uma empresa de e-commerce, podemos citar o aumento do nível de segurança, difusão da cultura de segurança da informação entre os seus colaboradores e clientes entre outras. Sem mencionar que uma companhia que tem seu site invadido passa a imagem de incompetência, o que pode abalar ou estancar negócios junto aos clientes e parceiros.

Diante do cenário que é apresentado atualmente, podemos afirmar que uma política de segurança da informação é imprescindível para uma empresa, e que neste mundo cada vez mais globalizado, sem limites geográficos para a concorrência, é necessário garantir a continuidade e competitividade no negócio.

A política de segurança da informação torna-se assim o grande pilar de sustentação de equilíbrio do ambiente informatizado, onde o fundamental é preservar os três princípios básicos de segurança: integridade, disponibilidade e confidencialidade.

8. Bibliografia

1. Segurança e Auditoria da Tecnologia da Informação

Autora: Claudia Dias

Editora: Axcel Books do Brasil Editora

2. e- Commerce no Brasil – Oportunidade de negócios no maior mercado sul-americano

Coordenação e edição: Thomas Timm e Lars Grabenschröer

Editora: Câmara Brasil Alemanha