FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

ESPECIALIZAÇÃO EM GESTÃO DE REDES E SEGURANÇA DA INFORMAÇÃO

JOÃO EDUARDO BATISTA DE DEUS ANSELMO

ARACAJU-SE
2012

JOÃO EDUARDO BATISTA DE DEUS ANSELMO

SEGURANÇA DE REDES: Usuários educados, ambientes mais Seguros.

Projeto apresentado como requisito básico para a Conclusão do Curso de Pós-graduação em Gestão de Redes e Segurança da Informação da Faculdade de Administração e Negócios de Sergipe (FANESE).

Orientador (a):

ARACAJU-SE
2012

SUMÁRIO

RESUMO

O constante uso de equipamentos informáticos como instrumento de trabalho provocou um aumento significante da preocupação com a Segurança de Informação. Para conseguir níveis confiáveis de segurança, o objetivo de muitas empresas vem sendo investir primeiramente em tecnologia e processos, deixando de lado os recursos humanos que trabalharão diretamente com essas tecnologias e farão os processos funcionar.

O volume de conhecimento a ser apreendido em contra partida com aumento exponencial da ignorância, o crescimento da infraestrutura e da complexidade das redes de comunicação e do número de usuários amplia a importância do fator humano como elemento vulnerável dentro da cadeia de recursos que forma a Segurança da Informação. Cada vez mais pessoas, com pouco tempo, têm se conectado com equipamentos e programas que funcionam sobre tecnologias que elas mal sabem que existem sujeitas a ataques e ameaças que crescem não apenas em quantidade, mas também em suas diversas formas de atuação.

Esse trabalho tem como objetivo mostrar que as tecnologias e os processos são incapazes de garantir a Segurança da Informação. Sendo que o mais simples treinamento dos recursos humanos também se mostra fragilizado diante da continua desatualização dos conhecimentos ensinados. É preciso educar as pessoas, e não apenas passar instruções eventualmente.

PALAVRAS-CHAVE

Segurança, Informação, Tecnologia.

ABSTRACT

The constant use of computer as an instrument of work caused a significant increase in concern about Information Security. To achieve reliable levels of security, the goal of many companies has been investing primarily in technology and processes, leaving aside the human resources who will work directly with these technologies and processes will work.

The amount of knowledge to be learned in counter starting with an exponential increase of ignorance, infrastructure growth and complexity of communication networks and the number of users increases the importance of human factor as an element within the chain vulnerable resource that forms the Security Information. More and more people, with little time, have been connected with equipment and programs running on technologies that they hardly know that there are subject to attacks and threats that grow not only in quantity but also in its various forms of action.

This work aims to show that the technologies and processes are unable to ensure information security. Since the simplest training of human resources also shows remains fragile in the face of outdated knowledge taught. We must educate people, not just pass any instructions.

KEYWORDS

Security, Information Technology.

1 INTRODUÇÃO

Todos os dias milhares de pessoas que utilizam os serviços de correio eletrônico estão sujeitas a se deparar com mensagens do tipo, "Atualize dados cadastrais de sua conta no Banco XPTO". Essas mensagens provavelmente são tentativas de roubo de dados. No entanto, sempre há o usuário que abre todas as mensagens sem verificar suas autenticidades. Assim começa os casos de fraude bancária.

A fotógrafa Margarete Barreiro, após instalar um discador de conexão com a internet, caiu na situação que é o temor de muitos brasileiros. A vítima preencheu os dados que lhe pediram sem pensar. No mesmo dia a conta foi bloqueada e só percebeu que era um golpe após efetuar contato com o banco. Sua conta possuía gastos que chegavam a R$ 100 mil, divididos entre pagamentos de contas pessoais, despachantes etc.

De acordo com o levantamento do instituto de pesquisa de marketing Synovate, o Brasil é o terceiro país em número de fraudes via internet banking. Seja por falha humana ou invasão, o estudo indica que o Brasil realmente precisa repensar suas diretrizes de segurança.

A cadeia formada por processos, pessoas e tecnologia denomina-se Segurança da Informação, dentre os elos dessa cadeia as pessoas ainda são apontadas como sendo a parte mais fraca segundo os especialistas.

Mesmo tendo investimentos afortunados em tecnologia e processos, a bolha da segurança pode estourar a partir das atitudes de alguns funcionários:

- Mal qualificados que põem em risco os ativos de rede da empresa.
- Negligente, sabem o que é necessário para lidar com os aspectos da segurança da informação, mas desfazem as proteções criadas para os ativos da empresa.

- Demitidos e descontentes, aproveitam-se do conhecimento sobre tecnologia e das informações adquiridas acerca dos processos da empresa para sabota-la.

Os dois primeiros tipos agem por omissão ou ignorância. Os demais atuam de forma intencional e criminosa. Com relação à educação cabe dizer que lhes falta: treinamento, conscientização e educação.

Essas carências manifestam-se em situações de falta de comprometimento, ausência de atitude proativa e perda de eficiência frente a situações de rotina. Por mais esquisito que pareça, pouco é o investimento feito nas pessoas quando se fala em segurança de redes e informação.

2 DADOS E RELATOS

Depois de 25 anos na área, o consultor americano constata que nenhuma iniciativa de conscientização em segurança supera a natureza humana.

Winn Schwartau tem escrito, ensinado e prestado consultoria sobre segurança por mais de 25 anos. Para o fundador da Security Awareness Company, a tecnologia pode ter mudado, mas o fator mais influente em segurança– o funcionário ou o usuário final - não.

Afirma Schwartau, *"Nós não tocamos em redes, nós tocamos nas pessoas", "Porque, no fim, o elo mais fraco em todas essas coisas é a pessoa que está à frente da tela".*

Segundo Schwartau, *"Muitas empresas dizem ter algum tipo de política sobre o comportamento do usuário, mas dada a retidão política do mundo, mesmo que você tenha uma política que diz 'não faça isso ou pagará o preço', geralmente o preço não é pago".*

3 SOBRE AS FALHAS HUMANAS

Falhas humanas podem ser divididas em três tipos. As ações necessárias para prevenir falhas posteriores vão depender do tipo de falha humana envolvida.

I. Erros baseados em habilidades: deslizes e esquecimentos

   a. Deslizes - acontecem quando uma pessoa está executando tarefas familiares automaticamente. A ação da pessoa não ocorre conforme o planejado, como por exemplo, acionar o interruptor errado em um painel de controle.

   b. Esquecimentos (lapsos) - acontecem quando uma ação é feita fora da ordem habitual ou um passo da sequência é perdido.

Esses tipos de erros podem ser previstos e medidas podem ser tomadas para prevenir sua probabilidade como, o uso de codificações coloridas, checklist, bloqueios, etc.

II. Enganos: erros de julgamento (baseados em regras ou em conhecimento)

   a. Enganos baseados em regras - ocorrem quando uma pessoa tem uma série de regras sobre o que fazer em certas situações e aplica a regra errada num determinado momento.

   b. Enganos baseados em conhecimento - acontecem quando uma pessoa está diante de uma situação não familiar para a qual ela não tem regras. Neste caso o trabalhador utilizando seu conhecimento chega a conclusões erradas.

Capacitação, procedimentos de trabalho seguros e completos e design dos equipamentos são importantes na prevenção desses tipos erros.

III. Violações (quebra de regras)

   a. Violações - falhas deliberadas ao seguir regras, tomando atalhos para poupar tempo e esforço, para aumentar a produtividade ou melhorar o resultado. São impostas por constrangimentos ou por falhas dos sistemas e aceitas tacitamente na empresa.

Este tipo de comportamento pode ser previsto e só se revela enquanto “problema” depois da ocorrência de evento adverso.

Capacitação adequada, regras práticas simples, supervisão de rotina e monitoramento de desempenho podem reduzir falhas humanas. Quando estiver avaliando como evitar falhas humanas, mantenha em mente o fato de que elas não ocorrem isoladamente.

4 COMO REDUZIR OS PROBLEMAS DE SEGURANÇA?

Os ataques são cada vez mais frequentes as pequenas e médias empresas que utilizam aplicações em rede. Algumas soluções de segurança integradas, abrangentes e acessíveis, são oferecidas e adaptadas às necessidades das empresas. Estas soluções ajudam a garantir a continuidade da atividade empresarial, manter a privacidade dos clientes e reduzir custos operacionais.

4.1 ALGUNS PROBLEMAS DE SEGURANÇA

De acordo com pesquisas recentes, o maior desafio que as pequenas e médias empresas enfrentam, é a segurança. As ameaças são contínuas e podem prejudicar gravemente as atividades empresariais, afetando a satisfação do cliente e a rentabilidade da empresa. Sobre tudo, é uma necessidade, atuar em conformidade com novos regulamentos e leis criados para proteger a privacidade dos consumidores e as informações electrónicas.

4.1.1 WORMS E VÍRUS

Os worms e os vírus informáticos ainda são as ameaças de segurança mais comuns, 75% das pequenas e médias empresas foram afetadas por pelo menos um vírus no último ano.

Os worms e vírus podem ter um efeito devastador na continuidade e rentabilidade da atividade empresarial. Estão cada vez mais inteligentes e destrutivos, pois tem o poder de infectar varias redes em segundos.

Enquanto as empresas se debatem por atualizar os seus computadores com patches de sistema operacional e programas de software antivírus, novos vírus podem furar estas defesas a qualquer momento. Por outro lado, os empregados disseminam vírus e spyware quando transferem material inseguro ou abrem anexos de correio electrónico. Esses ataques podem provocar significativas perdas financeiras. Os sistemas de segurança têm de detectar e afastar worms, vírus e spyware em todos os pontos da rede.

4.1.2 DISPONIBILIDADE DOS SERVIÇOS

Os worms e vírus não são as únicas ameaças para as empresas. Ataques do tipo, negação de serviço, (denial-of-service) podem encerrar websites e operações de comércio electrónico, fazendo com que estes falhem ou não consigam processar tráfego devido. Novamente, os resultados serão desastrosos: perda de dados e encomendas, e pedidos de clientes sem resposta. A imagem das empresas é comprometida após estes ataques serem tornados públicos, a credibilidade é posta em duvida e a empresa acaba prejudicada.

4.1.3 ROUBO DE INFORMAÇÕES

O roubo de informações é lucrativo. Piratas da informática penetram em redes empresariais para roubar números de cartões de crédito, de segurança social para proveito próprio. As pequenas e médias empresas são encaradas como um alvo mais fácil do que as grandes empresas. A proteção do perímetro da rede é um bom começo, mas não é suficiente, pois muitos roubos de informação são auxiliados por uma pessoa infiltrada de confiança.

4.1.4 O NOVO, A SURPRESA, O DESCONHECIDO.

A par de cada avanço na área da informática e das comunicações surgem novas formas de explorar essa tecnologia para obter proveito próprio ou prejudicar terceiros. Essas oportunidades são potencializadas pelo lançamento de novo hardware ou software. Com a ausência da capacidade preventiva, desconhecendo o que virá a seguir, a melhor defesa é aquela que se consiga adaptar facilmente a futuras ameaças e que seja financeiramente acessível.

4.2 CONTROLE DE FRAGILIDADES

Vários nomes assustadores são comuns aos administradores de redes e sistemas: os *crackers* (invasores, ou ainda erradamente propagado pela mídia, *hackers)*.

Como obter um ambiente de rede mais confiável e seguro, diante destas ameaças? Reconhecendo a importância e a necessidade de um bom trabalho de administração de redes e sistemas e lançando mão de todos os programas de apoio à segurança. Entretanto para obter mais controle, alguns administradores, utiliza-se em paralelo ao uso das ferramentas de segurança, algumas premissas e estabelecem objetivos.

O primeiro passo é oferecer apenas os serviços necessários. Retirar tudo que não está sendo usado. Tentar limitar o número de opções e facilidades disponíveis. Esses procedimentos implicam em mais da metade do caminho para se conseguir pleitear um ambiente mais seguro.

Todo esse recurso deve ser empregado somente em sistemas não comprometidos. Não adianta instalar tais ferramentas em uma máquina que acabou de ser invadida, sem que se tenha uma ideia precisa do estado do sistema, tudo isso, pode atrapalhar muito mais que ajudar.

É bem importante também que os hardwares e os componentes do sistema estejam funcionando de forma correta. Sendo assim, *patches* devem ter sido aplicados.

Vale ressaltar, que a utilização dessas ferramentas é somente uma parte do bem maior, que consiste em definir e adotar de normas e política de segurança para a organização.

4.2.1 TIPOS DE FERRAMENTAS

As ferramentas de segurança podem ser inicialmente classificadas em:

Ferramentas de segurança de *hosts*, voltadas para análise, correção, implementação de novos controles, em sistemas computacionais, e ferramentas de segurança de rede, direcionadas para a verificação e implementação de controles sobre o tráfego de uma rede, como os filtros de pacotes.

Outra categorização é referente à função:

Verificação da integridade e vulnerabilidade: programas que analisam ou controlam a situação de sistemas, relacionando os serviços disponíveis, mudanças em programas, etc.

Autenticação: ferramentas relacionadas à identificação de usuários em um sistema (senhas de acesso).

Privilégios: mais relacionadas com um ambiente de operação, restringindo os privilégios de usuários ao mínimo necessário para a execução das tarefas.

Criação de programas seguros: bibliotecas com novas funções para a elaboração de programas "resistentes" às técnicas mais comuns para quebra de segurança.

5

5.1 POLITICAS DE SEGURANÇA

A Política de Segurança da Informação é um documento que registra os princípios e as diretrizes de segurança adotado pela organização, a serem observados por todos os seus integrantes e colaboradores e aplicados a todos os sistemas de informação e processos corporativos. (FABRÍCIO BASTO, 2011).

A política de segurança do ponto de vista dos administradores de sistemas deve ser vista como a política de segurança, utilizada por uma nação para receber estrangeiros (ZWICKY, 2000).

De acordo com (Ribeiro, 1998), o objetivo da política de segurança resume-se em manter sob controle o armazenamento da informação, que muitas vezes, é o bem mais valioso de uma empresa devendo seguir estes quatro paradigmas básicos:

- Integridade: A condição na qual a informação ou recursos da informação é protegido contra modificações não autorizadas.

- Confidencialidade: Propriedade de certas informações que não podem disponibilizadas ou divulgadas sem autorização prévia do seu dono.
- Disponibilidade: possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas qualidades.
- Legalidade: Estado legal da informação, em conformidade com os preceitos da legislação em vigor, no que se refere à aplicação de medidas punitivas.

Por outro lado (Zwicky, 2000) considera quatro questões para a formulação da política de segurança:

- Capacidade financeira: Quanto Custa a segurança?
- Funcionalidade: Pode-se utilizar o sistema de forma plena?
- Compatibilidade cultural: A política de segurança proposta está em conflito como a forma que as pessoas normalmente interagem com os que estão do lado de fora da empresa?
- Legalidade: A política de segurança está de acordo com os requerimentos legais exigidos?

Para (Ranieri Marinho, 2009), as principais ameaças que devem ser tratadas na política de segurança são:

- Integridade: Ameaças de ambiente (fogo, enchente e tempestades, etc), erros humanos, fraudes e erros de processamento.
- Indisponibilidade: Falhas em sistemas ou nos diversos ambientes computacionais.
- Divulgação da Informação: Divulgação da informação premeditada e da informação acidental.
- Alterações não-Autorizadas: Alteração premeditada e acidental.

5.1.1 SOBRE O DOCUMENTO DA POLÍTICA DE SEGURANÇA

Para (ZWICKY , 2000), um documento de política de segurança é uma forma de comunicação entre administradores e usuários.

Ressalta (MARCELO LOPES, 2007), é importante que o documento seja explicito e compreensível sobre todas as decisões que serão tomadas. A maioria das pessoas não irá seguir as regras a não ser que compreenda a sua importância.

Um documento de política de segurança esclarece expectativas e responsabilidade entre os usuários e administradores, permite a todos saberem o que esperar de cada um. (LOPES, 2007)

Na opinião de (BASTO, 2011) para a política de segurança ter aceitação, é preciso que a cúpula estratégica (dirigentes) apoie e participem do processo de implantação. É de suma importância o aval da diretoria para que todos aceitem, respeitem as normas e procedimentos vinculados na política de segurança.

Para (LOPES, 2007), escrever o documento de política de segurança não é tão importante quanto segui-lo. Significa que quando a política não é seguida, algo deve acontecer para consertar a situação e alguém precisa ser responsável por fazer as correções.

Alguns exemplos do que deve especificar a política de segurança:

- Gerentes de certas áreas têm autoridade de revogar acesso a um usuário;
- Gerentes são responsáveis por efetuar correções em casos de transgressão;
- Penalidades que estão reservas aos transgressores.

Nenhuma política de segurança é perfeita. Entretanto, podem-se especificar as possíveis providencias e as penalidades em casos que não constem no documento, sempre sujeito a revisões e reavaliações futuras.

Tudo na informática muda muito mais rápido do que em qualquer área, desde o hardware até a área de atuação de mercado da empresa. Isto implica na necessidade de revisões constantes no documento de política de segurança.

6 COMO OCORRE O PROCESSO DE EDUCAR

De acordo com W. Victor Maconachy, Core D. Schou, Daniel Ragsdale e Don Welch, que apresentaram em um Workshop da IEEE em Segurança da Informação, o processo de aprendizagem é como um continuum que começa com a conscientização, passando pela "alfabetização", treinamento e finalizando com a educação.

6.1 CONSCIENTIZAÇÃO

A primeira etapa para obter ambientes com mais segurança é conscientizar os funcionários acerca deste problema. Outra meta a ser alcançada diz respeito à maneira que o usuário enxerga o seu comportamento com relação à segurança da informação da empresa em que trabalha.

O Auditor de Sistemas Fernando Nicolau Freitas Ferreira (CISM–Certified Information Security Manager pelo ISACA) afirma que: "... a garantia de que uma organização possui um grau de segurança razoável está diretamente ligado ao nível de conscientização de seus colaboradores".

A conscientização dos novos e antigos colaboradores de uma determinada empresa pode ser alcançada com uso de vários recursos: boletins informativos, campanhas, provas periódicas ou entrevistas para avaliar conhecimentos adquiridos.

Em 2001 a NASA começou a criar um programa de treinamento em segurança em TI para capacitar todos os seus funcionários. Para Scott Santiago, responsável pela proteção dos sistemas de informação da agência americana, *"mudar a mentalidade das pessoas que trabalham na organização será a melhor solução para garantir a segurança do órgão"*.

Vale ressaltar que funcionários treinados e conscientes aumentam consideravelmente o grau de conhecimento, aumentando com ele a capacidade de resistência de se cair em armadilhas.

6.2 ALFABETIZAÇÃO

Na segunda etapa, é necessário saber como tratar dele ou como operar os diversos equipamentos e softwares. Para se navegar na internet como também para lhe dar com documentos e dados aos quais se tem acesso no mundo empresarial é preciso ter um mínimo de informação de segurança.

É necessário então este processo de se alfabetizar os funcionários com relação aos perigos, ameaças e vulnerabilidades aos quais eles estão sujeitos. Diante dos conceitos básicos, o funcionário adquirirá familiaridade com o meio digital.

Ao se falar em conhecimentos elementares, dois conceitos costumam ser aplicados:

Conhecimentos "simples": devem ser passados para os usuários numa linguagem compreensível a todos. Como funciona a internet, o correio eletrônico, a criptografia etc.

Conhecimentos "de base": são aqueles que os administradores e desenvolvedores de sistemas deveriam conhecer para poder melhor desenvolver, operar e configurar os diversos dispositivos de segurança que lhe são confiados.

6.3 TREINAMENTO

A terceira etapa é o treinamento que visa aprimorar, e realizar com mais eficiência algo que já se sabe. Define Marcus Vinicius Pereira, “treinamento é uma atividade educacional focada na melhoria do desempenho, de forma a fazer melhor uma determinada tarefa”

Treinamento, voltando a citar o artigo de Marcus Vinicius,

“(...)É sempre focado na pratica e isso parece não estar claro para as empresas quando contratam ou programam essa atividade... No Brasil, o índice de horas de treinamento por pessoa ao ano, apesar de apresentar-se em ascensão, ainda representa apenas 40% do tempo utilizado nos países desenvolvidos”(MARCUS VINICIUS, 2003).

O treinamento é focado na pratica e tem como objetivo ensinar não apenas como fazer, mas também como fazer da melhor forma. Com ele espera-se obter um melhor desempenho que pode ser medido para saber se o treinamento foi eficaz ou não.

6.4 EDUCAÇÃO

Se a tecnologia e os conhecimentos fossem estáticos poderíamos parar na terceira etapa, porém ambos evoluem, entretanto, os perigos e ameaças também evoluem de forma incrivelmente rápida.

A quarta etapa torna-se necessária quando os treinamentos começam a ficar obsoletos. A questão não é saber apenas como fazer, mas entender como acontece para nos prevenir quando acontecer de forma ligeiramente diversa. Os treinamentos deixam nossa

resposta automática, porem somos mais que autômatos. Retornos Pavlovianos tem os animais. Por isso é que se treina cachorros, e as pessoas se educam.

Ao finalizar o processo de aprendizagem deve se obter como resultado pessoas educadas na Segurança da Informação.

7 CONSIDERAÇÕES FINAIS

Uma vez que estabelecidos os procedimentos, tendo os funcionários já conscientizados, treinados e educados, as falhas que cometerem de forma consciente devem ser punidas como danosas ao patrimônio da empresa e servirem de exemplo.

Para os americanos, quando o conhecimento e a orientação são passados e o comportamento dos funcionários contraria ambos, resta a penas a plicar a punição. A empresa tem que confiar em seus funcionários. Se não confiam que eles vão fazer o que se espera deles e para que eles foram contratados, está na hora de trocar de colaboradores.

Alguns exemplos de comportamento que deveriam ser punidos incluem:

- Uso de e-mail para pornografia;
- Liberação de acesso para outros;
- Fornecimento de senhas particular aos colegas;
- Instalação de softwares não permitidos;
- Burlas nos mecanismos de segurança.

É importante observar que somente a tecnologia não pode evitar quebras de segurança e se tudo já foi feito na área da educação, algo de forma complementar deve ser feito, seja através de uma punição, ou obtendo a colaboração dos que erraram com o objetivo de fortalecer os mecanismos de segurança já existentes.

8 REFERÊNCIAS BIBLIOGRÁFICAS

ARBULU, Rafael. **Fraudes bancárias: a culpa é sua ou do banco?** Disponível em: http://olhardigital.uol.com.br/negocios/seguranca/noticias/brasil-o-terceiro-maior-pais-em-fraudes-bancarias Acesso em: 26 jan. 2012.

CARVALHO, Sandra. **Laptop e HD externo com dados de pesquisas da Petrobras foram roubados durante transporte.** Disponível em: http://info.abril.com.br/aberto/infonews/022008/14022008-11.shl Acesso em: 16 jan. 2012.

G1, **Empresa responsabiliza capitão pelo naufrágio do cruzeiro na costa italiana.** Disponível em: http://www.wscom.com.br/noticia/internacional/NAUFRAGIO+EMPRESA+CONFIRMA+FALHA+HUMANA-119273 Acesso em: 26 jan. 2012.

GOODCHILD, Joan. **Engenharia social: pessoas ainda são elo mais fraco, diz especialista.** Disponível em: http://idgnow.uol.com.br/seguranca/2010/05/25/engenharia-social-pessoas-ainda-sao-elo-mais-fraco-diz-especialista/ Acesso em: 20 jan. 2012.

IMPROTA , Luiz Eduardo. **Os ataques a sites do governo… Calma não foi tão feio assim!** Disponível em: http://www.tiespecialistas.com.br/2011/06/os-ataques-a-sites-do-governo-porque-devemos-nos-preocupar/ Acesso em: 18 jan. 2012.

SYMANTEC. Pesquisa Symantec 2010 sobre Proteção das Informações nas Pequenas e Médias Empresas. Disponível em: http://www.symantec.com/pt/br/theme.jsp?themeid=smb_survey Acesso em: 12 jan. 2012.

_____, **Apenas 40% dos funcionários respeitam segurança de TI onde trabalham.** Disponível em: http://www.tiinside.com.br/07/12/2011/apenas-40-dos-funcionarios-respeitam-seguranca-de-ti-onde-trabalham/sg/253020/news.aspx Acesso em: 18 jan. 2012.

_____, **Falha humana é a principal causa de acidentes na construção civil.** Disponível em: http://www.sinduscon-joinville.org.br/noticias/falha-humana-e-a-principal-causa-de-acidentes-na-construcao-civil.html Acesso em: 22 jan. 2012.

_____, **Os riscos na Indústria de Petróleo e Gás.** Disponível em: http://blog.nei.com.br/index.php/2011/08/04/os-riscos-na-industria-de-petroleo-e-gas/ Acesso em: 26 jan. 2012.

BASTO, Fabrício. **Política de Segurança da Informação – Como fazer?** Disponível em: http://analistati.com/politica-de-seguranca-da-informacao-como-fazer/ Acesso em: 18 abr. 2012.

SCHNEIER, Bruce. **Segredos e mentiras sobre a proteção na vida digital**. Rio de Janeiro: Campus, 2001

SOARES, Luiz Fernando Gomes. **Redes de Computadores - das LANS, MANS e WANS às redes**. Rio de Janeiro: Campus, 1995.

_____, **Sobre As Falhas Humanas.** Disponível em: http://www.blogecooil.com/2011/05/analise-das-informacoes-parte-3.html Acesso em: 16 jan. 2012.