Criando uma estratégia para proteção abrangente na internet

Índice

Resumo executivo

No ano 2000, os Estados Unidos contavam com, aproximadamente, 135 milhões de usuários da internet.1 Por mais dramático que esse número parecesse há 10 anos, o número de usuários da internet cresceu exponencialmente: em 30 de junho de 2010, aproximadamente dois bilhões de pessoas utilizavam a internet.[2] Esta taxa de adesão é, inclusive, mais sólida, dada a penetração do uso da internet na Austrália, Europa e América do Norte, onde 61%, 58% e 77% da população está conectada, respectivamente.[3] Mesmo em outros setores do mundo, que apresentam um percentual mais baixo de usuários da internet, eles crescem rapidamente, com aumentos apresentados na Îfrica e Oriente Médio de mais de 2.300% e 1.800%, respectivamente, nos últimos 10 anos.[4]

Esse aumento e essa corrida para a conexão apresentam uma variedade de causas, incluindo a redução de custos de equipamentos habilitados para internet, a disponibilidade disseminada de conectividade sem fio de velocidade mais alta, a integração em celulares de dispositivos de comunicação de dados e de voz, bem como o aumento contínuo no valor e na diversidade de serviços disponíveis por meio da internet.

Como os sistemas e ambientes operacionais se tornam mais simples de desenvolver, implantar e utilizar, o mundo se torna menor e as pessoas interagem mais do que nunca. A localização do servidor ou do cliente não é mais óbvia ou necessária; existimos em um universo relativamente plano e as barreiras para a comunicação global e para o negócio global estão diminuindo. Virtualmente, temos acesso, sem precedentes, à informação e a ferramentas para colaboração.

Os aplicativos de internet fortalecem bastante esta nova comunicação e oferecem mais conteúdo novo e interessante, que atrai a referida onda da geração de novos usuários. Ao contrário de páginas de internet que surgiram em meados dos anos de 1990, sendo que cada uma era, principalmente, estática e pouco interativa, os aplicativos incorporados à internet atuais são reforçados por novas linguagens como a tecnologia JavaTM, JavaScript, Adobe® Flash player, XML e Hypertext Preprocessor (PHP). Os referidos aplicativos incorporados à internet apresentam um conteúdo rico e interessante e podem ser dinamicamente alterados, com base na identidade, tipo ou interesses dos usuários, que interagem com eles.

Grandes oportunidades, grandes riscos

Esta nova forma de interatividade significa um avanço real na disponibilidade de serviços e dados. Na geração atual de interatividade na internet, o usuário com apenas um navegador pode facilmente acessar sistemas e recursos, normalmente sem efetuar o download de qualquer software novo. Praticamente qualquer tipo de aplicativo ou serviço pode ser aberto a partir de dispositivos conectados " como desktops e smartphones. Os usuários abrem os navegadores em um número crescente para executar aplicativos no trabalho, receber e pagar contas em casa, preparar e pagar impostos, bem como para gerenciar todos os tipos de dados sensíveis, de cadernetas de poupança a prontuários médicos. Em resumo, novos aplicativos de internet estão transformando a experiência com a internet e com o mundo.

Este crescimento da internet e de seus aplicativos criou setores inteiros e alterou ou descartou outros. A localização física perde importância e a ausência de intermediação cria relações mais diretas e significativas para os clientes e para os fornecedores de produtos ou provedores de serviço. As relações são mais próximas, Como os clientes e parceiros de negócios podem acessar dados e realizar transações que há tempos eram restritas somente a funcionários. Como resultado, as empresas podem aproveitar as novas oportunidades para colaborar; melhorar a eficiência e simplificar pedidos, pagamentos, verificação de estado e suporte.

Poucas inovações se mostraram tão flexíveis e valiosas como os aplicativos de internet e, embora possam ser extremamente poderosos, também podem ser bastante vulneráveis. O aumento na popularidade de aplicativos de internet levou a um crescimento similarmente rápido na demanda de desenvolvedores para criá-los. Dezenas de novos produtos, plataformas e frameworks simplificam o desenvolvimento de aplicativos de internet ao ponto que praticamente qualquer pessoa pode criá-los. Infelizmente, a capacidade de criar um aplicativo seguro, ou a capacidade de revisar um aplicativo quanto a problemas de segurança, não é simples ou comum. Além da referida falta de capacitação, há verdadeiras pressões para lançamento rápido do produto no mercado sobre as equipes de desenvolvimento de aplicativos de internet; frequentemente, os aplicativos são apressados para o lançamento no mercado sem foco suficiente sobre a segurança.

Os riscos desta falta de rigor e preocupação são enormes, uma vez que a segurança de uma organização depende da segurança dos aplicativos que lhe dão suporte. Este documento discute os diversos riscos que rodeiam os aplicativos de internet e o respectivo desenvolvimento e revisões quanto às quatro camadas de segurança que uma organização deve estabelecer para implementar uma estratégia abrangente de proteção de aplicativos de internet.

Os riscos de segurança dos aplicativos de internet se multiplicam

Os aplicativos de internet apresentam uma variedade de desafios únicos de segurança. Um deles é a exposição: como os aplicativos de internet atingem milhões de usuários, também atingem milhões de hackers potenciais. Os aplicativos de internet se estendem por múltiplas camadas de infraestrutura e incorporam várias camadas de processo, elementos que provocam a exposição a uma ampla variedade de ataques possíveis.

Como os aplicativos de internet se tornam mais complexos, também se tornam mais vulneráveis; Como se tornam mais úteis e disseminados, também se tornam alvos de maior valor. E os criminosos virtuais percebem isso.

Figura 1: As informações e os serviços importantes, acessíveis por meio de um aplicativo voltado para internet, atraíram um adversário novo e muito mais sofisticado. E a motivação para os referidos ataques é a mudança e o amadurecimento, de curiosidade para ganho financeiro até espionagem real. As técnicas que os hackers empregam também são avançadas, tornando-as mais difíceis de evitar e detectar. A seta representa um rápido aumento na probabilidade de dano e impacto geral dos ataques nos aplicativos como um todo.

As violações públicas de dados, por meio de aplicativos de internet, são frequentes e podem resultar em consequências graves, incluindo perda de renda e de oportunidades de negócio, revelação de informações altamente confidenciais e danos à informação, erosão da marca e reputação, atenção adversa da imprensa, escrutínio indesejado dos advogados do cliente e custos crescentes para acatar processos judiciais e acordos.

Considere algumas seleções em uma ampla variedade de ataques que estão disponíveis para os hackers:

- **Cross-site request forgery (CSRF ou XSRF) –** também conhecido como ataque em um clique ou session riding, este tipo de exploração maliciosa de um site, onde um hacker transmite comandos não autorizados a partir de um usuário em quem o site confia. Diferentemente do cross-site scripting, que abusa da confiança de um usuário quanto a um site particular, o CSRF capitaliza a confiança que o referido site tem no navegador do usuário.
- **JavaScript Object Notation (JSON) hijacking –** este tipo de ataque explora um subconjunto da linguagem de programação JavaScript. As preocupações de segurança sobre o centro JSON no uso de um intérprete de JavaScript para executar dinamicamente um texto JSON como JavaScript, expondo assim um programa a um script errante ou malicioso que um agressor pode inserir no texto de consulta. Esta é uma preocupação principal ao lidar com dados recuperados a partir da internet.
- **Divisão de respostas HTTP –** esta é uma forma de vulnerabilidade de aplicativos de internet que resulta de uma falha do aplicativo ou de seu ambiente em resolver, adequadamente, valores inseridos. Os hackers podem utilizar divisão de respostas HTTP para realizar cross-site scripting, cross-user defacement, contaminação do cache da internet e ataques semelhantes.

- **Injeção SQL –** esta técnica de injeção de código manipula uma vulnerabilidade de segurança que ocorre em uma camada do banco de dados do aplicativo. A vulnerabilidade está presente quando a inserção do usuário é insuficientemente filtrada quanto a caracteres que possam provocar execução real de comandos SQL a partir de campos de preenchimento como janelas de login ou quando a inserção do usuário não é confidencial, de modo a evitar que tipos inadequados de informação sejam passados para um aplicativo e executados de modo inadvertido. Esta classe mais geral de vulnerabilidades pode ocorrer quando uma linguagem de programação ou scripting é incorporada em outra.
- **Injeção de Lightweight Directory Access Protocol (LDAP) –** este tipo de ataque explora o LDAP, um protocolo de aplicativo utilizado para consultar e modificar serviços de diretório executados em TCP/IP e pode executar comandos arbitrários como concessão de permissões a consultas não autorizadas.
- **Injeção de XML Path Language (XPath) –** esta é semelhante à injeção SQL, mas manipula a XPath, uma linguagem para selecionar nodos a partir de um documento XML. XPath também é utilizada para computar valores (strings, números e valores booleanos), a partir do conteúdo de um documento XML.
- **Injeção shell command –** este ataque insere um código malicioso na proteção, ou no intérprete de linguagem de comando, que executa comandos lidos a partir de um teclado.
- **Injeção server-side include (SSI) –** este insere um código malicioso no SSI, uma linguagem de scripting simples do lado servidor, utilizada quase que exclusivamente para a internet. Como o próprio nome diz, o uso primário do SSI é incluir, dinamicamente, o conteúdo de um arquivo em outro, quando este último é disponibilizado por um servidor web.
- **Cross-site scripting (XSS) –** este tipo de vulnerabilidade de segurança do computador é tipicamente encontrado em aplicativos de internet que permitem a injeção de código por meio de usuários maliciosos na internet, em páginas visualizadas por outros usuários.
- **Diretório transversal (ou path transversal) –** este tipo explora a validação insuficiente de segurança ou resolução de nomes de arquivo fornecidos pelos usuários. Nesta instância, caracteres que fazem com que o aplicativo seja executado dentro de outro, áreas inesperadas do sistema de arquivo são passadas para interfaces de programação de aplicativos de arquivos (APIs).

A prevenção é crítica

As empresas que adiam esforços para proteger aplicativos da internet podem enfrentar consequências significativas. Em 2009, nos Estados Unidos, o custo médio de uma violação de dados foi de US$ 6,75 milhões[5], e é esperado que a probabilidade de um hacker explorar qualquer aplicativo de internet continue a aumentar conforme se multiplicam os ataques automatizados e os bots. Estudos recentes realizados pela equipe IBM X-Force revelaram que, no primeiro semestre de 2010, os aplicativos de internet contabilizaram 55% de todas as violações de vulnerabilidade.[6]

Em vez de atingir usuários com código malicioso, os hackers podem agora injetá-lo em sites populares e deixar que os usuários entrem em contato com ele. Os escâneres automáticos ajudam os agressores a identificar quais sites são vulneráveis e podem ser facilmente infectados. Os plug-ins de navegadores são alvos particularmente susceptíveis aos referidos ataques. De acordo com um relatório recente da equipe IBM X-Force, no primeiro semestre de 2010, os plug-ins contabilizaram 88% das vulnerabilidades encontradas, relativas a aplicativos de internet.[7]

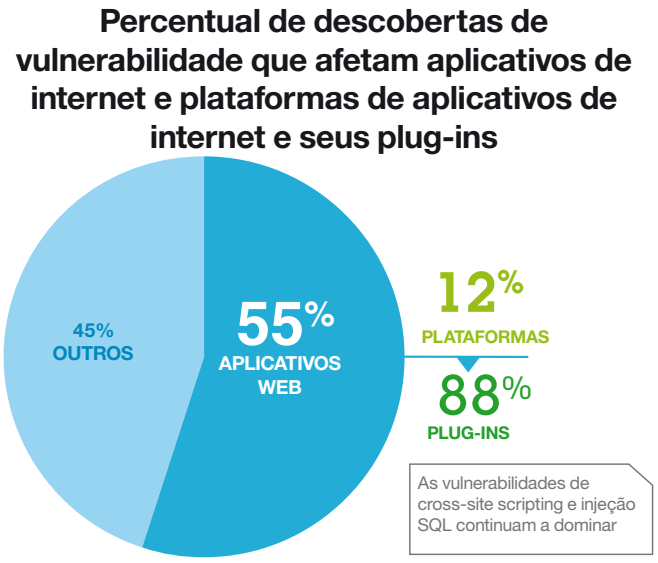

Figura 2: Os ataques em aplicativos de internet se multiplicam, tornando uma estratégia abrangente de proteção na internet, inclusive, mais crítica para os negócios que interagem com os clientes on-line[8].

Ademais, se os hackers obtêm acesso a informações sensíveis, as organizações estão em risco de não estar em conformidade com um host de obrigações jurídicas e outros requisitos, incluindo o Payment Card Industry Data Security Standard (PCI DSS), que apresenta requisitos específicos de segurança de aplicativo. A não aderência pode custar às empresas multas mensais de centenas de milhares de dólares.

Soluções existentes de segurança de ponto resultam em falhas

Os aplicativos de internet são o novo vetor de ataque para a exploração de hackers. Assim como outras ameaças de TI, a reação inicial para combater o risco é introduzir uma solução de ponto para cada ameaça. Mas as soluções existentes de segurança de ponto apresentam limitações de programação:

- Os escâneres tradicionais de vulnerabilidade efetuam a varredura de servidores web, mas não de aplicativos de internet.
- O teste manual de penetração é eficaz, mas não é escalável nem focado na resolução.
- Os firewalls tradicionais de rede oferecem proteção básica a aplicativos de internet, mas não direcionam as necessidades de aplicativos customizados de internet.
- Os firewalls de aplicativos de internet são caros para compra e gerenciamento; podem ser eficazes, mas são desafiadores e consomem tempo para implantação e ajuste adequados.
- A maioria dos aplicativos de internet é customizada, sendo difícil para os firewalls de aplicativos de internet interpretar seu comportamento como bom ou ruim.

Cada uma das referidas limitações resulta em falhas de segurança. O problema é que as soluções de ponto não foram programadas considerando-se os requisitos de segurança de aplicativos de internet.

As organizações de segurança nas empresas de hoje demandam uma solução integrada a partir de um distribuidor confiável que provê uma abordagem holística e baseada na relação custo-benefício para a segurança de TI. Para a segurança completa na internet, as empresas necessitam de uma proteção web abrangente que se adapte à estrutura de governança de segurança, gerenciamento de risco e aderência.

A IBM oferece uma estrutura de segurança abrangente em domínios-chave que acata os padrões de Control Objectives for Information and related Technology (COBIT). A IBM também fornece e vincula serviços profissionais, serviços gerenciados e soluções de hardware e software para cada domínio. Vamos explorar os requisitos da proteção abrangente de internet e entender por que a IBM está em uma posição de liderança para ajudar sua empresa a determinar e implementar uma solução de segurança para aplicativos de internet que direciona suas necessidades únicas.

Camadas em uma estratégia abrangente de proteção na internet

Maximizar a proteção de internet envolve quatro camadas de segurança – desenvolvimento de novos aplicativos habilitados à segurança enquanto são protegidos os aplicativos existentes; prevenção de invasões a sites com proteção em tempo real; implantações de service-oriented architecture (SOA) e XML ou outro tráfego de serviço na internet e controle de acesso aos aplicativos de internet.

Para simplificar cada camada de proteção, a IBM integra soluções líderes no setor que facilitam uma proteção web abrangente e que foram programadas para reduzir os riscos em transações habilitadas pela web, sites e tráfego na internet. Vamos observar mais detidamente cada uma das camadas necessárias.

Desenvolver novos aplicativos, ricos em segurança enquanto são protegidos os aplicativos existentes

Um primeiro passo fundamental em aprimorar a proteção web é identificar as vulnerabilidades nos aplicativos de internet existentes. Uma das formas com a melhor relação custo-benefício para tanto é automatizar o processo de teste. É necessário um meio de efetuar automaticamente a varredura de aplicativos, identificar vulnerabilidades e gerar relatórios com recomendações fixas inteligentes.

Para estar à frente de hackers e permitir um desenho mais seguro, a solução deve testar não apenas os aplicativos de internet atuais, mas também aqueles em desenvolvimento – durante todo o ciclo de vida de desenvolvimento. A solução deve efetuar a varredura e testar as vulnerabilidades comuns de aplicativos de internet, incluindo aquelas identificadas pela classificação de ameaça do Web Application Security Consortium (WASC).

Para atender a estes requisitos, a IBM desenvolveu as soluções IBM Rational AppScan Source Edition e IBM Rational AppScan Standard Edition. O software Rational AppScan Source Edition analisa o código-fonte utilizado para construir aplicativos, revisa códigos quanto a problemas e erros antes da implantação e pode poupar tempo e dinheiro consideráveis em problemas de garantia da qualidade (GQ), identificados posteriormente no ciclo. As soluções IBM Rational AppScan Source Edition e Standard Edition também compartilham características principais que oferecem cobertura de varredura de aplicativo para tecnologias de internet novas e antigas. As ferramentas do Rational AppScan podem avaliar os seguintes itens:

- A análise e execução de aplicativos JavaScript e Adobe Flash
- Protocolos relativos às tecnologias Asynchronous JavaScript e XML (AJAX) e Adobe Flex, tais como JSON, Action Message Format (AMF) e Simple Object Access Protocol (SOAP)
- Elaborar ambientes SOA
- Configuração adaptada e capacidades de relatório para aplicativos do tipo mashup e orientados ao processo

Como os ataques continuam evoluindo, uma solução de varredura precisa de atualizações constantes. Para ajudar a habilitar soluções Rational AppScan para manter e testar os últimos ataques e vulnerabilidades, as equipes de pesquisa e de desenvolvimento da IBM fornecem atualizações automáticas de software. Como identificar vulnerabilidades isoladas não torna os aplicativos de internet mais seguros, o software Rational AppScan também inclui recomendações inteligentes de resolução.

A aderência é crítica e uma solução automatizada de varredura pode simplificar o processo de aderência. As soluções Rational AppScan incluem mais de 40 relatórios padrão de aderência de segurança, como para PCI DSS, ISO 17799 e ISO 27001, a Lei Pública de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA), a Lei Gramm-Leach-Bliley (GLBA) e as recomendações da Convenção da Basileia II.

Depois que a solução encontra as vulnerabilidades do aplicativo, a organização precisa de tempo para corrigi-las. A segunda camada em uma estratégia abrangente de proteção na internet deve ser uma blindagem de proteção contra ataques.

Evite invasões no site com proteção em tempo real

GUma boa prevenção contra invasão precisa de ter ciência do aplicativo de internet. A segurança de aplicativo de internet IBM Proventia está incluída em toda solução para prevenção de invasão Proventia. Estas soluções, líderes de mercado, para bloquear ataques no perímetro de rede e nos níveis de servidor, incluem agora a proteção de um firewall de aplicativo de internet. Devido ao crescimento em importância dos aplicativos de internet, a IBM oferece o mecanismo principal de proteção da segurança de aplicativo de internet Proventia em toda sua linha de produtos Proventia.

Quatro requisitos principais orientaram o desenho da solução do IBM Proventia:

- **Prevenção proativa –** em vez de auditar ataques e reagir a eles, como várias soluções de proteção de internet fazem, a segurança de aplicativo de internet Proventia ajuda a direcionar e limitar as fontes primárias de ataque.
- **Configuração simplificada para aprimorar a segurança –** é possível economizar tempo com a segurança de aplicativo de internet Proventia, Como esta é configurada de modo inovador com as políticas recomendadas pela IBM X-Force, que são automaticamente atualizadas. Com o uso desta característica inteligente, é possível construir mais facilmente políticas adicionais de segurança que ajudam a proteger os aplicativos de internet adaptados.

- **Aderência aprimorada –** a segurança de aplicativo de internet Proventia direciona os requisitos PCI para a proteção de aplicativos de internet.
- **Proteção abrangente de um firewall de aplicativo de internet –** o firewall é implantado por meio da combinação do IBM Security Network Intrusion Prevention System (anteriormente denominado IBM Proventia Network Intrusion Prevention System) com um offloader Secure Sockets Layer (SSL).

A IBM oferece soluções Proventia em fatores de três formas para direcionar diferentes requisitos de implantação. A solução Security Network Intrusion Prevention System oferece proteção de internet em alta largura de banda para grandes empresas com farms de servidores de internet. A solução IBM Proventia Network Multi-Function Security oferece toda a proteção em escritório remoto ou escritório filial, com suporte virtual à rede privada (VPN). Escritórios pequenos, sem um sistema de prevenção contra a invasão da rede ou VPN podem utilizar a solução IBM Proventia Server Intrusion Prevention System para descriptografar e inspecionar o tráfego criptografado SSL.

Proteger implantações SOA e XML e tráfegos de serviço de internet

A terceira camada em uma estratégia abrangente de segurança de internet é proteger as implantações SOA e XML, bem como o tráfego de serviços de internet, que frequentemente são os componentes principais dos aplicativos de internet. Todavia, a salvaguarda dos referidos componentes exige um tipo diferente de proteção em tempo real que tipicamente poderia bastar para proteger os aplicativos de internet. Os serviços de internet geram tráfego em alta velocidade e de alto volume; inspecionar este tipo de tráfego pode facilmente degradar o desempenho do aplicativo.

A família de aplicativos WebSphere DataPower da IBM apresenta hardware com finalidade de incorporação e especializado, com capacidades de inspeção de segurança em alta velocidade e de alto volume. Os aplicativos WebSphere DataPower servem como um ponto de reforço da segurança para implantações SOA e transações de serviços de internet e XML, incluindo criptografia, filtragem por firewall, assinaturas digitais, validação de esquemas, Web Services Security (WS-Security), Web Services Policy (WS-Policy) Framework,Web Services Security Policy Language (WS-SecurityPolicy), controle de acesso a XML e XPath.

Controle de acesso a aplicativos de internet

Para ajudar a garantir que somente usuários autorizados obtenham acesso adequado aos aplicativos de internet, a solução de autenticação e autorização deve contar com as seguintes características:

- Centralização de autenticação, acesso e políticas de auditoria, permitindo que sejam facilmente definidas e gerenciadas
- Uma auditoria estabelecida e serviço de relatórios que coleta dados de auditoria de múltiplos pontos de reforço e em todas as plataformas e aplicativos de segurança
- Opções simplificadas de single sign-on (SSO)
- Códigos de segurança que são separados dos códigos de aplicativos
- Direitos seletivos e controle de acesso em nível de dados

Para atender a estes requisitos, a IBM oferece o IBM Tivoli Access Manager e o software IBM Tivoli Security Policy Manager. Por meio da integração com controle de acesso rigoroso e capacidades de gerenciamento de identidade, a família Tivoli de soluções permite controles adequados para segurança, monitoramento e gerenciamento do aplicativo.

Alcançar uma proteção abrangente na internet

A proteção de internet baseada na relação custo-benefício não limita a oportunidade na internet; pelo contrário, possibilita. Isso pode ajudar seu negócio a reduzir o risco, aprimorar a aderência, proteger a reputação da marca, ganhar flexibilidade e reduzir os custos de segurança em longo prazo por meio da construção da segurança no desenvolvimento de aplicativo.

Aproveitando sua ampla e profunda experiência em segurança e ofertas, a IBM pode oferecer uma estratégia abrangente para ajudar seu negócio a gerenciar, efetivamente, a segurança de aplicativos de internet. Como uma das mais prolíficas criadoras de software do mundo e como uma consultoria de segurança e de recurso estratégico para organizações de grande porte e de atuação global, a IBM apresenta suas soluções com realidades de orçamento, cronogramas e prioridades competitivas. A IBM está orientada a ajudar os clientes na criação de aplicativos de internet que são ricos em segurança por meio da programação, com base em todos estes insights, e reforça a posição da IBM como uma consultoria e colaboradora valiosas para qualquer esforço de desenvolvimento de aplicativo rico em segurança.

Para mais informações

Para mais informações sobre como aproveitar a vantagem das soluções comprovadas da IBM para ajudar a salvaguardar os aplicativos de internet de sua empresa, entre em contato com seu representante da IBM, com um parceiro de negócios da IBM ou visite:
ibm.com/security/application-process.html

Adicionalmente, as soluções financeiras do IBM Global Financing possibilitam o gerenciamento eficaz da verba, proteção contra a obsolescência da tecnologia, custo total aprimorado da propriedade e retorno do investimento. Ademais, nossos Global Asset Recovery Services ajudam a direcionar as questões ambientais com soluções novas e mais preocupadas com a relação entre energia e eficiência. Para mais informações sobre IBM Global Financing, visite:
ibm.com/financing

[1] Computer Industry Almanac, http://www.c-i-a.com/internetusersexec.htm

[2, 3, 4] Internet World Stats, "Internet Usage Statistics, The Internet Big Picture," http://www.internetworldstats.com/stats.htm

[5] Ponemon Institute, *2009 Annual Study: Cost of a Data Breach*, January 2010.

[6, 7, 8] IBM, *IBM X-Force 2010 Mid-Y ear Trend and Risk Report*, August 2010.

IBM Brasil Ltda.
Rua Tutóia, 1157
CEP 04007-900
São Paulo – Brasil

O site da IBM pode ser encontrado em:
ibm.com

Por favor, recicle

Rational. software

RAW14246-BRPT-00