UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

XX Curso de Pós-graduação em Teleinformática e Redes de Computadores

TATIANA SILVA NOVO

SEGURANÇA DA INFORMAÇÃO NO USO DE SMARTPHONES EM AMBIENTE CORPORATIVO

MONOGRAFIA DE ESPECIALIZAÇÃO

Curitiba – PR

2011

TATIANA SILVA NOVO

SEGURANÇA DA INFORMAÇÃO NO USO DE SMARTPHONES EM AMBIENTE CORPORATIVO

Monografia apresentada como requisito parcial para a obtenção do título de Especialista em Teleinformática e Redes de Computadores da Universidade Tecnológica Federal do Paraná, UTFPR.

Orientador: Prof. Msc. Lincoln Herbert Teixeira

Curitiba 2011

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Diretoria de Pesquisa e Pós-Graduação do *Campus* Curitiba
Departamento Acadêmico de Eletrônica
Especialização em Teleinformática e Redes de Computadores

TERMO DE APROVAÇÃO

Título da Monografia
Segurança da informação no uso de smartphones em ambiente corporativo

por

Tatiana Silva Novo

Esta monografia foi apresentada às 21:00h do dia 15 de dezembro de 2011 como requisito parcial para a obtenção do título de ESPECIALISTA EM TELEINFORMÁTICA E REDES DE COMPUTADORES, Universidade Tecnológica Federal do Paraná. A candidata foi argüida pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado com a nota 10,0 (dez inteiros).

Prof. Lincoln Herbert Teixeira
(UTFPR)

Prof. Walter Godoy Junior
(UTFPR)

Visto da Coordenação

Prof. Dr. Walter Godoy Júnior
Coordenador do Curso

O perigo desaparece quando ousamos enfrentá-lo.

(François Chateaubriand)

RESUMO

Esta pesquisa tem o objetivo de apresentar e analisar as principais tecnologias de segurança da informação no uso de dispositivos móveis via rede wireless. O enfoque deste trabalho está na evidência do uso crescente de Smartphones em ambiente corporativo e a importância da implantação de soluções de gestão da informação utilizando tecnologias de segurança que assegurem a integridade dos dados acessados por qualquer dispositivo. Aborda também os principais métodos de segurança no uso de smartphones pessoais e faz uma rápida descrição da segurança de Tablets. Esta pesquisa faz paralelamente uma análise do fenômemo chamado de “SHADOW IT” ou IT Invisível e o desafio do departamento de TI para garantir segurança a toda informação da organização. Este trabalho discute a importância da gestão de informação corporativa e o enfoque na segurança de dados acessados por dispositivos móveis. Descreve um estudo de caso utilizando smartphones Blackberry da RIM em redes corporativas, e faz um estudo comparativo entre o Blackberry e o iPhone da Apple, apresentando as características e principais funcionalidades de cada aplicativo de segurança analisado. Traz como resultado uma ampla documentação sobre as ameaças e vulnerabilidades existentes no uso de dispositivos móveis e qual o melhor método e ação para assegurar maior integridade e confiabilidade no uso da informação por dispositivos móveis via rede wireless.

Palavras-chaves:

Smartphones, Segurança da Informação, Rede Wireless, SHADOW IT, Tablets.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

TI - Tecnologia da Informação

TIC - Tecnologias da Informação e da Comunicação

WI-FI - Wireless Fidelity

AP - Access Point

IEEE - Institute of Electrical and Electronic Engineers

ERB - Estação Rádio Base

WLAN - Redes locais sem Fio

WMAN - Redes metropolitanas sem fio

WWAN - Redes de longa distância sem fio

WLL - Wireless Local Loop

WPAN - Wireless Personal Area Network

WiMAX - Worldwide Interoperability for Microwave Access

RIM - Research in Motion

MDM - Mobile Device Management

BES - Blackberry Enterprise Server

BYOD - Bring Your Own Device

CIO - Chief Information Officer

SMS - Short Message Service

GLOSSÁRIO

Hacker - indivíduos que elaboram e modificam software e hardware de computadores e tem grande conhecimento de informática. Em português o significado é Decifrador. [36]

Cracker - expressão original para invasores de computadores, peritos em informática que fazem o mau uso de seus conhecimentos, utilizando-o tanto para danificar componentes eletrônicos, como para roubo de dados, sejam pessoais ou não. [36]

Malware - proveniente do inglês *malicious software*. Software destinado a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Vírus de computador, worms, trojan horses (cavalos de tróia) e spywares são considerados malware. [37]

Jailbreak - método para desbloquear dispositivos da Apple, como o iPhone, iPad ou iPod. É também possível habilitar algumas funções como gravação de vídeo, utilizar mais de um aplicativo ao mesmo tempo, personalizar o tema do sistema operacional ou mandar mensagens multimídia. [38]

Bluetooth - é uma especificação industrial para áreas de redes pessoais sem fio (Wireless personal area networks – PANs). O Bluetooth provê uma maneira de conectar e trocar informações entre dispositivos como telefones celulares, notebooks, computadores, impressoras, câmeras digitais e consoles de videogames digitais através de uma frequência de rádio de curto alcance. [39]

1. INTRODUÇÃO

A informação é um dos bens mais valiosos das organizações e a segurança da informação é extremamente importante nos dias de hoje à medida que o número de ataques a redes de computadores e a infecção por vírus aumenta de maneira significativa. E devido ao crescimento vertiginoso do uso de dispositivos móveis, e portanto a massificação do uso de aparelhos como smartphones e tablets, esta tendência traz um desafio a área de TI: a importância de assegurar a confiabilidade e segurança da informação acessada por dispositivos móveis, da mesma maneira que a segurança da informação aos computadores pessoais. [4]

As redes Wi-Fi, que funcionam sem a necessidade de fios, estão cada vez mais comuns. Os equipamentos para construir esse tipo de rede estão com preços bem acessíveis e não é difícil configurá-los. Notebooks, netbooks, smartphones e até tocadores digitais, como o iPod touch, possuem conectividade Wi-Fi. Às vezes a comodidade é tanta que preocupações com segurança nem passam pela cabeça do usuário.

A internet portátil traz esta nova realidade. Os smartphones são utilizados para muito mais que simples trocas de e-mail e com a popularização desses aplicativos e o uso para outros tipos de movimentações, como acesso a contas bancárias e redes sociais, é preciso voltar a atenção para a segurança da informação, já que muitas empresas já utilizam smartphones em ambiente corporativo para a sincronização de e-mails, calendários e troca de outras informações de uso restrito da companhia.

A ISO 27000 estabelece diretrizes e normas que permitem aos colaboradores em geral das organizações seguir padrões de comportamento, no que se refere a Segurança da Informação, adequados às necessidades de negócio e de proteção legal da organização e do indivíduo. Mas agora surge a dúvida, como TI pode monitorar um colaborador que se utiliza de tablets e smartphones? [3]

É preciso analisar também o uso crescente de "SHADOW IT" e a consequência disso, pois esse fenômeno tem obrigado o departamento de TI a atuar de forma cada vez mais integrada e aderente às demandas do negócio da companhia, de um modo geral. [9]

Enfim, é necessário que as empresas estejam conscientes das ameaças e vulnerabilidades que a internet portátil traz ao ambiente corporativo, e também ao usuário final que pode ter a conta bancária ou outros dados importantes roubados. Existem tantos métodos e formas de ataques de hackers para o roubo de informações corporativas que é de extrema importância a implementação de sistema de segurança que garanta

a integridade e confidencialidade dos dados em todo o ambiente corporativo, assim como dicas úteis de segurança ao usuário final.

O objetivo deste trabalho é apresentar e analisar as principais tecnologias de segurança da informação no uso de dispositivos móveis via rede wireless em ambiente corporativo. Entretanto o enfoque desta pesquisa está no uso de smartphones corporativos, dispositivo móvel muito utilizado no momento para troca de informações dentro da organização. Este trabalho faz uma análise do uso crescente de “SHADOW IT” ou *TI Invisível* e o desafio do departamento de TI para garantir segurança da informação em todo o ambiente corporativo. Ao final é feito a conclusão desta pesquisa com os principais métodos utilizados hoje para segurança da informação no uso de dispositivos móveis.

No capítulo 2, são apresentados os conceitos de Dispositivos móveis se concentrando nos dispositivos mais populares atualmente, o Smartphone e o Tablet. É também analisada a tendência do uso crescente destes dispositivos e ao final deste capítulo, são apresentadas e discutidas as principais ameaças e vulnerabilidades encontradas no uso de dispositivos móveis. No capítulo 3 aborda-se o fenômeno de SHADOW IT com a discussão da gestão de TI com o uso crescente de TI Invisível.

No capítulo 4 são apresentadas as principais tecnologias de segurança da informação, com foco na segurança de Smartphones Corporativos. E no capítulo 5 é apresentado um estudo de caso utilizando o Smartphone Blackberry da RIM e também um estudo comparativo entre as vantagens e desvantagens entre o Blackberry e o iPhone da Apple.

Por fim a conclusão do trabalho ressaltando a importância de segurança para uso de dispositivos móveis e as melhores soluções.

2. DISPOSITIVOS MÓVEIS

Mobilidade é o termo utilizado para identificar dispositivos que podem ser operados a distância ou sem fio e permitem a comunicação com outras pessoas e a obtenção de informações em qualquer lugar, a qualquer hora.

A primeira tecnologia a utilizar o termo mobilidade foi o telefone celular. O conceito de telefone celular foi desenvolvido em 1960, tornando-se comercialmente disponível a partir do início dos anos 80. A introdução do telefone celular ao mundo foi em 1981, no Japão e na Escandinávia, e nas Américas, em 1983. E essa tecnologia se expandiu muito rapidamente. Em menos de 30 anos alcançou cerca de 5 bilhões de telefones celulares ao redor do mundo.

Cada região atendida pelo Serviço de Telefonia Móvel Celular é dividida em pequenas áreas, chamadas células, que possuem uma Antena Celular (ou ERB - Estação Rádio Base), para receber e emitir informações aos telefones celulares que estão em operação naquela célula.

Ao longo da última década, o número de novos dispositivos foi ampliado largamente, com os laptops e seus modems 3G, netbooks, iPods, smartphones e tablets. Esses novos dispositivos tendem a multiplicar aceleradamente nos próximos 10 anos.

De acordo com Lichty, "o indivíduo móvel é um nômade, que se move de um lugar para outro sem perder contato com o coletivo da “aldeia” eletrônica. Desde que estejam em sua rede de recepção, eles ainda estão (presumivelmente) disponíveis". [8]

O design para dispositivos móveis se difere do design para outras interfaces de várias maneiras e a maioria destas diferenças estão relacionadas ao fato do usuário levar o dispositivo para qualquer lugar aonde vá.

Nos últimos anos, os equipamentos sem fio para internet e serviços móveis como telefonia móvel, cresceram de forma acelerada, tendo em vista o surgimento de novas tecnologias nesta área, de redes sem fio e serviços móveis. Com tendência a tomar um espaço cada vez maior com o passar dos anos, devido aos imensos benefícios proporcionados pelos mesmos. [14]

2.1. Comunicação entre dispositivos móveis e redes sem fio

A comunicação entre a rede móvel (dispositivos móveis) e a rede sem fio (wireless) é feita através da **Estação Rádio Base** (ERB), que é a responsável pelo envio e recebimento de dados de e para um *hospedeiro*

sem fio, equipamentos sem fio, associado a ela, sendo responsável pela coordenação de transmissão desse hospedeiro. As ERBs podem ser torres de celulares (em redes de celulares) e pontos de acesso (em uma WLAN - sem fio). [14]

Um hospedeiro (equipamento sem fio) pode estar associado a uma estação-base de duas maneiras:

- O equipamento está dentro do alcance de comunicação sem fio da estação-base;
- O equipamento usa a estação-base para retransmitir dados entre ele e a rede maior.

E por fim opera em modo de infra-estrutura quando ele está associado com uma estação-base, desta forma todos os serviços básicos são fornecidos a ele pela rede a qual está associado. Os hospedeiros podem realizar transferências (handoff), mudando seu ponto de conexão com a rede maior, quando se deslocam para fora da faixa de alcance de uma ERB.

Figura 1. Dispositivos Móveis. [40]

2.2. SMARTPHONES

Smartphone significa telefone inteligente, numa tradução livre do inglês, é um telefone celular com funcionalidades avançadas e sistema operacional. Os smartphones são a combinação de duas classes de dispositivos: os celulares e os assistentes pessoais (Palms e PDAs). A principal vantagem dos smartphones, comparados aos antecessores, é que podem se conectar à web através de conexões 3G ou WI-FI, o que permite que eles ofereçam uma enorme variedade de recursos.

Um smartphone pode concentrar um grande volume de funções em um aparelho de pouco peso, pode ser carregado no bolso e tem acesso contínuo à web. Hoje em dia, mesmo um modelo de smarthphone relativamente simples e barato pode navegar na web, acessar e-mail e chats, fazer chamadas VoIP, fazer uso da camera fotográfica, servir como player de música, exibir e gravar vídeos e tambem utlizar outros recursos com o navegador GPS. [17]

O grande trunfo está na possibilidade de instalar aplicativos adicionais, o que permite que os smartphones executem inúmeras outras funções. Esse conjunto de fatores tem feito com que eles se tornem cada vez mais indispensáveis.

Os principais modelos e marcas que encontramos hoje no mercado são: iPhone da Apple, Blackberry da RIM, Motorola Spice key, Galaxy s da Samsung, XPeria da Sony Ericsson, Nokia C7, Optimus da LG, e outros. Estes aparelhos são baseados em diversas plataformas, incluindo o Android, o Symbian, o Windows Mobile e o sistema do Blackberry.

2.3. TABLETS

Após o lançamento do iPad pela Apple e do Galaxy Tab pela Samsung, houve um grande avanço no universo da mobilidade via rede wireless. Eles fazem parte de uma nova era de tablets. No passado era comum ver no mercado uma versão anterior de tablet, chamada de Tablet PC, que era um computador pessoal com o formato de prancheta, que com um toque de uma caneta especial era possível accessar aplicacões, sem a necessidade de mouse ou teclado.

O novo conceito do Tablet de hoje, após o iPad, é um dispositivo pessoal em formato de prancheta com acesso à internet, que não deve ser igualado a um computador completo ou um Smartphone, embora possua diversas funcionalidades dos dois. Este novo dispositivo disponibiliza vários

recursos como leitura fácil e rápida de jornais, revistas e livros, visualização de fotos, vídeos, organização pessoal e entretenimento com jogos 3D. [18]

A popularização do Tablet se iniciou com o lançamento do iPad, da Apple. Logo após entraram no mercado outros modelos de fabricantes concorrentes, como o Galaxy Tab da Samsung. Alguns novos modelos, como da HP, inseriram alguns recursos adicionais aos do iPad, como câmera para videoconferência, portas USB, entrada para cartão de memória e plugin para visualização.

Alguns dos Tablets mais conhecidos, além do iPad e do Galaxy Tab, sao: HP Slate 500, Motorola Xoom, Toshiba Tablet, Blackberry Playbook, LeNovo IdeaPad U1 Hybrid, Coby Kyros entre outros que sugem no mercado.

E uma curiosidade, existem os tablets específicos para a área hospitalar, como o CL900 ou C5V, da Motion computing.

2.4. O FUTURO DOS DISPOSITIVOS MÓVEIS

Análises e estudos referentes a dispositivos móveis, sugerem que ao final desta década a mobilidade vai superar largamente os limites atuais da telefonia móvel e que haverá cerca de 55 bilhões de dispositivos móveis, entre celulares comuns, Smartphones, iPods, Tablets e outros novos dispositivos. [7]

As tecnologias de computação móvel encontram-se em franca evolução, parecem destinadas a se transformar no novo paradigma dominante da computação atual e, provavelmente, das gerações futuras (Myers et al., 2003 apud MARÇAL, ANDRADE e RIOS, 2005). [8]

Um exemplo é a internet móvel que se aproxima dos 800 milhões, incluindo os usuários de laptop, de celulares de terceira geração (3G), Smartphones, iPods e Tablets. E com o desenvolvimento amplo de softwares e aplicativos para dispositivos móveis, a tendência é o aumento crescente de usuários e novas tecnologias para este fim. Pois ao longo da última década, o número de novos dispositivos tem aumentado consideravelmente, com os laptops e seus modems 3G, netbooks, iPods, tablets e iPads. Esses novos dispositivos tendem a multiplicar aceleradamente nos próximos 10 anos.

Haverá grande expansão do número de pessoas que utilizarão a computação móvel, o comércio móvel (m-comm), a videoconferência, a TV móvel e diversas outras aplicações voltadas para este fim.

Num evento ocorrido neste ano em Barcelona, no Mobile World Congress 2011, foram divulgados dados da Wireless Intelligence (www.wirelessintelligence.com), que mostram a expansão incomum do

número de países que já tem mais celulares do que habitantes, incluindo os Smartphones. Na América Latina, a Argentina alcança a média de 133 celulares por 100 habitantes e o Brasil supera os 107% de celulares. O Brasil disputa hoje o sexto lugar entre os maiores mercados de telefonia móvel do mundo, com 206 milhões de celulares em serviço. O primeiro lugar está atualmente com a China, com 842 milhões. [7]

E recentemente um novo elemento vem tomando grandes proporções no mercado de mobilidade, que é o Tablet, e a tendência é que e sua utlização seja adotada por milhões de usuário em futuro próximo.

2.5. AMEAÇAS E VULNERABILIDADES

Cada vez mais populares, smartphones e tablets estão na mira de cibercriminosos, segundo pesquisas e especialistas em segurança. Infelizmente os usuários não estão cientes das ameaças e da vulnerabilidade do uso de dispositivos móveis, e por isso dispensam menos cuidados com a segurança de um smartphone do que os mesmos cuidados que teriam com os computadores pessoais. [21]

Hoje é muito frequente e também muito preocupante a rapidez com que é desenvolvido malware nos smartphones. Esses dispositivos possuem muita informação confidencial e portanto é imprescindível protegê-la.

A ameaça não é recente. O primeiro vírus para celular foi descoberto em 2004 e tinha como foco a plataforma Symbian, a mais usada até então. O número de vírus e de malwares para celular só aumentou, a estimativa é de 2 mil tipos diferentes, voltados a todos os sistemas operacionais. Com isso as previsões não são nada animadoras, o volume tende a crescer ainda mais. [20]

Dois dos vírus mais comuns em celulares são o Skulls, transmitido por downloads, que substitui todos os aplicativos do celular e transforma os ícones em caveiras e o Crossover, que pode ser transmitido via bluetooth, e apaga todo o conteúdo da pasta “Meus Documentos”. [10]

Uma ameaça recentemente descoberta é a aplicação clandestina chamada "Carrier IQ" a qual foi construída para uso da maioria dos smartphones, e não somente faz o rastreamento da sua localização, como retém o registro de suas teclas. E embora o "Carrier IQ" atinja a maioria de celulares com o sistema Android, os aparelhos Blackberry e Nokia também são alvos de ataque. [22]

Os sistemas operacionais também apresentam vulnerabilidade. O Android, do Google, é hoje o alvo preferencial dos hackers, por ser o sistema

para smartphone mais popular nos dias de hoje e principalmente por sua natureza aberta onde é possível instalar aplicativos vindos de qualquer origem.

Outra novidade de ataque voltada para dispositivos móveis, é uma nova versão do SpyEye que opera nas plataformas Symbian, Blackberry e Android com o objetivo de invadir os sistemas de dupla autenticação para acessar informações do usuário. O SpyEye é um cavalo de tróia capaz de gerar uma “rede zumbi” e roubar contas bancárias. Segundo a empresa de segurança ESET, as ações dos hackers envolvidos já resultou no roubo de mais de 3 milhões de dólares. O SpyEye tem maior atividade na Europa e Canadá, ainda não sendo tão comum no Brasil. [13]

Com este cenário é fácil perceber que os smartphones passaram a ser alvos fáceis dos hackers, principalmente porque as pessoas estão usando seus aparelhos para fazer pagamentos e acessar contas e portanto o smartphone passou a ser visto como uma forma lucrativa e fácil.

Quais são as ameaças:

- Um vírus para celular pode permanecer imperceptível e utilizar plano de dados da conta do usuário indevidamente
- Uma vez infectado, o usuário pode servir como um retransmissor de mensagens SMS, na maioria das vezes mensagens mal intecionadas
- Por utilizar dados e SMS indevidamente, a conta do usuário pode apresentar cobranças de serviços não utilizados
- Um vírus ou um malware pode ser programado para captar informações confidenciais como número e senha da conta do usuário

A preocupação com estas vulnerabilidades estende-se aos mais variados tipos de dispositivos e os ataques podem surgir de várias formas. O download de aplicativos é a forma mais fácil de contaminação, mas mensagens via SMS e Bluetooth também são portas de entrada latentes. Uma das técnicas usadas por criminosos é enviar SMS com links para endereços mal intencionados, que, ao serem clicados, instalam o malware instantaneamente. Essa mesma mensagem pode enviar dados sigilosos do usuário para o hacker que desenvolveu o malware. [20]

No Capítulo 4 serão abordados as principais tecnologias de segurança para proteção de dados no smartphone.

3. SHADOW IT (TI Invisível)

O fácil acesso a softwares e aplicações juntamente com o avanço de novas tecnologias e as novidades da Internet (Web 2.0) provocaram um impacto inusitado na informática corporativa. Apesar de todo o controle e padronização, a informática clandestina tem crescido assustadoramente e feito um alerta aos administradores de segurança de TI das organizações. [8]

Shadow IT é o termo recentemente utilizado para descrever sistemas e soluções de TI desenvolvidos e utilizados dentro de uma organização mas sem a aprovação da organização. A shadow IT é aquela feita fora do alcance das áreas centrais. As soluções Shadow IT frequentemente não estão alinhadas com as padronizações e requisições da organização quanto a controle, segurança e confiabilidade. Não se trata de uma descentralização planejada, mas intencional ou não, a prática de Shadow IT se manifesta através da compra de pequenos equipamentos (ex. dispositivos móveis), de aplicativos específicos e outros. E com o surgimento em larga escala de serviços e utilitários de uso pessoal, o uso de TI Invisível tem invadido o mundo corporativo. Do uso pessoal para alguma utilidade de negócios é só um pulo, pois o acesso é muito simples e fácil para o usuário, basta uma conexão à rede e nada de infra-estrutura, sem necessidade de acordo ou contratos, ou seja à sombra de TI.

Pesquisas realizada pela IDC para a Unisys, em maio de 2011, descobriu que 95 por cento dos profissionais da informação utilizam tecnologia pessoal no trabalho - ou seja, aproximadamente o dobro do que os executivos das mesmas empresas entrevistadas estimaram. E a IDC prevê que o uso de smartphones de propriedade dos empregados no local de trabalho vai dobrar até 2014. [15]

Alguns exemplos deste fluxo de dados irregulares (não autorizados), são drives USB, ou outro dispositivo portátil de armazenamento de dados, o MSN Messenger ou outro software similar de mensagens, Google Docs ou outro software online de compartilhamento de documentos, e também desenvolvimento próprio de aplicações em Excel, Access, macros, etc.

As razões para uso de Shadow IT são inúmeras, geralmente se acredita que os funcionários de uma organização procurem por um jeito mais fácil de se conseguir o que precisam para finalizar seus trabalhos. Por exemplo, eles podem usar planilhas para análise de dados, e por ter acesso livre a aplicação, eles podem trocar informação com qualquer um e ainda obter o resultado que precisam.

Um estudo confirma que 35% dos empregados sentem que precisam contornar as medidas de segurança ou protocolo, para serem capazes de realizar o seu trabalho de modo eficiente. E 63% das pessoas empregadas,

enviam documentos do email corporativo pora o endereço de email pessoal, para continuarem o trabalho de casa, mesmo quando estão cientes de que isto não seria permitido. [19]

As implicações destas acões de Shadow IT, além dos riscos de segurança, também causam: lógica de negócios inconsistentes; perda de tempo; abordagem de negócio inconsistente; desperdício do investimento feito; Ineficiência, e por fim a barreira do aprimoramento do negócio ou tecnologia.

3.1. O PAPEL DE TI E A GESTÃO DE "SHADOW IT"

O surgimento de Shadow IT e o uso crescente de dispositivos móveis dentro das organizações, traz um desafio a área de TI: a segurança. Usuários têm acesso a inúmeras soluções que dispensam qualquer suporte especializado. Este cenário mostra como é importante posicionar o departamento de TI para essa nova realidade.

Nathan Clevenger, arquiteto chefe de software de dispositivos móveis da empresa de gestão ITR e autor do livro "iPad na empresa" (Wiley, 2011), diz que o iPhone e iPad são os catalisadores para o consumo de TI. Desta maneira, departamentos de tecnologia podem permitir que eles sejam usados de forma segura ou assumir as conseqüências do risco. "É melhor que a TI suporte os dispositivos e as tecnologias demandadas pelos usuários, porque de qualquer modo eles usarão a tecnologia pessoal para fins comerciais", diz Clevenger. [15]

Neste novo cenário, os departamentos de TI estão aprendendo a conviver e a lutar para gerenciar dados corporativos com segurança, mas ainda é preciso encontrar um meio termo em manter a tecnologia de consumo fora do local de trabalho mas também permitir o acesso irrestrito à rede a partir de qualquer dispositivo. É necessário uma solução de gestão que garanta a segurança da informação corporativa, mas que também permita gerir os custos com um impacto mínimo nas operações de TI e infra-estrutura.

A TI encontra um dilema nos dias de hoje, precisa descobrir como tirar a Shadow IT do escuro e trazê-la para a luz, garantindo suporte e segurança, ou se arriscar à medida que líderes de negócio, cada vez mais familiarizados com tecnologia, tomarem os processos de inovação em suas mãos.

Por final TI deve tomar as seguintes iniciativas abaixo, a fim de melhorar o relacionamento com os colaboradores e assim ter um melhor controle dos sistemas e aplicações utilizadas dentro da organização: [16]

- procurar ser um parceiro de negócio melhor
- oferecer opções de TI mais flexíveis
- educar os usuários sobre os riscos e falta de segurança ao utilizar dispositivos e aplicações não padronizadas pela organização.

4. TECNOLOGIAS DE SEGURANÇA

Apesar de crescente, a quantidade de ataques a smartphones e Tablets é ainda pequena se comparada ao grande número de vírus que circulam todos os dias pela web e que atacam desktops e notebooks. Mesmo assim, prevenção é uma das melhores formas de se proteger. E com o rápido aumento do uso de dispositivos móveis dentro das organizações, é importante que todos tenham consciência da necessidade de proteção a estes dispositivos, mesmo que seja um simples Pendrive. No caso deste, recentemente foi lançado pela Kingston, o modelo DTLocker+ que garante a segurança do conteúdo do pendrive através do registro de senha, seguindo o padrão "strong password", e protege o acesso aos dados armazenados.

Quanto aos dispositivos móveis que são a sensação no mercado atual, o Smartphone e o Tablet, um relatório da AVG Technologies divulgado em março indica que mais de 0,2% dos aplicativos baixados na Android Market eram mal intencionados. Levando em conta que 3,9 bilhões de aplicativos foram baixados desde a inauguração da loja, pode-se estimar que 7,8 milhões de aplicativos contendo algum tipo de ameaça foram instalados. E este número é alarmante. [20]

Como visto no capítulo 2 sobre Ameaças e Vulnerabilidades dos dispositivos móveis, o risco de um dispositivo ser infectado por vírus ou malwares como o SpyEye e outros, tem aumentado a cada dia. Por essa razão tanto os usuários como as empresas devem tomar as medidas de proteção e seguir os protocolos e políticas de segurança a fim de proteger dados confidenciais.

Com foco neste tema, de segurança no uso de Smartphones e recentemente a do Tablet, serão abordados nos próximos tópicos deste capítulo o conceito da Segurança da Informação e de segurança em Rede Wireless, e então são apresentadas as principais tecnologias de segurança aplicadas ao uso de smarthones, corporativos e também de uso pessoal. ao final deste capítulo é mencionado também as novidades de segurança para uso de tablets.

4.1. SEGURANÇA DA INFORMAÇÃO

O conceito de Segurança em Informática ou Segurança de Computadores está totalmente relacionado com o de Segurança da Informação. O conceito se aplica a todos os aspectos de proteção de informações e dados. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade. [1]

Com a rapidez que surgem novas tecnologias, o acesso à informação está cada vez mais rápido e simples, entretanto esta facilidade tem tornada a informação também mais frágil. Com isso foram criadas normas específicas para a padronização dos sistemas de informação em geral.

> A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita ser adequadamente protegido (NBR ISO/IEC-17799, 2001). [1]

Em setembro de 1997 foi lançada a RFC2196, definida em sua literatura como um "guia de desenvolvimento de políticas de segurança de computadores e procedimentos para sites que tem seus sistemas na Internet" (FRASER, 1997). E também surgiu a NBR ISO/IEC-17799, homologada pela ABNT (Associação Brasileira de Normas Técnicas) em setembro de 2001. [1]

Atualmente a ISO 27000 trata de Segurança da Informação. Esta norma estabelece diretrizes que permitam que padrões de comportamento, referente a Segurança da Informação, sejam seguidos e adequados às necessidades de negócio e de proteção legal da organização e do indivíduo. A norma busca preservar as informações da organização no que tange a confidencialidade, integridade e a disponibilidade. [3]

Sabendo-se que a organização reserva-se o direito de monitorar e registrar todo o uso das informações, sistemas e serviços, isso requer gestão e o controle apropriado de todos os registros de atividades em todo os pontos e sistemas da empresa, incluindo computadores (desktop/notebooks), acesso a internet, correio eletrônico e sistemas. Recentemente este controle também deve abranger as atividades e o uso de dispositivos móveis para acesso de informação da organização.

As grandes empresas estão lançando mão de novos recursos e tecnologias que visam a segurança da informação para este fim, o de monitoramento dos colaboradores que utilizam "Smartphones" e "tablets" assegurando integridade e confidencialidades às informações acessadas via dispositivos móveis.

A velocidade da informação e das mudanças tecnológicas exigem que o profissional de Tecnologia da Informação (hardware e Software), Compliance (Normas e Riscos), Auditoria e Controladoria aprimore suas atividades profissionais e evidencie que todos fazem parte da validação e da normatização (ISO 2700) na busca pela segurança de nossas informações. [3]

É importante salientar que as maiores ameaças de Segurança da Informação em 2011 foram os ataques às redes sociais e Smartphones, de acordo com o relatório de segurança da Sophos referente a dados de 2010 e 2011. [5]

4.2. SEGURANÇA EM REDES WIRELESS

A rede wireless também conhecida como rede sem fio é caracterizada por qualquer tipo de conexão para transmissão de informação sem a utilização de fios ou cabos.

As primeiras redes sem fio baseadas em ondas de rádio ganharam notoriedade no início dos anos 90, quando os processadores se tornaram mais rápidos a ponto de suportar tal aplicação. Nesta mesma década, as atenções se voltaram para o novo modelo do IEEE (Institute of Electrical and Electronic Engineers), o 802.11b. Em 1999 o IEEE finalizou o padrão 802.11b (11Mbps a 2,4GHz) e em 2002 foi distribuído ao mercado o 802.11a (54Mbps a 5GHz), que é incompatível com o padrão 802.11b. No mesmo ano foi ratificado o padrão 802.11g (54Mbps a 2,4GHz), que opera na mesma velocidade do 802.11a e na mesma frequência do 802.11b. [2]

Pode-se citar algumas tecnologias que utilizam este modelo de comunicação através de rede sem fio, como o WI-FI, InfraRed (infravermelho), Bluetooth e WiMax.

Quanto a categoria, os tipos de rede são: Redes Locais sem Fio ou WLAN (Wireless Local Area Network), Redes Metropolitanas sem Fio ou WMAN (Wireless Metropolitan Area Network), Redes de Longa Distância sem Fio ou WWAN (Wireless Wide Area Network), redes WLL (Wireless Local Loop) e o novo conceito de Redes Pessoais Sem Fio ou WPAN (Wireless Personal Area Network).

Em uma rede wireless, o dispositivo transceptor (transmissor e receptor) ou ponto de acesso (AP - access point) é conectado a uma rede local Ethernet convencional, ou seja, com cabo. Os pontos de acesso não apenas fornecem a comunicação com a rede convencional, como também intermediam o tráfego com os outros pontos de acesso. O ponto de acesso tem a mesma função central que o Hub desempenha nas redes com fio, que é a retransmissão dos pacotes de dados. E no caso da rede sem fio, as antenas são utilizadas ao invés dos cabos de rede.

Pela facilidade de instalação e uso, as redes sem fio estão crescendo cada vez mais. Além da questão da praticidade, as redes wireless podem ser utilizadas em casos onde não é viável usar cabos. A transmissão sem fio é atualmente um método comum de comunicação de dados utlizados por WLANs (Redes Wireless), telefones celulares, PDAs, pagers, e recentemente pelos mais populares dispositivos móveis, os Smartphones e os Tablets.

Como já visto, as redes Wi-Fi estão cada vez mais comuns. Os equipamentos para construir esse tipo de rede estão com preços bem

acessíveis e não é difícil configurá-los. Notebooks, Netbooks, Smartphones, Tablets e outros dispositivos, possuem conectividade Wi-Fi. Por esta demanda de uso da rede sem fio, a segurança em rede wireless é essencial, assim como a definição de políticas e padrões para dispositivos sem fio também é essencial.

Usando o exemplo de um notebook que utiliza a rede sem fio, este dispositivo ao acessar uma LAN através de comunicação wireless, deverá ativar a rede através da tecnologia VPN (Virtual Private Network), além de fazer uso da proteção de anti-vírus e de firewall.

Alguns fatores que definem a segurança em uma rede sem fio pode ser resumida aos seguintes elementos: controle de acesso, autenticação e criptografia. [11]

Existem atualmente três padrões de encriptação, o WEP de 64 bits, o WEP de 128 bits e o WPA, o padrão mais recente e mais seguro. Embora nenhum dos três esteja livre de falhas, elas são uma camada essencial de proteção, evitando que a rede utilizada seja um alvo fácil. O WEP é relativamente fácil de quebrar, usando ferramentas como o kismet e ao aircrack, mas o WPA pode ser considerado relativamente seguro. [6]

A regra básica é que os computadores ou dispositivos móveis possuam a chave correta para se associarem ao ponto de acesso e acessarem a rede. Em geral os pontos de acesso permitem que você especifique várias chaves diferentes, de forma que cada acesso pode usar uma chave diferente.

Uma rede sem fio deve garantir: [2]

- Sigilo - o sinal transmitido pela rede não pode ser decodificado por qualquer receptor atuante na área em que o sinal estiver ativo.
- Integridade da Informação - garantir que os dados trafegados na rede não sejam alterados entre o receptor e o transmissor.
- Disponibilidade da Rede - manter a rede acessível.
- Autenticidade - fazer a autenticação do acesso à rede.

4.3. SEGURANÇA EM SMARTPHONES

Como visto no capítulo 2, são várias as ameaças e vulnerabilidades encontradas no uso de smartphones, pois os usuários ainda não tem consciência da importância de proteger o seu aparelho contra ataques de vírus e de malwares. Principalmente por serem multi-função e possuírem

uma grande capacidade de memória estes aparelhos podem armazenar muitas informações confidenciais como conta de banco, agenda de contatos, compromissos, arquivos e planilhas, conta de e-mail e de redes sociais.

Mesmo procedimentos básicos como a senha de proteção do aparelho, os usuários se descuidam. Estudos revelaram que menos de 20% dos usuários protegem o celular com senha, por exemplo.

O download de aplicativos, mensagens via SMS e Bluetooth são as formas de ataques mais utilizados. E os sistemas operacionais também apresentam vulnerabilidades, uns são mais vulneráveis que outros. O iOS (iPhone e iPad), por exemplo, tem um nível de segurança maior, já que a Apple acompanha com rédeas curtas todo aplicativo disponível na App Store. Por esse motivo, o chamado "jailbreak" (desbloqueio) é desaconselhável quando se fala em segurança, já que o aparelho fica "aberto" e passa a rodar aplicações que não foram previamente aprovadas pela Apple. O Android e o Symbian, em contrapartida, permitem instalar aplicações provenientes de lojas alternativas. Isso aumenta consideravelmente o risco de ser atacado por algum tipo de vírus ou instalar um malware. Então como se proteger? Tanto a App Store, da Apple, quanto a Android Market, do Google, já oferecem opções de antivírus gratuitas e pagas. Mantê-los atualizados é sempre uma boa forma de prevenção. [20]

4.3.1. Smartphones Corporativos

Por ser o principal foco deste trabalho, o assunto sobre segurança em Smarphones corporativos será descrito mais detalhadamente pois conforme o uso de smartphones aumenta até mesmo no setor de negócios, em ambientes corporativos, as empresas atentam mais para a importância de se proteger este tipo de dispositivo quanto a troca de informações corporativas, e portanto garantir a segurança da informação.

Como já visto em Shadow IT, é muito frequente que colaboradores de negócio e até o presidente da empresa tragam seus dispositivos móveis pessoais para uso na empresa, como o recém-adquirido iPad ou a nova versão do iPhone. E atentos a esse novo fenômeno, já é possível encontrar no mercado soluções específicas que possibilitam uma melhor gestão do uso destes dispositivos móveis. Além de dar ao responsável pela área de TI uma maior segurança em relação aos aparelhos que acessam externamente a rede da empresa, estas soluções permitem a tomada de medidas emergenciais. No caso de um roubo ou perda, por exemplo de um iPhone ou Blackberry, é possível acessar o dispositivo remotamente e apagar todo o seu conteúdo. A seguir serão abordadas as principais solucões em segurança da informação em rede corporativa.

A preferência por BlackBerry no mercado corporativo não é novidade, mas agora foram divulgados números de uma pesquisa do IDC referentes à América Latina que dão a exata medida dessa liderança. Segundo o levantamento, 67% de toda a base instalada de smartphones corporativos na região são BlackBerry. Ou seja: dois terços. Em segundo lugar vem a Nokia, com 12,1%, seguida de Apple (8,3%), Motorola (5,2%), Samsung (4,1%), LG (2,2%), HTC (1,1%), Sony Ericsson (1%) e Palm (0,3%). É importante destacar que esses percentuais se referem a todos os smartphones em serviço no momento e de posse de grandes corporações. Não estão incluídos, portanto, aparelhos pessoais usados para trabalho por executivos. Os dados foram divulgados pela RIM, fabricante do BlackBerry, em evento da empresa realizado no Rio de Janeiro em novembro deste ano. [24]

A RIM possui mais de 70 milhões de assinantes no mundo inteiro. Somente na América do Norte a empresa tem mais de 1 milhão de usuários no mercado corporativo. Segundo a companhia, 90% das 500 maiores empresas globais na lista da Fortune são usuárias de BlackBerry.

Um dos principais motivos por esse número expressivo da RIM é a solução de gestão corporativa, o BES (Blackberry Enterprise Server), para gerenciamento corporativo dos smartphones da companhia, que a RIM vende para as empresas para instalarem em servidores próprios, bastante utilizado atualmente e muito confiável para aparelhos Blackberry corporativos no mundo todo. Também o MDM (Mobile Device Management) vem se juntar ao lado do BES dentro do firewall corporativo. Algumas das características deste serviço incluem bloqueio remoto do aparelho e comando remoto de Wipe (para limpeza dos dados), se o aparelho for perdido ou roubado. O MDM juntamente com o o BES permite criar definições de política e segurança assim como disponibiliza aplicativos de gerenciamento e outras funções de IT para melhor gestão e monitoramento dos aparelhos Blackberry corporativos.

Mas como o mercado corporativo de smartphones e tablets continua a crescer, o fenômeno BYOD (Bring Your Own Device) em particular, tem levado a um aumento na diversidade de dispositivos móveis em uso dentro das companhias, como já visto no capítulo 3 sobre Shadow IT, e consequentemente traz novos desafios para o CIO (Chief Information Officer) e departamento de TI, que lutam para gerenciar e controlar as informações confidenciais da empresa na rede sem fio corporativa. Isso resultou no aumento da demanda por soluções de gerenciamento de dispositivo móvel.

Uma das soluções encontradas pela RIM, a fim de atender a essa demanda, foi o lançamento do Mobile Fusion, uma nova solução MDM em resposta a esse novo contexto, apelidado pelo instituto Gartner de "Consumerização". O novo serviço MDM da RIM é uma solução de gerenciamento de terminais que abrange não somente os aparelhos de

Blackberry mas também os aparelhos dos sistemas operacionais Android e iOS. Porém o MDM não garante a smartphones Android ou iPhone o mesmo nível de segurança de dados do Blackberry mas fornece algumas ferramentas de gestão para aparelhos de fabricantes diversos em um único portal web para os administradores de TI. [25]

O BlackBerry Enterprise Server agora passa a integrar a nova solução, que também inclui o gerenciamento do tablet Playbook, lançado mês passado no Brasil, além dos dispositivos móveis de outras plataformas.

O BlackBerry Mobile Fusion está em fase de testes, e a RIM espera fazer o lançamento comercial da nova solução até março de 2012. O lançamento reafirma o foco da estratégia da RIM, companhia canadense no segmento corporativo, onde o mais importante é segurança pois a BlackBerry é a única fabricante de smartphones que oferece a solução (MDM) de ponta-a-ponta de gerenciamento de dispositivos móveis. [26]

Quanto a Apple, principal concorrente da RIM, para gerenciar dados corporativos em iPhones, deve-se configurar o iPhone ao ambiente corporativo como descrito abaixo ou ainda, o departamento de TI de uma empresa pode lançar mão de uma solução da SAP para este gerenciamento.

O iPhone pode ser integrado perfeitamente em ambientes empresariais com os seguintes cenários de implantação: [27]

- Microsoft Exchange ActiveSync
- Standards-based Servers
- Virtual Private Networks
- Wi-Fi
- Digital Certificates
- Security Overview
- Mobile Device Management
- Deploying iTunes

Como mencionado acima é possível integrar, proteger e implantar o iPhone em uma empresa de modo seguro. O iPhone se conecta perfeitamente com o Microsoft Exchange e servidores baseados em padrões de acesso a e-mails corporativos, calendário e contatos. Os dados são protegidos com criptografia de hardware e os usuários podem acessar dados

com segurança de redes corporativas com suporte para VPN e Wi-Fi, incluindo protocolos SSL VPN. Também é possível implantar o iPhone com o MDM (Mobile device Management) e o Wireless App Distribution para aplicações in-house.

No site da apple (http://www.apple.com) se encontram todas as documentações necessárias para a integração e implantação do iPhone em ambiente corporativo nos cenários já descritos acima. É também disponibilizado na loja da Apple alguns aplicativos de segurança empresarial, como o *McAfee Enterprise Mobility Management (EMM)* que permite a conexão de usuários de iPhone/iPad/iPod Touch aos serviços de IT existentes na organização, como email, VPN e accesso Wi-Fi. Na loja também é possível encontrar a aplicação *Good for Enterprise*, desenvolvido especialmente para iPhone e iPad.

A IBM também lançou recentemente um novo serviço de proteção e segurança de dados corporativos em dispositivos móveis. Denominado Hosted Mobile Device Security Management, o novo produto inclui um aplicativo de segurança para smartphones e tablets, além de serviços de monitoramento de informações e gerenciamento das políticas de segurança. Segundo a IBM, o programa auxilia as empresas na prevenção de riscos que podem ser causados por roubo, acesso não autorizado, malwares, spywares e aplicativos não apropriados. [23]

A IBM trabalhou em conjunto com a Juniper Networks para desenvolver este novo serviço, que estará disponível muito em breve para os mais diversos sistemas operacionais móveis do mercado, como Apple iOS, Google Android, BlackBerry, Symbian e Windows Mobile.

4.3.2. Smartphones Pessoais

Como mencionado no início deste capítulo, o download de aplicativos, as mensagens via SMS e Bluetooth são as principais formas de ataques de vírus e de malware. Como exemplo uma mesma mensagem pode enviar dados confidenciais do usuário, como conta bancária ou número de cartão de crédito, para o hacker que desenvolveu o malware. Portanto uma das primeiras regras básicas é ficar atento à procedência dos SMS e só ativar o Bluetooth quando houver a necessidade de usá-lo, para evitar que outras pessoas enviem arquivos indevidamente. Quando a função do Bluetooth está ativada, o usuário está sujeito a receber mensagens, propaganda e até mesmo vírus.

E o primeiro cuidado que o usuário deve ter logo ao adquirir um smartphone é configurar uma senha para acesso ao celular. Assim, caso o

aparelho seja perdido ou roubado os dados continuarão em segurança. Deve-se escolher uma senha difícil de ser descoberta e que não tenha relação com informações pessoais como datas de nascimento, placas do carro ou numero de telefone.

Outra regra básica é proteger o smartphone dos ataques de vírus, diminuindo o risco do celular ser infectado. Existem versões dos Antivírus mais populares especialmente desenvolvida para os Smartphones: [12]

- AVG (http://www.avgbrasil.com.br)
- Kaspersky (http://brazil.kapersky.com)
- Avira (http://www.avira.com)
- App Store, Android Market e Ovi Store possuem algumas opções de antivírus pagas ou gratuitas.

A seguir algumas dicas importantes para proteger um Smartphone:

- ✓ Deixar um antivírus instalado. Já mencionado acima.
- ✓ Preferir as lojas de aplicativos oficiais do respectivo sistema operacional. A probabilidade de existirem aplicativos mal intencionados é pequena, apesar de existente.
- ✓ Procurar análises e opiniões de outros usuários que já fizeram o download do aplicativo. Evite ser um dos primeiros a baixar um aplicativo.
- ✓ Não abrir links de mensagens recebidas por SMS ou MMS (mensagens com fotos ou vídeos). Pessoas mal intencionadas costumam se passar por empresas e operadoras, tornando quase impossível identificar a procedência das mensagens.
- ✓ Evitar procedimentos de desbloqueios não-oficiais, como o Jail Break do iPhone e versões modificadas de firmware no sistema operacional. Além de causar a perda da garantia, as alterações podem incluir vírus ou programas que permitem o controle remoto do aparelho.
- ✓ Utilizar o aplicativo que acompanha o Smartphone para realizar cópias de segurança, backups, dos dados armazenados no celular periodicamente.
- ✓ Não abrir no celular e-mails com fonte desconhecida. O mesmo cuidado aplicado nos e-mails no computador deve ser aplicado no smarphone.
- ✓ Navegue de forma segura. Manter o mesmo nível se segurança de um desktop ou notebook ao navegar na web. Sites com vírus podem ser desenvolvidos para infectar somente smartphones.

Estas dicas valem tanto para o uso de smartphones pessoais, como os smartphones corporativos e outros dispositivos móveis, incluindo o tão famoso Tablet.

4.3.3. Blackberry Protect

Pelo fato do Blackberry ser ainda o aparelho mais popular atualmente, ao lado do iPhone, neste tópico será abordado a ferramenta de segurança da RIM (Research in Motion) para uso de smartphone pessoal, chamada Blackberry Protect.

É importante observar que não é possível usar o BlackBerry Protect com smartphones ativados em um BlackBerry Enterprise Server ou em smartphones com a criptografia de memória ativada.

O BlackBerry Protect é um aplicativo projetado para: [31]

- Fazer backup e restauração dados do smartphone BlackBerry por meio de uma rede sem fio
- Localizar o smartphone se ele for perdido
- Proteger dados do smartphone ao bloqueá-lo ou excluir dados por meio da rede sem fio

Para usar o BlackBerry Protect é necessário obter os seguintes itens:

- Conta do BlackBerry ID
- Plano de dados do provedor de serviços sem fio
- Conta do BlackBerry Internet Service

E por fim esta ferramenta de segurança consiste em três componentes:

- Aplicativo que pode ser baixado na loja on-line BlackBerry App World e instalado no smartphone
- Site que pode ser usado para enviar comandos para o smartphone por meio de uma rede fio - www.blackberry.com/protect
- Infra-estrutura do BlackBerry Protect hospedada pela Research In Motion em um centro de dados

É possível restaurar dados do smartphone BlackBerry em um smartphone existente se os dados foram excluídos ou restaurá-los em um novo smartphone. O BlackBerry Protect fornece a opção de restaurar todos os dados em que foram realizados backup em um momento específico ou selecionar os tipos de dados que você deseja restaurar.

4.4. SEGURANÇA EM TABLETS

Como visto no tópico acima, as mesmas dicas para smartphones devem ser utilizadas para os Tablets. Tablets são equipamentos que podem trazer produtividade para os usuários e também às empresas mas junto com sua mobilidade trazem riscos de segurança.

Atualmente, devido aos Tablets serem a sensação do momento os crackers tem voltado sua atenção para o sucesso dos iPad´s e demais tablets com sistema Android, da Google.

Mesmo com toda a restrição que a Apple mantém aos seus sistemas e hardwares, e com o iPad isso não é diferente, ainda assim o iPad é alvo de ataques e portanto é imprescindível se proteger de vírus e de malwares.

A quantidade de aplicativos desenvolvidos para o iPad é gigantesca, mas antes de serem disponibilizados para os usuários eles precisam ser enviados à Apple que durante algumas semanas faz testes e análises dos códigos para somente depois publicar a aplicação para downloads. Com todo esse controle, desenvolver uma aplicação com o um código malicioso e publicar na App Store é muito pouco provável, mas existem outras formas de infectar o dispositivo. Muitos usuários de iPad não satisfeitos com essa política ou querendo baixar os aplicativos sem pagar por eles, já que muitos disponíveis não são grátis, efetuam o chamado JailBreak. [29]

O JailBreak é um iOS modificado, a instalação dele é contra os termos de garantia da Apple. Ao efetuar a instalação desse iOS é possível instalar qualquer aplicativo no iPad sem acessar a AppStore mas consequentemente pode causar danos ao aparelho e a perda a garantia do produto. Com a utilização do JailBreak, os usuários se tornaram vítimas dos crackers e hackers.

Diferentemente da Apple, a Google possui a política de liberdade para tudo o que produz, incluindo o sistema Android que é baseado no Linux e portanto tem código aberto. No caso da Android Market as aplicações são publicadas diretamente pelo usuário, não passam por um controle de qualidade, o que é muito bom para quem desenvolve, inclusive os crackers e hackers. Com a facilidade de desenvolver e publicar aplicações a Android

Market vem sofrendo com vírus sendo publicados e distibuidos para seus usuários. [29]

Com o aumento dos usuários de tablets em todo mundo, os crackers e hackers têm trabalhado para conseguir lucrar com o novo “nicho” de usuários.

As seguintes recomendações devem ser implementadas para garantir um bom nível de segurança nos Tablets: [28]

- As mesmas recomendações de segurança de smartphones portanto é necessário colocar senha de acesso (no iPhone e iPad há a opção de formatação em caso de erro em 10 tentativas) e também não desbloquear o aparelho (para se prevenir de JailBreak)
- Autenticação
- Funcionalidades de perda/roubo - Quando disponível, habilitar bloqueio remoto, localização e wipe de disco (Exclusão sem reversão de dados do disco)
- Autorização - Funcionalidades de autorização de acesso a aplicativos em específico, implementação de padrões corporativos de acesso
- Antivirus e Antimalware
- Tráfego - Conexão apenas a redes seguras
- Proteção de dados - Encriptação de dados nos equipamentos
- Gerenciamento de equipamentos - Quando em uso corporativo podem ser habilitadas funcionalidades de gerenciamento centralizado

E mais, a AVG lançou em março de 2011 o primeiro Software de Antivírus específico para tablets (AVG AntivirusFree). A versão é diferente da já existente para Smartphones, mas é uma prova que as empresas de segurança estão atentas aos ataques crescentes aos dispositivos móveis. O antivírus protege os aplicativos, configurações de dados e arquivos de mídia. Possui também a função de backup dos dados que podem ser armazenados em um cartão SD. Em caso do tablet ser perdido ou roubado existe a função de ser localizado e bloqueado pelo programa caso esteja conectado. [29]

5. ESTUDO DE CASO: BLACKBERRY EM AMBIENTE CORPORATIVO

O BlackBerry ainda é líder em segurança e dominante nas empresas, mesmo com a concorrência de outros smartphones no mercado. O BlackBerry representa atualmente 65,4% de participação de mercado entre smartphones fornecidos pelas empresas aos funcionários. [26]

Por esse motivo, o estudo de caso apresenta um cenário onde uma empresa com mais de mil funcionários, oferece aos executivos e funcionários da área de negócios o aparelho Blackberry para dar mobilidade e continuidade a realização do negócio. Neste estudo é analisada e discutida a principal solução de gestão corporativa da RIM, o BES (Blackberry Enterprise Server) mostrando detalhadamente a sua arquitetura e uso dentro das organizações, permitindo uma maior segurança no tráfego de informação entre a empresa e os usários Blackberry.

5.1. Ambiente Analisado

Uma empresa multinacional, com filiais espalhadas em vários pontos do mundo e com mais de mil funcionários e colaboradores ativos. Mantém dois centros de serviços compartilhados para atender às diversas linhas de negócios, em diversos países.

A empresa oferece aos seus executivos e todos os funcionários da área de negócios e também do departamento de TI, aparelhos Blackberry para acesso a emails, calendário, contatos, mensagens instantâneas e internet.

5.2. Análise de vulnerabilidade

São várias as ameaças e vulnerabilidades que atingem os smartphones. Como já abordado no sub-capítulo 2.5 deste trabalho, cada vez mais populares os smartphones e tablets estão na mira de ciber criminosos principalmente porque esses dispositivos possuem muita informação confidencial.

Entre as ameaças, os smartphones podem ser infectados por vírus desenvolvidos especialmente para celulares e uma vez infectado, o usuário pode servir como um retransmissor de mensagens SMS, na maioria das vezes mensagens mal intecionadas. Vale lembrar que o download de aplicativos é a forma mais fácil de contaminação, mas mensagens via SMS e Bluetooth também são portas de entrada latentes.

Os Smartphones também são alvos de ataques de malware, entre eles o SpyEye com versão voltada para dispositivos móveis nas plataformas Blackberry, Android e Symbian, com o objetivo de invadir os sistemas de dupla autenticação para acessar informações do usuário. O SpyEye é um cavalo de tróia capaz de gerar uma “rede zumbi” e roubar contas bancárias e outros dados importantes. Um vírus ou um malware pode ser programado para captar informações confidenciais como número e senha da conta do usuário.

Com esse número crescente de ameaças e vulnerabilidades, é fácil perceber que somente um bom antivírus não oferece a segurança necessária para a proteção dos dados confidenciais armazenadas no Smartphone. É imprescindível ter uma boa solução de gestão corporativa a fim de garantir a segurança da informação acessada pelos dispositivos móveis, em especial o Smartphone.

5.3. Ações para garantia de segurança e gerenciamento

A opção escolhida como melhor solução de segurança para smartphones em ambiente corporativo é a da RIM, o Blackberry Enterprise Server (BES). A justificativa desta escolha é a estabilidade e confiabilidade desta solução, já no mercado móvel por alguns anos com boa avaliação das empresas clientes, de acordo com o percentual já citado pela lista da Fortune, 90% das 500 maiores empresas globais na lista da Fortune são usuárias de BlackBerry. E também a escolha foi feita pelo motivo da RIM com o seu Blackberry ser a única fabricante de smartphones que oferece no mercado a solução de gerenciamento de dispositivos movéis de ponta a ponta com o MDM. [26]

O MDM (Mobile Device Management) complementa o gerenciamento juntamente com o BES dentro do firewall corporativo. Algumas das características deste serviço incluem bloqueio remoto do aparelho e comando remoto de Wipe se o aparelho for perdido ou roubado. E permite criar definições de política de segurança assim como disponibiliza aplicativos de gerenciamento e outras funções de IT para melhor gestão e monitoramento dos aparelhos Blackberry corporativos.

Abaixo serão analisadas e discutidas as principais soluções de gestão corporativa da RIM, para aparelhos Blackberry. Ao final também será abordada a mais recente solução da RIM para o fenômeno de Shadow IT ou BYOD.

5.3.1. Blackberry Enterprise Server

O Blackberry Enterprise Server (BES) é projetado para ser uma ligação altamente segura entre a infra-estrutura existente de uma organização e os Smartphones Blackberry.

O BlackBerry Enterprise Server consiste em vários componentes projetados para executar as seguintes ações:

- fornecer ferramentas de produtividade e dados a partir dos aplicativos de uma organização aos usuários de dispositivos BlackBerry
- monitorar outros componentes do BlackBerry Enterprise Server
- processar, rotear, compactar e criptografar dados
- comunicar-se com a rede sem fio

A descrição mais detalhada de cada um dos componentes do BES pode ser vista no ANEXO I.

Abaixo um diagrama da arquitetura do Blackberry Enterprise Server.

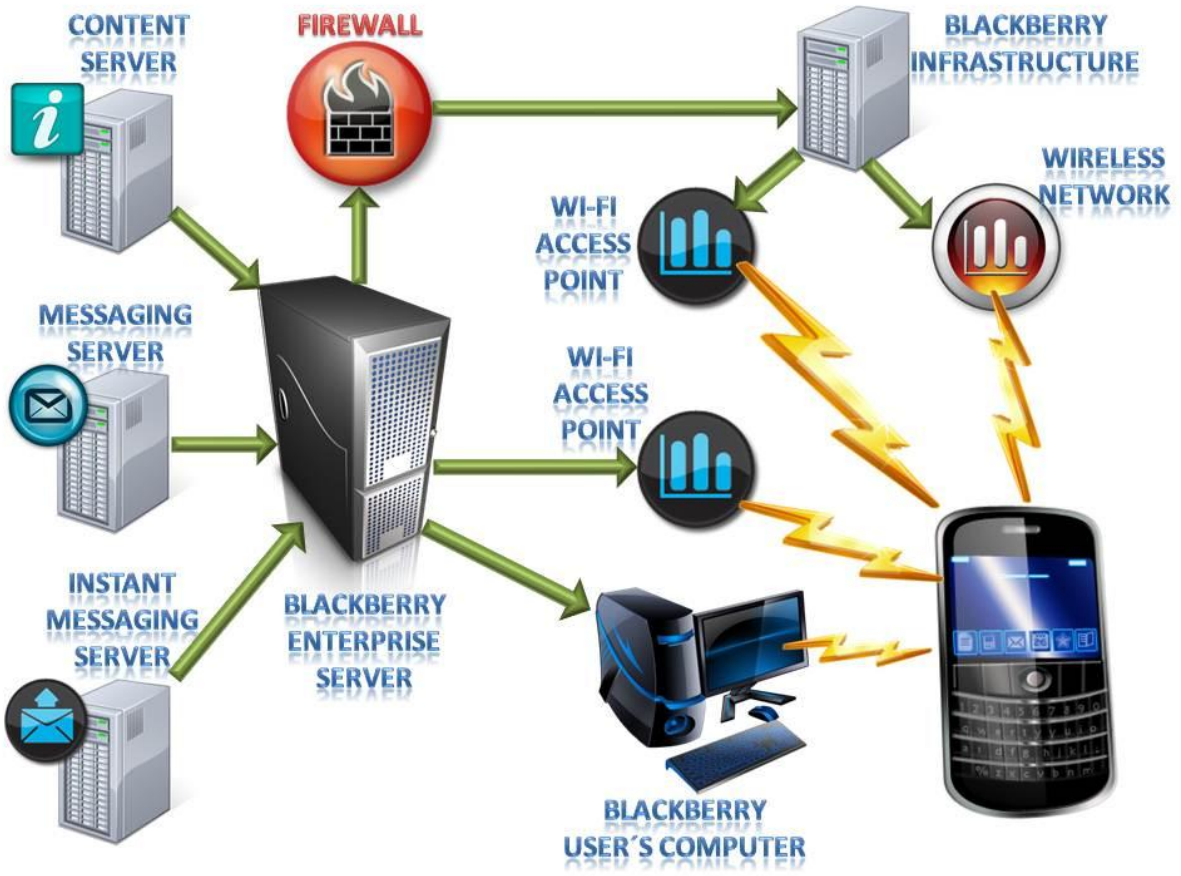

Figura 2. Arquitetura BES. [32]

Para melhor entender o processo, é descrito logo abaixo o fluxo do processo quando uma mensagem de um aparelho Blackberry é enviada e passa pelo Blackberry Enterprise Server.

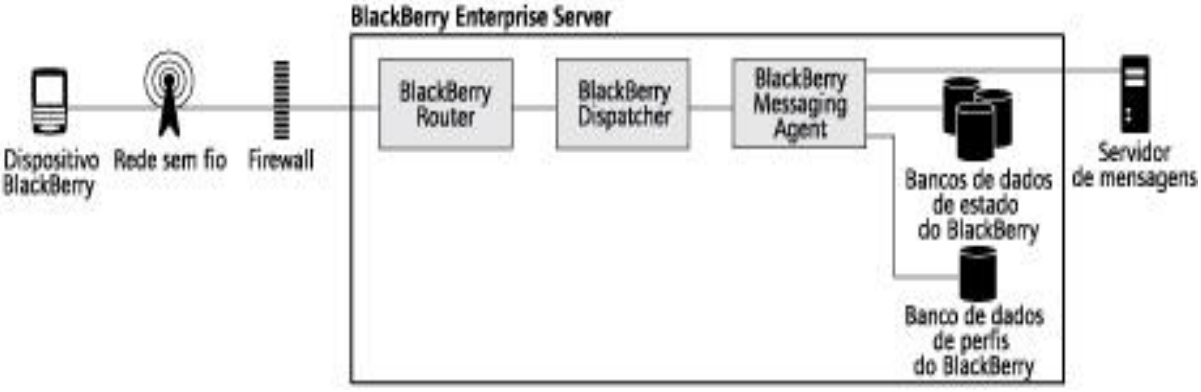

Figura 3. Fluxo do Processo de envio de mensagem pelo Blackberry. [34]

Este fluxo do processo se aplica a novas mensagens, mensagens reconciliadas (mensagens movidas, excluídas ou marcadas como lidas ou não lidas pelo usuário) e a entradas de calendário sem fio. [34]

Durante o processo, vários componentes do Blackberry Enterprise Server são utilizados e executados para garantir a segurança do tráfego da informação, como mostrado nas etapas abaixo:

1. Um usuário envia uma mensagem de um dispositivo BlackBerry.

   O dispositivo BlackBerry atribui um Ref ID à mensagem. Se a mensagem for um convite para reunião ou uma entrada de calendário, o dispositivo BlackBerry anexará as informações de calendário à mensagem. O dispositivo BlackBerry compacta e criptografa a mensagem e a envia à rede sem fio pela porta 3101, ou pela porta 4101 se o dispositivo BlackBerry for habilitado para Wi-Fi e estiver conectado à rede Wi-Fi corporativa.

2. A rede sem fio envia a mensagem ao BlackBerry Enterprise Server.

   O BlackBerry Enterprise Server aceita apenas mensagens criptografadas do dispositivo BlackBerry.

3. O BlackBerry Dispatcher usa a chave de transporte de dispositivo do dispositivo BlackBerry para descriptografar e descompactar a mensagem.
   Se o BlackBerry Dispatcher não descriptografar a mensagem usando a chave de transporte de dispositivo, o BlackBerry Enterprise Server ignorará a mensagem e enviará uma mensagem de erro ao dispositivo BlackBerry.

4. O BlackBerry Messaging Agent executa uma das seguintes ações:

   - Se a mensagem for nova, o BlackBerry Messaging Agent criará uma entrada no banco de dados de estado do BlackBerry.
   - Se a mensagem for uma resposta que inclui o texto original ou uma mensagem encaminhada, o BlackBerry Messaging Agent encontrará a entrada no banco de dados de estado do BlackBerry para correlacionar a mensagem recebida à mensagem original no arquivo de mensagem do usuário.

   O banco de dados de estado do BlackBerry contém um link para a mensagem original. Como o BlackBerry Messaging Agent encaminha apenas a primeira parte de uma mensagem ao dispositivo BlackBerry, o BlackBerry Messaging Agent deve localizar e recuperar o texto completo da mensagem para encaminhá-la ou respondê-la com o texto original.

5. O BlackBerry Messaging Agent envia a mensagem à caixa postal para que o roteador de servidor de eMail envie ao aplicativo de e-mail do usuário.
   Se o usuário estiver no mesmo domínio do servidor de eMail que o BlackBerry Enterprise Server, o BlackBerry Messaging Agent armazenará a mensagem na caixa postal localizada no BlackBerry Enterprise Server. Se o usuário estiver em um domínio separado do BlackBerry Enterprise Server, o BlackBerry Messaging Agent armazenará a mensagem na caixa postal localizada no servidor de mensagens do usuário.

6. O BlackBerry Messaging Agent envia uma cópia da mensagem para o modo de exibição Sent (Enviados) no arquivo de e-mail do usuário localizado no servidor de mensagens.

7. O servidor de mensagens entrega a mensagem aos destinatários.

Este foi o exemplo de uma das ações mais simples executadas por usuários de Smartphones, mas o Blackberry Enterprise Server gerencia e monitora todas as demais ações de usuários Blackberry, desde o envio de anexos pelo smartphone, o recebimento de mensagens criptografadas, pesquisa do catálogo de endereço de uma organização, envio e recebimento de mensagens instantâneas, enfim todo o fluxo de processo de gerenciamento de dispositivos móveis de uma empresa.

O gerenciamento do BES inclui os métodos de ativação dos aparelhos Blackberry. Os administradores podem acompanhar a ativação de um smartphone no Blackberry Enterprise Server utilizando um dos seguintes métodos:

- Blackberry Administration Service
- Blackberry Desktop Manager
- Blackberry Web Desktop Manager

- Over the Wireless network
- Over the enterprise Wi-Fi network

No caso da empresa apresentada neste estudo, o método escolhido é o *Over the Wireless Network* por ter o seguinte benefício: fácil uso tanto para o administrador como para o usuário. O recurso de ativação sem fio permite que um usuário smartphone ative o aparelho no Blackberry Enterprise Server sem a necessidade de conexão de rede física. Para ativação do smartphone Blackberry, o administrador gera uma senha de ativação e então comunica o usuário que inicia o processo de ativação. A única limitação deste método é que requer sinal forte da antena wireless e com qualidade de sinal. [32]

5.3.2. IT Policies / Políticas de TI

Cada smartphone BlackBerry, na ativação, é adicionado a uma base customizada de política de TI para garantir um nível mínimo de segurança. A partir deste ponto de partida, os administradores podem criar grupos de usuários e facilmente modificar as políticas para atender às necessidades de segurança da organização.

Uma política de TI é um conjunto de regras que um administrador usa para definir a funcionalidade do smartphone Blackberry. Essas regras podem definir muitas opções, incluindo como as mensagens de e-mail são tratadas e quais funcionalidades que o usuário Blackberry pode usar. Usuários Blackberry podem ser associados a uma política de TI personalizada, não pré-configurados, mas cada usuário só pode ser resolvido com uma política de TI de cada vez. [32]

Políticas podem ajudar o administrador a reforçar a segurança na organização. As políticas são configuradas no BES e podem ser aplicadas a grupos de usuários ou ao usuário individual. Qualquer recurso que está no aparelho Blackberry pode ser gerenciado através de políticas.

No estudo de caso, algumas políticas de TI são aplicadas para garantir mais segurança no uso do smartphone Blackberry corporativo:

- Somente um endereço de email pode ser utlizado no smartphone Blackberry, o endereço corporativo.
- Somente anexos com extensões de formatos essenciais ao trabalho na empresa são permitidos. Ex.: .doc, .docx, .txt, .xls, .ppt, .html
- Não é permitido fazer downloads de aplicativos nos aparelhos Blackberry.

- Uso restrito de mensagens instantâneas, somente uso do Blackberry Messenger e do Windows Live.

E novas políticas podem ser criadas a cada necessidade de gerenciamento do administrador de rede.

5.3.3. Blackberry Enterprise Solution

O Blackberry Enterprise Solution é uma solução de TI amigável e flexível que permite aos usuários de celulares o acesso seguro via rede wireless aos emails corporativos e aplicações críticas de negócios. [33]

Para soluções mais robustas de segurança em dispositivos móveis, podem ser implementadas todos os recursos do *Blackberry Enterprise Solution*, descritas no ANEXO II.

Mas para o estudo de caso apresentado, a implementação do Blackberry Enterprise Server juntamente com as políticas de segurança permitem um bom nível de segurança no gerenciamento de dados trafegados entre usuários Blackberry e a empresa.

5.3.4. Blackberry Mobile Fusion

Como descrito no sub-capítulo 4.3.3 sobre segurança em Smartphones corporativos, devido ao fenômeno de Shadow IT e do BYOD (Bring Your Own Device), tem aumentado a diversidade de dispositivos móveis em uso dentro das companhias, e usuários incluindo o presidente, diretor ou executivos das empresas querem utilizar o seu recém adquirido dispositivo como o iPhone, o iPad, ou Galaxy no trabalho e este tem sido um grande desafio para o departamento de TI, o de gerenciar e controlar as informações confidenciais da empresa na rede sem fio corporativa.

E uma das soluções encontradas pela RIM a fim de atender a essa demanda, foi o lançamento do Mobile Fusion, uma nova solução MDM em resposta a esse novo contexto. Este serviço MDM abrange não somente os aparelhos de Blackberry mas também os aparelhos dos sistemas operacionais Android e iOS.

Portanto para este estudo de caso analisado, para solucionar a questão do Shadow IT, será adquirido o Mobile Fusion com a solução MDM pois o BlackBerry Enterprise Server agora passa a integrar a nova solução, que também inclui o gerenciamento do tablet Playbook, lançado mês passado no Brasil, além dos dispositivos móveis de outras plataformas.

Porém o MDM não garante a smartphones Android ou iPhone o mesmo nível de segurança de dados do Blackberry mas fornece algumas ferramentas de gestão para aparelhos de fabricantes diversos em um único portal web para os administradores de TI. [25]

5.4. ESTUDO COMPARATIVO – Blackberry x iPhone

Enquanto o Blackberry é a primeira escolha para dispositivo móvel confiável em ambiente corporativo, o iPhone tem os seus recursos para torná-lo efetivamente seguro. Um ou outro dispositivo pode ser usado como ferramenta de negócio seguro, se ele estiver devidamente configurado e usado corretamente.

O Blackberry pode ser a solução mais madura e com capacidade de provisionamento remoto, entretanto sua flexibilidade aumenta sua complexidade. Administradores podem desenvolver soluções detalhadas e customizadas, mas isso leva muito tempo para implementação e também sem a solução corporativa, o BES - Blackberry Enterprise Server, o Blackberry oferece pouco ao gerenciamento dos aparelhos. [30]

Quanto ao iPhone da Apple, ele possui características de segurança adequadas ao uso corporativo. As ferramentas de configuração são em sua maioria intuitivas, no entanto a Apple não tem capacidade remota de provisionar, configurar, auditar e reforçar a segurança dos aparelhos. Se a Apple adicionasse estas funções, isto colocaria o iPhone no mesmo nível que o Blackberry.

Ambos, o iPhone e o Blackberry são vulneráveis ao risco de malware, e qualquer decisão de políticas em um ou outro dispositivo pode trazer riscos de segurança.

Abaixo uma tabela mais detalhada para melhor comparar os recursos entre o iPhone e o Blackberry. [30]

Tabela 1. ***Configuração de Aplicações:***

Características Gerais	**iPhone**	**Blackberry**
Wipe Remoto	O comando remoto de Wipe no iPhone pode ser executado através de: -> Exchange 2007 Management Console	O wipe remoto é uma característica fundamental do dispositivo e pode ser habilitado ou acionado pelo BES (Blackberry Enterprise Server).

	-> Outlook Web Access -> Exchange ActiveSync Mobile Administration Web Tool -> Exchange 2003 - Exchange ActiveSync Mobile Administration Web Tool	
Provisionamento	Requer configuração local.	Permite provisionamento local e remoto.
Restauração remota	Não	Sim
Senha	Regras de segurança de senha. Utilizando o Apple Configuration Utility pode ser configurado restrições mais robustas para acesso corporativo.	Rico gerenciamento de políticas de senha. Com complexidade comparável ao ambiente de Desktop.

Tabela 2. ***Gerenciamento de Políticas:***

Gerenciamento de Políticas	iPhone	Blackberry
Execução (Enforcement)	Pode ser implantado um perfil para iPhone, requer autenticação de senha para substituição.	Pode ser configurado controles para os dispositivos com uma opção de política sobre o que pode e o que não pode ser editado pelo usuário. Flexível mas complicado de se configurar.
Auditoria	Não possui funcionalidade de gerenciamento para ser auditada.	Sim, baseada na política. Logado localmente ou centralmente.
Correções (Patching)	Correções não podem ser instaladas automaticamente pela rede. São entregues pelo iTunes quando o usuário se conecta e opta pela atualização. iTunes não pode ser gerenciado centralmente, logo um administrador não pode ditar o lançamento de uma correção. É baseado na noção de segurança do próprio usuário.	Correções podem ser instaladas remotamente pelo BES (Blackberry Enterprise Server). Status completo de auditoria e gerenciamento da correção podem ser executados remotamente sem necessidade de intervenção do usuário. Quando uma reinicialização é necessária, a política pode definir se o usuário tem escolha de deixar para um instante

		posterior.
Atualizações	Atualizações dos perfis não são automaticamente instaladas e requerem que o usuário decida se quer aplicar a política.	Atualizações podem ser instaladas remotamente pelo BES e aplicadas em background sem interação com o usuário.
Controle de Aplicações	Perfis podem ser configurados para restringir recebimento de aplicações, e o administrador não tem poder para enviar aplicações remotamente. Aplicativos podem ser criados especificamente para o dispositivo, mas devem ser checados e assinados pela Apple.	O BES provê a capacidade de entrega de pacotes e aplicações especificas remotamente. Restrições podem ser aplicadas a aplicações, permitindo ao usuário instalar aplicações de uma lista branca corporativa, ou somente habilitando ao administrador instalar. Políticas específicas podem ser associadas a cada aplicação, permitindo acessos a recursos individualizados a cada aplicativo (acesso a rede, dados locais, alterações de configuração, etc.). Todas estas podem ser gerenciadas remotamente de acordo com a configuração empresarial. Extremamente customizável.
Gerenciamento de direitos do usuário	Por padrão, um conjunto de restrições está providenciado: conteúdo explícito, Safari, Youtube, iTunes, habilitar o usuário a instalar aplicativos, habilitar o uso de câmera, capturas de tela.	Políticas específicas por aplicação podem ser configuradas, embora possam ser intimidadoras.

Tabela 3. ***Segurança de Tráfego:***

Segurança de Tráfego	**iPhone**	**Blackberry**
VPN	Sim, autenticação baseada em senhas e tokens está disponível. Requer interação do usuário.	Provê tunel encriptado ao BES para transferência de dados e suporte a VPN explícito.
Gerenciamento Remoto	Não	Sim

E-mail	Sim, suporta SSL por vários protocolos. Depende da configuração do servidor (Exchange é o padrão). Também habilita o uso de certificados de autenticação.	Sim, por padrão por túnel encriptado ou diretamente ao servidor de email.
Proxy	Proxy pode ser configurado para o Carriers Access Point. Todo tráfego pode ser forçado através do VPN, o qual pode ser configurado para passar pelo proxy.	Política de uso do proxy pode ser configurada ao nível do BES (roteando todo tráfego de volta ao servidor central e roteando por um único ponto). Pode também definir políticas de conexão personalizadas caso a caso.
Certificados	Possui capacidade de usar um servidor SCEP para controlar a publicação e revogação de certificados ao aparelho. Também é possível criar um perfil contendo certificados separados ao uso do servidor SCEP.	Pode gerenciar certificados e instalar remotamente.

6. CONCLUSÃO

Este trabalho apresentou um cenário atual em TI, o crescimento vertiginoso do uso de dispositivos móveis em ambiente corporativo e a massificação do uso de aparelhos como Smartphones e Tablets nas organizações. Esta tendência traz um alerta à área de TI, o fenômeno de Shadow IT e o desafio de garantir a segurança da informação acessada por qualquer dispositivo móvel da mesma maneira que é assegurada aos computadores pessoais. A internet portátil traz esta nova realidade, se tornando um dos principais motivos de preocupação nas grandes empresas nos dias de hoje.

As ameaças e vulnerabilidades abordadas e discutidas neste trabalho são inúmeras e os Smartphones são alvos fáceis para os cibercriminosos . Isto demonstra que os cuidados com a segurança deve ser constante por isso foram apresentadas as mais recentes tecnologias de segurança, assim como métodos e ações simples para se manter o Smartphone seguro.

No estudo de caso a escolha do BES para gerenciamento de smartphones Blackberry da RIM, como melhor solução para gestão de smartphones corporativos, é justificada pela estabilidade e confiabilidade desta solução no que se refere a garantia da integridade e confidencialidade dos dados em todo o ambiente corporativo. E também por apresentar uma nova ferramentas de gestão para aparelhos de fabricantes diversos, o MDM e o Mobile Fusion, facilitando o trabalho dos administradores de TI quanto ao fenômeno de Shadow IT.

No estudo comparativo do Blackberry e do iPhone, os recursos de segurança do iPhone estão presentes e podem ser implementados para uso corporativo. Também é possível implantar o iPhone com o MDM (Mobile device Management) e o Wireless App Distribution para aplicações in-house. Porém após análise de todos os recursos, o Blackberry demonstra ser mais completo para o objetivo final de segurança corporativa.

A medida que as empresas estiverem mais conscientes das ameaças e vulnerabilidades do uso indevido de smartphones e outros dispositivos móveis dentro da organização, e o grande risco envolvido nisso, a tendência é que novos aplicativos e novas soluções tecnológicas de segurança surgirão para atender a essa demanda.

Por fim, conclui-se que a segurança da informação não depende somente de seus administradores mas sim da consciência de todos, desde o simples usuário até o diretor da empresa e governantes de TI, sobre a importância de tomar os devidos cuidados de segurança no uso de qualquer dispositivo.

7. REFERÊNCIAS

1. Deziderá, Ariane Gomes da Silva. Monografia Segurança da Informação - 2008
2. Bertão, Jucilei de Fátima. Monografia Segurança de Redes Wireless - 2006.
3. Assi, Marcos - Segurança da Informação e Smartphones. Artigo acessado na Internet em 02/11/2011: http://marcosassi.com.br/seguranca-da-informacao-e-smartphones
4. De Bom, Leandro - 5 dicas para blindar smartphones e tablets. Artigo acessado na Internet em 02/11/2011: http://computerworld.uol.com.br/seguranca/2011/03/23/especialista-da-5-dicas-para-blindar-smartphones-e-tablets/#ir
5. Sophos - Security threat report 2011. Artigo acessado na Internet em 02/11/2011: http://www.sophos.com/sophos/docs/eng/papers/sophos-security-threat-report-2011-wpna.pdf
6. Morimoto, Carlos E. Rede Wireless. Artigo acessado na Internet em 02/11/2011: http://www.hardware.com.br/livros/hardware/rede-wireless.html
7. Siqueira, Ethevaldo - Mundo terá 55 bilhões de dispositivos móveis em 2020. Artigo acessado na Internet em 02/11/2011: http://blogs.estadao.com.br/ethevaldo-siqueira/2011/02/21/55-bilhoes-de-dispositivos-moveis/`
8. Moreira da Silva, Maria da Graça, Treinero Consolo, Adriane - Uso de Dispositivos Móveis na Educação. Artigo acessado na Internet em 02/11/2011: http://www.5e.com.br/infodesign/146/Dispositivos_moveis.pdf
9. Birman, Fernando - Tirando a “Shadow IT” da sombra. Artigo acessado na Internet em 02/11/2011: http://computerworld.uol.com.br/gestao/fernando_birman/idgcoluna.2008-09-11.0882981082/
10. Hungria, Camila - Cuidado! Vírus calling. Artigo acessado na Internet em 02/11/2011: http://pensandogrande.com.br/tag/seguranca-da-informacao/
11. NICHOLS, RANDALL - Wireless Security - Models, Threats and Solution
12. Sudré, Gilberto - Dicas de segurança para seu Smartphone. Artigo acessado na Internet em 02/11/2011: http://www.tiespecialistas.com.br/2010/09/dicas-de-seguranca-para-seu-smartphone/
13. Figueiró, Felipe - Pesquisadores encontram versão do SpyEye para smartphones. Artigo acessado na Internet em 05/11/2011: http://www.linhadefensiva.org/2011/10/pesquisadores-encontram-versao-do-spyeye-para-smartphones/
14. Pereira da Silva, Luciano E. Redes sem Fio e Redes Móveis. Artigo acessado na Internet em 05/11/2011: http://knol.google.com/k/redes-sem-fio-e-redes-m%C3%B3veis#
15. Tynan, Dan - Dez verdades que a TI deve aprender a aceitar. Artigo acessado na Internet em 05/11/2011: http://cio.uol.com.br/gestao/2011/09/06/dez-verdades-que-a-ti-deve-aprender-a-aceitar/
16. Overby, Stephanie - Dicas para domar a TI clandestina. Artigo acessado na Internet em 05/11/2011: http://cio.uol.com.br/gestao/2011/10/11/dicas-para-domar-a-ti-clandestina/
17. Morimoto, Carlos E. Smartphones, Guia Prático. Artigo acessado na Internet em 05/11/2011: http://www.hardware.com.br/livros/smartphones/
18. Wikipedia - Tablet PC. Artigo acessado na Internet em 05/11/2011: http://pt.wikipedia.org/wiki/Tablet_PC
19. RSA,November 2007,The Confessions Survey: Office Workers Reveal Everyday Behavior That Places Sensitive Information at Risk. Artigo acessado na internet em 06/11/2011: http://www.rsa.com/company/news/releases/pdfs/RSA-insider-confessions.pdf
20. Vitulli, Rodrigo - Segurança em smartphones e tablets: saiba quais os riscos e como se proteger. Artigo acessado na Internet em 06/11/2011: http://tecnologia.uol.com.br/ultimas-noticias/redacao/2011/06/27/seguranca-em-smartphones-e-tablets-saiba-quais-os-riscos-e-como-se-proteger.jhtm
21. GBrasil - Pesquisas e especialistas em segurança apontam que smartphones e tablets são o alvo do cibercrime. Artigo acessado na Internet em 06/11/2011: http://gbrasilcontabilidade.com.br/noticias/pesquisas-e-especialistas-em-seguranca-apontam-que-smartphones-e-tablets-sao-o-alvo-do-cibercrime/
22. Clark Estes, Adam - Your Smartphone Is Spying on You. Artigo acessado na Internet em 01/12/2011: http://news.yahoo.com/smartphone-spying-204933867.html

23. Barros, Thiago - IBM estreia serviço de segurança para smartphones e tablets. Artigo acessado na Internet em 06/11/2011: http://www.techtudo.com.br/noticias/noticia/2011/11/ibm-estreia-servico-de-seguranca-para- smartphones-e-tablets.html
24. TeleTime - BlackBerry domina 67% do mercado corporativo na América Latina. Artigo acessado na Internet em 06/11/2011: http://www.teletime.com.br/30/11/2011/blackberry-domina-67-do-mercado-corporativo-na-america-latina/tt/252030/news.aspx
25. Weinschenk, Carl - Is RIM Becoming an MDM Company? Artigo acessado na Internet em 12/11/2011: http://www.itbusinessedge.com/cm/blogs/weinschenk/is-rim-becoming-an-mdm-company/?cs=49209
26. Jordan, Georgia - RIM anuncia solução de segurança corporativa para smartphones concorrentes. Artigo acessado na Internet em 12/11/2011: http://www.telesintese.com.br/index.php/plantao/17785-rim-anuncia-solucao-de-seguranca-corporativa-para-smartphones-concorrentes
27. Apple - iPhone in Business. Artigo acessado na Internet em 12/11/2011: http://www.apple.com/iphone/business/docs/iPhone_Business.pdf
28. Santos, Alfredo - Boas práticas de segurança em Tablets. Artigo acessado na Internet em 13/11/2011: http://alfredoluiz.blogspot.com/2011/05/boas-praticas-de-seguranca-em-tablets.html
29. Carvalho, Julio - A "Segurança" dos Tablets. Artigo acessado na Internet em 19/11/2011: http://www.tiespecialistas.com.br/2011/06/a-seguranca-dos-tablets/
30. Sophos - iPhone vs. BlackBerry. Artigo acessado na Internet em 19/11/2011: http://www.sophos.com/en-us/security-news-trends/security-trends/iphone-vs-blackberry.aspx
31. Blackberry.com - BlackBerry Protect Version: 1.1. Artigo acessado na Internet em 19/11/2011: http://docs.blackberry.com/en/smartphone_users/deliverables/32146/BlackBerry_Protect-Security_Note--1758826-0802040611-001-1.1-US.pdf
32. Blackberry (WES 2010) - Introducing Blackberry Enterprise Server
33. Blackberry.com - BlackBerry Enterprise Solution Architecture. Artigo acessado na Internet em 26/11/2011: http://us.blackberry.com/ataglance/solutions/architecture.jsp
34. Blackberry.com - Fluxo do processo: enviando uma mensagem de um dispositivo BlackBerry. Artigo acessado na Internet em 26/11/2011: http://docs.blackberry.com/pt-br/admin/deliverables/12908/PF_Sending_a_message_from_the_BB_device_224465_11.jsp
35. Blackberry.com - BlackBerry Enterprise Solution Versão: 5.0. Artigo acessado na Internet em 26/11/2011: http://docs.blackberry.com/en/admin/deliverables/26261/BlackBerry_Enterprise_Solution--1315426-0402092236-012-5.0.3-PT.pdf
36. Wikipedia. Hacker. Artigo acessado na internet em 04/12/2011: http://pt.wikipedia.org/wiki/Hacker
37. Wikipedia. Malware. Artigo acessado na internet em 04/12/2011: http://pt.wikipedia.org/wiki/Malware
38. Starck, Daniele. O que é Jailbreak. Artigo acessado na internet em 04/12/2011: http://www.tecmundo.com.br/3223-o-que-e-jailbreak-.htm
39. Wikipedia. Bluetooth. Artigo acessado na internet em 04/12/2011: http://pt.wikipedia.org/wiki/Bluetooth
40. Figura Dispositivos Móveis acessado na internet em 01/11/2011. http://dayanepedagogia.blogspot.com

ANEXO I

Descrição dos componentes do Blackberry Enterprise Server: [32]

- **BlackBerry Administration Service**

O BlackBerry Administration Service é um aplicativo da Web que você pode usar para gerenciar contas de usuário, atribuir grupos de usuários, funções de administrador e configurações de software, aplicar políticas de TI a contas de usuário e gerenciar servidores e instâncias de componentes em um BlackBerry Domain. Você pode abrir o BlackBerry Administration Service no navegador de qualquer computador que possa acessar o computador que hospeda o BlackBerry Administration Service. Você pode compartilhar tarefas administrativas com vários administradores que podem acessar o BlackBerry Administration Service simultaneamente usando nomes de usuário e senhas exclusivos. Quando os controles do Microsoft ActiveX são ativados em seu navegador, você pode conectar dispositivos BlackBerry aos seus computadores e gerenciar os dispositivos BlackBerry enquanto estiver conectado ao BlackBerry Administration Service.

- **BlackBerry Attachment Service**

O BlackBerry Attachment Service converte os anexos de mensagens compatíveis em um formato que o usuário pode exibir no dispositivo BlackBerry.

- **BlackBerry Collaboration Service**

O BlackBerry Collaboration Service fornece uma conexão entre o servidor de mensagens instantâneas da organização e o cliente de colaboração em dispositivos BlackBerry.

- **BlackBerry Configuration Database**

O BlackBerry Configuration Database é um banco de dados relacional que contém dados de configuração usados pelos componentes do BlackBerry Enterprise Server. O BlackBerry Configuration Database inclui os seguintes dados:

- detalhes sobre a conexão do BlackBerry Enterprise Server com a rede sem fio
- lista de usuários
- mapeamentos de endereços entre PINs e endereços de e-mail para os recursos de envio do BlackBerry MDS Connection Service
- cópia somente leitura de cada chave mestra de criptografia

- **BlackBerry Controller**

O BlackBerry Controller monitora os componentes do BlackBerry Enterprise Server e os reinicia quando param de responder.

- **BlackBerry Dispatcher**

O BlackBerry Dispatcher compacta e criptografa todos os dados enviados de/para dispositivos BlackBerry. Por meio do BlackBerry RouterBlackBerry Router, ele envia os dados de/para a rede sem fio.

- **BlackBerry Manager**

O BlackBerry Manager se conecta ao BlackBerry Configuration Database. Você pode usar o BlackBerry Manager para gerenciar o BlackBerry Domain, incluindo a administração de contas e dispositivos de usuários. O BlackBerry Domain consiste em um único BlackBerry Configuration Database e todas as instâncias usadas pelo BlackBerry Enterprise Server.

- **BlackBerry MDS Connection Service**

O BlackBerry MDS Connection Service permite que os usuários acessem conteúdo da Web, a Internet ou a intranet da organização e ainda permite que aplicativos nos dispositivos BlackBerry se conectem aos servidores de aplicativos ou de conteúdo da organização para acessar dados e atualizações de aplicativos.

- **BlackBerry MDS Integration Service**

O BlackBerry MDS Integration Service fornece integração em nível de aplicativo para aplicativos do BlackBerry MDS Runtime em dispositivos BlackBerry. Você pode usar o BlackBerry MDS Integration Service para instalar os aplicativos do BlackBerry MDS Runtime armazenados no BlackBerry MDS Application Repository em dispositivos BlackBerry. Você também pode usá-lo para gerenciar, atualizar e remover aplicativos do BlackBerry MDS Runtime.

- **BlackBerry MDS Application Repository**

O BlackBerry MDS Application Repository armazena aplicativos do BlackBerry MDS Runtime que os desenvolvedores da organização podem criar e publicar usando o BlackBerry MDS Studio ou as ferramentas do desenvolvedor do BlackBerry Plug-in for Microsoft Visual Studio. Você pode usar o BlackBerry Manager para gerenciar os aplicativos do BlackBerry MDS Runtime armazenados no BlackBerry MDS Application Repository.

- **BlackBerry Messaging Agent**

O BlackBerry Messaging Agent conecta-se ao servidor de mensagens da organização para fornecer serviços de mensagem, gerenciamento de calendário, buscas de endereços, exibição e download de anexos e geração de chaves de criptografia. O BlackBerry Messaging Agent age como um gateway para que o BlackBerry Synchronization Service acesse dados do organizador no servidor de mensagens. O BlackBerry Messaging Agent sincroniza dados de configuração entre o BlackBerry Configuration Database e o banco de dados de perfis BlackBerry.

- **BlackBerry Policy Service**

O BlackBerry Policy Service executa serviços de administração pela rede sem fio. Ele envia políticas e comandos de administração de TI e aprovisiona cadernos de serviços. As políticas e os comandos de administração de TI definem a segurança do dispositivo BlackBerry, configurações para sincronizar dados pela rede sem fio e outras configurações nos dispositivos BlackBerry. O BlackBerry Policy Service também envia cadernos de serviços para definir as configurações de recursos e componentes nos dispositivos BlackBerry.

- **BlackBerry Router**

O BlackBerry Router conecta-se à rede sem fio para enviar dados de/para dispositivos BlackBerry. Ele também envia dados pela rede da organização a dispositivos BlackBerry conectados a computadores por meio do BlackBerry Device Manager.

- **Bancos de dados de estado do BlackBerry**

Os bancos de dados de estado do BlackBerry contêm dados que vinculam as mensagens enviadas ou recebidas nos dispositivos BlackBerry a mensagens correspondentes em aplicativos de e-mail dos usuários. Os dados nos bancos de dados de estado do BlackBerry oferecem suporte a recursos como reconciliação de e-mail, encaminhamento e arquivamento de mensagens e resposta com texto.

- **BlackBerry Synchronization Service**

O BlackBerry Synchronization Service sincroniza dados do organizador entre dispositivos BlackBerry e o servidor de mensagens pela rede sem fio.

- **Servidor de aplicativos ou de conteúdo da organização**

O servidor de aplicativos ou de conteúdo da organização fornece aplicativos de envio e conteúdo da intranet para o BlackBerry MDS Services.

- **Servidor de mensagens instantâneas**

O servidor de mensagens instantâneas armazena contas de mensagens instantâneas.

- **Servidor de mensagens**

O servidor de mensagens armazena contas de e-mail.

- **Computador do usuário com o BlackBerry Device ManagerBlackBerry**

Com o BlackBerry Device Manager instalado no computador, o usuário pode conectar o dispositivo BlackBerry ao computador usando uma conexão serial ou USB. O BlackBerry Enterprise Server e os dispositivos BlackBerry usam essa conexão para enviar dados entre eles.

O tráfego de dados de dispositivos BlackBerry ignora a rede sem fio enquanto os dispositivos são conectados aos computadores dos usuários. O BlackBerry Device Manager conecta-se ao BlackBerry Router, que envia dados diretamente aos dispositivos BlackBerry.

Os usuários podem instalar o BlackBerry Device Manager separadamente do BlackBerry Desktop Manager ou com ele como parte da instalação completa do BlackBerry Desktop Software. O BlackBerry Device Manager é um componente opcional, mas é necessário para oferecer suporte a uma conexão de desvio com o BlackBerry Router.

ANEXO II

BlackBerry Enterprise Solution

O BlackBerry Enterprise Solution consiste em vários produtos e componentes que são projetados para estender os métodos de comunicação de sua organização a dispositivos BlackBerry. O BlackBerry Enterprise Solution foi projetado para ajudar a proteger os dados em trânsito em todos os pontos entre um aparelho e o BlackBerry Enterprise Server. Para ajudar a proteger os dados em trânsito pela rede sem fio, o BlackBerry Enterprise Server e o aparelho usam criptografia de chave simétrica para criptografar os dados enviados entre eles. O BlackBerry Enterprise Solution foi projetado para evitar que terceiros, inclusive provedores de serviços sem fio, acessem as informações potencialmente confidenciais de sua organização em formatos descriptografados. [35]

O BlackBerry Enterprise Solution usa confidencialidade, integridade e autenticidade, que são princípios básicos à segurança das informações, para ajudar a proteger sua organização contra perda de dados ou alteração.

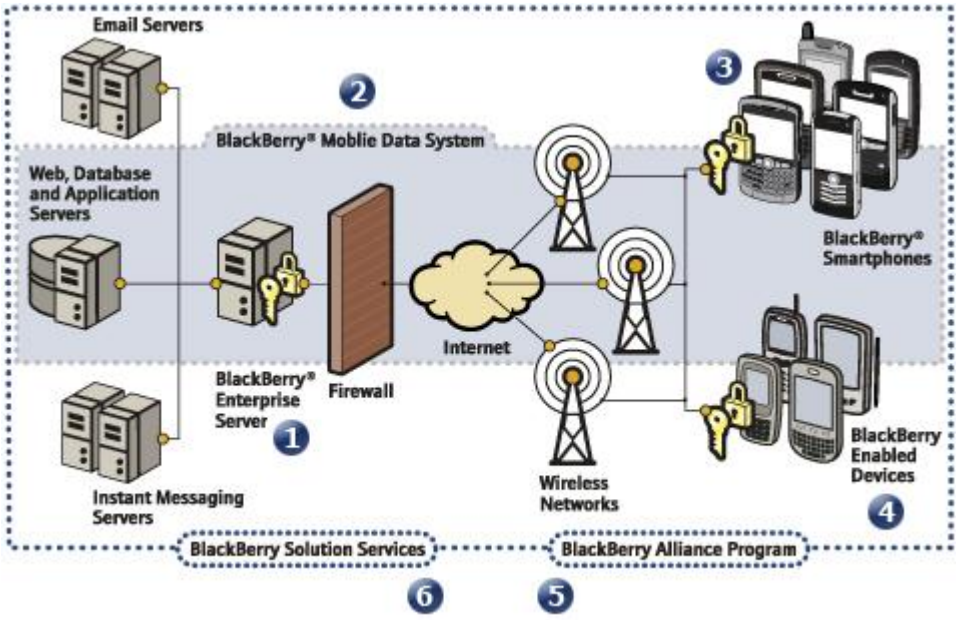

Figura 4. Diagrama do Blackberry Enterprise Solution [35]

Arquitetura: BlackBerry Enterprise Solution

A BlackBerry Enterprise Solution consiste em vários componentes que permitem estender os métodos de comunicação de sua organização a aparelhos BlackBerry.

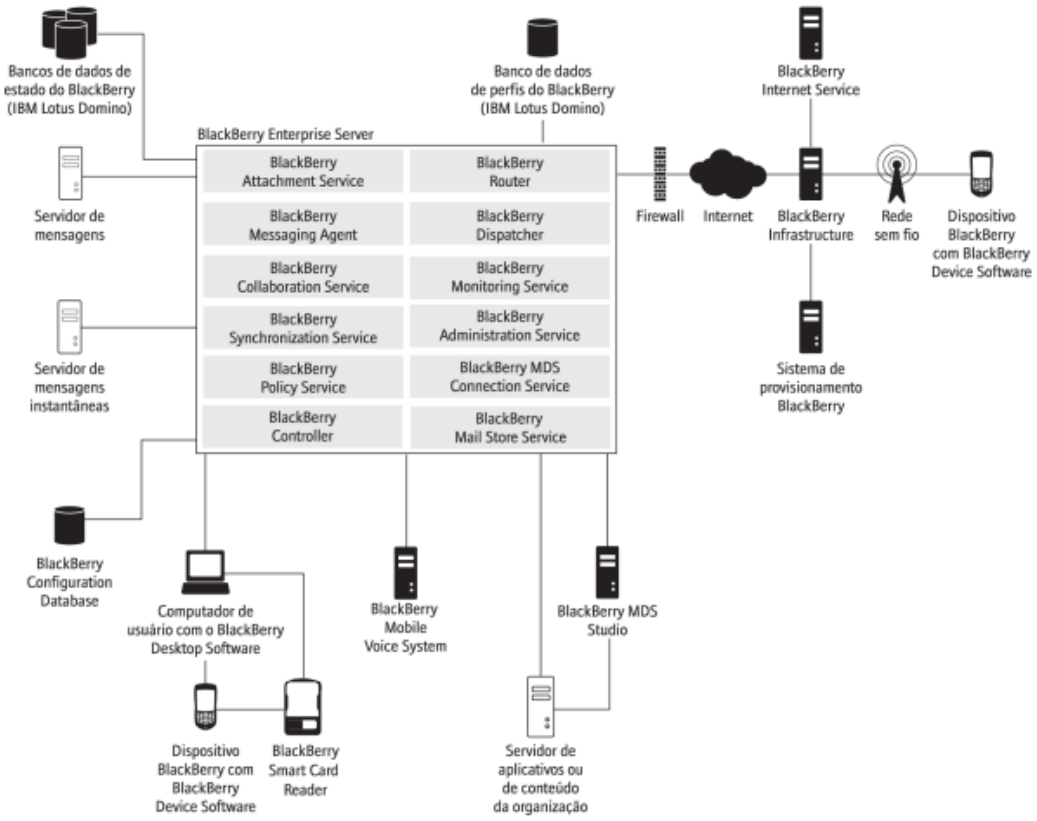

Figura 5. Arquitetura: Blackberry Enterprise Solution [35]