FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Douglas Spadari

ASPECTOS DE SEGURANÇA DA INFORMAÇÃO NA IMPLANTAÇÃO DE SISTEMAS DE VAREJO

Americana, S. P.

2016

FACULDADE DE TECNOLOGIA DE AMERICANA

Curso Superior de Tecnologia em Segurança da Informação

Douglas Spadari

ASPECTOS DE SEGURANÇA DA INFORMAÇÃO NA IMPLANTAÇÃO DE SISTEMAS DE VAREJO

Trabalho de Conclusão de Curso desenvolvido em cumprimento a exigência curricular do Curso Superior de Tecnologia em Segurança da Informação da FATEC – Americana, sob a orientação da Prof. Esp. Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, S. P.
2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

Spadari, Douglas
S722a Aspectos de segurança da informação na implantação de sistemas de varejo. / Douglas Spadari. – Americana: 2016.
31f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Edson Roberto Gaseta

1.Segurança em sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518.5

Douglas Spadari

Aspectos de segurança da informação na implantação de sistemas de varejo

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – FATEC/Americana.
Área de concentração: Segurança da Informação.

Americana, 21 de junho de 2016.

Banca Examinadora:

Edson Roberto Gaseta
Especialista
CEETEPS – Faculdade de Tecnologia de Americana

Pedro Domingos Antoniolli
Doutor
CEETEPS – Faculdade de Tecnologia de Americana

Renato Kraide Soffner
Doutor
CEETEPS – Faculdade de Tecnologia de Americana

AGRADECIMENTOS

Agradeço inicialmente a Deus, por todas as bênçãos e por sempre olhar por mim nos momentos que necessitei.

Agradeço aos meus pais e minha família, por sempre poder contar com o apoio de todos nos momentos da minha vida e por mais essa nova fase que passo em meus estudos.

Ao meu orientador Edson Roberto Gaseta por todo o apoio e confiança, por me auxiliar e participar de cada passo com suas ideias e opiniões, pelo seu conhecimento e experiência dedicados e também por sua grande paciência e comprometimento, que me incentivou a tornar possível a conclusão desta monografia.

A minha noiva Valéria, por estar ao meu lado me auxiliando sempre que necessário, com todo seu amor, paciência, carinho e dedicação.

Aos meus amigos de classe que me sempre me acompanharam, agradeço pelo apoio e pela grande amizade.

A todos os professores do curso que me forneceram conhecimentos e experiências didáticas que foi de grande importância em todo o curso de Segurança da Informação e agregou notória evolução em toda minha vida acadêmica.

Por fim, agradeço a todos que são importantes em minha vida e que tornou possível atingir os objetivos para a realização desta monografia. Muito obrigado!

Dedico este trabalho a minha família, pelo apoio incondicional, carinho e paciência, a minha noiva e aos grandes amigos que me apoiaram e serão constantemente lembrados por toda ajuda e dedicação.

RESUMO

Este trabalho apresenta aspectos que contemplam a segurança da informação na implantação de sistema ERP no segmento de varejo, de forma a prevenir, resguardar e auxiliar os dados e informações das empresas envolvidas, identificando as vulnerabilidades presentes no ambiente de trabalho, as dificuldades enfrentadas no processo de implantação de um sistema de varejo, os aspectos que devem ser seguidos para garantir segurança dos dados assim como a proposta de um gerenciamento adequado na condução da implementação do sistema. O levantamento e análise das vulnerabilidades existentes no ambiente onde será implantado o sistema de varejo devem ser feito antes da respectiva implantação. Durante o estudo foram apresentados recursos que facilitam a análise e correção das vulnerabilidades identificadas e sugestões de melhorias e atualizações essenciais nos equipamentos que compõem a estrutura de TI da empresa.

Palavras-chave: Segurança da informação; implantação de sistema; ERP – *Enterprise Resource Planning*; vulnerabilidade; ambiente seguro.

ABSTRACT

This paper presents aspects that include information security in the ERP system implementation in the retail segment, in order to prevent, protect and assist the data and information of the companies involved, identifying the vulnerabilities present in the workplace, the difficulties faced in the process deployment of a retail system, aspects that must be followed to ensure data security as well as the proposal for an appropriate management in the conduct of system implementation. The survey and analysis of vulnerabilities in the environment where the retail system will be implemented must be done prior to their deployment. During the study were presented features that facilitate the analysis and correction of identified vulnerabilities and improvements and critical updates suggestions on equipment that make up the company's IT structure.

Keywords: Information security; system implementation; ERP – Enterprise Resource Planning; vulnerability; secure environment.

SUMÁRIO

1 INTRODUÇÃO 1

1.1 METODOLOGIA DE PESQUISA 2

2 SEGURANÇA DA INFORMAÇÃO 4

2.1 ASPECTOS DA SEGURANÇA NA IMPLANTAÇÃO 5

2.2 MECANISMOS PARA TORNAR O AMBIENTE SEGURO 6

3 SISTEMA ERP 7

3.1 LEVANTAMENTO DE RECURSOS DE TI 9

3.2 IMPLANTAÇÃO 10

3.3 GERENCIAMENTO DOS DADOS 10

3.4 DIFICULDADES NA IMPLANTAÇÃO 11

4. *HARDENING* 13

5 ESTUDO DE CASO 15

5.1 TOPOLOGIA 15

5.2 ANÁLISE DO AMBIENTE 16

5.3 CORREÇÕES DE VULNERABILIDADES 20

5.4 IMPLANTAÇÃO DO SISTEMA 22

5.4.1 Análise 22

5.4.2 Projeto 23

5.4.3 Aplicação 23

5.4.4 Testes 23

5.4.5 Treinamento e Acompanhamento 24

5.5 PROCESSOS E ATUALIZAÇÕES 24

5.6 RISCOS ENVOLVIDOS 25

5.7 CONSCIENTIZAÇÃO DAS EQUIPES 26

6 CONCLUSÃO 27

7 REFERÊNCIAS 29

LISTA DE FIGURAS

Figura 1 – Estrutura típica de funcionamento de um sistema ERP 9
Figura 2 – Topologia Física.....15
Figura 3 – Relatório MBSA.....17
Figura 4 – Detalhamento das Estações de Trabalho 18
Figura 5 – Atualizações de Segurança.....18
Figura 6 – Detalhamento das Atualizações de Segurança.....19
Figura 7 – Vulnerabilidades Administrativas.....20
Figura 8 – Correção de Vulnerabilidades 21

LISTA DE TABELAS

Tabela 1 – Relação de Equipamentos 16
Tabela 2 – Endereçamento de Rede.....16

LISTA DE ABREVIATURAS E SIGLAS

E-MAIL – Electronic Mail

ERP – Enterprise Resource Planning

IP – Internet Protocol

MBSA – Microsoft Baseline Security Analyzer

SI – Segurança da Informação

TI - Tecnologia da Informação

1 INTRODUÇÃO

Em um cenário empresarial onde há uma constante preocupação com as informações armazenadas e processadas, cria-se necessidade de garantir maior ênfase aos pilares da segurança da informação, prezando-se cada vez mais por ferramentas eficientes e íntegras que visem um bom gerenciamento da informação.

> "É um fato que a evolução da tecnologia mudou a forma dos negócios. Hoje, a nova estrutura dos negócios corporativos é a tecnologia da informação, o seu sistema nervoso é a informação, e o seu ambiente, alcança, também, o ciberespaço. O mundo virtual e a sua capacidade de processamento tornaram a vida melhor ao facilitarem muitas coisas, e trouxeram consigo não só benefícios mas também ameaças à segurança da informação" (DANTAS, 2011, p. 6).

Os sistemas de gerenciamento ERP - *Enterprise Resource Planning*, tomam grande espaço e relevância no mercado varejista, sendo reconhecidamente que esse setor do mercado empresarial exige alto poder de gerenciamento de seus processos e alcance de um resultado eficaz na utilização de recursos, conciliando com uma disponibilidade contínua para atingir os objetivos do seu negócio.

A informação utilizada pela organização é um bem valioso, precisa ser protegida e gerenciada (FONTES, 2006, p.19).

Com a criação de novas ferramentas e indicadores, fica evidente que grande parte do segmento varejista passa a necessitar de sistemas ERP que proporcionem dados concretos de suas transações, controle de processos e que ainda possibilite visualizar seu potencial de crescimento, sempre ponderando que essas informações permaneçam sigilosas.

O mercado tem-se tornado mais competitivo, local e globalmente, e as empresas, como resposta a estas características, buscam aumentar sua eficiência e reduzir seus custos por meio de melhorias e mudanças de processos (ALBERTIN, 2009, p. 8).

Para tanto, se tem a necessidade de investimento em recursos que possibilitem a gestão da segurança da informação no ambiente corporativo, que em parte do mercado é restringido pela falta de conhecimento do contratante e/ou não é corretamente posicionada a importância e relevância para essa questão.

Planejar a aquisição de recursos de TI, incluindo aplicações e infraestrutura, não começa com bits e bytes ou com um *Web site*. Em vez disso, começa com a

obtenção de uma perspectiva holística do que a empresa deseja alcançar e como fazê-lo (TURBAN, 2005, p. 396).

O objetivo geral do trabalho é estudar os aspectos da Segurança da Informação nas implantações de sistemas ERP que gerenciam o mercado varejista, demonstrando as melhores práticas para conduzir o processo de implantação do sistema, assim como a preparação do ambiente de trabalho e equipamentos que os colaboradores utilizarão durante e após a implementação do sistema ERP.

Partindo dessa questão serão identificados os fatores que contribuem para o aumento da vulnerabilidade no ambiente interno de trabalho, tendo em vista as especificações técnicas que não são atendidas, atualizações de segurança não executadas, procedimentos da segurança da informação não respeitados ou ignorados, que por sua vez podem prejudicar as informações e processo executados pelos usuários do sistema através das diversas ferramentas que serão disponibilizadas.

Será mostrada uma ferramenta que auxilia o gerenciamento de vulnerabilidades e rastreamento de atividades de risco, apresentando também as dificuldades na implantação de rotinas, com o intuito de criar um ambiente seguro ao processo de implantação do sistema ERP.

1.1 Metodologia de Pesquisa

No desenvolvimento do trabalho foram utilizadas metodologias de pesquisa exploratórias através de dados obtidos através de dados bibliográficos para o aprofundamento e embasamento teórico das políticas, normas e práticas voltadas para a segurança da informação nas implantações de sistema. Como define Fontes (2012, p. 3) “A informação possibilita o conhecimento da organização. Este conhecimento é a base para a geração de valor nas corporações”.

Como forma de embasamento prática e científica para aplicação em um contexto real, foram realizados estudos e análises em ambientes de produção de clientes, onde o sistema foi instalado e homologado, utilizando processos descritos no trabalho, com ferramentas de verificação de vulnerabilidades apresentadas no estudo de caso. Como esclarece Wazlawick (2009, p. 40) “Assim, deverá ser suficiente trilhar o caminho descrito pelo método para se alcançar o objetivo”.

Sendo assim, com as informações coletadas voltadas para a segurança da informação, já utilizadas na organização, foi possível realizar um estudo aprofundado com embasamento científico e conhecer um exemplo prático visualizando os processos de rastreamento e coletas de dados, como os procedimentos sugeridos são cumpridos pelos colaboradores, quais as dificuldades encontradas na implantação do sistema e as vulnerabilidades encontradas e o modo de monitora-las e mitiga-las.

2 SEGURANÇA DA INFORMAÇÃO

Torna-se evidente que temas relacionados a SI (Segurança da Informação) ganham cada vez mais espaço nas organizações empresariais, devido à importância dos dados e informações que são constantemente processadas no ambiente corporativo, com isso esse ativo gera uma maior necessidade de obter-se alta disponibilidade.

Conforme explica Fontes (2006, p.11) “Segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem como objetivo proteger o recurso informação, possibilitando que os negócios da organização sejam realizados e sua missão seja alcançada”.

Informação é muito mais que um conjunto de dados. Transformar esses dados em informação é transformar algo com pouco significado em um recurso de valor para nossa vida pessoal e profissional (FONTES, 2006, p.2).

A relevância atribuída na segurança da informação para os sistemas ERP a torna um aliado de grande importância para proteção dos dados armazenados e utilizados pelos usuários, para protegê-lo e garantir sua disponibilidade.

A função básica da área de Segurança da Informação é proteger o ativo de informação, minimizando os ricos a níveis aceitáveis (FERREIRA; ARAUJO, 2006, p. 44).

A segurança da informação aplicada no setor de varejo restringe certos grupos de usuários do sistema de gestão o acesso e controle de processos críticos que possam prejudicar ou suprir informações de relevância para o bom funcionamento dos aplicativos e gerenciamento do negócio.

Há que se entender que o objetivo da Segurança da Informação é aprender a lidar e conviver com o risco, e não eliminá-lo completamente, o que na maioria das vezes é impossível (DAWEL, 2005, p. 32).

Em cada situação pode-se alterar o modo de execução dos processos para atender os pilares da segurança da informação seja respeitada e seguida, porém, para uma boa proteção dos dados e condução segura na implantação do sistema é importante identificar e destacar os pilares da segurança da informação.

Na era atual, a informação vale dinheiro; portanto, a empresa precisa proteger não só seus ativos reais, mas principalmente seu capital intelectual e as suas informações (DAWEL, 2005, p. 55).

2.1 Aspectos da Segurança na Implantação

Nas implantações de sistema ERP no mercado de varejo, a preocupação com os dados armazenados e processados no sistema, torna a segurança da informação um item imprescindível para garantir a continuidade de negócio.

Sabendo que a informação armazenada nos computadores da empresa ou em outros meios possui um alto valor para a continuidade dos negócios, o profissional de segurança deve se preocupar com o todo (DAWEL, 2005, p. 18).

Disponibilidade: Garantia de que a informação estará disponível para uso de pessoas autorizadas e deverá estar de acordo com a legislação e ser auditada. Os dados devem ser confiáveis e de fácil acesso (FERREIRA; ARAUJO, 2008, p. 44).

Integridade: Asseguram que os dados não sejam modificados ou excluídos sem autorização, que continuem com os mesmos aspectos de sua ultima utilização. As características da informação devem estar armazenadas com o formato original, estas devem ser protegidas e acessadas somente por pessoas autorizadas (FERREIRA; ARAUJO, 2008, p. 44).

Confidencialidade: Capacidade de um sistema de permitir que alguns usuários acessem determinadas informações ao mesmo tempo em que impede que outros, não autorizados, a vejam (LYRA, 2008, p.3).

Legalidade: O uso da informação deve estar de acordo com as leis aplicáveis, regulamentos, licenças e contratos, bem como com os princípios éticos seguidos pela organização e desejados pela sociedade (FONTES, 2006, p.12).

Auditabilidade: O acesso e o uso da informação devem ser registrados, possibilitando a identificação de quem fez o acesso e o que foi feito com a informação (FONTES, 2006, p.12).

Não-Repudio: Capacidade do sistema de provar que um usuário executou uma determinada ação (LYRA, 2008, p.4).

Ao se falar em segurança da informação, deve-se levar em consideração essas qualidades da informação, pois toda ação que venha a comprometer qualquer uma dessas qualidades estará atentando contra a sua segurança (DANTAS, 2011, p. 11).

2.2 Mecanismos para Tornar o Ambiente Seguro

Nas implantações de sistemas, deve-se contar com alguns mecanismos auxiliares para facilitar o gerenciamento de ameaças no ambiente de TI, apontando vulnerabilidades presentes e bloqueando processos danosos que podem ocorrer na rede interna e nos aplicativos utilizados na organização.

Os *firewalls* são dispositivos importantes para mitigar a fragilidade da rede, como salienta Lyra (2008, p.34), “São recursos de segurança que têm o objetivo de controlar o acesso às redes de computadores. Consistem basicamente numa barreira de proteção entre um computador e seu ambiente externo. O tráfego de informações é examinado e bloqueado quando não atende a critérios predefinidos pela política de segurança”.

Todos os computadores que serão utilizados pelos usuários para operar o sistema ERP devem estar protegidos por um sistema de antivírus.

> “Um bom sistema de antivírus é um elemento essencial para a proteção de redes conectadas à Internet. O *software* antivírus ajuda a impedir ataques vasculhando arquivos periodicamente em busca de mudanças inesperadas em tamanho de arquivos, sequência de códigos similares às armazenadas em uma base de dados de vírus conhecidos, anexos de *e-mails* e outros sinais de alerta” (LYRA, 2008, p.36).

A atualização periódica da lista de vírus e a versão do sistema de antivírus são essenciais para o bom funcionamento dessa importante ferramenta de escaneamento de ameaças.

Se um antivírus não possuir uma lista de assinaturas completa, pode ser que ele vasculhe um arquivo contaminado, mas, por não “conhecer” o vírus, deixa-o ileso (FERREIRA; ARAUJO, 2008, p.66).

3 SISTEMA ERP

As empresas de varejo necessitam de um sistema eficaz que agrega informações de custos, processos e suprimentos do negócio e assim consiga determinar parâmetros e melhorias que possam ser seguidos, tendo a possibilidade de tomar decisões baseadas nas informações processas e geradas pelo sistema.

A introdução de um sistema ERP em uma empresa tem um grande impacto nas operações que são realizadas diariamente em seus negócios. Estes sistemas são atraentes, pois surgiram com a promessa de resolver problemas de integração, disponibilidade e confiabilidade de informações, ao incorporar em um único sistema as funcionalidades que suportam diversos processos de negócios em uma empresa (OLIVEIRA; RAMOS, 2002).

Souza & Zwicker (2000) esclarecem o ERP como sistemas de informação integrados, que são obtidos na forma de pacotes comerciais, para estruturar a maioria das operações de uma empresa (compras, fiscal, manutenção, financeiro, folha de pagamento, contabilidade, etc.).

Os sistemas ERP também são chamados no Brasil de Sistemas Integrados de Gestão Empresarial, tem essa nomenclatura por controlar, em sua grande maioria vários processos das organizações, como os operacionais, fiscais, comerciais, produtivos e administrativos.

Esses sistemas tratam dos vários processos que ocorrem simultaneamente, de forma automática, e *on-line*. Daí, a necessidade no mundo globalizado das empresas se adequarem ao relacionamento do ERP para o auxílio da tomada de decisão (OLIVEIRA; RAMOS, 2002).

Turban (2004) expõe que, a solução integrada dos sistemas ERP consiste em um processo que envolve planejamento e gestão geral dos recursos da empresa e sua utilização. O principal objetivo dos sistemas ERP é integrar todos os departamentos e funções de uma empresa em um sistema unificado de informática, com capacidade de atender a todas as necessidades da organização.

O sistema ERP tem uma abrangência ampla nos processos das organizações, envolvendo grande maioria dos funcionários e setores de trabalho, iniciando uma informação unificada que passa a ser compartilhada com os responsáveis envolvidos de cada segmento, é nesse ponto que os dados trafegados

passam a ganhar notoriedade e a atenção com a Segurança da Informação deve ser contemplada com os procedimentos.

Conforme expõe Vico Manãs (2010, p.79), “A informação passou a ser analisada sob o aspecto estratégico de maior relevância de uma empresa. A informação é que nos conduz ao controle. O controle é, na prática, a possibilidade de, a partir de um acompanhamento, nos levar ao redirecionamento correto”.

Os sistemas têm como intuito dar suporte, através das informações processadas, à tomada de decisões gerenciais de uma organização como um todo (CÔRREA; GIANESE; CAON, 2001).

O sistema ERP necessita de uma equipe treinada que possa inserir e manusear e gerar informações com precisão para o sistema, para posteriormente serem processadas e então definir uma linha para melhora contínua dos processos gerados no negócio.

Muscatello, Small e Chen (2003, p. 852) entendem que “sistemas ERP consistem de um conjunto de módulos, sendo cada módulo normalmente responsável pela coleta e processamento de informações para funções administrativas específicas ou grupo destas funções”.

O ERP compõe uma estrutura típica de funcionamento, concentrando todos os componentes ligados à empresa (fornecedores, clientes, diretoria, RH, funcionários, venda, representantes, manufatura, administrativo, finanças) para a base de dados central, onde são armazenadas todas as informações importantes aos processos realizados na organização, conforme mostrado na Figura 1.

Figura 1 – Estrutura típica de funcionamento de um sistema ERP

Fonte: DAVENPORT (1998).

3.1 Levantamento de Recursos de TI

É essencial que em todas as implantações de sistemas sejam realizadas uma análise preliminar para se identificar e se definir os recursos físicos e lógicos para que seja possível determinar os *upgrades* necessários nos equipamentos e atualizações de sistema recomendadas.

Estes sistemas são bastante complexos e necessitam de um planejamento cuidadoso para garantir o sucesso de sua implantação (GUPTA, 2000).

O levantamento técnico da infraestrutura disponibilizada pela empresa deve-se considerar de maneira geral, as especificações e requisitos mínimos exigidos pelo ERP, para o bom funcionamento do sistema. Sendo assim, esse levantamento realizado anteriormente a efetiva implantação do sistema ERP torna o processo menos impactante ao cliente.

3.2 Implantação

Após realizados os processos de análise, correções e melhorias, a instalação do sistema ERP pode ser inicializada, observando o comportamento do ambiente de TI e demais processos que agregam a estrutura da organização.

Colangelo (2001) define que, a implementação do sistema ERP em uma organização é compreendida de três etapas: pré-implantação, implantação e pós-implantação.

Podemos entender a etapa de pré-implantação, tendo em vista com o principal objetivo decidir pela continuidade do processo ou não, realizando uma análise minuciosa da viabilidade do sistema ERP na organização, assim como o levantamento dos equipamentos que serão utilizados no processo.

A próxima etapa, a de implantação do sistema, são definidos os processos que serão focados nos negócios da empresa. Essa definição visa levantar informações para a configuração do sistema ERP. Ao final desse processo o sistema já estará operacional aos seus colaboradores.

Por fim, na etapa de pós-implantação são realizados testes de desempenho para verificar a estabilidade do sistema implantado.

Para Souza (2000, p.38), a etapa de implementação é definida como: “[...] o processo pelo qual os módulos do sistema são colocados em funcionamento em uma empresa”.

No processo de instalação do sistema, uma etapa importante é a checagem da gravação de *logs* realizada pelo sistema ERP, afim de posteriormente checar de forma conclusiva as operações realizadas por cada usuário do sistema.

3.3 Gerenciamento dos Dados

Com o sistema já implantado, é necessário conscientizar a equipe da importância da informação inserida no sistema. Os dados inseridos de forma imprópria podem criar uma falsa informação processada pelo sistema ERP, por consequência atingir a tomada de decisão pelo setor gerencial, impactando diretamente no negócio da empresa.

A implantação de um sistema ERP tem como objetivo, a padronização dos dados, padronização dos processos, transformação e mudanças contínuas e planejadas da organização. O ERP possibilita que um fluxo de informações que integrem toda a empresa numa única base de dados. É uma ferramenta de melhoria de processos do negócio e não pelas funções, permitindo um cenário global em tempo real desses processos (STAMFORD, 2000).

Com a instalação do sistema ERP os dados passam a ser gerenciados de modo abrangente pelos departamentos da organização, ligando ao fato que a informação disponível passa a ser tratada de forma global, onde cada registro inserido eleva o grau da informação, ganhando mais importância ao negócio.

É importante que todos os sistemas possuam registros das atividades realizadas pelos seus usuários (LYRA, 2008, p.46).

3.4 Dificuldades na Implantação

Toda mudança de rotina pode ser interpretada como algo não correto e prejudicial, na questão dos sistema ERP para o setor de varejo, onde o colaborador da empresa tem contato direto e constante com o sistema. Cria-se um bloqueio e repúdio maior, dificultando o aprendizado e entendimento das novas rotinas definidas pelo sistema, com intuito de aprimorar os processos e garantir que as informações geradas pelos usuários sejam íntegras.

Muitas pessoas relutam diante das inovações. Outras tantas relutam sempre, mas de alguma forma se adaptam, inovam ou convivem com as inovações (VICO, 2010 p. 36).

Por ser um sistema integrado, a informação inserida em qualquer departamento da organização estará disponível para acesso nos demais setores da empresa, podendo gerar problemas nos resultados gerados através de relatórios que são disponíveis para os gestores do negócio.

Por ser um processo complexo, causa alguns impactos na empresa, alterando a cultura de processos aplicados, os negócios e a organização de trabalho.

Obtendo um planejamento bem elaborado e adequado nas definições estabelecidas previamente para a implantação do sistema, os impactos do processo

são notavelmente reduzidos para o colaborador da empresa, diminuindo a percepção de mudança e dificuldade de adaptação para o usuário final do mercado de varejo.

4. *HARDENING*

Com a constante evolução computacional, ficou indispensável o resguardo dos dados armazenados nos servidores ERP, sendo necessário gerar rotinas e serviços voltados à segurança da informação, com intuito de minimizar os impactos e elevar o nível de segurança das informações trafegadas no sistema.

Os procedimentos que são tomados para mitigar as vulnerabilidades no ambiente corporativo são conhecidos como *hardening*. Essa técnica dificulta intrusos de executar instruções que possam comprometer a funcionalidade do sistema ERP, quebrando pilares básicos da Segurança da Informação – SI.

Hardening é uma técnica utilizada para estruturar diversas ameaças e posteriormente efetuar possíveis correções nos sistemas, prevenindo certas tentativas de ataques ou violações na segurança da informação (FACINA, 2009).

Algumas rotinas passam a ser utilizadas para mapear as ameaças, para posteriormente corrigi-las, utilizando ferramentas próprias que facilitam a identificação de vulnerabilidades.

“O *hardening* consiste na realização de alguns ajustes finos para o fortalecimento da segurança de um sistema. Muitos administradores sem experiência em segurança preparam seus servidores com uma instalação básica e depois que suas aplicações estão disponíveis nenhum procedimento é feito para manter a integridade do sistema” (REIS; VERBENA; JULIO, 2011, p. 21).

Com o *hardening* é possível explorar as vulnerabilidades e ameaças que possam impactar no processo de implantação do sistema ERP, assim quando identificadas, possibilitam a correção e preparação para por fim tornar o sistema melhor protegido, robusto e confiável.

“*Hardening*, ou blindagem de sistemas, consiste na utilização de técnicas para prover mais segurança a servidores que disponibilizam serviços externos, como servidores *Web*, ou até mesmo serviços internos, como servidores de banco de dados, de arquivos, entre outros” (REIS; VERBENA; JULIO, 2011, p.1).

Utilizando-se o *hardening* para os sistemas operacionais que utilizam o sistema ERP de varejo, possibilita que as máquinas trabalhem com maior fluidez e aumente a segurança da informação no equipamento, pois quando removidos aplicações e serviços irrelevantes ao negócio, as máquinas ficam com capacidade maior para realizar tarefas, priorizando a utilização do sistema ERP.

O fácil acesso e comodidade a rede de computadores para transferências e compartilhamentos de arquivos pode trazer vulnerabilidades. Essas podem comprometer a segurança da informação das empresas, quando elas não têm um limite determinado para restrição de uso e acesso de seus usuários (VIEGAS, 2008).

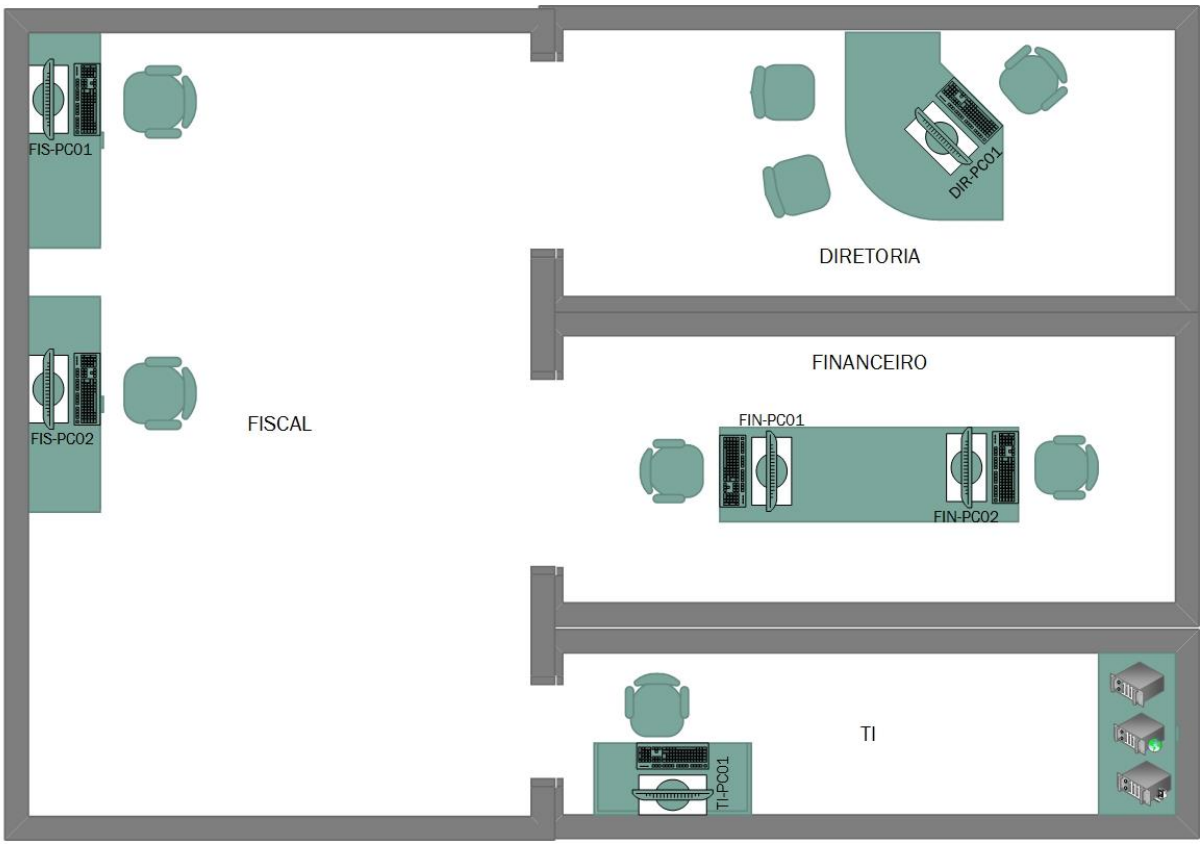
A restrição de gravação de arquivos gerais de usuários e arquivos executáveis no compartilhamento do servidor ERP deve ter um alto grau de restrição, evitando contaminação em massa pela rede e propagação de vírus e trojans na organização.

5 ESTUDO DE CASO

5.1 Topologia

O escopo do projeto foi realizado em um supermercado de varejo de pequeno porte. A infraestrutura do escritório onde se encontram todos os equipamentos de TI, está concentrada em um espaço total de 104 m², divididos em quatro salas operacionais, conforme mostrado na Figura 2.

Figura 2 – Topologia Física



Fonte: Autoria própria.

O sistema ERP irá operar em um total de seis estações de trabalho, duas no setor financeiro, duas no setor fiscal, uma na diretoria e uma para o administrador de TI, conforme mostrado na Tabela 1.

Tabela 1 – Relação de Equipamentos

Tipo	Descrição	Hostname	IP	Sistema Operacional	Marca/Modelo
Desktop	Desktop Finan. 01	FIN-PC01	DHCP	WIN 7	Dell Otiplex 3030
Desktop	Desktop Finan. 02	FIN-PC02	DHCP	WIN 7	Dell Otiplex 3030
Desktop	Desktop Fiscal 01	FIS-PC01	DHCP	WIN 8	Dell Otiplex 3030
Desktop	Desktop Fiscal 02	FIS-PC02	DHCP	WIN 8.1	Dell Otiplex 3030
Notebook	Desktop Diretoria 01	DIR-PC01	DHCP	WIN 10	Dell Latitude3440
Notebook	Desktop TI 01	TI-PC01	DHCP	WIN 10	Dell Latitude3440

Fonte: Autoria própria.

A organização ainda contará com dois servidores que serão instalados no ato da implantação do sistema, sendo necessária reserva prévia de endereço de IP.

A estrutura de rede opera no endereçamento indicado na Tabela 2.

Tabela 2 – Endereçamento de Rede

Rede	Máscara	Função
192.168.0.1	/24	Rede única para *desktops*, dispositivos de rede e visitantes.

Fonte: Autoria própria.

5.2 Análise do Ambiente

A análise preliminar foi realizada através a ferramenta MBSA (*Microsoft Baseline Security Analyzer*) disponibilizada pela Microsoft, que possibilita uma rápida e eficaz análise de vulnerabilidades presentes no ambiente corporativo.

A ferramenta identifica atualizações não efetivadas de correções e melhorias aplicadas pelo fabricante do sistema nos sistemas operacionais que são utilizados nos equipamentos de TI da empresa, assim como erros de configuração

relacionados à Segurança da Informação, seguindo recomendações de segurança disponibilizadas pela própria Microsoft.

Todo comportamento anormal de um sistema deve ser examinado para que possa ser ou não considerado um incidente de segurança. Essa monitorização, bem como as providências a serem a tomadas em cada caso, devem fazer parte da política de segurança e contribuem para a melhoria do processo de desenvolvimento de *software* (LYRA, 2008, p. 101).

Com a utilização dessa ferramenta, torna possível um gerenciamento eficaz da segurança da informação, tornando a implantação do sistema ERP, mitigando as falhas que podem comprometer os dados inseridos e manuseados no processo.

Ao início é gerado um relatório com todos os computadores da empresa que foi possível a ferramenta MBSA analisar, demonstrando o nome da estação de trabalho, o endereço de IP, a avaliação de risco gerada pelo sistema e a data de escaneamento, conforme mostrado na Figura 2.

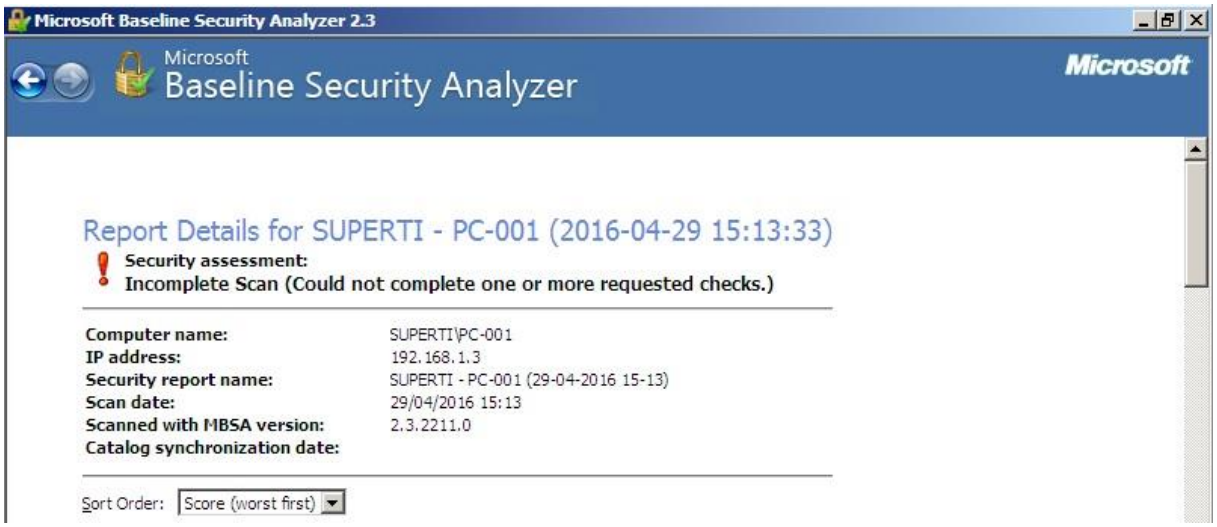
Figura 3 – Relatório MBSA

Fonte: Autoria própria.

Com o relatório disponibilizado pelo MBSA das estações de trabalho, é possível identificar as máquinas e obter um escopo inicial abrangente para início das operações, podendo catalogar as informações dos equipamentos listados.

Posteriormente o sistema possibilita uma análise detalhada de cada estação de trabalho identificada na varredura da ferramenta MBSA, trazendo uma tabela detalhada dos riscos identificados, conforme mostrado na Figura 3.

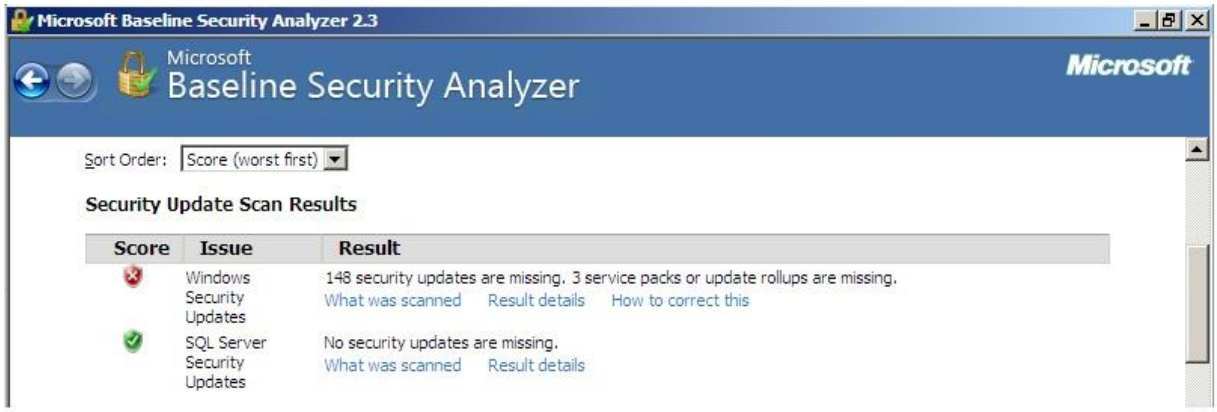
Figura 4 – Detalhamento das Estações de Trabalho



Fonte: Autoria própria.

Com o detalhamento é possível obter uma análise minuciosa dos status de segurança identificado pelo MBSA, observando de modo geral o comportamento frente à segurança da informação das vulnerabilidades presentes em cada estação de trabalho, conforme mostrador na Figura 4.

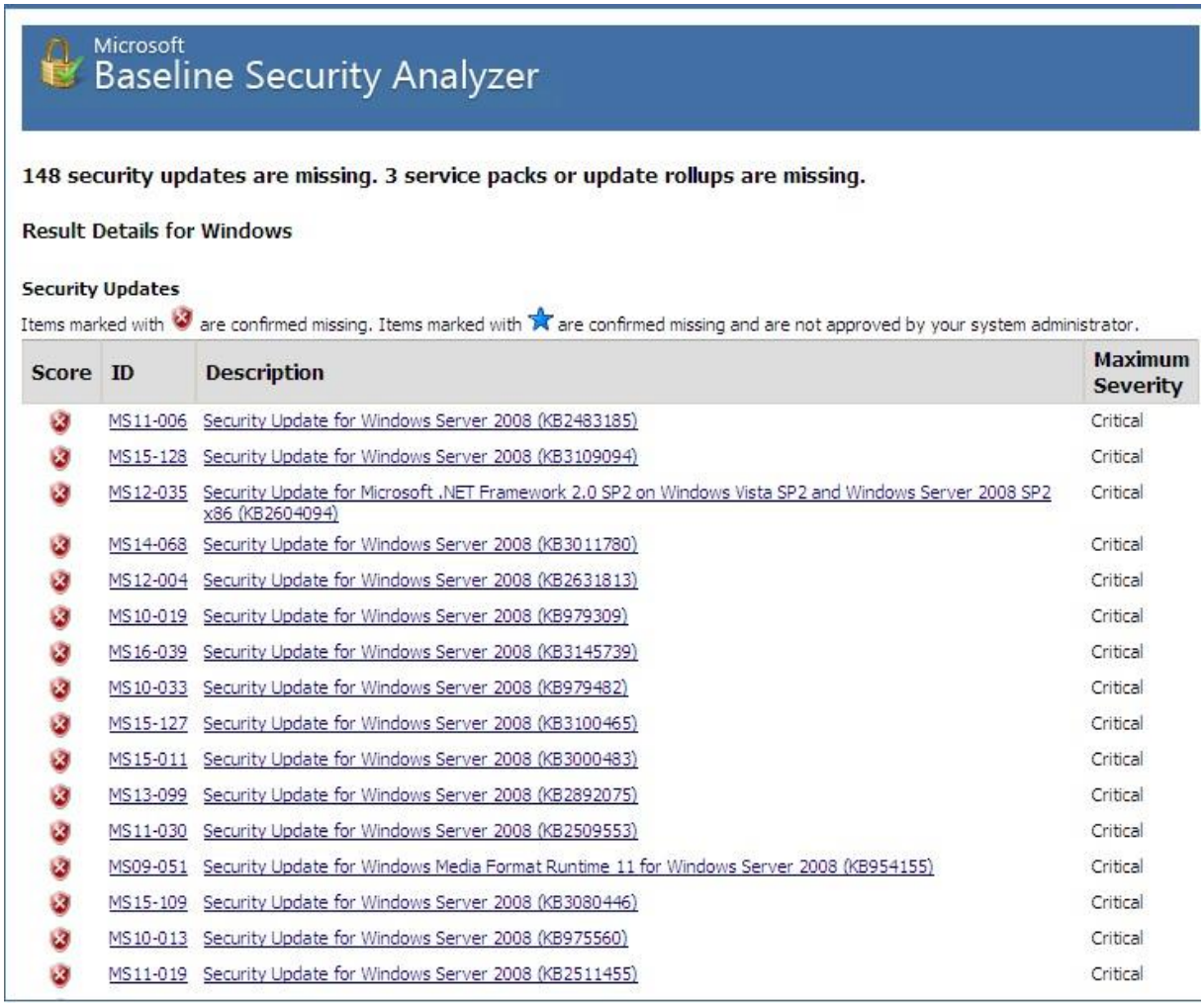
Figura 5 – Atualizações de Segurança



Fonte: Autoria própria.

O MBSA identifica as atualizações de segurança disponíveis, porém não instaladas na estação de trabalho, fazendo uma distinção para cada produto da Microsoft, conforme mostrado na Figura 5.

Figura 6 – Detalhamento das Atualizações de Segurança



Microsoft
Baseline Security Analyzer

148 security updates are missing. 3 service packs or update rollups are missing.

Result Details for Windows

Security Updates

Items marked with are confirmed missing. Items marked with are confirmed missing and are not approved by your system administrator.

Score	ID	Description	Maximum Severity
	MS11-006	Security Update for Windows Server 2008 (KB2483185)	Critical
	MS15-128	Security Update for Windows Server 2008 (KB3109094)	Critical
	MS12-035	Security Update for Microsoft .NET Framework 2.0 SP2 on Windows Vista SP2 and Windows Server 2008 SP2 x86 (KB2604094)	Critical
	MS14-068	Security Update for Windows Server 2008 (KB3011780)	Critical
	MS12-004	Security Update for Windows Server 2008 (KB2631813)	Critical
	MS10-019	Security Update for Windows Server 2008 (KB979309)	Critical
	MS16-039	Security Update for Windows Server 2008 (KB3145739)	Critical
	MS10-033	Security Update for Windows Server 2008 (KB979482)	Critical
	MS15-127	Security Update for Windows Server 2008 (KB3100465)	Critical
	MS15-011	Security Update for Windows Server 2008 (KB3000483)	Critical
	MS13-099	Security Update for Windows Server 2008 (KB2892075)	Critical
	MS11-030	Security Update for Windows Server 2008 (KB2509553)	Critical
	MS09-051	Security Update for Windows Media Format Runtime 11 for Windows Server 2008 (KB954155)	Critical
	MS15-109	Security Update for Windows Server 2008 (KB3080446)	Critical
	MS10-013	Security Update for Windows Server 2008 (KB975560)	Critical
	MS11-019	Security Update for Windows Server 2008 (KB2511455)	Critical

Fonte: Autoria própria.

Selecionando a opção para detalhamento de atualização, possibilita identificar com minúcias cada pacote não instalado, que proporcionaria maior segurança ao equipamento vasculhado. É possível também verificar o nível de criticidade ponderado pelo sistema MBSA, para cada atualização de segurança disponibilizada, conforme mostrado na Figura 6.

Figura 7 – Vulnerabilidades Administrativas

Fonte: Autoria própria.

O sistema disponibiliza a verificação de vulnerabilidades administrativas ligadas ao sistema operacional Windows, como a não configuração de atualizações automáticas de segurança, senha de usuário para acesso ao sistema expirado, atualizações incompletas, *Firewall* do Windows não ativado, usuário do sistema sem cadastro de senha para acesso, e a quantidade de administradores registrados no sistema operacional.

5.3 Correções de Vulnerabilidades

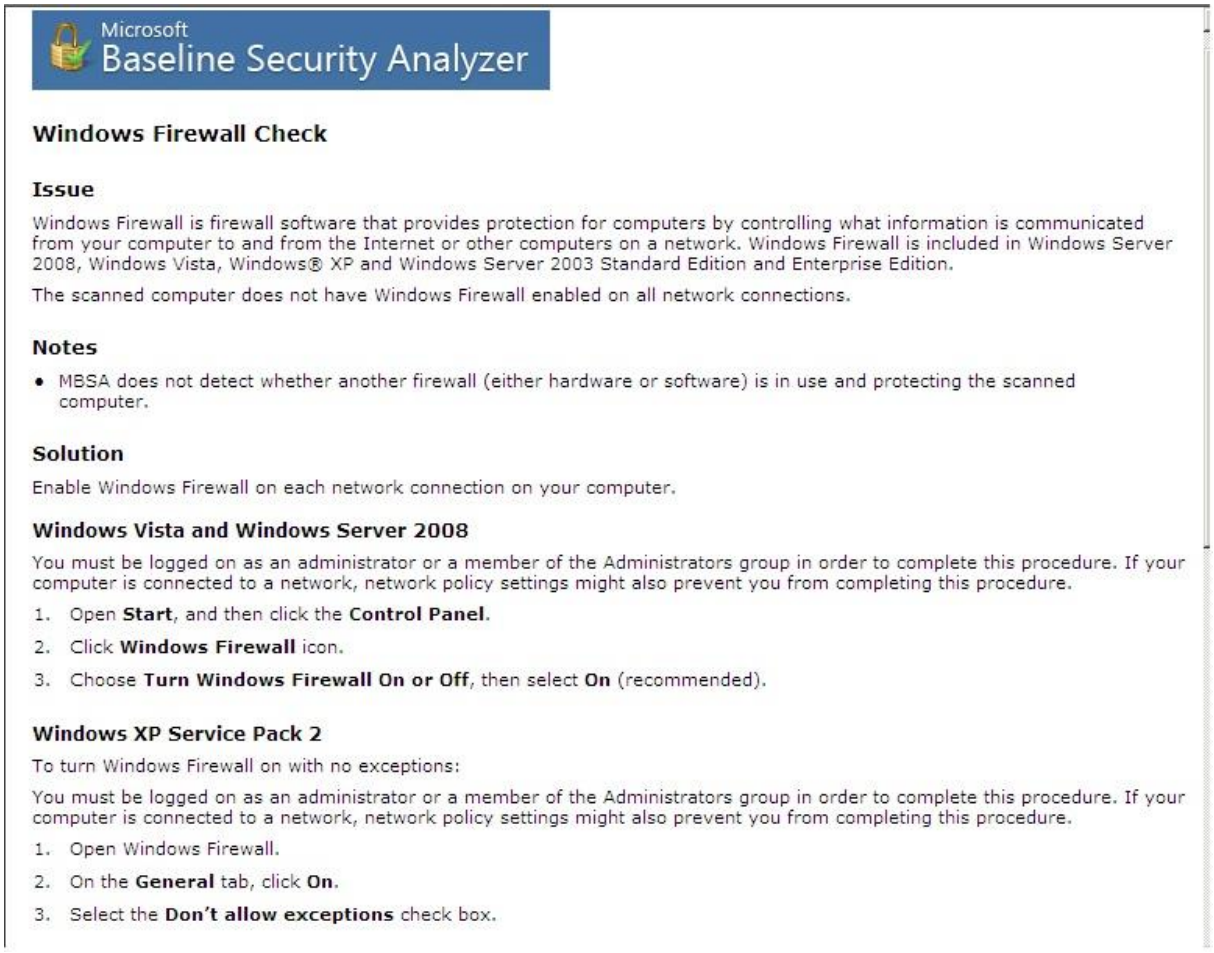
Ao término da coleta dos dados realizados através do sistema MBSA, são iniciadas as correções que serão identificadas através dos resultados obtidos no relatório que é disponibilizado pelo aplicativo, ao término da varredura de vulnerabilidades.

São aplicadas as correções de atualizações críticas, falhas de configuração nos produtos da Microsoft, senhas fracas e compartilhamentos disponibilizados na rede indevidos.

Todas as falhas identificadas pela ferramenta MBSA utilizadas na análise de ambiente, impactam diretamente na implantação do sistema ERP, podendo dificultar a instalação do aplicativo nas estações de trabalho, ou comprometer os dados que são trafegados na rede através do sistema.

O sistema MBSA disponibiliza em sua *interface*, de um modo explicativo, a maneira correta para corrigir as vulnerabilidades encontradas na fase de análise de ambiente, facilitando a identificação e correção, conforme Figura 7.

Figura 8 – Correção de Vulnerabilidades



Fonte: Autoria própria.

5.4 Implantação do Sistema

A fase de implantação só é iniciada ao término das análises de ambiente e correções de vulnerabilidade. No trabalho são apresentadas as fases da implementação do sistema, que terão inicio logo após mitigar todas as vulnerabilidades identificadas nas fases anteriores, com um foco específico na segurança da informação. Para isso é importante utilizar as ferramentas que permitem auxiliar no processo, como um todo.

Quando o sistema ERP é efetivamente adquirido pela empresa, o produto não está adaptado as necessidades do cliente, ou seja, o sistema não está pronto e configurado para o início das atividades da organização. Entre o período de aquisição do sistema e a efetiva utilização do produto pelos colaboradores da empresa, existe um estado intermediário que é definido como implantação. Esse processo de implantação do sistema pode assim ser definido como uma sequência pré-definida de processos e transformações que estabelecem a transição entre esses estados identificados acima.

A relação das fases do processo é disponibilizada de forma abstrata, conseguindo visualizar apenas de modo geral o andamento dos processos, assim é possível identificar os passos não seguidos ou até mesmo falta de execução desses processos.

O processo de implantação do sistema ERP para o varejo pode ser dividido em cinco fases principais, na qual cada uma dessas fases possibilita produzir um resultado intermediário. Assim, possibilita o implantador gerar avaliações, processar ajustes e, por fim, passar para próxima fase, garantindo a continuidade do processo. As fases definidas são: análise, projeto, aplicação, testes e treinamento e acompanhamento.

5.4.1 Análise

O objetivo principal desta fase é compreender o perfil da empresa e verificar a relação com o ERP adquirido, possibilitando a identificação dos ajustes necessários. A análise deve incluir todas as dimensões da segurança da informação que serão afetadas direta ou indiretamente pela implantação do ERP.

O levantamento é necessário para identificar os processos utilizados pela organização, consiste em verificar os atuais procedimentos operacionais executados pelos usuários, focando também nas atividades que são realizadas nesses processos, mas não possuam um fluxograma devidamente estabelecido pela empresa.

Nesse processo é possível identificar problemas que possam comprometer a segurança da informação que são identificadas na análise.

A análise é importante também para identificar as necessidades da empresa, podendo planejar as ações de segurança de forma eficaz.

5.4.2 Projeto

Com base nas informações coletadas na fase de análise. O objetivo dessa fase é definir e estruturar o que será realizado nas próximas fases. Tal definição se aplica à implantação do ERP. Portanto, a segurança da informação deve ser abordada de forma prática e usual para que seja aplicada nas próximas fases.

5.4.3 Aplicação

Nesta fase são realizadas as maiores transformações responsáveis por efetivar o sistema ERP em modo de produção. Nessa fase a segurança dos dados fica em maior vulnerabilidade, devido às constantes mudanças que serão aplicadas.

5.4.4 Testes

O maior objetivo da fase de testes é validar os processos executados na aplicação do sistema, verificando e ajustando os requisitos operacionais do ERP, seguindo o que foi determinado nas fases de análise e de projeto. Nessa fase é possível rastrear eventuais falhas que possam comprometer ou dificultar o acesso aos dados contidos no sistema ERP.

Os testes finais, antes da efetiva utilização do sistema, devem ser realizados pelos colaboradores da empresa, com a supervisão da equipe que implanta o sistema na organização. É na etapa de testes que os usuários ganham uma relação estreita com o sistema, conduzindo para a equipe que realiza o projeto

particularidades de suas operações que são importantes em sua rotina diária e possam ser ajustadas antes da entrada em produção (MOLINARI, 2003).

5.4.5 Treinamento e Acompanhamento

Visualizando o processo de implantação como um todo, a fase de treinamento e acompanhamento é a mais desafiadora aos usuários do sistema ERP, que irão utilizar o novo sistema recém implantando. Nesta fase, o sistema já está praticamente pronto para utilização efetiva, sendo necessário apenas preparar os colaboradores, acompanhar os processos definidos no projeto, e preparar a transição.

A aplicação efetiva para os usuários com as melhores práticas para o manuseio dos dados contidos no sistema é realizada nessa fase.

O processo de implantação deve ser planejado detalhadamente para diminuir as chances de falhas no processo que possam adiar a implementação do sistema, ou até mesmo abortar o procedimento.

Mitigando as possíveis falhas na execução da implantação do sistema e seguindo um planejamento bem elaborado, os riscos de impactos aos usuários diminuem, assim como o descontentamento dos clientes finais do negócio, evitando desconforto e saturação da equipe colaboradora.

5.5 Processos e Atualizações

As atualizações para melhoria de desempenho e segurança dos sistemas ERP podem impactar na utilização do sistema durante sua execução. As alterações no banco de dados necessitam que o sistema fique inoperante durante o processo, podendo causar transtornos aos colaboradores.

Souza (2000) aborda a necessidade atualização do sistema ERP, considerando os riscos envolvidos nas manutenções:

> “A complexidade dos sistemas ERP, sua abrangência e sua integração levam a dificuldades nas operações de manutenção, tais como atualização de versões, paradas para manutenção de máquinas, realização de *backups*, testes e mudanças de parametrização durante o uso” (SOUZA, 2000, p.53).

A programação da atualização do sistema ERP deve ser agendada previamente, definindo com os gestores da empresa um período adequado e repassada a informação aos colaboradores que utilizam a ferramenta, evitando contratempos nos processos dos setores que contemplam o sistema ERP (financeiro, fiscal, contábil, compras, etc.).

5.6 Riscos Envolvidos

A análise do projeto necessita considerar alguns fatores que podem prejudicar o processo de implantação do sistema e esboçar planos de ação para mitigar os impactos que possam ocorrer no projeto. A empresa deve estar preparada quanto a atrasos e dificuldades em adaptação do *software* por parte de seus colaboradores, assim como identificar fatores que possam ser ajustados no novo sistema implantado.

Conforme explica Stamford (2000), os principais problemas da implantação de um sistema ERP estão relacionados à reestruturação de processos, os serviços de customização pertencentes à implantação, à falta de experiência da equipe de suporte e apoio, à implantação demorada da ferramenta, ao alto custo envolvido em práticas de consultorias e treinamentos, à complexidade na customização do sistema e aos benefícios que em alguns casos não são atingidos.

Os riscos nas implantações de sistemas de ERP são divididos em três partes, riscos relativos ao projeto de implantação do sistema, riscos relativos ao sistema ERP, e riscos relativos ao negócio.

Os riscos relativos ao projeto de implantação do sistema são os riscos que atingem o planejamento do projeto e seus recursos, podendo impactar diretamente na condução e finalização do projeto, ocasionando cancelamentos ou atrasos.

Os riscos relativos ao sistema ERP são os riscos que atingem as características ou o desempenho do sistema que podem comprometer a sua utilização, ocasionados por falta apropriação do sistema com as necessidades da empresa.

Os riscos relativos ao negócio são os riscos que atingem os negócios da organização, podendo causar impactos financeiros à empresa, ocasionados pela falta ou incapacidade de integração do sistema ERP com os negócios da empresa.

5.7 Conscientização das Equipes

Dempsey (1999) explica que, “como o projeto é amplo, muitas empresas perdem de vista as motivações originais e naufragam diante das dificuldades encontradas. Muitos sistemas têm uma *interface* ruim com o usuário. Para solucionar esse problema, elas adotam outro sistema com a *interface* gráfica mais atraente, que facilite o uso pelo usuário”.

É importante que no decorrer do processo de implantação do sistema, sejam expostos de forma clara as informações e tarefas a serem executadas, priorizando os prazos de cronograma do projeto. A comunicação com as equipes de trabalho é essencial, todos os envolvidos devem estar cientes de suas obrigações e conhecer a sequência de processos que está definida. Os colaboradores da empresa devem estar comprometidos durante a fase de implantação e ter ciência das mudanças, impactos, aumento inicial de trabalho e alterações de rotinas internas que ocorrem.

Para Daft (1999), uma mudança em uma cultura organizacional traz mudanças de hábitos de cada indivíduo pertencente a esta, do modo de execução das funções por estes mesmos indivíduos, além de influenciar significativamente nas rotinas e modos de execução da empresa como um todo.

6 CONCLUSÃO

Foi possível concluir que a Segurança da Informação é de grande importância para as implantações de sistema no setor de varejo, essa por sua vez, com o passar dos anos, tem ganhado espaço e sendo vista com bons olhos pelas organizações, devido à segurança que fornece aos dados trafegados nas empresas.

Para que haja uma implementação do sistema ERP adequada, deve-se antes realizar uma análise minuciosa do ambiente, a fim de garantir que as estações de trabalho estejam protegidas de ameaças que expõe vulnerabilidades, sendo essas identificadas pelo sistema MSBA (*Microsoft Baseline Security Analyzer*).

As estações de trabalho devem ser rastreadas periodicamente, até que a implantação do sistema esteja concluída, tendo a possibilidade de continuidade após as fases de treinamentos, combatendo as vulnerabilidades permanentemente.

Com o estudo da Segurança da Informação nas implantações de sistema de varejo, foi possível abranger de forma clara as ameaças e vulnerabilidades que são identificadas no processo, também definir a correta utilização das ferramentas de análises para identificar e aplicar as correções apontadas, assim proporcionando meios para gerenciar as vulnerabilidades de maneira simples e de fácil utilização.

Vale apontar que com o estudo, possibilitou aprofundar em critérios da Segurança da Informação que devem ser propostos em uma implantação de sistema no ramo varejista, como realizar varreduras de ameaças utilizando ferramentas específicas para o trabalho.

A análise de ambiente voltada para a Segurança da Informação na implantação do sistema na organização abrangerá claramente os riscos e vulnerabilidades que possam ser combatidos previamente a efetiva utilização do sistema, garantindo que os dados utilizados na empresa tenham maior segurança durante o processo.

O principal problema identificado foi a pouca empatia e conhecimento prestados a Segurança da Informação pelos gestores das organizações e usuários do sistema, criando uma barreira intangível que pode abrir espaço para ameaças e vulnerabilidades quando essas não são respeitadas.

Por fim, foi possível concluir que a verificação prévia do ambiente de TI, através da ferramenta de análise de vulnerabilidades MBSA, conduz o processo de implantação de sistemas nas empresas de varejo de forma mais segura e controlada,

eliminando ameaças que possam comprometer a infraestrutura da organização, entre outros fatores que puderam ser analisados durante a condução do processo.

7 REFERÊNCIAS

ALBERTIN, Alberto Luiz. **Tecnologia de informação e desempenho empresarial**: as dimensões de seu uso e a sua relação com os benefícios de negócio. 2ª ed. São Paulo: Atlas, 2009.

COLANGELO, L.F. **Implantação de sistemas ERP (Enterprise Resource Planning):** um enfoque de longo prazo. São Paulo: Atlas, 2001.

CÔRREA, Henrique L.; GIANESE, Irineu G. N; CAON, Mauro. **Planejamento, programação e controle da produção**. 4. ed. São Paulo: Atlas, 2001.

DAFT, R. L. **Administração**. Tradução: Fernando Gastaldo Morales. Rio de Janeiro: LTC. cap. 12, p. 230-247: Mudança e desenvolvimento. 1999.

DANTAS, Marcus Leal. **Segurança da informação**: uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial**: como as organizações gerenciam o seu capital intelectual. Rio de Janeiro: Campus, 1998.

DAWEL, George. **A segurança da informação nas empresas**. Rio de Janeiro: Ed. Ciência Moderna, 2005.

DEMPSEY, Michael. Pacote de ERP não resolve tudo. **Gazeta Mercantil**. São Paulo, p. 3-4. jun. 1999.

FACINA, A. L. **Hardening no OpenBSD**.2009. Disponível em: <http://www.vivaolinux.com.br/dica/Hardening-no-OpenBSD>. Acesso em: 07 abr. 2016.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**: Guia prático para elaboração e implementação. 2ª ed. Rio de Janeiro: Ed. Ciência Moderna, 2008.

FONTES, Edison, CISM, CISA. **Políticas e normas para a segurança da informação**: como desenvolver, implantar e manter regulamentos para a proteção da informação nas organizações. Rio de Janeiro: Ed. Brasport, 2012.

FONTES, Edison, CISM, CISA. **Praticando segurança da informação.** Rio de Janeiro: Ed. Brasport, 2008.

FONTES, Edison, CISM, CISA. **Segurança da informação**: o usuário faz diferença. São Paulo: Ed. Saraiva, 2006.

GUPTA, A., **Enterprise resource planning: the emerging organizational value systems**, Industrial Management & Systems, Vol. 100 No. 3, pp. 114-18, 2000.

LYRA, Maurício Rocha. **Segurança e auditoria em sistema de informação**. Rio de Janeiro: Ed. Ciência Moderna, 2008.

MOLINARI, Leonardo. **Produzindo sistemas melhores e mais confiáveis**. São Paulo. Ed. Érica, 2003.

MUSCATELLO, Joseph R.; SMALL, Michael H.; CHEN, Injazz J.. Implementing enterprise resource planning (ERP) systems in small and midsize manufacturing firms. **Int Jrnl Of Op & Prod Mnagemnt,** [s.l.], v. 23, n. 8, p.850-871, ago. 2003. Emerald.

OLIVEIRA, M.A., RAMOS, A.S.M. Fatores de sucesso na implementação de sistemas integrados de gestão empresarial (ERP): estudo de caso em uma média empresa. In: **Encontro Nacional de Engenharia de Produção**. Anais. Curitiba, 2002.

PROVSUL. **Sistemas ERP**. Disponível em: <http://www.provsul.com.br/gestao.htm> Acesso em: 28 Mar. 2016.

REIS, F. A. D.; VERBENA, M. F.; JULIO, E. P. **Segurança**. Infra Magazine, v. 1, n. 01, p. 19-30, 2011.

STAMFORD, P. P.. **ERPs: prepare-se para esta mudança**. 2000. Disponível em: <http://www.kmpress.com.br/>. Acesso em: 29 abr. 2016.

SOARES, Gildo. **A ferramenta Microsoft Baseline Security Analyzer (MBSA)**. Disponível em: <https://technet.microsoft.com/pt-br/library/cc668448.aspx> Acesso em: 30 mar. 2016.

SOUZA, C. A. & ZWICKER, R. **Ciclo de vida de sistemas ERP**. Caderno de Pesquisa em Administração, vol. 1, num. 11, 1º. Trim., 2000.

SOUZA, C. A. **Sistemas integrados de gestão empresarial**: estudos de casos de implementações de sistemas ERP. 2000. 305 f. São Paulo: Dissertação (Mestrado em Administração) - Departamento de Administração da Faculdade de Economia, Administração e Contabilidade, Universidade de São Paulo, 2000.

TURBAN, Efraim. **Administração de tecnologia da informação**: teoria e prática. Rio de Janeiro: Ed. Elsevier, 2005.

TURBAN, E. et al. **Tecnologia da Informação para Gestão**. Porto Alegre: Ed. Bookman, 2004.

VICO MANÃS, Antonio. **Administração de sistema de informação**. 8ª ed. São Paulo: Ed. Érica, 2010.

VIEGAS, Alberto Luiz. **Segurança de aplicações WEB:** Hardening nos servidores baseados em software livre. 2008. 121 f. Monografia (Especialização) - Curso de Latto Sensu, Instituto Brasileiro de Tecnologia, Recife, 2008.

WAZLAWICK, Raul Sidnei. **Metodologia de pesquisa para ciência da computação**. Rio de Janeiro: Ed Elsevier, 2009.