Universidade Católica de Brasília - UCB
Pró-Reitoria de Pós-Graduação e Pesquisa - PRPGP
MBA - Gestão de Sistemas de Informação - GSI

Segurança da Informação
Prof. Ly Freitas

SEGURANÇA DA INFORMAÇÃO EM AMBIENTES CORPORATIVOS

Equipe:

Alexandre Bittencourt de Oliveira
Alexandre Menezes Ferreira
Anderson Almeida das Dôres

Segurança da Informação em Ambientes Corporativos

Alexandre Bittencourt de Oliveira, Alexandre Menezes Ferreira e Anderson Almeida das Dôres

Resumo

Estre trabalho procura apresentar e analisar a segurança da informação em ambientes corporativos. Primeiramente, são descritos os conceitos de alguns tópicos abordados no trabalho, como redes de computadores, ambientes corporativos, segurança, firewall, política de segurança e vírus.

A principal ênfase do trabalho foi dada à amostragem dos dados encontrados na pesquisa. Posteriormente, foi realizado um comparativo da segurança dos anos 2000, 2001 e 2002, através de dados da pesquisa nacional da empresa Módulo.

Ao final, conclui-se a situação da segurança da informação em ambientes corporativos em âmbito regional e nacional.

Palavras-Chave

Sistemas de Informação (S.I.); Práticas de trabalho; Teconologia da Informação; Recursos-Humanos; Objetivos Organizacionais; Informação; Gerenciamento.

Safety of the Information in Corporate Atmospheres

Summary

This work search to present and to analyze the safety of the information in corporate atmospheres. Firstly, the concepts of some topics are described approached in the work, as nets of computers, corporate atmospheres, safety, firewall, politics of safety and virus.

The main emphasis of the work was given to the sampling of the data found in the research. Later, a comparative of the safety of the years 2000 was accomplished, 2001 and 2002, through data of the national research of the company Module.

At the end, the situation of the safety of the information is concluded in corporate atmospheres in regional and national extent.

keywords

Information Systems (I.S.); work Practices; Technology of the Information; Resource-human; Organizational objectives; Information; Administration.

1 Introdução

Os altos índices de informatização, conectividade, negócios pela Internet e compartilhamento de dados tornaram a informação um dos bens mais valiosos e mais vulneráveis das empresas. Com isso, incidentes nas redes de computadores passaram a afetar diretamente os resultados do negócio e o valor das empresas. As grandes empresas já se preocupavam bastante com o assunto de segurança de dados. Porém os ataques terroristas (físico) e muitos outros, na forma digital, vêm mostrando uma grande preocupação dos responsáveis pela área. Os ataques e tentativas vêm aumentando gradativamente ao longo do tempo.

Surgem tecnologias novas de softwares, posteriormente as vulnerabilidades são encontradas e exploradas a fim de denegrir a imagem da corporação. Existem muitas pesquisas voltadas ao assunto, com o intuito de caracterizar o nível de segurança das empresas em todo o mundo. Este trabalho foi desenvolvido com o propósito de analisar a real situação da segurança da informação nos diferentes ambientes corporativos da regiões. A pesquisa elaborada seguiu o molde das maiores pesquisas nacionais e mundiais (Módulo, Informationweek, Cert). Através dela será possível perceber se a região está se preocupando com a segurança de dados nos aspectos de tecnologias, consciência e investimentos.

2 Revisão da Literatura

2.1 Redes de Computadores

Há muito tempo atrás, a única maneira de comunicação existente entre pessoas era através de cartas. A evolução da tecnologia permitiu o aparecimento do telefone, que possibilitou a comunicação entre pessoas no mesmo instante que desejasse. Ao longo dos anos os meios de comunicações foram aumentando, telefones, rádios, televisões e satélites de comunicação. A comunicação é muito importante para o desenvolvimento e evolução dos seres humanos e da sociedade em geral. Sem ela, não se consegue trabalhar, estudar e se divertir.

O computador pessoal foi uma das invenções mais importantes nos últimos tempos. Os textos que antes eram escritos em máquinas de escrever sem nenhuma maneira de armazenamento exceto em papel, hoje são escritos e atualizados rapidamente e podem ser armazenados digitalmente em quantidades imensas. A sua principal função: "cálculo de funções matemáticas para solução de problemas complexos", é realizado em segundos. Com estas inovações, o computador tornou-se uma ferramenta de trabalho essencial na comunidade mundial, porém, isoladamente, eles estavam limitados.

Resolveu-se então, conectá-los afim de que suas funções fossem compartilhadas por diversas pessoas. Nesta nova fase, funções e recursos podiam ser compartilhados economizando e aumentando a eficiência e a produtividade dos serviços. Este novo grau de comunicação acabou se tornando essencial na vida pessoal e profissional das pessoas e empresas. Daí surgiu o conceito de redes de computadores. As redes de computadores se tornaram mais populares com o advento da Internet, que nada mais é do que várias redes de computadores conectadas, formando uma grande rede mundial.

2.2 Ambientes Corporativos

As informações agora são primordiais para o sucesso das negociações. Com isso o grau de proteção e preocupação com estas informações cresceu consideravelmente dentro deste ambiente integrado. Medidas e cuidados de segurança devem ser tomados e sempre verificados. A informática deixa de ser uma ferramenta para se tornar um dos elementos principais na organização e metodologia dos negócios, definindo modelos e características de organizações, fluxo e segurança de informações e tecnologias aplicáveis na gestão dos negócios. Como qualquer cidade que começa a crescer e passa a ter problemas com o aumento da violência, uma rede de computadores também sofre com esses inconvenientes. Em ambientes corporativos que tratam de diferentes culturas humanas, tecnológicas e sociais, a preocupação com a segurança se torna fato primordial para que a organização tenha uma imagem firme e segura. A segurança da informação em ambientes complexos deve seguir padrões pré-estabelecidos, incluindo todos os envolventes no assunto, tanto pessoas como processos.

2.3 Segurança da Informação

O compartilhamento de recursos e informações através das redes de computadores não é uma tarefa simples. Em uma rede podem existir muitos computadores cada qual com sua função determinada. As informações trocadas entre

eles nem sempre podem ser vistas e compartilhadas por todos, muitas delas são confidenciais e devem ser compartilhadas por apenas algumas pessoas.

Para o controle da rede devem existir funções específicas a cada usuário da rede, definindo quem, onde e o que se pode acessar, delimitando o espaço de cada um dentro do sistema inteiro.

Como pode ser visto uma rede de computadores não é apenas conectar um ou mais computadores para trocar informações. Estas informações devem ser gerenciadas com todo o cuidado, se preocupando com os três principais tópicos de redes: integridade, confidencialidade e disponibilidade.

2.4 Segurança da Informação em Ambientes Corporativos

A complexidade dos ambientes corporativos se dá devido aos diferentes tipos de comunicação existentes entre as redes integradas, cada qual com sua tecnologia, seus usuários, sua cultura e sua política interna. A integralização de todos estes fatores é tarefa importantíssima na segurança.

2.5 Criptografia

A criptografia é o ato da transformação de informação numa forma aparentemente ilegível, com o propósito de garantir a privacidade, ocultando informação de pessoas não autorizadas.

Através da criptografia os dados são codificados e decodificados, para que os mesmos sejam transmitidos e armazenados sem que haja alterações realizadas por terceiros não autorizados. Como a Certificação Digital o principal objetivo da criptografia é prover uma comunicação segura, garantindo confidencialidade, autenticidade, integridade e a não-repudiação (NAKAMURA, 2002).

Existem duas possibilidades de encriptação de mensagens por códigos ou cifras. Por códigos, o conteúdo das mensagens é escondido através de códigos predefinidos entre duas partes. Este tipo de solução tem dois grandes problemas: a facilidade de deciframento devido ao intenso uso dos códigos e o envio de apenas mensagens predefinidas.

Existe um outro método, a cifra, onde o conteúdo da mensagem é cifrado através da mistura e/ou substituição das letras da mensagem original. A mensagem é decifrada fazendo-se o processo inverso ao ciframento. As cifras consistem na implementação de longas seqüências de números e/ou letras que determinarão o formato do texto cifrado através de algoritmos associados a chaves.

Este tipo de criptografia se baseia na classificação quanto ao número de chaves utilizadas, simétrica e assimétrica.

2.6 Hackers

A definição correta de “hacker” (OTILIO, 2000) é: uma pessoa que, por fins próprios, se interessa exageradamente por assuntos relacionados à informática (sistemas

operacionais, redes e afins). Utiliza seu conhecimento avançado para descobrir falhas e vulnerabilidades de segurança. Erroneamente, o termo “hacker” passou a ser usado para qualquer pessoa que efetuasse algum tipo de crime cibernético.

O termo “cracker“ é o correto nome para alguém que utiliza seus conhecimentos para quebrar a segurança, ganhar acesso a sistemas de outras pessoas, sem a devida permissão e cometer estragos no mesmo. Ou seja, o “cracker” é um “hacker” atuando negativamente. Com a evolução das tecnologias, ocorreu uma mudança no perfil dos “crackers” e dos “hackers”. Antes, eles eram pessoas com alto grau de conhecimento em informática (sistemas operacionais, redes e tecnologia em geral). Devido a grande facilidade de troca de informações pela Internet, qualquer pessoa passou a ter acesso a informações sobre segurança. Outro fator muito importante foi as ferramentas (de console ou gráficas) criadas por “hackers” mais experientes que trouxeram aos usuários comuns a possibilidade de invasão a sistemas particulares. Os motivos de pessoas infringirem leis invadindo sistemas e computadores são os mais variados possíveis.

Abaixo segue alguns deles:

- Lazer;
- Supremacia de grupos rivais;
- Roubo de informações;
- Protestos;
- Desafios propostos por sites e empresas de informática.

2.7 Firewall

Firewalls são mecanismos de proteção de redes de computadores, que forma uma barreira interposta entre uma rede privada de qualquer organização e uma rede externa (por exemplo: Internet). Existem na forma de hardware, ou software, ou uma combinação de ambos (NAKAMURA, 2002).

Sua principal função é analisar o tráfego entre a rede interna e a rede externa em tempo real, permitindo ou bloqueando o tráfego de acordo com regras pré-definidas. Atualmente, é o principal instrumento de defesa de redes corporativas, controlando e monitorando o acesso aos sistemas e aos hosts da organização e a filtragem de tráfego entre duas redes. Com ele pode-se dispensar a instalação de softwares adicionais nos hosts, centralizando a administração e a configuração de toda a rede.

Algumas funções dos Firewalls:

Filtragem de serviços – consiste em filtrar serviços que não são considerados seguros, aumentado a segurança da rede e dos hosts, podendo rejeitar pacotes de uma determinada origem.

2.8 Pragas Virtuais

2.8.1 Vírus

Vírus é um programa malicioso que possui a habilidade de auto-replicar e infectar partes do sistema operacional ou de programas de aplicação, com o intuito de causar a perda ou dano nos dados.

- Vírus de arquivos ou programas – Vírus que normalmente ficam alojados em arquivos com extensões: *.COM, .EXE, .DLL, .SYS, .BIN e .BA*T. Exemplos de vírus de programa conhecidos são Jerusalém e Cascade;

- Vírus de setor de boot – Vírus que ficam armazenados na inicialização do sistema. Exemplos de vírus de setor de boot são: Form, Disk Killer, Michelangelo e Stoned;

- Vírus de macro – Vírus que infectam arquivos dos programas Microsoft Office (Word, Excel, PowerPoint e Access);

- Vírus Multipartite – Vírus que infectam setores de boot, disquetes e arquivos executáveis. Exemplo: Dead.Boot.488, Pieck.4444.A, Delwin.1759;

- Vírus Stealth – Vírus que utiliza técnicas para ocultar as alterações executadas e enganar o antivírus. Exemplo: AntiCNTE Boot, Natas.4988, Bleah;

- Vírus Polimórficos – Vírus que se auto modificam a cada nova disseminação. De forma que um único vírus pode ter inúmeras formas diferentes. Exempo: Satan Bug, Spanska.4250, W95/HPS.

2.8.2 Worm (Verme)

Os worms são parecidos com os vírus, porém se diferenciam na forma de infecção. Eles somente fazem cópias deles próprios e as propagam. Exemplo: LittleDavinia, Navidad.

Worm (COFFEE, 2000) é um código de programa auto-replicante que, normalmente, não causa danos ao sistema, porém se duplica por meio de redes de computadores. A percepção da contaminação por worms se dá quando sua replicação descontrolada consome recursos do sistema, atrasando ou interrompendo outras tarefas. Porém existem alguns worms que além das características normais também danificam o sistema.

2.8.3 Trojan Horse (Cavalos de Tróia)

Termo "Cavalo de Tróia" vem de uma lenda antiga, onde os gregos deram aos troianos um grande cavalo de madeira como sinal de que estavam desistindo da guerra, desejando a paz. Tal cavalo escondia no seu interior um grupo de soldados gregos, que abririam os portões da cidade para o exército grego, depois que os troianos levassem o cavalo para dentro da cidadela.

2.9 Sistema de Detecção de Intrusos – IDS

Os sistemas de detecção de intrusos (IDS) são sistemas de monitoramento de tráfego de redes de computadores a procura de situações ilegais. Eles funcionam analisando tráfego ou eventos suspeitos, caso encontre algo estranho dos padrões estabelecidos, é enviado um aviso ou é gerada uma rotina de correção (NAKAMURA, 2002). A detecção de intrusos pode ser realizada de dois modos: Sensores procuram por "assinaturas" de ataques, que são os métodos utilizados por invasores e catalogados no IDS; Os IDS de rede têm a vantagem de proteger todo um segmento de rede, embora sejam limitados por não poder "ver" o que acontece "dentro" dos servidores. Os IDS de rede examinam os tipos e o conteúdo dos pacotes trafegados. IDS baseados em servidores examinam as trilhas de auditoria e log de atividades. Uma implementação completa de IDS deverá utilizar ambos os tipos de IDS.

Para a perfeita monitoração do sistema, um IDS deve seguir alguns aspectos básicos (PELISSARI, 2002):

2.10 VPN – Virtual Private Network

Atualmente, a troca eletrônica de informações é um bem comum entre os indivíduos. A comunicação e a troca de dados entre os ambientes corporativos ocorre constantemente sendo necessário um meio de comunicação seguro e confiável. Os meios de comunicações dedicados são bastante utilizados, porém com alto valor de aquisição e manutenção. A solução encontrada para diminuir o custo da comunicação foi utilizar uma rede pública (Internet) como meio de comunicação. Mas a segurança, a confiabilidade e a integridade neste tipo de comunicação são pontos que comprometem o serviço devido ao conteúdo trafegado por ela ser acessível a todos, podendo ser interceptado e capturado (PELISSARI, 2002).

A VPN utiliza exatamente este conceito de comunicação, todavia com os quesitos mínimos de segurança, integridade e confiabilidade nos seus serviços (NAKAMURA, 2002).

Além disso, a Internet sendo de alcance mundial facilita a comunicação em lugares onde a situação é irregular, possibilitando assim uma total abrangência de comunicação. Para que a abordagem de VPN se torne efetiva, ela deve prover um conjunto de funções que garanta Confidencialidade, Integridade e Autenticidade.

Existem muitas técnicas que podem ser usadas na implementação de VPN, abaixo são listadas algumas:

- Modo Transmissão – somente os dados são criptografados, não havendo mudança no tamanho dos pacotes;

- Modo Transporte – somente os dados são criptografados, podendo haver mudança no tamanho dos pacotes;

- Modo Túnel Criptografado – os dados e o cabeçalho dos pacotes são criptografados, sendo empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e

de destino. Modo Túnel Não Criptografado – tanto os dados quanto o cabeçalho são empacotados e transmitidos segundo um novo endereçamento IP, em um túnel estabelecido entre o ponto de origem e destino.

2.11 Tendências futuras

2.11.1 Smartcard (cartão inteligente)

Com o formato e tamanho de um cartão convencional, conta com um chip embutido, que pode processar e armazenar dados eletrônicos protegidos por características avançadas de segurança.

2.12 Biometria

A biometria tem se tornado uma forma de segurança bastante efetiva na autenticação de usuário.

Pode-se definir biometria como sendo uma forma de verificação de identidade de pessoas por meio de característica física e única. Dentre muitas formas de biometria, pode-se destacar a impressão digital, scanner de íris e projeção facial.

Mesmo com o pequeno avanço, a biometria já obtém sucesso, baixando o índice de fraudes.

O funcionamento do sistema consiste em verificar uma certa identificação em algum registro. Para isso, cada usuário configura uma característica física, biológica ou comportamental junto ao sistema, a fim de que seja utilizada na verificação da identidade do usuário.

A verificação consiste na captura da característica do usuário através de sensores e comparação da mesma com o modelo biométrico armazenado no banco de dados do sistema.

Abaixo estão relacionadas algumas formas de biometria:

- Identificação de íris;
- Impressão digital;
- Reconhecimento de voz;
- Reconhecimento da dinâmica da digitação;
- Reconhecimento da face;
- Identificação da retina;
- Geometria da mão;
- Reconhecimento da assinatura.

A pesquisa da Informationweek (VALIM, 2002) informa que o uso de algum tipo de sistemas biométricos pelas empresas brasileiras, no ano passado era de 1% e este ano foi para 6,1%.

3 ESTUDO DE CASO

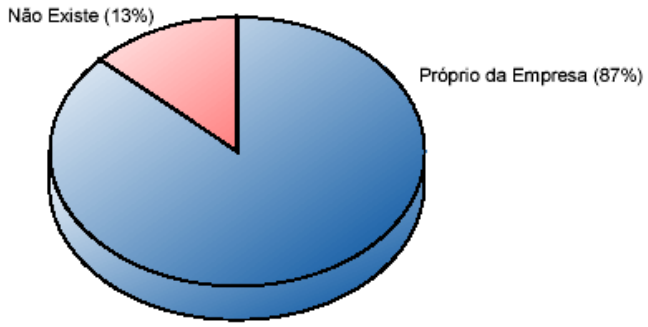
Foram definidas empresas grandes e pequenas de diferentes áreas de atuação. Os contatos foram feitos através de telefone e e-mail e marcadas entrevistas (reuniões para o preenchimento da pesquisa).

As entrevistas foram feitas pessoalmente, junto às empresas divulgando o trabalho e objetivando respostas sérias e corretas.

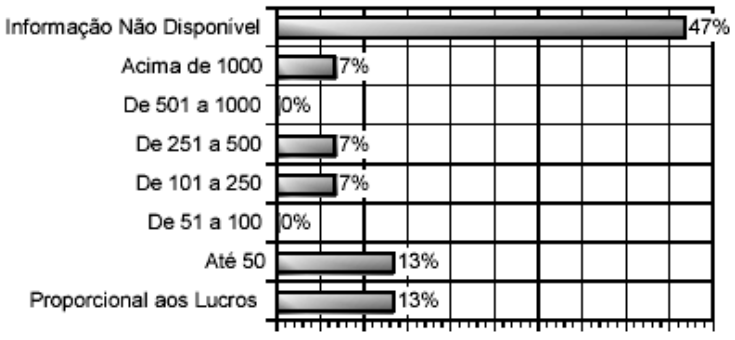
Entrou-se em contato com 21 empresas, embora apenas 15 delas aceitaram participar da pesquisa. Das empresas que não participaram, 3 delas alegaram falta de tempo dos responsáveis pela segurança e o restante (3) sequer responderam o questionário.

Empresas contatadas	21	100%
Empresas que sequer responderam o primeiro contato	03	14%
Empresas que responderam a entrevista	15	72%
Empresas que não concordaram em responder o questionário	03	14%

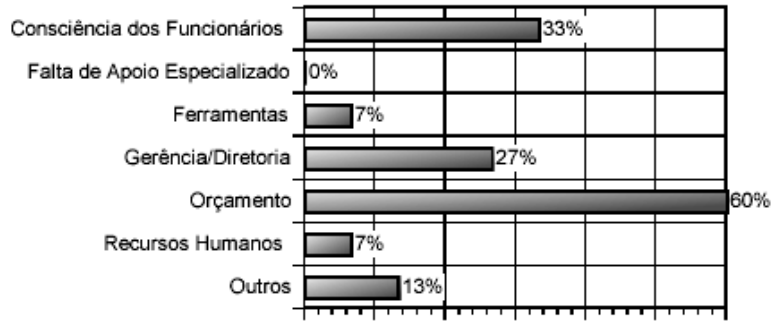
3.1 Departamento de Segurança



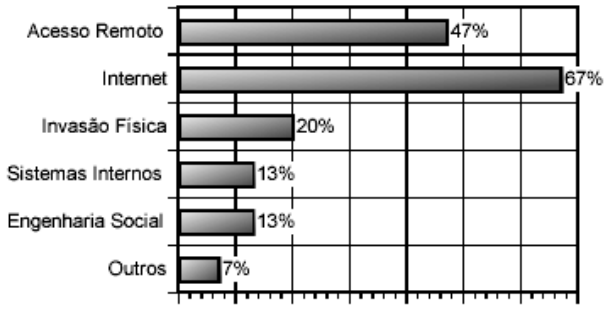
3.2 Orçamento Destinado a Área de Segurança



3.3 Principais Obstáculos para implementação da Segurança



3.4 Principais pontos de invasão



4 CONCLUSÃO

Através do trabalho pode-se afirmar que a conscientização das pessoas é o principal fator da falta de segurança tanto física como eletrônica. Se houvessem palestras a todos os funcionários (próprios, terceiros e chefias) abordando assuntos relacionados com a informática, de como utilizar as ferramentas adequadamente, não abusando da liberdade, se protegendo de possíveis problemas, os usuários do sistema iriam ajudar a conservá-lo e a preservá-lo. Não é uma tarefa fácil, pelo contrário modificar a educação de pessoas é uma tarefa muito complexa, mas quando aplicada com sucesso é eficiente e muito produtiva. São investimentos ao longo prazo que bem implantados são recompensadores.

Investimentos em políticas de segurança estão sendo muito aplicados. Aos poucos os responsáveis pela segurança conseguem impor os métodos e procedimentos corretos na utilização de sistemas computacionais. Planos de contingências também estão sendo desenvolvidos na maioria das empresas. Ameaças de ataque têm preocupado bastante. E caso aconteçam desastres, quem tiver um plano formalizado, conseguirá amenizar os prejuízos rapidamente. Políticas de segurança, firewall e antivírus são dispositivos de segurança essenciais em empresas, porém sozinhos eles não são nada. São necessários outros dispositivos como criptografia, IDS, VPN, que gradativamente estão sendo implementados nas empresas.

A facilidade dos próprios funcionários das empresas de se aventurarem em lugares onde não tem acesso é o principal fator de ocorrência, devido à má configuração e permissão de acesso no sistema. O grande protetor das redes, o firewal, nestes casos não consegue fazer nada, pois ele a protege de invasões de fora para dentro. Por isso a necessidade de outros mecanismos de segurança como IDS.

Estes conflitos refletem prejuízos tanto à empresa quanto ao próprio funcionário. A empresa acaba pagando horas desnecessárias e os funcionários acabam perdendo o acesso a Internet por não saber usá-la.

As empresas devem investir em conscientização para este fim também. Muitas empresas liberam o acesso a qualquer funcionário, no entanto, assim que são contratados recebem um código de conduta ética, com informações sobre a política da empresa, incluindo utilização da Internet. Caso não sigam as instruções, são convidados a se retirar da empresa no mesmo instante.

As medidas de segurança devem ser preventivas com políticas de segurança, palestras, planos de contingências, configuração adequada e ferramentas suficientes. A plena segurança nunca existirá, todavia para se implementá-la suficientemente deve-se levar em conta recursos físicos e lógicos, cultura, conscientização, capacitação e pessoas.

5 BIBLIOGRAFIA

MÓDULO SECURITY SOLUTIONS. 4ª Pesquisa Nacional sobre Segurança da Informação. 1998. Disponível em: <http://www.modulo.com.br/empresa/noticias/pesquisa/pesquisa98.htm>. Acesso em: 20 mai. 2003

PC WORLD, MÓDULO SECURITY MAGAZINE. Lista classifica os dez vírus mais perigosos. 27 ago. 2002. Disponível em: <http://www.modulo.com.br/index.jsp>. Acesso em 20 mai. 2003.

P**C WORLD, MÓDULO SECURITY MAGAZINE**. Lista classifica os dez vírus mais perigosos. 27 ago. 2002. Disponível em:http://www.modulo.com.br/index.jsp>. Acesso em 20 mai. 2003.

SYMANTEC. Pesquisa da Symantec aponta que 67% das empresas já sofreram ataques de segurança. 15 ago. 2002. Disponível em: <http://www.symantec.com.br/region/br/press/2002/n020815.html>. Acesso em 20 mai. 2003.

TANENBAUM, A. S. Redes de computadores. Rio de Janeiro: Campus, 1997. 923p. VALIM, C. E. Acesso negado. Informationweek Brasil, Sorocaba (SP), n. 74, p38-48, 20 mail. 2003.