Fonte

ISSN 1808-0715

Tecnologia da Informação na Gestão Pública

Ano 4 - Número 07 Julho / Dezembro de 2007

www.prodemge.gov.br

Segurança da Informação

Tecnologia e comportamento na prevenção e combate aos crimes virtuais

prodemge

UNIVERSIDADE CORPORATIVA PRODEMGE

Certificação Digital Certisign

Autenticidade e confiabilidade das informações nas suas mãos

Certisign:
uma das 5 empresas de segurança digital mais confiáveis do Brasil segundo Pesquisa da INFO*
* Revista INFO, ed. 254, maio/2007

Única Autoridade Certificadora credenciada a operar em múltiplas hierarquias, a CERTISIGN é uma empresa 100% especializada em Certificação Digital.

Nosso portfolio de produtos e serviços utiliza a tecnologia de Certificação Digital e proporciona aos nossos clientes um AMBIENTE DIGITAL MAIS SEGURO.

Proteja informações, "desmaterialize" e simplifique seus processos. REDUZA O RISCO DE FRAUDES em sua empresa.

Consulte-nos para DESENVOLVER, IMPLANTAR E GERENCIAR projetos de Certificação Digital.

GARANTA AUTENTICIDADE E CONFIABILIDADE para suas informações onde quer que você esteja.

MKT Certisign – 057/07

Conheça mais sobre nossos produtos e serviços em certisign.com.br

CERTISIGN
A sua identidade na rede

Editorial

Nesta edição, a revista **Fonte** traz aos seus leitores um tema que, de forma crescente, vem ocupando a pauta de executivos e usuários das tecnologias da informação e comunicação (TICs) em todo o mundo: a segurança da informação. A preocupação também atinge os usuários domésticos, que, a cada dia, se deparam com novos golpes que ameaçam suas informações e privacidade e, em casos extremos, sua integridade física.

O desenvolvimento das TICs trouxe, em sua trajetória, benefícios inquestionáveis para o desenvolvimento de toda a sociedade, democratizando serviços e informações, facilitando a vida dos cidadãos, provendo os administradores de recursos para executar de forma mais eficaz seus projetos e concretizar estratégias.

No entanto, e infelizmente, essa evolução, com seu caráter essencialmente democrático, também é acessível a pessoas ou organizações que agem de forma inescrupulosa e reproduzem, no mundo virtual, um ambiente de risco e contravenção. Na maioria das vezes motivados por objetivos financeiros e pelo desafio de burlar sistemas de segurança, os chamados hackers inovam de forma permanente, utilizando recursos tecnológicos e eventualmente prescindindo deles, amparados pela engenharia social para executar seus projetos criminosos.

Os reflexos do risco que representam para a sociedade são percebidos na crescente necessidade de investimentos das organizações em ferramentas de segurança, na reengenharia de processos e na capacitação de colaboradores; no impacto sobre os negócios e transações realizadas pela internet; em prejuízos às empresas, especialmente dos setores financeiro e de e-commerce; e, de forma geral, na ameaça à privacidade.

O debate que a revista **Fonte** promove, nesta sua sétima edição, procura tornar mais transparente para os leitores os riscos e ameaças que caracterizam a comunicação em rede, oferecendo insumos para que organizações públicas e privadas e usuários domésticos possam se prevenir, conhecendo formas de identificar vulnerabilidades e as soluções que o mercado desenvolve para fazer frente a essa realidade.

Para isso, foram ouvidos especialistas nas mais diversas áreas ligadas à segurança da informação, resultando na apresentação de um panorama dos problemas e das soluções que envolvem a questão. Entre os colaboradores desta edição está o consultor americano Kevin Mitnick, que se tornou famoso como o maior hacker da história da internet. Com a experiência de quem esteve do lado oposto da lei, mostra como agem os contraventores na rede. A advogada Patrícia Peck, especialista em direito digital, dá sua contribuição na seção Diálogo, analisando as mudanças culturais impostas pelas tecnologias e seus reflexos na legislação. O advogado Alexandre Atheniese aborda a questão das relações trabalhistas e privacidade, e os analistas da Prodemge, Paulo César Lopes e Mário Velloso, fazem um alerta sobre cuidados que os pais podem adotar com relação a seus filhos, na internet. Professores, empresários, pesquisadores e especialistas apresentam estudos, tendências e experiências práticas, como os programas de segurança da Cemig, em Minas Gerais, e da Receita Federal.

A Prodemge espera contribuir para a ampliação do debate sobre as questões relativas ao valor da informação nas organizações e entre os usuários domésticos, sinalizando riscos e vulnerabilidades e indicando soluções. Com a experiência de 40 anos gerenciando as informações do Estado de Minas Gerais, a Prodemge valoriza conceitos como integridade, disponibilidade e sigilo. Essa mesma experiência, numa trajetória paralela à história da informática, dá à Companhia o conhecimento dos riscos e das tecnologias disponíveis para prevenção e combate ao problema, que se pretende compartilhar com os leitores da revista **Fonte**.

Diretoria da Prodemge

Sumário

Fonte
Ano 04 - Julho/Dezembro de 2007
prodemge
Tecnologia de Minas Gerais

Uma publicação da:

prodemge
Companhia de Tecnologia da Informação do Estado de Minas Gerais

Ano 4 - nº 07 - Julho/Dezembro de 2007

Filiada à Aberje

Prodemge - Rua da Bahia, 2.277 - Bairro Lourdes
CEP 30160-012 - Belo Horizonte - MG - Brasil
www.prodemge.gov.br
prodemge@prodemge.gov.br

Inter@ção

A revista **Fonte** agradece as mensagens enviadas à redação, entre as quais algumas foram selecionadas para publicação neste espaço destinado a acolher as opiniões e sugestões dos leitores. Continuem participando: o retorno é fundamental para que a revista evolua a cada edição.

e-mail: revistafonte@prodemge.gov.br

Revista **Fonte** - Companhia de Tecnologia da Informação do Estado de Minas Gerais
Rua da Bahia, 2.277, Lourdes,
Belo Horizonte, MG - CEP: 30160-012

OPINIÕES DOS LEITORES

Recebemos os exemplares da nova edição da revista **Fonte**. Tenho a impressão de que a presença da RNP nessa edição vai ser marcante na história de nossa comunicação. Foi a informação certa, no momento certo, no veículo certo. Houve uma feliz sincronia entre o que estamos realizando – implementação da rede nacional de alto desempenho e extensão dessa infra-estrutura até a última milha para conexão de instituições de ensino superior e pesquisa em todo o País – e a excelente visão geral que essa edição da **Fonte** construiu acerca do cenário de redes de comunicação, no Brasil e no mundo. Parabéns pelo trabalho.

Marcus Vinicius Rodrigues Mannarino
RNP – Gerente de Comunicação e Marketing

AGRADECIMENTOS

Primeiramente, gostaria de agradecer à equipe da revista **Fonte**, por eu ter recebido, no ano que passou, todos os exemplares. Sou consultor de TI – Software, nesta capital, e me surpreendo a cada exemplar publicado por este veículo de comunicação, no qual a Prodemge retrata os temas abordados com muita clareza. Parabéns mais uma vez aos colaboradores desta publicação tão elementar em nosso dia-a-dia, contribuindo para o acesso às informações que merecem destaque em TI. Aproveitando, gostaria de reiterar o meu interesse em assinar a revista **Fonte** neste ano que se inicia, com o firme objetivo de estudos e atualização diária em meu ambiente de trabalho.

Cristiano A. Firmino
Belo Horizonte/MG

SOLICITAÇÕES DE ASSINATURA

Nosso departamento, na prefeitura de Pará de Minas, é o responsável direto e está completamente envolvido com as redes de comunicação locais e wireless. Conversando com um dos nossos fornecedores sobre as opções que temos à disposição para integração dos pontos remotos mais distantes, normalmente localizados em áreas rurais e sem visada com as antenas, recebemos dele uma revista trazendo uma matéria sobre o Wimax. Essa revista foi a **Fonte**, ano 4, número 6, da qual extraímos muita informação e que nos agradou bastante pelo conteúdo claro e abrangente. Gostaríamos de ser incluídos na sua lista de assinantes.

Francisco V. Severino Sobrinho
Departamento de Processamento de Dados
Prefeitura Municipal de Pará de Minas/MG

Sou formando do curso de Ciência da Computação da Universidade Federal de Viçosa. Estou fundando uma empresa para consultoria em automação comercial e gestão de informações. Gostaria muito de assinar a revista pois os conteúdos sempre atualizados e bem formulados seriam de grande ajuda para aplicação na minha empresa, além de poder disponibilizá-la para meus clientes e parceiros.

Fabrício Passos
Viçosa/MG

Sou jornalista e trabalho na Secretaria Municipal de Meio Ambiente da Prefeitura de Montes Claros. Fazemos parte da Rede Brasileira de Fundos Socioambientais Públicos do Brasil, criada em junho de 2006. Gostaria de receber exemplares da revista **Fonte**. Esse material poderá contribuir para o fortalecimento do Fundo Único de Meio Ambiente, que faz parte da Rede citada acima. www.montesclaros.mg.gov.br/semma.

Andréa Fróes
Projetos e Captação de Recursos / Fundo Único de Meio Ambiente (FAMA)
Secretaria Municipal de Meio Ambiente
Montes Claros/MG

Estou lendo a revista **Fonte** pela primeira vez e adorando o conteúdo dela, bem atual e falando de tecnologias que ainda não são bem conhecidas no mercado de informática. Por isso, gostaria de receber as próximas edições da revista.

Renato Carvalho
Salvador/BA

Consegui, por um amigo, algumas edições da revisa **Fonte** e achei bastante interessante. Meu nome é João Pedro e sou acadêmico do curso Sistemas de Informação na Universidade dos Vales do Jequitinhonha e Mucuri – Diamantina (UFVJM) e tenho certeza de que a revista **Fonte** vai auxiliar muito na minha formação profissional. Gostaria de saber o que faço para adquirir a revista.

João Pedro Campos Ferreira
Diamantina/MG

Bom dia, meu nome é Fabiano, sou estudante na área de informática e trabalho em uma empresa que presta serviços de implantação de tecnologias e serviços na área de informática. Tive conhecimento da revista **Fonte** através de um amigo e achei-a muito interessante, pois fornece informações inovadoras e novas fontes de pesquisas. Em mãos, tenho apenas a edição número 6. Gostaria de ter as anteriores e a seqüência dela em diante.

Fabiano G. S. P.
Santos/SP

Tive acesso ao exemplar número 4, gostei do nível dos artigos, e gostaria de ser assinante da revista, para poder ter acesso a ela e a seus artigos que muito me interessam. Gostaria de saber o custo da assinatura. Sou aluno do 4º período de Sistema de Informação.

Leonardo Leite Torres
Porto Velho/RO

A nossa instituição tem interesse em receber a revista **Fonte** – tecnologia da informação na gestão pública, que foi solicitada para esta biblioteca pelo coordenador-adjunto do curso de Sistemas de Informação, professor Álisson Rabelo Arantes, por entendê-la de grande relevância para os acadêmicos do referido curso.

Maria Irene de Oliveira Faria
Sociedade Mineira de Cultura
Arcos/MG

O interessado em assinar a revista **Fonte** deve enviar seu nome e endereço completo para o e-mail revistafonte@prodemge.gov.br, informando, quando for o caso, a empresa ou instituição a que é vinculado. As revistas seguirão via Correios, de acordo com a disponibilidade de exemplares.

Diálogo

Sociedade digital:

cenário virtual impõe mudanças culturais e ordenamento jurídico globalizado

Divulgação

Patricia Peck Pinheiro, advogada especialista em Direito Digital, sócia do escritório PPP Advogados, formada pela Universidade de São Paulo, com especialização em Negócios pela Harvard Business School e MBA em Marketing pela Madia Marketing School. É escritora, tendo publicado o livro *Direito Digital* pela Editora Saraiva, além de participação nos livros *e-Dicas* e *Internet Legal*. É professora da pós-graduação da FAAP, Impacta, Fatec, IBTA e colunista do IDG Now e articulista da Gazeta Mercantil, Valor Econômico, Revista Executivos Financeiros, Info Exame, Info Corporate, About, Revista do Anunciante, entre outros. Iniciou sua carreira como programadora de games aos 13 anos. Já atuou em diversas empresas e possui experiência internacional com Direito e Tecnologia nos Estados Unidos, Portugal e Coréia. Atualmente assessora 127 clientes no Brasil e no exterior, já tendo treinado mais de 10.500 profissionais de diversas empresas nos temas de Gestão de Risco Eletrônico e Segurança da Informação.

A existência de um mundo virtual, criado à imagem e semelhança do mundo real, tem exigido adequações dos diversos setores da sociedade, a fim de manter, nessa nova dimensão, parâmetros comportamentais que garantam uma convivência social no mínimo ética. Nesta edição de **Fonte**, o Diálogo é com a advogada especialista em direito digital, Patrícia Peck Pinheiro, que apresenta um panorama do Direito e das relações sociais nesse contexto.

Nesta entrevista, ela fala da evolução do Direito, em função das transformações sociais, e da forma como as lacunas abertas por novos comportamentos são preenchidas por leis e

regulamentações. A advogada revela o grande desafio do Direito diante da evolução das tecnologias, enfatizando a educação e as mudanças culturais como as grandes perspectivas para a harmonia nos ambientes virtuais.

Patrícia Peck aborda ainda aspectos do exercício da cidadania na rede, da privacidade e anonimato na sociedade digital, da prática de monitoramento nas comunicações em ambientes corporativos e comenta as propostas de instalação de controles de acesso à internet. Entre outros vários temas, a especialista traça ainda um paralelo entre as necessidades de exigências legais nos dois mundos, fala dos crimes na internet e dá dicas para que os usuários possam se prevenir e se defender em casos de incidentes.

FONTE: *O Direito tem acompanhado as rápidas transformações sociais provocadas pela evolução da tecnologia e suas conseqüências positivas e negativas na vida das pessoas? Com que velocidade a legislação tem se adequado às novas exigências?*

O Direito muda conforme a sociedade evolui, então é natural, sim, que o Direito acompanhe as novas questões trazidas pela tecnologia, mas o tempo desta adaptação não é rápido. Em termos de leis, as normas atuais já alcançam e tratam bem várias questões relacionadas com a internet e com as ferramentas tecnológicas, mas há leis que precisam ser criadas, para preencher lacunas naturais, já que há novos comportamentos e riscos. Mas esse processo legislativo leva alguns anos, já há projetos de lei, mas o trâmite deles é de, aproximadamente, uns 10 anos.

FONTE: *Sob esse ponto de vista, quais são as experiências recentes mais relevantes no País? Há experiências adotadas em outros países que podem ser consideradas bem-sucedidas?*

As experiências recentes estão alinhadas com o princípio de auto-regulamentação muito forte no Direito Digital, onde as regras são estabelecidas pelos próprios agentes sociais, tais como provedores de internet, provedores de e-mail, internautas. Isso tem ocorrido por meio de Termos de Uso, Políticas Eletrônicas, inserção de cláusulas específicas em contratos. Este tempo é mais rápido e atende à demanda a curto prazo de adequação do Direito às novas exigências da sociedade, enquanto, em paralelo, são elaboradas novas leis. Já foi atualizado o Código Penal em 2002 e 2005 e já foram acrescidos novos tipos penais, especialmente no tocante a crimes eletrônicos no ambiente da Administração Pública. Tem sido assim em outros países, a atualização do próprio Código Penal.

FONTE: *Você acredita que todo o arcabouço legal existente no Brasil pode acobertar e tipificar todos os crimes virtuais? Se não, quais seriam as leis que faltam?*

O arcabouço legal atual está bem adequado. O problema tem sido mais de prova de autoria do que de tipificação de condutas. Ou seja, a questão passa pelo anonimato e a falta de guarda de provas em terceiros, como provedores, para permitir a identificação adequada do infrator e a sua punição. Falta uma lei que defina um prazo mínimo de guarda e o que tem de ser guardado sobre o acesso à internet e aos serviços eletrônicos, para que seja possível a investigação. Na Europa, já há medidas nesse sentido, determinando guarda por até dois anos de logs e dados de IP. No Brasil, uma iniciativa positiva já em vigor é a lei paulista sobre lan house e cybercafés, que exige identificação do usuário e guarda de dados. Há lei sobre cybercafés e lan house em vários Estados (São Paulo, Bahia, Minas Gerais); a lei de Minas não trata da obrigatoriedade de se fazer cadastro do usuário como forma de preservar os dados de autoria para uma eventual investigação. A lei de São Paulo já trata disso, e exige a guarda dos dados inclusive por cinco anos.

FONTE: *A internet apresenta-se, muitas vezes, como um meio sem regras e sem dono, onde os usuários sentem-se livres para fazer o que quiser. Quais os*

principais desafios que o Direito enfrenta ao lidar com esse mundo virtual?

O principal desafio do Direito começa na educação das pessoas. Independente das leis, há princípios de ética e valores que precisam ser ensinados às novas gerações da era digital. Além disso, é preciso orientar sobre as próprias leis que existem e são válidas e que estão sendo descumpridas. A constituição federal protege o direito à imagem, mas, mesmo assim, muitas pessoas fazem uso da imagem de outras sem autorização. Assim como protege a honra, e há cada vez mais ofensas digitais. Já é proibida a pirataria, assim como o plágio, mas muitas pessoas não acham que estão fazendo algo errado quando dão CTRL+C, CTRL+V e copiam o conteúdo alheio. A educação no uso ético, legal e seguro da tecnologia é o maior desafio do Direito, mais que criar outras leis.

FONTE: *No "mundo real", onde há leis consolidadas, estamos assistindo a prevalência da impunidade em inúmeros casos. O que os cidadãos podem esperar da resposta jurídica em ambientes digitais?*

> "A educação no uso ético, legal e seguro da tecnologia é o maior desafio do Direito, mais que criar outras leis".

É fundamental denunciar, por ser um exercício de cidadania. Por mais que em alguns casos não haja forma de punir o infrator, uma hora isso ocorre, e é o conjunto de denúncias que permite reunir provas. Isso serve tanto para um problema em uma loja virtual ou em uma comunidade do Orkut, como uma situação de fraude de cartão de crédito ou no internet banking. O cidadão deve cumprir com a parte dele, que é reunir informações e denunciar. É assim que conseguimos fazer a justiça andar e criar estatísticas que permitem alocação de investimentos e treinamentos.

FONTE: *Em recente artigo publicado na Folha de São Paulo, "Uma questão de privacidade", José Murilo Junior, do Global Voices Online, afirma: "Deve caber ao usuário definir os diferentes níveis de acesso às suas informações, e cabe aos serviços evoluir para prover essa funcionalidade de forma transparente". Na sua opinião, qual seria o papel do Estado para prover e exigir da sociedade que tais funcionalidades sejam disponibilizadas para os cidadãos?*

A questão da privacidade na sociedade digital envolve, sim, a participação conjunta de usuários e empresas para uso de bancos de dados. Em termos de leis, já temos a proteção da Constituição Federal e do Código de Defesa do Consumidor, onde fica claro que cabe às partes regular a questão em contrato. O que não pode haver é o usuário querer usufruir de serviços gratuitos, em que a empresa deixa claro no termo de uso que os dados desse usuário são objeto da contratação gratuita e, depois, este não querer que seus dados sejam usados. Na era da informação, os dados tornaram-se a moeda e muitos serviços que se dizem gratuitos, na verdade cobram pelos dados do usuário, esta é a troca. É importante estar transparente esta questão e haver funcionalidades que permitam atender à lei já existente para retificação de uma informação, para saber que informação a empresa possui do usuário, para pedir a retirada de um conteúdo que fira direito de imagem, direito autoral ou reputação, entre outros. Podemos, sim, programar o Direito nas interfaces gráficas e usar a tecnologia para fazer valer o cumprimento das leis, já que as testemunhas são as máquinas.

FONTE: *Quais os limites legais do governo eletrônico?*

No tocante ao Estado, cabe a este fazer o que estiver delimitado em lei. Sendo assim, o governo eletrônico é tratado em uma série de normativas que determinam sua capacidade de agir, diretrizes, entre outros. É uma tendência internacional que o Estado atenda e sirva o seu povo, os cidadãos, por meio de serviços de e-gov.

FONTE: *Quais as peculiaridades de tratamento das informações e sua guarda por parte de empresas públicas?*

As instituições da Administração Pública devem guardar os dados dos cidadãos com zelo, para garantir

o sigilo. E o Estado possui responsabilidade objetiva, ou seja, vai responder por danos causados, mesmo independente de culpa.

FONTE: *No caso de redes wireless estruturadas e disponibilizadas pela administração pública, como fazer o gerenciamento e controle de acessos?*

É fundamental que haja sempre uma autenticação de usuário, com dados completos, em virtude da questão atual da autoria em ambientes eletrônicos, onde essas informações são necessárias, se for preciso investigar um incidente. Sendo assim, mesmo em ambientes de inclusão digital, cabe a elaboração do termo de uso do serviço, mesmo que gratuito, determinando claramente os direitos e as obrigações dos usuários e a solicitação de dados detalhados de identidade. A não-coleta desses dados, a não-guarda, a não-autenticação contribuem para o anonimato e mesmo para práticas ilícitas.

FONTE: *Uma polêmica recente é a da realização de audiências remotas (videoconferência), para minimizar custos e dar maior dinamismo ao poder judiciário. Alguns juristas afirmam que a presença do detento na audiência é indispensável. Qual a sua opinião sobre o assunto?*

Minha opinião é a de que deve haver sim videoconferência, com a presença do advogado no mesmo recinto do preso. Isto não apenas gera economia, como reduz riscos de fuga. Ou seja, o ganho social coletivo justifica sim a aplicação desse recurso, e não há uma perda individual para o preso que justifique sua não-aplicação.

FONTE: *Quando se pensa em internet, pensa-se em relações internacionais, especialmente nos aspectos legais e jurídicos, já que cada país possui sua constituição e suas leis. Na internet realizam-se transações de compra e venda, trabalha-se num determinado país, para uma empresa que só tem sede em outro. Como tratar o Direito do Consumidor e o Direito Tributário? Como ficam os aspectos e questões que envolvem o Direito do Trabalho? E os Direitos Individuais?*

Realmente a sociedade digital cada vez mais pede por um ordenamento jurídico mais globalizado. No entanto, apesar de não haver barreiras físicas na web, o Direito é limitado ao seu país de origem e há regras de territorialidade para isso. Pode valer o local de domicílio do consumidor, da vítima de um crime, onde o crime ocorreu no todo ou em parte, ou onde é melhor a execução da ação para garantir eficácia de resultados. É difícil alinhar algumas questões até por diferenças culturais, do que é considerado certo ou errado em cada país, seu conjunto de valores. Mas há algumas questões que são comuns, recebem tratamento igual e podem estar alinhadas, como já tem sido feito há anos, por meio de tratados e convenções internacionais. A mais recente em discussão é a Convenção de Budapeste sobre crimes eletrônicos.

> “É uma tendência internacional que o Estado atenda e sirva o povo, os cidadãos, por meio de serviços de e-gov”.

FONTE: *Como a pessoa pode se proteger dos perigos do mundo virtual? Ao sentir-se prejudicada por alguma situação ocorrida na internet ou por meio dela, o que fazer?*

A melhor dica de proteção é não acreditar em tudo que vê na internet ou em e-mail. Na verdade, vale o mesmo princípio de proteção que usamos para o mundo real, ou seja, não deixar a porta de casa aberta, nem o computador aberto, não falar com estranhos, nem responder e-mails de estranhos, não passar informações pessoais ou de cartão de crédito ou banco por telefone sem ter certeza de quem está do outro lado da linha, e o mesmo na internet, do outro lado do site, do blog, do chat, da comunidade. Se a pessoa tiver um problema, deve entrar em contato com o provedor do serviço e, se necessário, com as autoridades por meio da Delegacia (se houve crime), do Juizado Especial Cível ou do Procon, em caso de problema de consumidor.

FONTE: *Qual a responsabilidade legal das empresas no tráfego de informações consideradas criminosas em suas redes corporativas, feitas por funcionários?*

A empresa responde legalmente pelo mau uso das suas ferramentas tecnológicas de trabalho que gere lesão a terceiros. Pelo crime em si, só responde quem o

cometeu (no caso, o funcionário), mas a responsabilidade civil pelo dano causado (moral ou material) pode caber à empresa, que depois tem o direito de regresso contra o funcionário, que foi o verdadeiro causador do dano.

FONTE: *É real a possibilidade de uma empresa monitorar os e-mails de seus funcionários. A questão da privacidade x segurança x direitos individuais é tema constante de discussão. Na sua opinião, como administrar interesses no contexto das organizações?*

Novamente, precisamos de educação, na verdade. Cabe à empresa deixar claro o limite de uso das ferramentas tecnológicas de trabalho e é dever da empresa monitorar para fazer valer suas normas internas, para fins de prevenção (evitar incidentes) ou para fins de reação (punir infratores). Sendo assim, se a empresa fizer o aviso legal de monitoramento claramente e previamente, pode monitorar os ambientes corporativos, o que inclui navegação na internet e uso de caixa postal de e-mail corporativa. Assim, já é comum a empresa inspecionar equipamentos móveis, como notebook, celular, pen drive, para evitar a pirataria, bem como vazamento de informação confidencial ou até mesmo contaminação por vírus. Mas tudo isso tem que estar claro em Políticas e Normas, documentado e, se possível, atualizado no Código de Conduta do Profissional ou em seu contrato de trabalho. Quanto melhor estiver a informação, menos riscos a empresa e o funcionário correm.

FONTE: *Várias empresas estão monitorando, além do e-mail, os acessos à internet, as ligações telefônicas e as atividades nas estações de trabalho. Algumas chegam a instalar monitoramento por circuito fechado de TV (CFTV) dentro das salas onde trabalham seus funcionários. Não estaríamos próximos do descrito em "1984"? Quais são os monitoramentos considerados legais? E quais são as exigências legais, para que se possam utilizar tais monitoramentos?*

Estamos vivendo uma síndrome do pânico, associada ao poder da tecnologia, que dá a sensação de que é possível controlar tudo. No entanto, já vimos em muitos trabalhos que é importante a empresa equilibrar as proteções e os riscos inerentes ao negócio, para permitir também que os profissionais trabalhem e que o excesso de proteção não gere queda de produtividade ou até inviabilize negócios. Não há uma receita de prateleira, depende muito de cada realidade empresarial, cultura interna e riscos envolvidos. Se o risco for relevante, deve sim ser implementada a proteção, o monitoramento. Mas é preciso avaliar cada caso.

FONTE: *Você utiliza o termo "esquizofrenia digital". Fale um pouco sobre o comportamento dos cidadãos que sofre transformações, nem sempre positivas, em seus respectivos "avatares", no mundo virtual.*

"Estamos vivendo uma síndrome do pânico, associada ao poder da tecnologia, que dá a sensação de que é possível controlar tudo".

É interessante observarmos que há pessoas que usam o mundo virtual para ser outra pessoa, totalmente diferente da que é no dia-a-dia e, inclusive, para praticar ilícitos ou até ter uma má-conduta, que jamais seria imaginada que a pessoa teria. Isso tem a ver com a facilidade que a tecnologia trouxe, em realizar ações e, de certo modo, anonimamente. Logo, muitos acham que ninguém vai descobrir e isso vira estímulo. Mas, na grande maioria dos casos, a pessoa é descoberta, pois as testemunhas são as máquinas e elas contam. Sendo assim...

FONTE: *A questão da responsabilidade individual sobre atitudes, ainda pouco praticada na internet, traz reflexos em mudanças nos valores e cultura de um grupo social?*

Sim. Temos visto muito isso em palestras que ministramos para o público mais jovem, quando se explica a responsabilidade individual de um ato e seu impacto coletivo, às vezes, inclusive, na vida de familiares (pais). Esta orientação ajuda na construção clara dos valores da sociedade digital, os quais continuam, de certo modo, balizados nos princípios: "não faça aos outros o que não gostaria que fizessem a você" e "diga-me com quem navegas que te direi quem és".

FONTE: *Várias foram as tentativas de se criar uma lei para controlar o acesso à web, inclusive a proposta que exigiria o CPF e a identificação de cada usuário, que sofreu questionamentos técnicos com relação à viabilização desses controles. Qual é a sua opinião sobre esta implementação e o conseqüente combate ao acesso anônimo aos recursos da internet?*

Sou a favor de um processo de verificação de identidade ou de concessão de uma identidade digital obrigatória, em que em algum momento no acesso à internet fosse possível registrar quem estaria navegando, quem seria o usuário. No entanto, isso não significa não permitir que a pessoa tenha um avatar ou um apelido, mas sim, em uma investigação, ter registros que permitam saber quem praticou a conduta indevida. É assim no mundo real para viajar em avião, em ônibus, dirigir um carro. Há atos da vida em sociedade que exigem o registro de uma identidade ou de um responsável legal (quando menor), e a tendência é isso acontecer na internet. Todos têm interesse em uma internet mais segura, mas a questão é quem paga esta conta, pois tecnologia já existe para isso.

> "A empresa responde legalmente pelo mau uso de suas ferramentas tecnológicas de trabalho, que venha a gerar lesão a terceiros".

FONTE: *Com os recursos já disponíveis da criptografia e da assinatura digital/virtual, há o risco de a internet abrigar dois grupos distintos, os não-anônimos, formais e legais, e os underground, que defendem e manterão o anonimato? Quais as tendências de formalização de uma identidade digital?*

Acredito que a internet pode ter seu lado anônimo, mas isso não é condizente com uma web transacional, principalmente, onde, em termos de questões legais, é essencial ter a prova de autoria. No entanto, mesmo quando falamos de uma web 2.0, por causa da falta de educação dos usuários é comum a prática de crimes, principalmente contra a honra e, portanto, o Direito precisa garantir a possibilidade de investigação e punição, sob pena de voltarmos para o estado da natureza, com a lei do mais forte, e não o estado democrático do Direito, que permite a liberdade de expressão, mas com responsabilidade. A pessoa pode dizer o que quiser, mas responde pelo que disse, pelo dano que causar. Está, assim, já na Constituição de 1988, no artigo 5º Inciso IV.

FONTE: *A discussão da identificação passa, naturalmente, pelos custos de operacionalizar novos procedimentos nesse sentido. A questão financeira sobrepõe-se a questões ideológicas relativas à manutenção do anonimato na internet?*

Sim.

FONTE: *Recentemente em São Paulo, um cartório não reconheceu a Nota Fiscal Eletrônica, o que leva à antiga discussão dos aspectos legais dos documentos e provas vinculadas ao papel. Chegará o dia em que o papel será substituído pelas mídias eletrônicas, garantindo-se todos os aspectos legais e jurídicos?*

Acredito que sim, mas não sei se iremos eliminar o papel totalmente, assim como até hoje temos contratos verbais, ou seja, o papel também não eliminou as relações entre as pessoas de modo menos formal. Assim como todo fax é uma cópia, e não deixamos de nos relacionar com este. Ocorre que, quando bem trabalhado, o meio eletrônico gera maior prova. Se não estiver bem arrumado, ao contrário, gera maior potencial de adulteração de conteúdo ou identidades. Mas a melhoria do processo em termos de segurança jurídica e da informação aumenta os custos, naturalmente. Logo, o que teremos é escolha, onde a pessoa pode decidir que grau de certeza jurídica quer ter sobre determinado fato e/ou obrigação e, assim, aplicar os meios necessários para garantir isso.

FONTE: *Na sua opinião, como a certificação digital se posiciona, atualmente, e quais as perspectivas para os próximos anos?*

A certificação digital é uma via de solução adequada, mas precisa de criação de cultura. Acredito que talvez a biométrica ande mais rápido, pela maior facilidade de entrar na rotina das pessoas e empresas, como já vem entrando. ■

Privacidade, integridade e sigilo

Os desafios da segurança da informação

Guydo Rossi

Tratada até pouco tempo atrás como um problema afeto exclusivamente aos departamentos de tecnologia das organizações, a segurança da informação vem ganhando, neste início de século, um status que, em muitos casos, se equipara ao tradicionalmente atribuído às suas áreas mais estratégicas. O uso crescente das redes, principalmente da internet, agregou-se à gestão das empresas e trouxe aos usuários, de forma geral, uma nova preocupação que se relaciona com a privacidade, segurança e continuidade dos negócios.

Ao analisar a "Sociedade em Rede", Manuel Castells conclui que "a nova economia está organizada em torno de redes globais de capital, gerenciamento e informação, cujo acesso ao know-how é importantíssimo para a produtividade e competitividade. Empresas comerciais e, cada vez mais, organizações e instituições são estabelecidas em redes de geometria variável, cujo entrelaçamento suplanta a distinção tradicional entre empresas e pequenos negócios, atravessando setores e espalhando-se por diferentes agrupamentos geográficos de unidades econômicas".

Se por um lado a tecnologia vem apoiando o desenvolvimento de novos negócios, promovendo ações sociais e direcionando o mundo para uma nova realidade de democratização de informações, serviços e conhecimento, por outro, como qualquer ferramenta, passou a ter uma ampla aplicação por indivíduos que identificam, nesse contexto, oportunidades de ganhos de forma ilícita.

Na sociedade do conhecimento, a informação é o principal ativo e o valor atribuído a ela é objeto de desejo de atores de empreendimentos, que visam ao desenvolvimento, e também daqueles que vislumbram possibilidades de ganhos fáceis. O problema da transferência natural dos crimes do mundo real para o espaço digital passa, dessa forma, a figurar nas agendas de profissionais dos mais diversos setores.

A exigência imposta às empresas, de desenvolver programas e iniciativas de segurança, vem não só da preocupação em manter níveis satisfatórios de serviço e de confiança dos clientes, mas também das diversas regulamentações impostas por organismos nacionais e internacionais, que definem posturas e normas às empresas, sob pena de serem responsabilizadas por eventuais problemas. E mais: ataques comprometem não só seus negócios e informações, mas também sua imagem.

O crescimento, a diversificação e a gravidade dos ataques criaram, ao mesmo tempo, um mercado bastante efervescente de serviços e produtos para prevenção e combate aos incidentes de segurança. Segundo dados do IDC, o mercado mundial de TI movimentou, em 2007, US$ 1,2 trilhão, dos quais, US$ 44,5 bilhões referem-se ao mercado de segurança. No Brasil, dos US$ 20,4 bilhões contabilizados no mercado de TI (2007), US$ 0,37 bilhão destinou-se à segurança, com uma taxa de crescimento médio de 15,3%, até 2010. Para a analista de segurança do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), Cristine Hoepers, embora não exista um comparativo mundial sobre a situação de todos os países, é possível ver que os problemas enfrentados aqui não são diferentes dos problemas encontrados em outros países.

Os investimentos são canalizados para a aquisição de software, hardware, consultorias especializadas, equipamentos para segurança física, capacitação dos colaboradores, programas de gerenciamento de cultura organizacional e racionalização de processos, alinhando as estratégias de segurança ao negócio da empresa.

Em sua publicação trimestral sobre alertas, vulnerabilidades e demais acontecimentos que se destacaram na área de segurança, o Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa destacou, no quarto trimestre de 2007, o tratamento de um total de 7.436 incidentes de segurança. Desses, 44,72% referem-se ao envio de spam em grande escala, 16,31% a tentativas de invasão de sistemas e 11,29% à propagação de vírus e worms através de botnets (computadores infectados e controlados a distância por atacantes). Também foram tratados 241 casos de troca de páginas, em que o atacante substituiu o conteúdo original de uma página da web ou incluiu conteúdo não autorizado na página atacada, e ainda 56 casos de phishing, ataques que têm por objetivo obter dados confidenciais de usuários (site Cais: www.cais.rnp.br).

Engenharia social e vulnerabilidades

Como se não bastassem os problemas ligados essencialmente ao uso das tecnologias, outra ameaça, a engenharia social, é foco de preocupação dos especialistas, por envolver um dos pontos considerados mais vulneráveis num programa de segurança: as pessoas.

O fato é que por mais que a tecnologia desenvolva e forneça soluções para prevenção e combate aos crimes virtuais, a informação ainda estará ameaçada, se o elemento humano não for contemplado adequadamente. Definida pelo especialista em segurança Kevin Mitnick como "a arte de fazer com que as pessoas façam coisas que normalmente não fariam para um estranho", a engenharia social é, na verdade, o grande temor das organizações que se preocupam em proteger suas informações.

Em seu livro *A arte de enganar*, Mitnick chama a atenção para o fato de que "a maioria das pessoas supõe que não será enganada, com base na crença de que a probabilidade de ser enganada é muito baixa; o atacante, entendendo isso como uma crença comum, faz a sua solicitação soar tão razoável que não levanta suspeita enquanto explora a confiança da vítima". Para isso, segundo o especialista, o perfil do engenheiro social é a combinação de uma "inclinação para enganar as pessoas com os talentos da influência e persuasão".

O analista de segurança do Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (Cais / RNP), Ronaldo Vasconcelos, explica que, em bom português, o engenheiro social é aquele que usa de lábia para conseguir as coisas e pode, ou não, utilizar a tecnologia para obter informações valiosas para seus objetivos.

"Essas pessoas são capazes de obter informações reservadas sem necessidade de instalar um 'cavalo de tróia', por exemplo. Podem passar por atendentes da operadora do cartão de crédito e solicitar o número do cartão do usuário, data da expiração; há golpistas que chegam ao refinamento de colocar fundo musical imitando um serviço de atendimento. As pessoas, na maioria das vezes, nem questionam. Outro exemplo comum de engenharia social são os seqüestros falsos, uma forma de extorquir dinheiro enganando as pessoas, sem usar a tecnologia ou a violência. O forte dessas pessoas é obter dados confidenciais, usando apenas a conversa".

A opinião prevalece entre os administradores de segurança, como o responsável pelo setor na Companhia Energética de Minas Gerais (Cemig), José Luís Brasil, para quem "a engenharia social existe porque as empresas investem em tecnologia e esquecem as pessoas. São elas que operam sistemas e máquinas, que fornecem informações. Se elas não sabem por que estão apertando um parafuso, não sabem a importância do seu trabalho, passam a ser um ponto fraco no processo".

Cultura de segurança

A analista do CERT.br, Cristine Hoepers, afirma que "existe uma grande tendência de associar o que ocorre via internet com algo 'virtual', ou que não oferece os mesmos riscos a que já estamos acostumados no dia-a-dia. Porém, a internet não tem nada de virtual: os dados são reais, as empresas são reais e as pessoas com quem se interage na internet são as mesmas que estão fora dela".

Desse modo, explica a especialista, é preciso levar para a internet as mesmas preocupações que temos no dia-a-dia, como por exemplo: visitar somente lojas confiáveis; não deixar públicos dados sensíveis; ter cuidado ao "ir ao banco" ou "fazer compras", etc. "Quando um usuário coloca comentários sobre sua rotina e suas preferências em um blog ou no Orkut, ele normalmente está pensando nos amigos e familiares. Porém, essas informações tornam-se públicas e do conhecimento de todos".

Cristine alerta para o fato de que, de modo similar, o usuário assume como verdadeiras informações prestadas por terceiros ou que parecem vir de amigos e familiares, armadilhas usadas com freqüência para tentar induzir um usuário a instalar "cavalos de tróia" ou outros códigos maliciosos. "Os golpes que são aplicados pela internet são similares àqueles que ocorrem na rua ou por telefone; a grande diferença é que na internet existem algumas maneiras de tornar o golpe mais parecido com algo legítimo. Portanto, o importante é que o usuário use na internet o mesmo tipo de cuidado que já usa fora dela".

Com relação aos hábitos de usuários da internet, o gerente de Soluções da IBM para a América Latina, Marcelo Bezerra, considera a existência de dois comportamentos importantes: segundo ele, uma pessoa que não é especialista em tecnologia, no ambiente de uma organização vai se adequar às exigências e procedimentos exigidos. "Vai adotar uma senha forte, com números e tipos de caracteres bem definidos, vai contar com software que faz controle de acesso, etc. Ela tem que se enquadrar até mesmo por exigência da empresa e acaba aprendendo procedimentos recomendáveis. Convive, inclusive, com restrições em relação ao que tem no computador".

Já em casa, esse comportamento vai ser muito diferente. "As pessoas costumam ter jogos, aplicações de música e outras. E, de forma geral, não querem ter a responsabilidade de cuidar dos procedimentos de segurança, querem ter essas coisas de forma tranqüila, fácil, querem ter mais liberdade".

No caso de um software em conflito com um antivírus, por exemplo: "na empresa, você vai pedir ajuda, considerar como funciona o sistema de segurança. Já em casa, é mais fácil mudar o software de segurança. Esses comportamentos são muito diferentes. Hoje, nas empresas, a questão está bem equacionada. Em casa, a tendência é desejar que o problema da segurança se adapte à nossa necessidade, enquanto o correto seria priorizar a segurança. Mas há coisas que se vê e aprende nas empresas e são levadas pra casa, como o caso dos e-mails, as pessoas em geral têm mais cuidado".

Marcelo Bezerra lembra que há também questões sobre as quais ainda não há definições, como a comercialização de músicas pela internet. "A Amazon lançou loja nos Estados Unidos que

comercializa músicas totalmente sem proteção. Não sabemos como a indústria do setor vai se comportar. Há coisas ainda sem definição, sobre as quais não se sabe se estão certas ou erradas. Muitas estão claras, como o fato de piratear software ser crime, apesar de a tolerância variar. Há países onde se alugam DVDs piratas. O Brasil já tem um nível melhor de esclarecimento sobre o assunto. Há ainda a questão cultural, que varia de país para país".

Além dos recursos tecnológicos, ele aconselha um trabalho de informação, especialmente com os novos usuários. "Com relação aos riscos para as crianças, que já estão na internet, oriento meus filhos para não passarem informações, alerto para o perigo de conversar com pessoas desconhecidas. Mas com relação à cultura, é importante também não pensar que isso basta. Há pessoas inventando novos golpes mais sofisticados, tecnologias novas, sistemas e vulnerabilidades. Daqui a pouco tempo, muitos cuidados podem não estar valendo mais e outros serão mais importantes. Isso porque os hackers também evoluem, há quadrilhas muito bem estruturadas, há o crime organizado sofisticando os ataques".

Guerra ao crime virtual

O valor da informação, aliado ao desenvolvimento tecnológico, em especial da consolidação de uso das redes, criou um universo virtual que, se por um lado facilita o fluxo de informações e as democratiza, por outro promove a ação de pessoas mal intencionadas, que vislumbram, nesse mundo, uma série de oportunidades de negócios ilícitos.

Especialistas de todo o mundo unem-se na guerra contra esses invasores por meio de entidades criadas com a finalidade de antepor a esses criminosos, identificando golpes, softwares, uma infinidade de formas de ataque, que são disseminadas pela internet numa luta constante.

Essas entidades mantêm na internet uma rede de informações atualizadas de forma permanente, e promovem encontros, seminários e congressos, onde os incidentes, ferramentas de prevenção e detecção são apresentados, buscando equipar os especialistas para garantir, da melhor forma, a integridade de informações corporativas e, não raro, resguardar as pessoas de golpes que se tornam, a cada dia, mais comuns e mais sofisticados.

Divulgação

Grupo do Cais/RNP

No Brasil, o Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Pesquisa (Cais/RNP) completou dez anos de criação e amplia sua atuação para toda a sociedade. Segundo a gerente do Cais, Liliana Solha, o Centro, criado para fazer frente à vulnerabilidade da rede acadêmica nacional, comemora seus dez anos com um saldo positivo de parcerias formadas, "desde a comunidade acadêmica, até os usuários domésticos. Todos eles são extremamente importantes em nosso trabalho, pois funcionam como multiplicadores da cultura de segurança", explica.

A criação dessa cultura de segurança, para uma convivência segura em um mundo relativamente novo – a internet – é um dos grandes desafios dos especialistas, que apontam, no elemento humano, não só o risco, mas também a melhor solução para prevenir o problema. Segundo o analista de Segurança do Cais, Ronaldo Vasconcelos, as pessoas que têm um certo tempo de vida na internet já estão entendendo a necessidade de uma mudança de postura, mas há sempre alguém que está chegando, começando a usar. "O que muitas pessoas viram e aprenderam há dez anos, outras estão aprendendo agora. De forma geral, estão aprendendo melhor, já sabem o risco de passar dados pessoais, clicar em qualquer coisa; aprendem a pensar com bom senso. Se alguém chegar na rua lhe pedindo nome, número de conta corrente, carteira de identidade, CPF, você não vai dar. Na internet é a mesma coisa, e essa resposta dos usuários tem melhorado".

Além de um site rico em informações e registros de incidentes (www.cais.rnp.br), o Cais tem ampliado sua atuação para a sociedade por meio da promoção e participação em eventos, como o Dia Internacional de Segurança da Informação (Disi), realizado anualmente. "Há uma boa resposta da comunidade, não só a comunidade acadêmica, mas o Brasil como um todo. As pessoas se interessam pelo tema", explica Ronaldo Vasconcelos. Para ele, um dos grandes méritos do Disi, realizado em 2007, no mês de novembro, foi o de sair um pouco do meio acadêmico. "Anteriormente, o evento focava prioritariamente os administradores de segurança, divulgando conteúdos mais técnicos. No entanto, foram ganhando notoriedade abordagens mais práticas para os usuários em geral, como medidas para desinfectar um ambiente, configuração segura de redes sem fio, por exemplo. Há maior participação dos usuários. A idéia é compartilhar essas informações, muito do que a equipe sabe pode ser útil para outras pessoas. Nosso objetivo é aumentar essa participação", enfatiza Vasconcelos.

Mantido pelo Comitê Gestor da Internet no Brasil, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é o grupo responsável por receber, analisar e responder a incidentes de segurança em computadores, envolvendo redes conectadas à internet brasileira.

A entidade mantém, na internet, a *Cartilha de Segurança para Internet*, um documento com recomendações e dicas sobre como o usuário da rede deve se comportar para aumentar a sua segurança e proteger-se de possíveis ameaças.

A analista do CERT.br, Cristine Hoepers, lembra que os computadores domésticos são utilizados para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias, sejam para compra de produtos e serviços; comunicação, por exemplo, por e-mails; armazenamento de dados, sejam eles pessoais, sejam comerciais, etc.

"É importante que o usuário se preocupe com a segurança de seu computador, pois ele, provavelmente, não gostaria que suas senhas e números de cartões de crédito fossem furtados e utilizados por terceiros; que sua conta de acesso à internet fosse utilizada por alguém não autorizado; que seus dados pessoais, ou até mesmo comerciais, fossem alterados, destruídos ou visualizados por terceiros; ou que seu computador deixasse de funcionar, por ter sido comprometido e arquivos essenciais do sistema terem sido apagados, etc."

Dessa forma, o material da Cartilha serve como fonte de consulta para todas as vezes em que o usuário quiser esclarecer dúvidas sobre segurança ou aprender como se proteger desses ataques e ameaças.

Projeto Honeypots

Uma importante iniciativa do CERT.br, na prevenção aos incidentes na internet brasileira, é o Consórcio Brasileiro de Honeypots - Projeto Honeypots Distribuídos, que tem o objetivo de aumentar a capacidade de detecção de incidentes, correlação de eventos e determinação de tendências de ataques no espaço internet brasileiro.

Operacionalmente, o projeto funciona com a instalação de múltiplos honeypots de baixa interatividade no espaço internet brasileiro e com o processamento centralizado pelo CERT.br dos dados capturados por esses honeypots. Um honeypot – "pote de mel", no inglês – é um recurso computacional de segurança dedicado a ser sondado, atacado ou comprometido em um ambiente próprio que permite que esses eventos sejam registrados e avaliados.

Cada instituição participante tem a chance de capacitar-se na tecnologia de honeypots, é livre para adaptá-los, conforme as suas necessidades, e para utilizar como quiser os dados capturados em seus honeypots. Por meio dos dados obtidos, é possível que o CERT.br identifique máquinas brasileiras envolvidas em atividades maliciosas e notifique os responsáveis por estas redes. Essas atividades incluem, por exemplo, máquinas que realizam varreduras ou que estão infectadas por worms.

Atualmente, o projeto conta com 35 instituições parceiras nos setores público e privado. Essas instituições mantêm honeypots que estão distribuídos em 20 cidades do Brasil e em diversos blocos de rede da internet no Brasil. Muitas das instituições participantes têm, por meio do projeto, a oportunidade de adquirir ou aprimorar conhecimentos sobre as áreas de honeypots, detecção de intrusão, firewalls e análise de artefatos. A simples participação no projeto faz com que elas se aproximem e outras possibilidades de cooperação sejam exploradas.

Na página do projeto são mantidas estatísticas diárias dos ataques coletados pelos sensores, além de outras informações relacionadas com o funcionamento do consórcio: http://www.honeypots-alliance.org.br/

Crimes mais comuns

O analista do Cais, Ronaldo Vasconcelos, enumera alguns dos incidentes considerados mais comuns: um deles é a tentativa de exploração de vulnerabilidades em aplicações web, que podem levar à "pichação" da página (defacement) ou roubo de dados sigilosos ou de contas.

"Outro incidente comum é a tentativa de controle remoto da máquina. Hoje, isso acontece principalmente pela tentativa de login por força bruta: tentativas exaustivas de combinações de usuário e senha em serviço SSH e de exploração de uma vulnerabilidade no software de controle remoto VNC (controle total de uma máquina remota), que permite login sem usuário e senha".

Com relação a golpes, o especialista afirma que phishing – mensagem falsa que induz a vítima a acessar um site falso, onde poderá contaminar-se com um "cavalo de tróia" ou enviar dados pessoais – ainda é popular. "A evolução mais comum desse golpe é o uso de software malicioso (bot ou "cavalo de tróia"), que se instala no computador da vítima, ou mensagens de phishing direcionadas a usuários de uma organização específica (spear phishing)".

Há ainda outro golpe muito comum que é a tentativa de lavagem de dinheiro proveniente de golpes on-line pelo uso de "mulas de dinheiro" (do inglês "money mules"). Por trás de uma oportunidade de dinheiro fácil, que chega por e-mail, muitas pessoas tentam receber porcentagens por transações. Na maioria dos casos, a vítima fica com a conta do primeiro fraudador para pagar.

Cristine Hoepers, do CERT.br, destaca que a maior parte das tentativas de fraude atuais está relacionada com a utilização de algum tipo de programa malicioso, em geral direcionado a computadores de usuários finais. "Existem duas maneiras de o usuário ser infectado por este programa malicioso: o ataque tenta levar a pessoa a acreditar em algum fato e a seguir um link ou instalar um código malicioso em seu computador. Se o usuário não está esclarecido sobre o problema e acredita no ardil utilizado, ele pode ser afetado pela fraude. Ou sua máquina pode ser comprometida automaticamente, via rede, por um worm ou bot. Ao ter acesso à máquina do usuário, o invasor não só poderá utilizar os recursos de processamento e banda, fazendo com que o usuário fique com a máquina e com a conexão internet lentas, mas também poderá furtar dados de sua máquina, como dados pessoais (contas, senhas, número de cartão de crédito, declarações de imposto de renda, cadastro em sites de relacionamento, etc.) e os endereços de e-mail de amigos e familiares, para serem posteriormente utilizados em listas de spam."

Também há informações mais detalhadas, específicas sobre fraudes, no documento: Cartilha de Segurança para Internet – Parte IV: Fraudes na Internet em http://cartilha.cert.br/fraudes/

Cuidado com as atualizações

Os cuidados para evitar danos começam pela consciência do usuário de que ele pode, com algumas atitudes, criar um ambiente seguro para trabalhar e se divertir. Ronaldo Vasconcelos, do Cais / RNP, admite que gostaria que todos conhecessem bem as ferramentas disponíveis e os riscos. "As pessoas devem estar bem atentas, o bom senso é muito importante: pensar, por exemplo, que o que você não faria no mundo real, não deve fazer no mundo virtual. Fornecer quaisquer tipos de informações é um grande risco; há tipos de ataque que enganam".

Ele dá outras dicas: manter antivírus atualizado, mas atenção: a vida útil dessas ferramentas está se tornando muito curta. Os softwares maliciosos mudam rapidamente e há grande variedade de malware – "nem sempre o perigo é só o vírus, há muita variedade de ataques e pode acontecer de determinadas versões não identificarem todos". Manter atualizado o navegador. Ronaldo Vasconcelos recomenda que o usuário deve manter, na verdade, toda a máquina atualizada e ter um cuidado especial com as ferramentas de comunicação: e-mail, MSN e navegador e atender notificações de atualização.

Ter um firewall pessoal para evitar conexões indesejadas à sua máquina. "Se a pessoa não tem firewall pessoal, fica muito vulnerável. Para usuários de laptops e acessos sem fio, cuidado especial, até mesmo dentro de casa, se tiver um access point; ele já tem um firewall pessoal ativado, mas o usuário tem que estar atento".

Pessoas que usam softwares para e-mail: é importante usar um bloqueador de spam. Tanto phishing quanto outros problemas são distribuídos por spam. O

especialista recomenda o uso de webmail, como Hotmail ou Yahoo, que já têm um bom filtro para spam. "Nesse caso, o usuário se beneficia do conhecimento de outras pessoas; pode aproveitar desse conhecimento coletivo. Pode também instalar pacotes 'spyware'; alguns vêm com essas ferramentas para spam, firewall, antivírus".

Ronaldo enfatiza o cuidado nas comunicações, com os relacionamentos feitos no Orkut e outras comunidades de redes sociais: "cuidado com o que recebe. Quem ataca, sabe o que é popular, o que agrada. Para ataques em massa, essas pessoas mal intencionadas vão usar algo popular e hoje o Orkut é importante na vida de muita gente. Atenção, portanto, usuários de redes sociais mais populares, bancos mais populares. Ao invés de uma pistola, o ataque é como uma metralhadora".

Atentos a essas dicas, os usuários podem também consultar orientações no site do Cais, onde há lista de incidentes e orientações on-line. "Mais do que isso, seria pedir que o paciente saiba mais que o médico. O especialista tem que trabalhar para prover segurança".

A analista do CERT.br, Cristine Hoepers, recomenda cuidados relacionados com o comportamento dos usuários:

- não acessar sites ou seguir links recebidos por e-mail, por serviços de mensagem instantânea ou presentes em páginas sobre as quais não se saiba a procedência;
- jamais executar ou abrir arquivos recebidos por e-mail, mesmo que venham de pessoas conhecidas;
- jamais executar programas de procedência duvidosa ou desconhecida;
- consultar sua instituição financeira sempre que tiver dúvidas sobre a utilização de mecanismos de acesso e segurança ou quando receber convites para cadastros em promoções ou atualização de dados, entre outros. Muitas vezes os fraudadores utilizam estes ardis para tentar convencer o usuário a fornecer dados de cadastramento.

Na página da Cartilha de Segurança para Internet é possível obter um folder com essas e com outras dicas de segurança: http://cartilha.cert.br/dicas/

Redes sem fio

Se para os usuários em geral as questões de segurança são tão importantes, aquelas que se conectam em redes sem fio devem ter atenção redobrada. O alerta é do gerente de Soluções da IBM para a América Latina, Marcelo Bezerra, que reconhece e aplaude os benefícios da tecnologia, mas recomenda cuidado. "Trata-se de um benefício enorme, que traz uma série de facilidades ao usuário. Os equipamentos, em sua maioria, já saem de fábrica com o recurso da conexão sem fio, já temos o iPod sem fio, acesso à rede via celular. Mas o problema da segurança existe".

Embora os manuais descrevam em detalhes os procedimentos para configuração segura de uma rede wireless, a tecnologia apresenta riscos adicionais: "a rede não tem um limite definido, é susceptível; outras pessoas podem usar uma determinada conexão até sem querer". Ele exemplifica com o fato ocorrido com a filha, que reclamou de quedas sucessivas em sua conexão. "Na rede que tenho em casa as configurações estão adequadas; o que estava acontecendo é que minha filha estava usando, sem querer, a rede do vizinho, que estava aberta, sem proteção. Como não há limites, o risco aumenta, seu computador pode ser invadido por alguém que você nem sabe onde está".

Ele adverte para o fato de que, se houver uma conexão da rede wireless com uma rede cabeada, o acesso é aberto também à segunda. "Existem hoje os chamados sniffers, que conseguem capturar todo o tráfego em um segmento de rede. Se o dado está sem criptografia, ele pode capturar tudo. Fazendo uma analogia com a rede física, seria como colocar um plug de rede na calçada, para que qualquer pessoa possa se conectar".

As redes sem fio estão sendo muito usadas em aeroportos, laboratórios, restaurantes, hotéis. "Tudo isso tem que ser muito bem configurado, senão a pessoa pode ter problemas como invasão de seu computador, ter seus dados capturados. Trata-se, basicamente, de configurar o ponto de acesso de forma que fique invisível para outras pessoas, e usar criptografia, limitando o acesso ao usuário que conhece a chave criptográfica. Há recurso para que você determine autorizações para quem você permite que entre. Colocando algumas dificuldades, a pessoa reduz sua exposição e a probabilidade de alguém invadir o seu computador".

Segurança Corporativa

O cuidado que usuários domésticos devem adotar com suas informações ganham dimensões superlativas quando se trata de uma organização. Para o presidente da Módulo Security, empresa especializada em tecnologia para Gestão de Riscos, Fernando Nery, a segurança da informação deve ser tratada não só do ponto de vista tecnológico, mas prioritariamente pela sua relação com o negócio da empresa. "Trata-se de um desafio do dia-a-dia da informática; gestores de segurança de TI compartilham angústias e dificuldades ao tratar a questão", afirma. Nery explica que atualmente o problema da segurança é abrangente: "começa dentro de casa, com os filhos alimentando seus blogs, relacionando-se pelo Orkut, a família fazendo compras pela internet; até mesmo pelo telefone, os riscos de extorsão existem".

Com a experiência de atuação no mercado corporativo, ele defende que os orçamentos dedicados à segurança da informação variam de acordo com a importância que a empresa dá a esse aspecto. "Quanto mais importante a segurança da informação é para o negócio da empresa, maior o orçamento destinado".

Nery ressalta ainda o desafio dos gestores de segurança para sinalizar aos responsáveis pelas áreas de negócios a importância de adotar medidas de segurança numa empresa. Ele explica que a segurança ou problemas relacionados, aparecem em casos críticos, quando há uma invasão, indisponibilidade ou queda de um sistema, e defende que é relevante tratá-la como algo positivo: "o risco pode ser positivo, considerando-se o conceito de que o risco é o efeito das incertezas nos objetivos. É trabalho do profissional de segurança conscientizar usuários e gestores".

Em palestra realizada durante o Security Meeting 2007, em Belo Horizonte, o executivo fez alerta aos profissionais da área sobre o conceito de Governança, Gestão de Riscos e Compliance (GRC). Segundo ele, é uma tendência, na forma de um conceito mais abrangente do que os três elementos tratados de forma individual. Ele explica que os três pontos, juntos, são capazes de contemplar uma capacidade de trabalho superior à da soma dos três, além de evitar redundâncias entre áreas da empresa.

Ele adverte para o fato de que a aplicação do GCR exige dois princípios básicos: a automação e a

Fernando Nery: governança, gestão de riscos e compliance.

integração; a importância da troca de informações, remete à colaboração: "é fundamental um clima propício à colaboração", ressalta.

Nery lembra que hoje existe uma boa base teórica e técnica para tratar a questão, que deve contemplar três conceitos básicos: a confidencialidade (resguardar sigilo e evitar vazamento), a integridade (combate a fraudes, conformidade com leis, normas, regulamentação) e a disponibilidade. Ele alerta ainda para o fato de que programas e normas de segurança hoje são compulsórios para as organizações quem têm alguma regulamentação, de acordo com a área de atuação.

E deixa um lembrete: "pense no todo. Comece pequeno. Crie um modelo escalável. Cresça rapidamente".

Para a analista do CERT.br, Cristine Hoepers, de forma geral, empresas, provedores e outras grandes instituições devem seguir as boas práticas de segurança de redes internet, possuir políticas e procedimentos adequados, ferramentas adequadas de proteção e investir fortemente em treinamento de pessoal. Ela ressalta que a qualificação de pessoal e a conscientização dos usuários é a chave para o aumento da segurança.

Para a implementação de um programa de segurança, afirma, é importante que a pessoa responsável pela gestão de riscos compreenda não só as implicações de segurança de cada solução de TI adotada, mas também entenda profundamente o negócio da empresa. "Somente somando esses conhecimentos, o profissional tem condições de avaliar quais as áreas prioritárias e qual a estratégia adequada para gerir os riscos de sua infra-estrutura".

Para o envolvimento dos colaboradores num projeto de gestão de riscos, Cristine afirma que não existe uma receita de sucesso, mas este depende do envolvimento de todos os setores no processo de definição da estratégia. "Se os setores-chave estão envolvidos no projeto e discussões e, conseqüentemente, compreendem a importância, fica muito mais fácil conseguir o comprometimento para atingir o sucesso".

Mais informações específicas para administradores de redes podem ser encontradas nos seguintes sites:

- Antispam.br – Área de Administradores - http://antispam.br/admin/
- Práticas de Segurança para Administradores de Redes Internet – http://www.cert.br/docs/seg-adm-redes/

Regulamentações

O problema da segurança das informações e a globalização, que coloca on-line na internet diferentes legislações e culturas, reflete profundamente na gestão das organizações, com maiores ou menores impactos, em função da natureza de seus negócios. Uma série de normas e regulamentações têm surgido, para enquadrar, num padrão desejado de segurança, determinados grupos de instituições que se relacionam pela rede.

Segundo o analista da Prodemge, Paulo César Lopes, os impactos atingem diretamente os departamentos de administração de risco e as áreas de tecnologia, que assumem novas funções, a partir dessas normas, visando à adequação. Marcelo Bezerra, da IBM, acrescenta que a questão pode se transformar num problema administrativo para organizações vinculadas às várias regulamentações.

O não cumprimento de determinadas normas pode desabilitá-las para prestação de serviços, já que estão sujeitas a auditorias e punições.

Uma das normas mais conhecidas internacionalmente é a Sarbanes-Oxley, a chamada SOX, uma regulamentação fiscal norteamericana aplicável a empresas de todo o mundo que tenham ações nas bolsas dos Estados Unidos. Segundo Marcelo Bezerra, como todas as transações baseiam-se na tecnologia da informação, nesse caso, os sistemas de dados contábeis, financeiros, operacionais e jurídicos têm que estar íntegros e aderentes às centenas de artigos que compõem a SOX.

Uma regulamentação importante, dirigida ao sistema financeiro, é o acordo de Basiléia, que procura, em sua essência, estabelecer padrões de qualidade para as instituições financeiras, aperfeiçoando-as. Os acordos de Basiléia I e II podem ser vistos também como um estímulo à transparência e à segurança para clientes, investidores, acionistas e controladores.

ENTREVISTA

Monty Brinton/John Wiley & Sons

Kevin Mitnick

Os perigos crescentes na rede mundial de computadores, especialmente aqueles produzidos por meio da engenharia social, são abordados, nesta entrevista, por um dos maiores especialistas no assunto. O consultor norte-americano na área de segurança da informação, Kevin Mitnick, fala com o conhecimento e a experiência do mais conhecido hacker da história da internet.

Após uma trajetória pouco convencional, quando se tornou famoso pelas ousadas investidas em redes de grandes organizações – entre elas o Comando de Defesa Aérea norte-americano – e pela perseguição por agentes do FBI, que culminou em sua prisão por crimes digitais, o especialista agora trabalha "no lado certo da lei", oferecendo o que ele chama de "serviços de hacker ético". Atendendo clientes em todo o mundo, com dois livros publicados sobre o assunto – *A arte de enganar* e *A arte de invadir* – ele se diz recompensado com a nova rotina.

Mitnick é fascinado pela mágica, conforme confessa em seu primeiro livro, e consolidou a expressão e a prática da *engenharia social*, a arte de manipular ou influenciar pessoas para conseguir delas informações importantes ou sigilosas.

Nesta entrevista exclusiva à revista **Fonte**, concedida por telefone, ele fala ainda sobre a importância da análise de riscos, os reais perigos da internet e de como prevenir incidentes ou reduzir vulnerabilidades, destacando o peso que as organizações devem dar aos aspectos tecnológico e humano.

Com a participação dos analistas da Prodemge Naira Faria e Paulo César Lopes.

ENTREVISTA

Em seu livro A arte de enganar (The art of deception), o senhor é enfático ao falar da vulnerabilidade dos sistemas de segurança. Como é prestar serviços provendo justamente segurança?

Eu me sinto muito melhor, claro, trabalhando no lado certo da lei e ajudando empresas, setores governamentais, universidades e protegendo seus sistemas de informação. É definitivamente uma carreira muito recompensadora; e o gerenciamento desses riscos é realmente imprescindível no hostil ambiente da computação atual.

Na prática, que serviços o senhor oferece aos seus clientes?

Os serviços que eu forneço são serviços de hacker ético. Empresas me contratam para tentar comprometer seus sistemas ou, em outras palavras, para encontrar todas as falhas de segurança que um hacker poderia usar para entrar em suas redes ou para ter acesso a informações críticas. E o que é desafiador nisso? Como um hacker, você só precisa encontrar um dos furos na segurança para burlar o sistema. Mas como um hacker ético, como um profissional de segurança, você tem que encontrar todas as vulnerabilidades e garantir que suas respectivas defesas sejam instituídas, porque se você deixar uma abertura, com certeza alguém irá explorá-la. É muito difícil trabalhar para proteger sistemas, mais difícil do que ser um invasor. Ser um hacker é mais fácil, porque você só vai precisar encontrar um problema de segurança, vai ter que encontrar apenas um furo, mas proteger o sistema é mais difícil, porque você vai ter que encontrar todos eles. É muito mais desafiador, na verdade, mais desafiador do que ser um hacker. É mais difícil proteger um sistema do que hackear um sistema. Pesquisar e garantir proteção ao seu cliente é melhor do que só encontrar uma única vulnerabilidade e invadir.

Atualmente, qual o grau de segurança (ou insegurança) na internet?

Bem, segurança na internet realmente depende da empresa ou do setor do governo que está conectado à internet. No geral, a internet, como uma imensa rede global, cria um ambiente rico em alvos, porque há muitos sistemas inseguros que podem ser hackeados. É um ambiente hostil e uma vez que você conecte seu sistema nessa rede, tem que adotar o devido cuidado para proteger seu sistema de ser comprometido. É, sem dúvida, uma rede hostil. E o que você tem que fazer como empresário ou indivíduo é adotar como padrão a devida precaução para se proteger.

O senhor acha que hoje é mais difícil invadir?

Na verdade, é mais fácil hoje em dia, porque muitas das façanhas identificadas por pesquisadores de segurança são publicadas. Muitas empresas e clientes têm empacotado seus sistemas e corrigido essas vulnerabilidades; há também a divulgação das vulnerabilidades "zero-day", para as quais não há solução. De fato, há anos, quando eu era um hacker, informações como essas não eram publicadas, você tinha que encontrar as vulnerabilidades de segurança por conta própria ou se associar a um pequeno grupo de pessoas que compartilhasse esses mesmos interesses e também as informações sobre vulnerabilidades. Atualmente, há muita informação disponível sobre como invadir um sistema, por isso é mais fácil. Temos que considerar, no entanto, que ao mesmo tempo, esse fato pode tornar a invasão mais difícil, porque muitas empresas, setores governamentais e universidades estão mais prevenidos, desenvolvendo tecnologias de segurança para garantir sua proteção. Então, nesse caso, a questão se torna mais desafiadora.

ENTREVISTA

Quais os principais pilares de um programa de gestão de risco?

A habilidade para identificar uma ameaça e determinar como e em que medida ela poderia afetar seu negócio. Você precisa identificar a ameaça e a probabilidade do seu sistema ser comprometido. E você quer desenvolver um programa de gerenciamento de riscos para avaliar que área do negócio você precisa proteger e como priorizá-la corretamente. E, ainda, qual seria o custo efetivo, porque em análise de riscos é importante saber quanto se perderia se um incidente de segurança ocorresse. Então, na análise final, você precisa identificar as vulnerabilidades que podem resultar numa perda significativa, para que você possa priorizar quais itens focar e quanto seria orçado para garantir sua proteção.

Há alguma peculiaridade, se considerarmos uma empresa pública?

Não necessariamente. Toda empresa está sob risco e não importa se é um setor do governo, uma empresa pública ou privada. Há, definitivamente, ameaças e você tem que gerenciá-las apropriadamente. É claro que hackers com intenções criminosas irão onde o dinheiro está. Mas não necessariamente precisa ser uma empresa pública, poderia ser uma empresa de serviços financeiros ou de transferência de dinheiro, que poderia ser atacada pela habilidade de roubar dinheiro. Geralmente, as grandes empresas têm um orçamento de segurança para comprar tecnologias apropriadas e treinar seu pessoal. Dessa forma, podem ser menos vulneráveis. Mas você não pode generalizar seus inimigos, isso, de fato, se resume à individualidade de cada empresa e o que elas fazem com seus programas de gerenciamento de segurança. Você pode ter uma empresa pública que possui uma segurança terrível e uma empresa pública que possui uma boa segurança. São todas diferentes, não é tudo igual para todas as empresas conectadas à internet.

Qual a importância do elemento humano nesse contexto?

A influência humana pode ser usada para o que é conhecido como "engenharia social", que significa que você pode enganar, manipular ou influenciar uma pessoa, uma vítima, para conseguir que ela atenda uma solicitação, geralmente pessoas confiáveis em uma organização. Então, claro, se as empresas não treinarem seus funcionários sobre o que é a engenharia social, sobre as diferentes abordagens utilizadas pelos engenheiros sociais e treinar funcionários nas políticas de segurança e motivá-los a não quebrá-las sob qualquer circunstância, as empresas estarão correndo risco de ser atacadas pela engenharia social.

As ferramentas para prevenir ou detectar ataques têm acompanhado a velocidade de sofisticação dos hackers?

Eu vejo prevenção e proteção como ferramentas da tecnologia e os hackers experientes, ao usá-las, deveriam saber como usar essas ferramentas para prevenir e detectar invasões. Mas isso realmente depende da habilidade do hacker. Há hackers que podem não estar familiarizados com determinada tecnologia; e há hackers profissionais. Isso realmente depende da experiência particular deles.

Pode-se falar em "crime organizado" na internet? Há quadrilhas de hackers? Como elas atuam?

Com certeza. Especialmente na Rússia e em algumas nações pobres, o crime organizado é definitivamente um sério problema, porque pela internet torna-se mais fácil roubar. Então, há muitas fraudes de cartões de crédito, fraudes financeiras,

ENTREVISTA

extorsões, esquemas de sites falsos que estão acontecendo todo dia, envolvendo até sites de relacionamentos. Há crimes organizados explorando pessoas por meio da construção de falsos relacionamentos e usando-as para conseguir sua ajuda involuntariamente; por exemplo, se você compra mercadorias com um cartão de crédito internacional, a vítima irá reenviar o produto para um país estrangeiro por acreditar tratar-se de algo legítimo. Mas eles irão pensar que estão fazendo isso para a namorada ou namorado que conheceram na internet. Mas, na verdade, é um esquema fraudulento.

Que crimes são mais comuns na rede?

Roubar dados de cartões de crédito, usar cartões fraudulentos para comprar produtos e serviços, esquemas de extorsão virtual, nos quais as empresas são ameaçadas, a fim de pagar para que seus web sites não sejam derrubados ou o hacker, de alguma forma, rouba seu domínio. Há ainda o roubo de informações privadas e spywares, que infectam o computador do consumidor com programas que, na verdade, agem como grampos: os hackers conseguem, dessa forma, roubar informações como credenciais bancárias on-line. Eles "logam" na conta bancária do cliente e a esvaziam. Todos esses tipos de crimes são cometidos na internet.

Quais os riscos reais em compras eletrônicas e no uso de serviços bancários pela internet?

Em e-commerce, são ladrões roubando os dados do seu cartão de crédito e usando esses dados para comprar outros produtos e mercadorias. Felizmente, nos Estados Unidos, se alguém rouba o número do seu cartão de crédito, você não é responsável pelo pagamento, mas sim o comerciante. Mas em alguns outros países, o dono do cartão assume o risco. Felizmente, na América, o banco assume o risco. O internet banking pode ser arriscado se um fraudador conseguir seu nome de usuário e senha da sua conta bancária, o que pode possibilitar que ele transfira dinheiro. A responsabilidade da dívida depende da lei do país onde o cliente do banco reside. Mas em alguns casos, o consumidor pode ser o responsável pelo prejuízo, isso realmente depende da lei do país, o que pode ser bastante desastroso para um consumidor. Planos de aposentadoria podem ser roubados. Se um fraudador tem acesso à carteira de investimento das pessoas e os proprietários dessas contas ficarem comprometidos e o dinheiro desaparecer, é o consumidor que assumirá o risco. Isto é bastante assustador.

Quais os erros mais comuns cometidos por empresas na implantação de programas de segurança?

Elas investem todo o dinheiro em tecnologia, elas podem comprar produtos, elas podem não configurá-los corretamente. A maioria dos produtos de segurança cria logs de auditoria. A não ser que algo suspeito ocorra, ninguém analisa logs para identificar incidentes de segurança. Em outras palavras, as empresas apenas compram tecnologia e esperam que esta gerencie a segurança por si só. Mas o departamento de TI precisa realmente gerenciar a tecnologia. E eles não fazem isso corretamente.

Que recomendações o senhor daria a esses empresários?

Para levar segurança a sério e não apenas focar em tecnologia unicamente, atente ao seu quadro de funcionários. Treine seu pessoal sobre a ameaça à segurança, que pode afetá-los, como a engenharia social. Desenvolva processos de segurança com um ciclo de vida, então você estará constantemente revendo os requisitos de sua segurança, mudando-os sempre que preciso e adquirindo tecnologia eficaz para reduzir o risco específico ao seu ambiente.

Mais informações sobre Kevin Mitnick em www.mitnicksecurity.com

Mercado e tendências

O desenvolvimento da indústria de segurança, em todo o mundo, tem acompanhado as necessidades dessa nova realidade. “Não é que a internet tenha trazido novidades de risco”, explica Marcelo Bezerra, da IBM. “Na verdade, o crime vai onde há oportunidades de ganhos. Há alguns anos, as pessoas ficavam à vontade para andar com quantias enormes de dinheiro nos bolsos. Muitas foram vítimas de assalto ou do velho golpe do bilhete premiado. Com a imposição de mudança nesse hábito, reduziu-se o número de pessoas que carregam dinheiro e muitas foram para a internet, onde realizam suas operações. O crime vai junto. As partes boa e ruim andam juntas; a tecnologia serve da mesma forma aos dois lados da sociedade”.

Ele lembra que a segurança física patrimonial também acompanhou as demandas da sociedade, desenvolvendo tecnologias sofisticadas para segurança de prédios comerciais ou residenciais, como alarmes, cercas, etc. “Esse movimento acompanha o crescimento da criminalidade; é uma característica da nossa sociedade”.

Marcelo Bezerra afirma que segurança da informação tornou-se um componente importante no universo de TI: “não se trata de uma aplicação em si, mas que possibilita que outras aplicações sejam feitas; uma vez que as empresas estão investindo em TI e internet, os recursos de segurança agregam a essas inovações a garantia de que elas aconteçam”.

Ele cita, como exemplo, a Web 2.0, que tem sido amplamente utilizada pelas organizações em seus relacionamentos com clientes e que se trata de um ambiente pautado fortemente pela interação. “Os programas são feitos para facilitar a comunicação, conversarem de forma interativa. Um determinado site também conversa com outros. Para facilitar toda essa dinâmica, novos protocolos e ferramentas de desenvolvimento são largamente utilizados, tudo com base no webbrowser, que funciona como um sistema operacional”.

Essa característica de interação, se por um lado torna as coisas mais fáceis para o usuário, por outro as torna mais acessíveis para os hackers, ou mais fáceis do que eram antes. Para que essas novidades sejam viabilizadas, segundo o gerente da IBM, “tem que haver segurança, senão você está abrindo novas portas, problemas que estavam resolvidos podem voltar. As empresas estão, em suas rotinas, utilizando novos softwares, protocolos, camadas de programas, ou seja, novas vulnerabilidades também surgem, podem ser novas janelas de ataque”.

Divulgação

Marcelo Bezerra, da IBM

Investindo maciçamente em produtos para segurança há cerca de dois anos, a IBM tem feito avanços e aquisições no setor e formou um portfólio abrangente de produtos para seus clientes. “São alternativas de segurança em quase todas as disciplinas. A IBM não é uma empresa de segurança da informação, mas tendo esse conhecimento dentro de casa, tem uma possibilidade muito boa de trazer essas soluções para seus clientes”, informa Bezerra.

Ele explica que no aspecto tecnológico a busca dos profissionais do setor é por sistemas mais automáticos, que detectem fraudes com base no mapeamento de comportamentos. “Existem no mercado investimentos para fazer isso de forma cada vez mais eficiente; programas que analisam comportamentos de sistemas, de pessoas e de tráfego na rede”.

Como funciona isso? Se um determinado programa no computador começa a ser executado e tenta acessar ou gravar informações em áreas que não são as usuais, ou a interagir com outros programas, com os quais não tem nenhuma relação, esse fato é identificado. “O acompanhamento pode ser feito tanto com relação ao comportamento de redes quanto de pessoas. Por exemplo, o caso de um colaborador que tem perfil de acesso a determinadas aplicações e de repente começa a mandar, de seu usuário,

dados criptografados para endereço desconhecido. Trata-se de um procedimento que foge à rotina ou comportamento diferente que pode ser identificado e analisado. Pode não ser nada, mas se for, há como intervir".

Segundo Marcelo, a indústria vem estudando padrões de comportamento e já tem mapeada uma série de padrões de comportamento de programas de ataque. Os vírus automáticos, por exemplo, que começam a partir de uma máquina contaminam cem, que por sua vez contaminam mais cem. "Quanto mais efetivo for o mapeamento de comportamento, melhor".

Outra tendência é a prevenção de perdas de dados. Ele explica que um problema hoje bem identificado é a perda de dados, sejam eles pessoais ou de empresas. O data lost prevention é uma solução que acompanha produtos de rede e é capaz de detectar, por exemplo, um número de CPF circulando pela rede. "Nesse caso, se passar pela rede um número de CPF, ele acusa". Da mesma forma, há inteligência para detectar fraudes no correio eletrônico.

Outra preocupação dos executivos de segurança, que vem recebendo resposta dos fornecedores, é a questão de ajustamento do ambiente às regulamentações exigidas por entidades no Brasil e no mundo. O funcionamento de muitos setores está condicionado ao cumprimento dessas exigências. "Na configuração, o sistema de segurança deve estar aderente a determinadas normas que são exigidas para aquela organização, de acordo com a sua natureza. O objetivo é facilitar a vida do administrador de segurança", explica Bezerra. Nesse grupo, enquadram-se as ferramentas de adequação.

Outro recurso de apoio à gestão da segurança é a chamada correlação de eventos, que gera informações importantes a partir do cruzamento de eventos. Por exemplo, o registro de um evento que houve no firewall e um outro de tentativa de ataque a um servidor podem ter vindo de um mesmo endereço IP, mostrando ao administrador uma informação que pode ser muito importante. Ou a tentativa repetida de logon, o chamado ataque de força bruta, também é detectado. "A associação de muitas informações pode mostrar fatos suspeitos que não seriam visíveis. Quanto mais fontes de dados disponíveis, mais forte o mecanismo se torna".

Certificação Digital

Num cenário de crescimento dos serviços oferecidos pela internet, a certificação digital posiciona-se como grande aliada da segurança em transações realizadas via web. A Receita Federal estima que, até 2010, o Brasil deve atingir a marca de 4 milhões de certificados emitidos, "um número ainda muito longe do ideal, considerando os riscos que a internet representa e o número de usuários", segundo o diretor da CertiSign, Sérgio Kulikovski. "Contudo já é um grande avanço, visto que o certificado digital é uma tecnologia relativamente nova".

A analista do CERT.br, Cristine Hoepers, entende que o certificado digital não é um mecanismo de segurança, mas sim de autenticação. "Ele é normalmente utilizado para comprovar a identidade de uma pessoa, empresa ou site, semelhante ao CNPJ, RG, CPF e carteira de habilitação de uma pessoa. Cada um deles contém um conjunto de informações que identificam a instituição ou pessoa; e a autoridade, para estes exemplos, órgãos públicos que garantem sua validade". Alguns usos típicos da certificação, segundo a analista, são assegurados pela tecnologia, como o acesso a um site com conexão segura, como a conta bancária do usuário pela internet, possibilitando checar se o site apresentado é realmente da instituição que diz ser, por meio da verificação de seu certificado digital.

Na opinião do coordenador-adjunto de TI da Receita Federal, Donizette Victor Rodrigues, já existem muitos benefícios no uso da certificação, tanto para pessoas físicas, quanto jurídicas. "Para profissionais de contabilidade, não ter o certificado acaba ficando caro, uma vez que há necessidade de deslocamentos e trâmites de papel, que podem ser feitos seguramente pela internet".

Ele afirma que a oferta de mais serviços é instrumento para popularizar o uso da tecnologia. "Hoje, muitos órgãos do Governo já exigem o certificado para vários serviços. Novas Autoridades Certificadoras estão sendo credenciadas e há cartórios, que oferecem serviços por certificação digital. Com isso, a tendência é reduzir o custo".

A questão do custo de obtenção e manutenção de um certificado digital é apontada, também pelo gerente da IBM, Marcelo Bezerra, como um obstáculo à sua popularização. "A certificação digital aumenta bastante a segurança nas transações para as duas partes envolvidas, mas o custo ainda é alto. A partir do momento em que haja mais serviços, o interesse aumenta; aumentando o interesse, crescerá o uso e o preço cairá. Trata-se de ir sofisticando, inventando serviços".

Divulgação

O presidente da CertiSign, *Sérgio Kulikovisk*, mostra um panorama da certificação digital no Brasil

Atualmente, o número de serviços oferecidos que utilizam a certificação digital não é grande e a maioria limita-se a serviços públicos. Qual a tendência para ampliação desses serviços?

Além da segurança e autenticidade de todo e qualquer tipo de mensagem trocada eletronicamente, características inerentes à tecnologia, a certificação digital tem como um dos seus principais benefícios a agilidade na tomada de decisões. É justamente neste sentido que temos direcionado o desenvolvimento de novas soluções e o que tem nos permitido crescer e atingir novos nichos de mercado.

Como popularizar a certificação digital?

Na condição de uma das três primeiras Autoridades Certificadoras do mundo e a primeira da América Latina, a CertiSign vê uma agressiva curva de crescimento na adoção da tecnologia de certificação digital no Brasil e a expectativa para 2008 é que surjam cada vez mais aplicações, principalmente no setor financeiro, judiciário e em órgãos públicos, desencadeando a disseminação definitiva desta tecnologia em nosso país.

Fale sobre o mercado de soluções para segurança da informação. Como a certificação digital figura nesse contexto?

A necessidade de implementação de medidas de segurança da informação tem crescido de maneira expressiva nos últimos anos. O valor da informação tornou-se mais expressivo para as empresas, que, muitas vezes, têm seu negócio e seu diferencial competitivo com base unicamente em informações.

Neste contexto, a certificação digital seria o equivalente a um Mercedes blindado trafegando nas vias inseguras das empresas e até mesmo dos cidadãos, apresentando em cada barreira um chip de identificação RFID, provendo ao mesmo tempo, base jurídica, identificação, autenticação e confidencialidade.

As instituições financeiras são as grandes demandantes de ferramentas de segurança. A tendência do crescimento das transações via internet levará à exigência de uso de certificados por todos os clientes?

Tudo depende de como as instituições financeiras irão posicionar-se. As que já adotaram a certificação digital deram-se muito bem, não apenas na redução dos riscos, mas também dos custos inerentes às suas políticas de segurança. A tendência é que haja cada vez mais o uso dos certificados digitais, mas ainda não é possível afirmar que haverá uma exigência desse mercado quanto ao uso dessa tecnologia.

Com relação ao comércio eletrônico, qual é o comportamento atual e quais as tendências?

A internet já vem se mostrando como uma excelente oportunidade para alavancar negócios no País. Decerto, há ainda uma significativa parcela da população que não tem acesso à rede ou não dispõe de banda larga para melhor usufruir dela, no entanto, os números já impressionam.

Não se trata aqui apenas de um espaço reservado a grandes varejistas, muito pelo contrário, o investimento inicial reduzido e a possibilidade de atingir um público maior, mais heterogêneo e disposto a comprar pela internet, têm atraído, cada vez mais, empreendedores e pequenos empresários. Segundo dados da Câmara Brasileira de Comércio Eletrônico (Câmara-e.net), já existem 14,9 mil pequenas e médias companhias que vendem na internet. E esse número, com certeza, deve aumentar cada vez mais.

O que tem surgido de novo nas tecnologias da certificação digital? A dinâmica é a mesma da época da sua criação?

Cada vez mais, as instituições estão aderindo aos certificados digitais na troca de informações. Como exemplo, posso citar o Troca de Informações em Saúde Suplementar (TISS), criado pela Agência Nacional de Saúde Suplementar (ANS), para padronizar os documentos de registro e de intercâmbio de dados entre operadoras de planos privados de assistência à saúde e prestadores de serviços de saúde. A nota fiscal eletrônica é outra aplicação que está em funcionamento, já com 84 empresas emitindo notas fiscais por meio eletrônico.

Quanto à dinâmica, com certeza a situação é outra, atualmente. As aplicações surgem mais rapidamente em relação à época da criação dos certificados e, cada vez mais estão-se adaptando às necessidades de cada órgão/cliente.

Há registros de quebra de chaves ou tentativas de quebra da segurança em transações com certificados digitais? Há estatísticas?

Até hoje não existe nenhum caso de fraude em certificação digital. A tecnologia é bastante forte e robusta, de modo que o nível de segurança das assinaturas eletrônicas possa ser aumentado com o passar dos anos.

Com relação aos sites seguros, como é hoje a situação em empresas públicas? O que levará as empresas em geral a adotarem certificação em seus sites?

Hoje, as empresas públicas já utilizam a certificação digital em seus sites. O principal benefício para elas é a possibilidade de aumento no número de negócios que podem ser feitos eletronicamente com muito mais segurança. Além disso, o cidadão fica satisfeito, pois é atendido de forma muito diferente da que está acostumado nas transações com o governo.

Em geral, o que levará as empresas públicas a adotarem a certificação digital está intrinsecamente ligado à questão da segurança, mas a transparência, a agilidade e a desmaterialização dos processos em papel também serão fatores decisórios para as empresas aderirem ao certificado.

Guydo Rossi

COMÉRCIO ELETRÔNICO

"O impacto da revolução da informação está apenas começando. Mas a forma motriz desse impacto não é a informática, a inteligência artificial, o efeito dos computadores sobre a tomada de decisões ou sobre a elaboração de políticas ou de estratégias. É algo que praticamente ninguém previu nem mesmo falava há 10 ou 15 anos: o comércio eletrônico, o aparecimento explosivo da internet como um canal importante, talvez principal, de distribuição mundial de produtos, serviços e, surpreendentemente, de empregos de nível gerencial. Essa nova realidade está modificando profundamente economias, mercados e estruturas setoriais; os produtos e serviços e seu fluxo; a segmentação, os valores e o comportamento dos consumidores; o mercado de trabalho. O impacto, porém, pode ser ainda maior nas sociedades e nas políticas empresariais e, acima de tudo, na maneira como encaramos o mundo e a nós mesmos dentro dele". As palavras, do "pai da administração moderna", Peter Drucker, de

certa forma dão uma dimensão da realidade e das perspectivas do comércio eletrônico e de outras tantas operações feitas pela internet.

No entanto, os riscos não podem ser desconsiderados e os especialistas alertam para procedimentos simples que podem evitar conseqüências desastrosas. Cristina Hoepers, do CERT.br, adverte para o fato de que "o perigo não está associado à utilização desses serviços em si, mas sim à falta de cuidados de segurança com o próprio computador do usuário. Ou seja, independente de qual serviço usado pela internet, a segurança da transação vai depender da segurança do computador do usuário".

Ela afirma que os bancos e sites de comércio eletrônico, atualmente, já têm implementados diversos mecanismos tecnológicos para dificultar a fraude. "Mas, se o usuário não entender a utilização do mecanismo e não compreender a importância de sua utilização, algum problema ainda pode ocorrer".

O gerente da IBM, Marcelo Bezerra, também comenta o serviço de internet banking: "os bancos investiram muito e continuam a fazê-lo. Promovem também a disseminação de informações alertando seus clientes. É difícil acontecer algum incidente e, nesse caso, o computador utilizado é que certamente está com problema".

Ele explica que o risco pode estar no computador do usuário, da seguinte forma: "se a máquina, a partir da qual você vai fazer a operação, não for bem protegida, há possibilidade de ter problemas. Pode haver programas rastreando números de cartões e senhas. Os bancos estão cientes de que não dá para esperar que o cliente tenha essa segurança e passaram a investir nisso. Usam uma série de recursos, como senhas dinâmicas, cartões de senhas, teclados virtuais que pedem senhas com números e letras, blindagem de software, que dificulta muito, evitando que outras aplicações interfiram neles".

Com relação às compras pela internet, ele recomenda cuidados adicionais: não comprar em lojas totalmente desconhecidas, mesmo que a oferta seja muito boa. "Aliás, se for boa demais, é melhor desconfiar da procedência do produto. Com relação às lojas desconhecidas, checar telefones para comprovar se elas de fato existem, conferir endereço. Há lojas fictícias esperando que alguém caia em seus golpes. Cuidado também com algumas lojas menores que, às vezes, têm seus websites invadidos e passam a disseminar outras invasões".

Marcelo Bezerra ensina: para fazer a compra com tranqüilidade, além de manter o computador atualizado, pesquisar em sites de busca de preços, que mostram pontuação das lojas em relação à qualidade de produtos e atendimento. "O risco reduz bastante, escolhendo bem em que loja comprar. Uma busca na própria internet vai tomar alguns minutos, mas vale a pena. Se ao fazer compras numa loja física as pessoas procuram aquelas mais conhecidas, observam aparência da loja, forma de atendimento do vendedor e mercadoria em exposição, devem fazer o mesmo na compra virtual".

Parcerias internacionais
no combate a incidentes

Criado em 1997 para cuidar da segurança na Rede Nacional de Pesquisa, o Centro de Atendimento a Incidentes de Segurança (Cais) completa uma década com propostas de abertura em sua atuação, buscando contemplar o usuário doméstico, e consolidando uma postura voltada prioritariamente à prevenção de incidentes.

"O que tem mudado na nossa atuação – explica o analista Ronaldo Vasconcelos – é que deixamos de aguardar as notificações e adotamos uma postura de buscar os incidentes. Efetivamos parcerias com comunidades internacionais na área de incidentes de segurança e, com o tempo, passamos a receber notificações do mundo todo e selecionar aquelas que diziam respeito à RNP, como máquinas infectadas. O Cais participa de várias comunidades internacionais, passou de uma atuação passiva a proativa, buscando incidentes novos, monitorando. Nessas comunidades, o que importa é a confiança. Não esperamos que alguém reclame de um spam, mas procuramos identificá-lo e combatê-lo".

Essa postura de prevenção consolidou-se, basicamente, em 2007, com reflexos expressivos nas estatísticas

de registros de incidentes da entidade. “Trata-se de cortar o mal antes que ele se instale”, enfatiza Vasconcelos. Uma das medidas mais importantes é a identificação e combate a botnets, capazes de provocar estragos de grandes dimensões. As chamadas botnets são, na verdade, grandes redes de máquinas infectadas. “Quando a máquina é infectada, torna-se vulnerável e passa a se comunicar com uma máquina central. Nessa rede de bots infectados, cada uma delas é um verdadeiro arsenal de ferramentas; utiliza-se IRC, um tipo de chat mais antigo, entra automaticamente no canal e começa a esperar comandos, podendo infectar até 30 mil máquinas e mandar spams a partir de várias máquinas ao mesmo tempo”.

Cortando a proliferação de botnets e também reduzindo alguns tipos de incidentes, como spams, o Cais tem evitado que a RNP tenha máquinas infectadas e torne-se um vetor de ataque.

Outra linha importante de combate a incidentes é a parceria com outras entidades que trabalham com os mesmos objetivos. Segundo Ronaldo Vasconcelos, há bastante interação entre o Cais e vários grupos, como por exemplo o Forum of Incident Response and Security Teams (First) e do Antiphishing Working Group (APWG). A gerente do Cais, Liliana Solha, faz parte do Comitê Gestor e tem apoiado a criação de grupos no Brasil e outros países da América Latina.

Há também iniciativas hacker positivas no Brasil, a exemplo de outros países, com a realização de conferências. O especialista chama a atenção para o uso do termo hacker, cujo sentido original refere-se à pessoa que gosta de pesquisar softwares na internet, que se interessa por essas questões e que ganhou o sentido pejorativo de criminoso na internet. Segundo ele, nesses eventos normalmente discutem-se problemas de vulnerabilidade, e o Cais tem participado. “O Brasil também tem esse tipo de evento, para discutir tecnologias e, pelo que tenho observado, não têm caráter underground”.

A colaboração entre entidades em todo o mundo é suporte também às atividades do CERT.br. Segundo Cristine Hoepers, “existe uma cooperação muito grande entre os grupos de segurança existentes. Aqui no Brasil, a interação é muito boa, havendo cooperação e troca de informações sobre tecnologias e tendências (lista de grupos brasileiros em: http://www.cert.br/contato-br.html). Do ponto de vista internacional, nós do CERT.br temos uma cooperação grande com outros CERTs com responsabilidade nacional (lista de grupos em: http://www.cert.org/csirts/national/contact.html). Desse modo, podemos atuar como facilitadores no contato entre grupos do Brasil e grupos internacionais, sendo a recíproca verdadeira”.

Ela explica que as comunicações são geralmente sob demanda, ocorrendo quando há um incidente de segurança envolvendo as redes atendidas por um dos grupos. “Em geral, até pelos desafios de fuso horário, a comunicação é toda feita pela internet, por meio de e-mails, que são cifrados, quando necessário”.

Glossário

Termos próprios de segurança da informação e jargões

ADS – Anomaly Detection System

Adware – forma de spyware, seu nome vem da justaposição de duas palavras da língua inglesa: ‘advertisement software’, e identifica um programa, ou parte de um programa de computador, que exibe propagandas, enquanto seu programa hospedeiro, ou aplicação principal, é executado. Veja ‘The Difference Between Adware & Spyware’ em http://www.webopedia.com/DidYouKnow/Internet/2004/spyware.asp.

Ataque de força bruta – uma estratégia de descoberta de senha que tenta todas as combinações possíveis de caracteres alfanuméricos e símbolos especiais. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Backdoors – ponto de entrada oculto que fornece um caminho secreto para o computador de um usuário, o qual é desconhecido do usuário. Usado também pelos programadores que desenvolvem um programa de software,

para que possam entrar no programa para corrigir problemas. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Cavalo de tróia – programa que contém um código malicioso ou prejudicial, criado para gerenciar os arquivos do computador da vítima ou para obter informações do computador ou da rede da vítima. Alguns deles foram criados para se ocultar dentro do sistema operacional do computador e espiar cada tecla digitada ou ação, ou para aceitar instruções por uma conexão de rede para executar alguma função, tudo isso sem que a vítima tenha consciência da sua presença. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Dead drop – lugar para deixar as informações, no qual é pouco provável que sejam encontradas por outras pessoas. No mundo dos espiões tradicionais, isso poderia estar atrás de um tijolo falso na parede; no mundo dos hackers de computadores, é comum haver um site da internet em um país remoto. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Defacement – roubo de dados sigilosos ou de contas.

Freeware ou software gratuito – qualquer programa de computador cuja utilização não implica no pagamento de licenças de uso ou royalties. (http://pt.wikipedia.org/wiki/Freeware)

IDP – Intrusion Detection and Prevention

IDS – Intrusion Detection System – detecção de invasões em rede

IPS – Intrusion Prevention System

ISS – Internet Security Systems

Malware – gíria para software malicioso, um programa de computador, tal como um vírus, um worm ou um Cavalo de Tróia, que executa tarefas prejudiciais. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Mail drop – termo da engenharia social para uma caixa postal alugada, em geral com um nome fictício, usada para o recebimento de documentos ou pacotes que a vítima foi convencida a enviar. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Mulas de dinheiro (do inglês Money Mules) – por trás de uma oportunidade de dinheiro fácil que chega por e-mail, muitas pessoas tentam receber porcentagens por transações. Na maioria dos casos, a vítima fica com a conta do primeiro fraudador para pagar.

Phishing – mensagem falsa que induz a vítima a acessar um site falso, onde se poderá contaminar com um Cavalo de Tróia ou enviar dados pessoais. São aquelas mensagens de recadastramento de bancos, de CPF, etc.

Shareware – uma modalidade de distribuição de software em que você pode copiá-lo, distribuí-lo sem restrições e usá-lo experimentalmente por um determinado período. No entanto, você se coloca no compromisso moral de pagar uma taxa (geralmente pequena em comparação a outros softwares proprietários), caso queira usá-lo sistematicamente. Passado o tempo de avaliação o software pode parar de funcionar, perder algumas funções ou ficar emitindo mensagens incômodas de aviso de prazo de avaliação expirado. (http://pt.wikipedia.org/wiki/Shareware)

SPAM – todo e-mail cujo remetente é inexistente ou falso, o destinatário não autorizou previamente o seu envio, não podendo, inclusive, requerer o não envio. E, ainda, o conteúdo do e-mail não condiz com o cabeçalho da mensagem, não apresentando qualquer classificação ou alerta de que o e-mail é de pesquisa ou marketing.

E-mails comerciais enviados a alguém sem solicitação. Vão para milhares de usuários ao mesmo tempo e congestionam a rede.

Spam zombies – são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bots, vírus e Cavalos de Tróia. Esses códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para envio de spam, sem o conhecimento do usuário. Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também. São muito explorados pelos spammers, por proporcionar o anonimato que tanto os protege. (TI Inside)

Spyware – software especializado usado para monitorar, de modo oculto, as atividades do computador de um alvo. Um dos meios mais comuns dessa prática é usada para controlar os sites visitados pelos compradores da internet, para que os anúncios on-line possam ser adaptados aos seus hábitos de pesquisa na internet. A outra forma análoga é grampear um telefone, só que o dispositivo alvo é um computador. O software captura as atividades do usuário, incluindo as senhas e as teclas digitadas, e-mail, conversas de chat, mensagens instantâneas, todos os sites web visitados e capturas de tela. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Surfar sobre os ombros – o ato de observar uma pessoa digitando no teclado do computador para descobrir e roubar sua senha ou outras informações do usuário.

Threat Intelligence – um pré-requisito para fazer uma análise de risco é conhecer quais são as ameaças – o que está aí fora que pode nos atacar, quão severas são as ameaças, como elas vêm evoluindo, etc. Isso é o que chamamos de Threat Intelligence e é um componente essencial do gerenciamento de riscos de uma organização.

Trojans – Cavalos de Tróia. Os Trojan horses propagam-se quando as pessoas abrem inadvertidamente um programa, porque pensam que a mensagem é proveniente de uma fonte legítima.

Virar latas – vasculhar o lixo de uma empresa (quase sempre em um lixo externo e vulnerável), para encontrar informações descartadas que têm valor ou que fornecem uma ferramenta a ser usada em um ataque de engenharia social, tal como números de telefones internos ou cargos. (*A arte de enganar* – Kevin Mitnick e William L. Simon)

Vírus – é um programa de computador que se replica, utilizando outro programa de computador. No jargão da computação, o vírus, semelhante ao vírus biológico, 'infecta' outro programa, para que se possa propagar pela internet. PC Worm é um programa de computador mais complexo e mais completo que o vírus. Ele, por si só, é capaz de se auto-replicar sem ajuda de qualquer outro programa de computador, já é programado para infectar outros computadores além daquele invadido inicialmente.

Divulgação

A segurança da informação freia ou acelera os negócios?

Marcos Sêmola*

Há quase dez anos publico opiniões relacionadas com a gestão de riscos, continuidade de negócios, governança, conformidade e inteligência competitiva e, desde então, vejo-me às voltas com novas normas, padrões, controles e, conseqüentemente, com o esforço do mercado em identificar os benefícios e os impactos diretos e indiretos dos programas de segurança da informação em seus negócios, bem como em tangibilizar os valores que adicionam e convertê-los em resultado.

Pois quando, finalmente, a segurança da informação deixou de ser um assunto restrito aos porões dos quartéis generais, às oficinas de desenvolvimento de inteligência e contra-inteligência e chegou às salas de reunião da diretoria, à mesa dos auditores, dos administradores e security officers, a confusão já estava formada.

O que nasceu com o propósito legítimo e unidimensional de proteger a confidencialidade das comunicações, foi-se transformando, acompanhando os requerimentos do novo mundo dos negócios e, assim, assumindo múltiplas aplicações e dimensões. A velocidade com que isso vem acontecendo, associada ao entusiasmo dos que querem realizar sem despender muito tempo na prancheta, revisando e revalidando conceitos ou, simplesmente, contrariando-os, a fim de buscar inovações metodológicas, aumenta a confusão.

Infelizmente, muitos dos que hoje, voluntária ou involuntariamente, envolvem-se com a tarefa de "fazer" segurança da informação, não têm uma visão holística de seu legítimo papel. É provável que tenham uma visão correta, porém isolada e focada no problema que está ao alcance de seus olhos e não, necessariamente, uma visão integrada dos riscos inerentes, presentes, residuais e, assim, a real percepção das implicações e das razões para se desenvolver um programa corporativo de segurança da informação. Tudo deveria funcionar como em uma orquestra, onde cada músico domina e sabe exatamente o que fazer com o seu instrumento, mas conta com o maestro que detém a visão do todo e é capaz de coordenar ações isoladas em busca de um resultado único que capture a essência original da obra.

Seria ingênuo pensar que agora o desafio multidimensional de proteger a confidencialidade, integridade e disponibilidade das informações estivesse claro para todos os níveis hierárquicos e em todas as camadas de atividade. Que compreendessem em sua plenitude a importância e os métodos de transmissão de dados, camadas de protocolo, chaves de sessão, algoritmos criptográficos, redes sem fio, sistemas operacionais e todos os seus "sabores", as técnicas de desenvolvimento de aplicações seguras e suas interfaces. E que, além disso,

ainda enxergassem os aspectos físicos, os processos, a segregação de perímetros, os sensores e trilhas de auditoria, a contingência, as políticas e os procedimentos, bem como todas as outras implicações advindas de aspectos humanos, mercadológicos, financeiros e legais que inevitavelmente giram em sua órbita.

Como qualquer outro produto ou serviço de que se tem notícia, a segurança da informação também tem um propósito essencial e este deve estar claro. Para produtos e serviços compostos, como o que ocorre aqui, é preciso compreender o propósito de cada camada de atividade para finalmente conhecer o propósito essencial.

Tomemos como exemplo a instalação de um sistema de backup em uma instituição financeira. Enquanto esta ação tem o propósito de primeiro nível de automatizar a confecção de cópias de segurança para garantir o máximo de disponibilidade da informação diante da perda do meio de armazenamento principal, o segundo nível é o de aumentar a aderência à política de backup da companhia. Este, por sua vez, adere ao propósito de terceiro nível de garantir a conformidade com auditorias setoriais externas, até que, finalmente, toca o propósito essencial de manter o nível adequado de operação do negócio, fazendo-o ser reconhecido como um fornecedor de produtos e serviços de alta qualidade. Seja por sua reputação diante da adoção de melhores práticas ou simplesmente por sua eficácia diante de situações de crise vividas anteriormente, a segurança da informação, de maneira geral, foi o instrumento de valorização do negócio, da marca, e aumentou também a percepção de valor do cliente final.

No mercado em geral e neste caso em particular, a segurança da informação oferece controles que analogamente a um veículo, representam o freio. Contudo, diferente da interpretação inicial que fazemos do freio para um veículo, este não tem o objetivo de impedir que o carro ande mais rápido. Ao contrário disso, a eficiência do freio é justamente a peça-chave para que os engenheiros de motores possam desenvolver veículos ainda mais velozes com a certeza de que estarão prontos para parar eficazmente diante de uma situação de crise. Na prática e sob a ótica dos negócios, possuir mecanismos eficazes de gestão de riscos da informação é justamente estar apto a ousar, a inovar dentro do nível de risco considerado aceitável. É estar mais confiante ao impor velocidades maiores ao negócio, ao diversificar, e oferecer ferramentas e métodos novos de trabalho que, finalmente, suportem o propósito essencial de gerar valor.

"Na prática e sob a ótica dos negócios, possuir mecanismos eficazes de gestão de riscos da informação é justamente estar apto a ousar, a inovar dentro do nível de risco considerado aceitável."

* Marcos Sêmola

Diretor de Operações de Information Risk da Atos Origin em Londres, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor. Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, professor da FGV com especialização em Negociação e Estratégia pela London School, bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Visite www.semola.com.br ou contate marcos@semola.com.br

Divulgação

Iniciativas e importância da segurança da informação e privacidade na saúde

Luis Gustavo Gasparini Kiatake*

A área de saúde está vivendo um momento histórico. O Conselho Federal de Medicina (CFM) acaba de publicar uma resolução que aprova o uso de documentos eletrônicos, permitindo a eliminação do papel. Essa ação deve ser um grande impulsionador para o maior uso das tecnologias de informação e comunicação na área de saúde. Aliás, já era tempo. Nos últimos anos, assistimos a uma tremenda evolução nos equipamentos médicos, mas o papel ainda persistia em ser o principal instrumento de representação dos prontuários, resultando em salas e salas destinadas aos lendários Serviços de Arquivo Médico e Estatística (SAMEs). Bem mais que isso, estando as informações de saúde de uma pessoa no formato digital, outros benefícios podem ser explorados, como a facilidade na comunicação para consultas de segundas opiniões, acompanhamento remoto em procedimentos complexos e até no apoio à tomada de decisões e redução de erros em prescrições. Ou seja, uma notória melhora no atendimento assistencial.

O cenário é muito promissor. Contudo, temos que admitir que é uma grande mudança de paradigma, que muda conceitos e processos. Conceitos, na medida em que, como pacientes, temos, com a internet, acesso a uma avalanche de informações e ferramentas, fazendo com que sejamos muito mais participativos e pró-ativos no tratamento da doença e, mais que isso, na promoção da saúde. Processos, já que não fazemos mais as coisas da mesma forma que antes e temos que aprender, pacientes e profissionais da saúde.

Em se tratando de segurança, do que estamos falando? Existem várias questões que envolvem a segurança da informação, mas as principais tratam da privacidade e da integridade das informações digitais e da identidade dos atores. Essas questões também estão presentes no mundo tradicional, mas no mundo digital ganham proporções muito maiores. Aquela pasta que era guardada e trancada no armário agora está em um servidor, que, potencialmente, pode ser acessado do outro lado do mundo. Só precisamos aprender como funcionam as trancas eletrônicas, ou seja, quem pode abrir, ler, alterar e excluir as informações. E como verificamos, em um arquivo digital, se ele foi ou não adulterado, da mesma forma que um papel escrito a tinta, que não poderia ser apagado sem deixar rastros?

Existem saídas tecnológicas para todas essas questões e vale ressaltar a importância da adoção de padrões nacionais e internacionais, de forma que propiciem interoperabilidade e níveis de qualidade. Nesse sentido, destaco algumas iniciativas em curso.

Uma das principais trata do uso da certificação digital. O Brasil já regulamentou, por meio da Infra-Estrutura de Chaves Públicas do Brasil (ICP-Brasil), as formas de uso e emissão de certificados digitais aos cidadãos, que podem ser usados para autenticação em aplicativos, em substituição ao

tradicional usuário e senha, e para gerar assinaturas digitais, com validade jurídica equivalente à assinatura manuscrita. Com o uso desse instrumento, será possível eliminar o papel. Além disso, também provê condições de verificar a integridade dos documentos assinados digitalmente, e possibilita a criptografia de arquivos, agregando sigilo. Ou seja, com esse instrumento pode-se atuar nos principais pontos de segurança mencionados.

Outra iniciativa está sendo conduzida pela Sociedade Brasileira de Informática em Saúde (SBIS), em convênio com o CFM, para estabelecer um processo de Certificação de Software de Registros Eletrônicos de Saúde. Os aplicativos poderão ser classificados em dois níveis de segurança, sendo que o primeiro avalia se um conjunto de controles básicos de segurança é seguido e, o segundo, obrigatório para programas que dispensarão o suporte em papel, inclui aspectos de certificação digital. O manual de certificação está disponível no site da SBIS (www.sbis.org.br). Vale lembrar que este é referência para uma das principais iniciativas de informatização da saúde que é o padrão para Troca de Informação na Saúde Suplementar (TISS), implantado pela Agência Nacional de Saúde Suplementar (ANS).

Finalmente, um novo e, talvez, o mais importante fórum de discussão e promoção da informatização do setor é a recém-criada Comissão de Estudo Especial em Informática em Saúde (CEEIS), da Associação Brasileira de Normas Técnicas (ABNT). Com suporte do Ministério da Saúde, por meio do Datasus, a comissão tem participado ativamente na International Organization for Standardization (ISO) na elaboração das normas internacionais e publicação de suas versões brasileiras. As questões de segurança e privacidade são discutidas no Grupo de Trabalho 4, específico para esse assunto. Entre os principais trabalhos em curso destacam-se dois: a ISO 27799, que trata da aplicação da ISO/IEC 27002, a principal norma de segurança da informação, especificamente para a área de saúde, e que tem programada a sua publicação no Brasil, tão logo a norma internacional seja publicada; e a ISO 25237, que trata de técnicas de pseudonimização, que visa impedir a possibilidade da identificação de um paciente por meio de seu conjunto de informações de saúde, como aquele contido em um prontuário do paciente, permitindo, contudo, que seja viável uma cobrança financeira a esse paciente.

Não há dúvidas que o uso da tecnologia na área da saúde trará muitos ganhos. Contudo, dada a alta sensibilidade de desse tipo de informação, podemos dizer que a segurança é um fator essencial e que, sem os devidos controles implantados, é melhor manter os processos tradicionais. Não há como pensar em uma situação na qual, sem a expressa autorização de um paciente, uma informação de saúde seja divulgada, seja uma doença, uma consulta, seja um diagnóstico. Esse é um direito dos cidadãos que, se violado, pode acarretar danos morais e até risco de vida, o que faz o assunto da segurança da informação e da privacidade ser discutido tão seriamente pelo setor.

"Não há como pensar em uma situação, na qual, sem a expressa autorização de um paciente, uma informação de saúde seja divulgada, seja uma doença, uma consulta, seja um diagnóstico."

* Luis Gustavo Gasparini Kiatake

Diretor Executivo da E-VAL Tecnologia e pesquisador do Laboratório de Sistemas Integráveis da EPUSP. Colaborador nos comitês ISO/IEC JTC1/SC27 (Information Technology/IT Security Techniques) e ABNT/CB-21/SC-02 (Comitê Brasileiro – Computadores e Processamento de Dados – Segurança). Professor nos cursos de pós-graduação em Segurança da Informação, do SENAC, IPT e EDUCC. Desenvolve seu doutorado na EPUSP, com foco em Comunicação Digital e Segurança de Informação.

Benchmarking

O crescimento do uso das redes, especialmente a internet, e o conseqüente agravamento dos problemas de segurança têm imposto às organizações públicas e privadas a adoção de medidas de prevenção e correção de problemas, que chegam aos seus colaboradores na forma de políticas e programas de segurança da informação.

O valor que a informação tem para o negócio da empresa, assim como sua dependência do uso de redes e a natureza de sua missão, determinam os investimentos direcionados à gestão de riscos e segurança da informação e à estruturação de políticas que orientem não só as equipes de Tecnologia da Informação (TI), mas todos os empregados. Essas políticas priorizam investimentos em ferramentas de última geração ou hardware e segurança física. No entanto, em um ponto, a grande maioria dos gestores dos programas de segurança concorda: o principal suporte de qualquer iniciativa dessa natureza são as pessoas, consideradas os principais atores na criação e consolidação de uma cultura voltada para a segurança.

Nesta edição, a seção Benchmarking mostra como duas organizações de grande porte – a Companhia Energética de Minas Gerais (Cemig), com 11 mil empregados, e a Secretaria da Receita Federal, com mais de 30 mil – conceberam, implantaram e como mantêm seus programas de segurança.

Cemig

Humor na construção de uma cultura de segurança

Investindo maciçamente em segurança da informação, há cerca de oito anos, a Cemig comemora os resultados provenientes de uma nova cultura na organização. Os incidentes estão controlados e o nível de consciência dos empregados sobre sua responsabilidade individual pode ser considerado satisfatório.

Segundo o coordenador da área responsável pela segurança da informação na Empresa – a Administração da Segurança da Informação (ASI), José Luís Brasil, essa nova postura dos empregados foi obtida com muito investimento em capacitação e um trabalho criativo de divulgação, desenvolvido em parceria com a área de comunicação empresarial.

Outro ingrediente dessa receita de sucesso é o humor. Utilizando recursos alternativos, como o teatro interativo e shows de música, empregados e até mesmo seus familiares são envolvidos num ambiente de descontração que valoriza atitudes corretas em toda e qualquer ação que envolva transações via rede, seja ela no trabalho, seja em casa.

Hoje, o programa encontra-se consolidado, com atividades de rotina e inovações que garantem o envolvimento dos empregados. O programa *Em dia com a segurança da informação* é o elemento de sustentação da política de segurança, veiculando informações sobre diversos assuntos ligados ao tema. Enquetes sinalizam novas ações e temas a serem abordados e, com isso, o conteúdo torna-se a cada dia mais consistente.

Atualmente, empregados de municípios do interior demandam visitas, que na medida do possível, são atendidas. “Houve ano em que visitamos 34 municípios, percorrendo mais de 5 mil km”, lembra José Luís Brasil. A usina mais distante, São Simão, a 900 km de Belo Horizonte, recebe também treinamentos presenciais. Brasil acrescenta que as visitas têm um

atributo adicional: “a assimilação das informações é facilitada pela disposição do empregado, que se sente valorizado com a nossa presença. Nós de fato acreditamos que o que faz a diferença são as pessoas”.

História

Desde 1993, a Cemig preocupa-se com a segurança de suas informações. Segundo o coordenador José Luís Brasil, com o mainframe já se adotava a utilização de software de gestão da segurança, ainda de forma centralizada. Em 1996, houve a primeira iniciativa de implantação de uma política de segurança na Empresa, que, no entanto, figurou somente no Manual de Organização da Cemig, entendida como mais uma norma da Empresa. Essa política foi escrita para toda a corporação, não só para a área de TI.

“Naquela época”, lembra Luís Brasil, “nem todo o ambiente de TI operava em rede e a conexão com a internet estava longe de ser como hoje. Os riscos eram, portanto, menores”.

Um problema com o site da Empresa, em 2000, foi o alerta para uma mudança mais orientada. Foi criado um grupo de trabalho formado por um representante de cada gerência de TI, com a missão de planejar a segurança da informação na Empresa. José Luís ressalta que um fator importante, identificado naquele momento, foi a necessidade de uma equipe específica que tivesse foco na questão da segurança de forma corporativa, sem se ocupar das questões operacionais. Ele explica que essa preocupação deveu-se à constatação de que o envolvimento natural dos profissionais com as rotinas operacionais não permitia uma visão mais ampla da questão; “é difícil ver o todo, estando envolvido com detalhes e precisávamos de uma visão corporativa, que pudesse inclusive estabelecer uma relação da segurança com os processos de negócios da Empresa”. Foi criada então a ASI, uma assessoria vinculada à Superintendência de TI.

A primeira iniciativa da nova equipe, formada por três profissionais da própria Cemig, foi elaborar um plano de segurança da informação considerando cinco pilares: análise de risco e vulnerabilidades; políticas; continuidade dos negócios; classificação das informações e conscientização dos usuários.

Isabela Abreu

Lucas Lanna, Ricardo Moleda, Jean Marcelo Oliveira, Arlindo Porto, Marcus Vinícius Belfort e José Luís Brasil

As primeiras etapas, segundo Luís Brasil, foram demoradas; compreendiam levantamentos de necessidades de continuidade e impactos nos negócios. A equipe deparou-se também com a dificuldade de disponibilidade orçamentária.

Enquanto isso, medidas com foco nas pessoas tiveram início já em 2001. “Foram adotadas medidas mais imediatas de conscientização dos usuários. A partir de 2002, tiveram início, ainda timidamente, os treinamentos”.

Luís Brasil ressalta que em todo o processo o foco principal do trabalho da ASI foi na adaptação da cultura da Empresa, na conscientização dos usuários. “Várias enquetes foram feitas pela nossa intranet e revelaram que a maioria dos empregados (97,5%) ignorava a existência da política de segurança; dos 2,5% que sabiam de sua existência, apenas 1,5% a tinha lido. Várias questões foram levantadas nessas enquetes, a fim de sinalizar, para a equipe, os pontos que deveriam ser tratados prioritariamente no trabalho de conscientização”.

A partir daí, em parceria com a equipe de comunicação empresarial da Cemig, tiveram início campanhas que visavam à divulgação de conceitos básicos de segurança da informação, engenharia social e política de segurança. Os empregados foram conhecendo e entendendo a existência e a missão da área criada. Para isso todos os recursos e mídias disponíveis foram e continuam sendo utilizados: quadros de aviso, intranet, eventos, banners, cartilhas e manuais. Todo empregado ou estagiário, ao ingressar na empresa, recebe informações sobre segurança no treinamento introdutório. Há treinamento específico também para a equipe de teleatendimento, capacitando-a para as demandas das áreas.

Luís Brasil explica que o planejamento das capacitações considerou um fato importante: a grande dispersão da Empresa em todo o Estado. “Como podíamos estar juntos a todos os empregados? A Cemig tem sete regionais: Centro (em Belo Horizonte), Triângulo, Sul, Mantiqueira, Norte, Oeste e Leste. Pensávamos que esse trabalho deveria ser algo interessante, diferente”. Foi contratado, então, o grupo de teatro empresarial Grafite, de Belo Horizonte, que criou roteiros personalizados com base nos temas fornecidos pela equipe da ASI. “Eles desenvolviam roteiros específicos e faziam uma apresentação prévia para nossa aprovação ou para adequações”.

Segundo Luís, houve uma receptividade muito boa. “O treinamento era composto de palestras e das peças de teatro, que representavam cenas dos conteúdos abordados nas palestras. Reforçaram, dessa forma, conceitos de segurança da informação, engenharia social e políticas de segurança. A duração era de meio expediente e acontecia em ambientes da Cemig, com um custo médio de R$40,00 por empregado”.

“Nunca utilizamos imagens como cadeados, que remetem à exclusão, enfatizando, ao contrário, a segurança da informação com abordagem de inclusão; nunca como policiamento”, ensina o coordenador do programa. Nenhum dos treinamentos é obrigatório.

Com esse roteiro, chegaram a treinar 1.500 pessoas em um ano. “Cada vez mais procurávamos a inovação, sempre resguardando a preocupação de proporcionar um treinamento agradável, com brindes, jogos, brincadeiras e o teatro. Sai barato para a empresa”, garante.

Dos primeiros sinais de mudanças de cultura para uma atitude pró-ativa, foi uma “guinada”, explica Brasil. “Em 2005, cerca de quatro anos depois do início do trabalho, os empregados começaram a solicitar informações e capacitações. Quando divulgamos o calendário do ano, empregados de cidades que não estão contempladas reclamam. Nós priorizamos aquelas com maior número de empregados e em centros de fácil acesso para cidades próximas, mas tentamos ir também nas demais”.

Os conteúdos de palestras e treinamentos são desenvolvidos pela própria equipe, privilegiando as imagens. “Percebemos que demonstrar a importância da segurança da informação para o empregado, seja na Empresa ou na sua própria residência, era mais eficaz do que mostrar apenas a visão da Empresa; foi por onde começou a mudar o comportamento”.

A política

Para o lançamento da política de segurança da Empresa, em 2005, a equipe manteve-se fiel à preocupação em oferecer algo diferente, “não podia ser algo convencional, tinha que ser diferente e agradável”, lembra Brasil.

O lançamento foi considerado pelos organizadores motivo de festa. A política é estruturada em Diretrizes (conteúdos-macro) e Instruções de procedimentos corporativas e restritas à área de TI. Seu objetivo é regulamentar o processo e servir de orientação e referência para todos os usuários da Empresa.

O lançamento foi realizado no auditório da Cemig, com exibição de filme institucional. A surpresa foi a palestra do ator e produtor artístico Haroldo Costa, que mostrou como uma escola de samba prepara-se para um desfile importante, ressaltando o valor da participação individual, das contingências e do sigilo das informações, para que tudo dê certo. Após a palestra, uma escola de samba apresentou-se para os presentes, com sambistas, passistas, bateria e muita animação.

Em 2006, a ASI cresceu e hoje tem seis pessoas: José Luís Brasil, Arlindo Porto, Marcus Vinícius Belfort, Jean Marcelo Oliveira, Ricardo Moleda e Lucas Lanna. Em 2007, o programa de conscientização foi estendido aos filhos dos empregados. “A percepção de que a questão ia além do local de trabalho foi sinalizada pelos próprios empregados, durante os treinamentos”, explica Luís Brasil. Em novembro de 2007, foi feito um piloto em Belo Horizonte, com 108 filhos de empregados com idade entre 12 e 16 anos. “Reunimos a garotada num sábado pela manhã para palestra da advogada Patrícia Peck, especialista em direito digital. Ela falou sobre

os perigos da internet e cuidados que devem ter em suas comunicações pela rede. Foram distribuídos brindes e uma cartilha com dicas para evitar 'pagar mico' na rede e exibido filme sobre utilização da internet, além de cinco cenas de teatro, escolhidas pela platéia. A programação foi encerrada com a apresentação de um show de rock, pelo grupo Tchai, que movimentou a meninada".

Treinamento on-line e classificação

Outra frente de ação é o treinamento on-line sobre a nova política disponível para todos os empregados. "Todos tiveram o direito de fazer", explica Luís Brasil. Cerca de 85% dos empregados já foram treinados em um ano e meio, contemplando todas as diretorias da Cemig. Os gerentes das diversas áreas acompanhavam a situação de suas respectivas equipes por meio de relatórios semanais e podiam, assim, estimular a participação dos empregados. A avaliação desses treinamentos permitiu aferir resultados e prover a ASI de informações para novas iniciativas.

Foi feita também pesquisa com empregados para avaliar o grau de assimilação das informações, o que norteou o planejamento da divulgação da Política de Segurança. Foram eleitos 14 temas e quinzenalmente um deles é destaque, com suas respectivas instruções, no programa *Em dia com a segurança da informação*.

Outra etapa importante do programa de segurança da Cemig foi a classificação das informações, considerada, pelos especialistas, uma das mais importantes em um programa de segurança. "Trata-se de identificar as informações mais importantes para o negócio da empresa e classificá-las, de acordo com seu grau de sigilo, a fim de organizar e priorizar ações diferenciadas para aquelas consideradas mais críticas", esclarece o coordenador.

Trata-se de uma ação complexa, que foi coordenada pela ASI e desenvolvida pelos próprios empregados. Para isso, foi criada uma metodologia para identificação das informações que deveriam ser classificadas. Mais de 200 pessoas foram capacitadas nessa metodologia. Cada área fez a classificação e tratamento das suas informações, num prazo de 30 dias. A capacitação para multiplicar informações sobre como classificar as informações contemplou 430 pessoas. O trabalho foi feito em Belo Horizonte e também no interior.

Nessa etapa do programa foi utilizado o recurso do teatro, apresentado em todos os andares do prédio, no hall dos elevadores, em Belo Horizonte. A informação sobre a classificação de cada informação da Cemig está disponível para todos os empregados em um portal específico. Brevemente, será lançado um game com 100 perguntas cadastradas que, randomicamente serão sorteadas. "É um jogo on-line", explica Brasil. Esse jogo também será referência para o planejamento de medidas da ASI, com base nos resultados.

Outra medida em andamento pela equipe é a definição da análise de vulnerabilidades, que permitirá a interligação da gestão de processos, pessoas e ferramentas. "Já podemos determinar índices de risco, temos indicadores definidos para isso. Estamos tratando e minimizando os riscos", afirma Luís Brasil.

Alinhamento com os negócios

Para 2008, a equipe da ASI vai priorizar a implementação de medidas de segurança que estejam alinhadas com as necessidades dos negócios da Empresa, levantando e avaliando a dependência que cada processo de negócio tem das tecnologias da informação e comunicação. O objetivo é definir, com base nos processos prioritários, medidas capazes de assegurar que os sistemas e rotinas de TI estejam de fato de acordo com as necessidades de confidencialidade, integridade e disponibilidade dos negócios da empresa.

Divulgação

Capacitação utiliza recursos lúdicos

Receita Federal

Certificação digital
é a chave da segurança

Divulgação Receita Federal

Donizette Victor Rodrigues

Antes mesmo da oferta de informações e serviços pela internet, a Receita Federal já adotava procedimentos para segurança de suas informações, desde 1994. O coordenador-adjunto de Tecnologia da Informação da Receita, Donizette Victor Rodrigues, lembra que no início as medidas eram ainda incipientes, uma vez que os riscos e preocupações eram também pequenos. “Os sistemas eram basicamente em mainframe, não havia muito perigo”, lembra.

Em 1995, a entidade passou a instalar e a utilizar redes locais, adotando microcomputadores, servidores e intensificando, ao mesmo tempo, o uso da internet, o que levou a uma preocupação maior com a segurança das informações. É dessa época a oferta das primeiras informações para os usuários na internet, em uma seção do site do Ministério da Fazenda, uma vez que a Receita ainda não tinha seu próprio site.

A criação da homepage da entidade, em 1996, ainda no site do Ministério da Fazenda, foi um importante passo para uma ação mais consistente de oferta de informações e serviços. A primeira homepage trazia informações para o preenchimento da declaração do imposto de renda e, pela primeira vez, o download do programa gerador da declaração, que até o ano anterior só estava disponível em disquete.

Ainda em 1996, no segundo semestre, foi criado o site da receita – www.receita.fazenda.gov.br – que veio acompanhado de medidas mais dirigidas à segurança da informação: são dessa época as primeiras normas e regulamentos relativos a acesso a sistemas, redes, correio eletrônico e internet. Segundo Donizette Rodrigues, a primeira política de segurança foi escrita nessa época e vem evoluindo e sendo aprimorada até hoje.

Certificados digitais

A grande aceitação dos serviços via internet e o crescimento dos acessos impuseram novas necessidades de tratamento dos riscos. O coordenador lembra que, na Receita Federal, uma importante evolução foi a adoção de certificados digitais, tanto para segurança interna, no acesso a sistemas, quanto no relacionamento com os contribuintes. Ele explica que “sites com serviços mais sensíveis, que envolvem sigilo fiscal, existem desde 2001 e a certificação digital é a garantia de proporcionar a mesma segurança que os contribuintes têm nas ações feitas de forma presencial”. Ele enfatiza que essa segurança tem viabilizado a pesquisa e a identificação constantes de novos serviços via internet. “A garantia de autoria, autenticidade, não repúdio, deu um impulso muito grande ao uso dessa tecnologia”, afirma.

A certificação digital é a chave para funcionamento do Centro Virtual de Atendimento ao Contribuinte (e-CAC), onde as pessoas podem executar, via internet, diversas operações, inclusive algumas protegidas pelo sigilo fiscal. Consulta a cadastros, alteração e retificação de dados, emissão de comprovantes, parcelamento de débitos e transações relativas ao Siscomex são alguns serviços disponíveis.

Exemplo dessa aceitação é a adesão de representantes das prefeituras municipais de todo o País para acesso às informações do Simples, com uso de certificados digitais. Segundo o coordenador, a adesão foi mais fácil do que o esperado. “Eles precisam das informações, não foi difícil; mais de 5.600 municípios já usam a certificação digital”.

Na Receita Federal, todos os funcionários utilizam, hoje, certificados digitais para controle de acesso a sistemas, totalizando 37 mil pessoas, no Brasil. Donizette considera a tecnologia um marco no processo de segurança da informação no órgão. Antes, os acessos eram controlados da forma tradicional, com usuário e senha e já há pesquisas para avanços no uso de ferramentas mais sofisticadas de segurança, como por exemplo, a biometria. Segundo ele, nos relacionamentos externos com os contribuintes, a certificação digital tem atendido de forma satisfatória.

Para suportar o volume de informações de forma segura, a área de TI adota um conjunto de ferramentas bastante avançadas de segurança, de transmissão e de recepção. “É algo sempre em evolução. O Receitanet, por exemplo, tem sempre novas versões”. Donizette afirma que essas proteções garantem, de fato, a integridade das informações: “a proteção e as garantias são muito grandes. Não temos ocorrências dignas de nota”.

Outro investimento importante é para a disponibilidade dos serviços, especialmente em infra-estrutura nos períodos de pico: “nossa estrutura é bastante escalável, nossos servidores priorizam aplicações para não haver impacto. Há esquema de dedicação quase exclusiva na época de pico. Nunca houve problema de congestionamento; pode haver problemas fora da Receita”, garante.

O coordenador adverte para a necessidade de obter equilíbrio entre os custos e os benefícios dessas inovações: “segurança da informação é algo em que se tem que pesar, também, o custo, buscando, naturalmente, o nível máximo de segurança, disponibilidade e facilidade de uso”.

Estrutura

O gerenciamento das ações de segurança da Receita está centralizado em Brasília, onde atua a coordenação de TI, com uma divisão de segurança da informação. Essa área é responsável pela normatização e disseminação das informações. Nas regionais, em todo o País, também existem divisões de TI. Cada unidade conta com estrutura própria, para supervisão geral da legislação e implantação.

Com quase dez anos de experiência com o tratamento e tráfego de informações sigilosas, Donizette aponta o elemento humano como um dos fatores mais importantes do processo: ele considera a cultura organizacional para segurança, na Receita, bastante sólida hoje. “Houve um trabalho intenso ao longo dos anos com foco na conscientização dos colaboradores com relação aos cuidados com segurança”, explica.

Os funcionários foram exaustivamente informados sobre o conceito e os riscos da engenharia social, por meio de campanhas de conscientização e disseminação e a publicação do Manual Institucional de Segurança, que contempla todos os aspectos relacionados ao tema, como software, engenharia social, controles de acesso. A Receita mantém ainda campanha permanente da intranet. “Hoje, o nível de consciência para TI é bastante alto, todos têm uma preocupação muito grande com a segurança. É um trabalho que não acaba nunca, não se pode dar trégua: são cartazes, alertas, palestras, filmes – é um trabalho permanente”. Donizette ressalta que “o mais importante é o trabalho com as pessoas, as normas por si só não fazem nada acontecer. Depende das pessoas, de um trabalho de divulgação, de conscientização”.

A entidade mantém, ainda, iniciativas relacionadas com a pesquisa em tecnologias existentes no mercado, por meio de uma divisão de prospecção, que procura novidades na área de software; “estamos sempre pesquisando, procurando novas idéias que possamos adotar, para melhorar cada vez mais. É um trabalho constante”.

Claudia Guerra

Informação sobre saúde na web

Isa Maria Freire*

Devemos aprender a aplicar critérios de qualidade nas informações sobre saúde disponíveis na web.

Quando a web se instalou, em meados da década de 90, milhões de usuários levaram suas inovações sociais para a rede e deram contribuição decisiva para a configuração e evolução da internet, especialmente na formação de comunidades virtuais e no estabelecimento dos valores de uma cibercultura.

O cenário do ciberespaço foi construído a partir das tecnologias digitais de informação e comunicação criadas no início dos anos 80, que, com a web, se tornaram um fenômeno econômico e cultural. Com base na cooperação 'anarquista' de milhares de centros informatizados no mundo, a internet tornou-se o símbolo de uma ferramenta social indispensável no cotidiano profissional e pessoal.

É nesse sentido que Manoel Castells fala da "sociedade em rede" e Pierre Lévy anuncia que estamos vivendo um momento histórico raro, "em que uma civilização inventa a si própria, deliberadamente". Seria o caso da ocorrência, aqui e agora, de um "fenômeno de alta cultura", que o historiador Giorgio Di Santillana explica como um salto quântico na cultura de uma civilização. No ocidente, dois fenômenos anteriores à emergência do ciberespaço são identificados no período da invenção das tecnologias da escrita e, depois, da imprensa. Agora, trata-se da nova relevância de um fenômeno antigo, a informação, desta vez viajando nos meios digitais de comunicação.

Os números são esclarecedores: aos milhões de usuários da internet, do século 20, somaram-se mais de 1,1 bilhão de usuários até 2007, que buscam, nos mais de 125 milhões de sites e 70 milhões de blogs, informações relevantes para diminuir a incerteza em face dos problemas do cotidiano. Um dos temas recorrentes dessa oferta de informações na web é a saúde, coletiva e individual.

Uma busca simples no Google com o termo saúde tem como resultado 132 milhões de links, elos para ligação com fontes de informação sobre saúde. E mesmo que o tema seja especificado, como em "saúde coletiva", o resultado ultrapassa 318 mil links disponíveis. Como selecionar uma fonte relevante e confiável, nesse mar de informações? Ademais, além de um direito social, a saúde é um bem pessoal e intransferível, que recebemos da vida e nos compete cuidar e preservar. É aqui que a noção de "segurança da informação" se introduz.

As informações sobre saúde têm como público-alvo profissionais e pesquisadores da área, estudantes e pacientes, além da população em geral. Quando disponibilizadas em sites de instituições de ensino e pesquisa, organizações da sociedade civil ou bases de dados de teses e dissertações acadêmicas e revistas científicas, as informações podem ser consideradas confiáveis, embora no último caso, muitas vezes, seja exigido o pagamento de uma assinatura. A questão da segurança impõe-se, quando se trata da informação dirigida à população em geral, à comunidade de usuários leigos que têm direito à informação que diminua a incerteza sobre problemas de saúde.

Sales e Toutain pesquisaram critérios de avaliação da informação em saúde na web, identificando "credibilidade, apresentação formal do site, links, design, interatividade e anúncios" como categorias recomendadas pela Agency for Health Care Policy and Research, do Health Information Technology Institute (Hiti). Para a Health On the Net (HON) Foundation, as categorias são "autoridade, complementaridade, confidencialidade, atribuições, justificativas, transparência na propriedade, transparência do patrocínio e honestidade da publicação e da política editorial". No Brasil, o Conselho Regional de Medicina de São Paulo propõe como critérios "transparência, honestidade, qualidade, consentimento livre e esclarecido, privacidade ética médica, responsabilidade e procedência", além de outros aspectos semelhantes aos propostos pelo Hiti e da HON Foundation.

Em artigo onde resume sua tese de doutorado, Lopes oferece um quadro com links para acesso a instituições que desenvolveram ckecklists para avaliação de sites sobre saúde na web. A autora também nos informa que o Centro de Vigilância Sanitária do Governo do Estado de São Paulo traduziu e adaptou o Guia Para Encontrar Informações Seguras produzido pela Organização Mundial da Saúde. Nesse Guia, são indicadas as questões que devem nortear os usuários na busca de informação relevante e confiável:

- Há indicações claras do nome e endereço do proprietário do site?
- Há alguma instituição responsável?
- Há indicação de patrocinadores?
- Há indicações claras sobre o propósito do site?
- Qual a data da publicação da informação?
- Instituições reconhecidamente qualificadas apóiam a publicação da informação?
- Se for o caso de resultado de pesquisa, há menção a testes clínicos?
- No caso de produtos novos, estes foram registrados e aprovados no país de origem?

No Brasil, o Comitê Executivo do Governo Eletrônico estabeleceu regras e diretrizes para sites na Administração Pública Federal, enfatizando como critérios, além da validação científica, a clareza, simplicidade, objetividade e organicidade da informação. Em 2006, foi apresentado projeto no Congresso Nacional sobre as responsabilidades associadas à produção e comunicação de informações sobre saúde em sítios e portais da internet.

Parece muito, mas, quando se trata de garantir a segurança da informação sobre saúde, ainda é muito pouco. A parte mais difícil, entretanto, será feita pelos usuários, no cotidiano anônimo, quando buscar informações na internet: adotar como norma a avaliação das fontes, como proposto pelas instituições nacionais e internacionais, não confiar apenas nos discursos e não esquecer os critérios de segurança.

"Em 2006, foi apresentado projeto no Congresso Nacional sobre as responsabilidades associadas à produção e comunicação de informações sobre saúde em sítios e portais da internet."

De modo que a informação na web represente, realmente, a diminuição da incerteza para um dado usuário e, no caso da saúde, propicie um caminho para o conhecimento e a cura.

* Isa Maria Freire
Doutora em Ciência da Informação
Líder do Grupo de Pesquisa Informação e Inclusão Social do IBICT (Instituto Brasileiro de Informação em Ciência e Tecnologia)
www.isafreire.pro.br

1 LEVY, P. A inteligência coletiva: por uma antropologia do ciberespaço. 3ed. São Paulo: Ed. Loyola, 2000.
2 Dados em O Globo, 27 ago. 2007.
3 SALES, A.L.C.; TOUTAIN, L.B.. Aspectos que norteiam a avaliação da qualidade da informação em saúde na era da sociedade digital. Anais. Salvador: Cinform, 2005. Disponível em: http://www.cinform.ufba.br/vi_anais/docs/AnaLidiaSales.pdf. Acesso em 6 dez. 2007.
4 LOPES, Ilza Leite. Estudos sobre qualidade da informação sobre saúde na Web e a visão de entidades de classe brasileiras. Tempus – Actas de Saúde Coletiva, v.1, n.1, 2007. Disponível em: http://164.41.105.3/portalnesp/ojs-2.1.1/index.php/tempus/article/view/398/381. Acesso em 6 dez. 2007.

Divulgação

A chave da segurança
está no treinamento

Erasmo Borja Sobrinho*

A internet no mundo globalizado é como uma árvore plantada junto a um ribeiro. Não lhe faltam nutrientes e seu crescimento é vertiginoso. Proporcionalmente, crescem os meios de usá-la de forma escusa. A segurança tornou-se fundamental. Segurança de rede não é mais algo estático, é dinâmico. Não existe hoje solução que preveja o futuro. No passado, a solução estava em procedimentos ou em simples prevenções contra vírus. Hoje, não há "solução vencedora". Tudo requer evolução e acompanhamento constantes.

Os agentes do mal não param de evoluir. O que antes era brincadeira, hoje virou negócio. A espionagem e os negócios escusos, com base em TI, são hoje rentáveis. Tem gente faturando com isto. Não é só com transferência de valores de contas bancárias invadidas que os criminosos virtuais estão ganhando dinheiro. Estes são os que a mídia mais veicula, por serem mais compreensíveis ao grande público. Existem várias empresas sendo atacadas por gente paga para fazê-lo. Por isso o outro lado também precisa de pessoal em evolução, por dentro das novidades, infiltrado nas comunidades de hackers, que entenda o pensamento do inimigo.

Boas ferramentas são fundamentais nessa guerra e precisam ser flexíveis. Por exemplo: dar segurança com todas as portas fechadas, não resolve. É como construir um bunker para proteger uma pessoa importante. Quando esta precisar entrar e sair desse bunker, os pontos fracos serão expostos. Na rede corporativa é a mesma coisa. A empresa precisa de acesso à internet em mão dupla. Tanto seus colaboradores precisam acessá-la dentro da empresa, quanto seus funcionários e clientes precisam de acesso a informações e serviços via internet, fora dela.

Existem empresas, até do Primeiro Mundo, que ainda têm rede interna separada da rede que tem ligação com a internet, por receio de roubo de dados estratégicos. Imagino quantos negócios estão sendo perdidos, porque seus executivos não podem acessar informações estando fora da empresa. Enquanto o concorrente soluciona o problema em minutos, o funcionário da empresa X tem que ligar para a matriz e pedir ao setor de engenharia para analisar a questão, usando a rede interna, e enviar uma solução por e-mail ou fax. Parece piada, mas funciona assim.

No mundo de hoje, empresas com essa mentalidade estão fadadas a fechar suas portas, engolidas pela concorrência. A solução está nas ações coordenadas com treinamento dos usuários, para que tenham procedimentos seguros dentro da rede. Ferramentas são fundamentais, como as portas de nossas casas. Têm que ter fechaduras e precisam estar trancadas, mas se cada um que entrar não tornar a trancá-las, em algum momento a casa estará vulnerável.

O treinamento não é simples. Não se padroniza o usuário. Enquanto uns têm acesso limitado, outros, em pontos superiores na escala de poder, têm acesso quase irrestrito. Enquanto uns estão bem acostumados aos recursos disponíveis, outros não têm o mínimo conhecimento e, muitas vezes, estão no topo da hierarquia.

As regras para a presidência são permissivas e, na maioria das vezes, é onde estão os usuários menos preparados. Via de regra, desprezam treinamentos. Não que os achem desnecessários ou menos importantes, mas por não terem tempo a "perder" com esses treinamentos.

O correio eletrônico, hoje, fonte da maioria das falhas de segurança, exige filtros cada vez mais complexos, capazes de distinguir as mensagens úteis das inúteis e, às vezes, perigosas. Barrar somente os famigerados spams não basta. Os filtros modernos têm que entender toda a estratégia de quem quer passar por eles e fechar as alternativas quase em tempo real.

Quem não quer se arriscar, não deve enviar e nem receber e-mails. Esta não é mais uma opção viável. Sem comunicação o profissional e a empresa não existem. As ferramentas mais uma vez requerem treinamento. Filtros podem barrar mensagens importantes simplesmente porque contêm alguma característica que as torna parecidas com um spam ou com um worm. Não será mais o setor de TI que irá vasculhar o lixo de cada usuário para procurar um falso positivo (mensagem barrada indevidamente nos filtros de correio). O usuário tem que saber acessar as ferramentas, para recuperar suas próprias mensagens.

O usuário que vai ter acesso à abertura de mensagens de risco tem que estar treinado, tem que saber o que faz, tem que identificar quando está recebendo um arquivo de risco. Não é porque o e-mail vem de um amigo, que a mensagem não tem risco. Os amigos também podem ser vítimas de pessoas que os usam para enviar mensagens perigosas. Talvez ele nem saiba disso. Sua máquina pode ter sido invadida e passar a ser um ponto de envio de spam.

Sem treinamento, o usuário pode não saber que algumas condutas são consideradas inadequadas, com relação a um código de ética que se estabelece no uso da internet. Com isso, causam problemas que acabam trazendo prejuízos para a instituição onde ele trabalha. Um simples e-mail respondido com letras maiúsculas pode ofender o destinatário, por exemplo.

O treinamento não pára no usuário final. O profissional de TI, no uso de cada ferramenta, precisa estar atento às opções no uso de cada programa, mesmo que o serviço de segurança seja terceirizado. Deve seguir as recomendações da empresa contratada. Sua atuação é fundamental para adequar as instruções à realidade da empresa e às peculiaridades de sua rede interna.

Terceirização, este é outro ponto importante em segurança. Até onde é seguro passar o controle a terceiros? Está cada vez mais difícil manter profissionais de TI atualizados com o que acontece no mundo da segurança de rede. Isto está-se tornando "assunto para especialistas". Uma empresa dedicada a essa tarefa tem equipe que trabalha só com segurança e pode replicar as atualizações e novidades a toda a sua base de clientes instantaneamente. Este nível de entendimento requer dedicação e competência. Dessa forma, os serviços de segurança deixam o setor de TI mais tranqüilo quanto às atualizações e novidades constantes. O treinamento da equipe encarregada, neste caso, pode ser focado na ferramenta escolhida e na estratégia de adequá-la ao objetivo da empresa.

"A SOLUÇÃO ESTÁ nas ações coordenadas com treinamento dos usuários, para que tenham procedimentos seguros dentro da rede."

Portanto, seja qual for o nível de envolvimento do usuário com o sistema, o treinamento passou a ser ponto fundamental para garantir a segurança.

* Erasmo Borja Sobrinho
Engenheiro Mecânico pela UFMG. Especialização em Engenharia Econômica – FDC. Sócio /Diretor da NetSol. Diretor da Assespro MG. Professor Titular na Universidade FUMEC.

Divulgação

Wireless LAN para ambiente corporativo: muito além de extinguir o cabo azul

Vitório Urashima*

A rápida diminuição de custo de concentradores e placas de rede sem fio – access points e wireless adapters, respectivamente, sendo que estas últimas já vêm integradas nos notebooks de ponta – tornou o uso de wireless LAN popular também no ambiente corporativo.

Entretanto, adotar wireless nas empresas vai muito além de extinguir o cabo azul que liga o ponto de rede ao notebook. O ambiente corporativo exige a solução de vários desafios antes de o acesso wireless ser utilizado de modo que proporcione uma verdadeira vantagem competitiva para as empresas. Para se ter idéia dos principais problemas, serão listados seis deles:

1. redes wireless isoladas e não gerenciadas com múltiplas configurações são difíceis de suportar;
2. o padrão mais utilizado, o 802.11 b/g, possui somente três canais de rádio disponíveis não sobrepostos e utiliza freqüências já congestionadas perto de 2.4 GHz, junto com telefones sem fio, celulares, bluetooth, etc.;
3. usuários podem montar redes wireless de compartilhamento em configuração *ad hoc* (conexões diretas entre estações) sem autorização e, provavelmente, sem proteção;
4. a instalação de access points de uso doméstico sem autorização da empresa também é comum. Este tipo de instalação geralmente é realizado com as configurações padrão de fábrica, que têm pouca ou nenhuma segurança de autenticação de usuários ou criptografia de dados;
5. a segurança WEP (wired equivalent privacy), utilizada inicialmente para proteger as redes wireless LAN, não é mais considerada segura. Já é possível, utilizando ferramentas disponíveis na internet, descobrir a chave de criptografia WEP, após a coleta de cerca de 1 milhão de pacotes. Isto equivale, em uma rede com alto tráfego, a aproximadamente 17 minutos de atividade;
6. o uso de wireless em ambientes dinâmicos – alterações na quantidade de usuários ao longo do dia, alterações em posições de obstáculos como máquinas, estoques de peças e até pessoas transitando – muda o ambiente de RF e cria áreas de sombra ou de interferência não previstas inicialmente.

Unified Wireless Network

Para solucionar estes problemas, empresas têm adotado a unified wireless network, cuja tradução é rede sem fio unificada. Controladores wireless concentram as informações dos access points. Os controladores, por sua vez, são agregados por meio de software de gerenciamento em servidores ou appliances dedicados. Dessa forma, há gerenciamento único valendo-se de interfaces gráficas e inteligência que indica a melhor configuração para cada caso. Em suma: a solução une o alcance e a flexibilidade que as redes sem fio oferecem sem abrir

mão do gerenciamento e da segurança necessários ao ambiente corporativo.

Com a unified wireless network, há possibilidade de criar templates de configuração e atualização de firmware centralizados e enviados automaticamente para os concentradores, desfrutando das últimas inovações disponibilizadas pelo fabricante.

O gerenciamento da rede RF, ativado com o uso dos controladores wireless, permite a reconfiguração de canais utilizados, níveis de potência, taxas de transmissão e tipo de modulação do sinal (maior alcance ou melhor confiabilidade para oferecer o melhor throughput). Com isso, pode-se melhorar a cobertura de acordo com as mudanças do ambiente, como falha em um dos APs ou mudanças no layout. Tudo isto de forma consistente e automática. Os cálculos das diversas configurações possíveis e escolha das melhores práticas são feitos pelo software de gerenciamento.

Outra vantagem que a centralização das informações da rede RF permite é a implementação de soluções de localização de dispositivos wireless, que podem ser APs não autorizados, notebooks, coletores de dados e, mais recentemente, tags wireless. Os softwares de gerenciamento permitem também a representação gráfica das áreas de cobertura e localização dos dispositivos wireless em mapas com precisão de metros. Soluções de localização que utilizam tags permitem o rastreamento e controle de ativos preciosos de qualquer tipo. Basta associar um tag ao dispositivo que se quer controlar e monitorá-lo pelo software de gerenciamento.

Em termos de segurança e disponibilidade do ambiente wireless, podemos citar as seguintes inovações:

- adoção de esquemas de segurança de dados com chaves dinâmicas (se forem quebradas, já terão sido mudadas);
- zero configuration deployment: impede a utilização, se um AP for roubado;
- detecção e contenção de APs não autorizados;
- IDS/IPS para detecção e prevenção contra ataques de rede wireless;
- load balancing entre APs;
- fast roaming transparente entre células para voice over wireless LAN;
- adaptação dinâmica de RF para melhor cobertura.

Com gerenciamento e segurança, vale a pena

Graças à flexibilidade de acesso aos dados de qualquer lugar, o wireless representa um salto na produtividade de nossas equipes. Dados da rede podem ser acessados em salas de reuniões, e-mails podem ser lidos e respondidos de qualquer lugar e não existe mais a necessidade de o usuário estar em sua mesa de trabalho para acessar as informações.

Parceiros também podem utilizar a rede wireless como visitantes, de forma segura e controlada, e consultar intranets e extranets para obter, por exemplo, novos descontos, consultar posições de entrega, resgatar documentos, requisitar ações imediatas em vez de acumular pendências, para quando voltarem para suas sedes.

"OS SOFTWARES DE gerenciamento permitem também a representação gráfica das áreas de cobertura e localização dos dispositivos wireless em mapas com precisão de metros"

Telefones wireless podem ser ramais que acompanham o usuário até o ambiente de fábrica ou depósito sem problemas de alcance ou degradação da qualidade da voz. Enfim, as soluções de wireless LAN têm muito a oferecer, mas devem ser disponibilizadas no ambiente corporativo de forma segura, gerenciada, centralizada e com escalabilidade.

Não devemos perder tempo e recursos nos prendendo a redes wireless voltadas para uso doméstico. Elas podem ser muito atrativas em um primeiro momento, devido ao baixo custo de aquisição, mas, em ambientes maiores, geram um alto custo de operação e restrição ao crescimento. Planejando de forma correta, estaremos criando um ambiente propício ao desenvolvimento das pessoas e dos negócios.

* Vitório Urashima
Engenheiro eletrônico pelo Instituto Tecnológico de Aeronáutica. Especialista em Networking e Segurança Digital da Tecnoset IT Solutions.

A segurança da informação em artigos acadêmicos inéditos, com abordagem de aspectos tecnológicos, legais e sociais. Experiências na área pública, as relações trabalhistas, os riscos para indivíduos e organizações.

Divulgação

Algumas recomendações para um modelo de governança da segurança da informação

Mauro César Bernardes

Doutor em Computação pela Universidade de São Paulo (ICMC/USP 2005). Atualmente, é diretor de divisão tecnológica no Centro de Computação Eletrônica da USP (CCE/USP) e professor no Centro Universitário Radial (UniRadial), atuando na área de Segurança da Informação e Governança de TIC.

RESUMO

Este artigo apresenta um conjunto de recomendações para o desenvolvimento de um modelo que permitirá, aos administradores de uma organização, a incorporação da governança da segurança da informação, como parte do seu processo de governança organizacional. A partir da utilização desse modelo, pretende-se que o conhecimento sobre os riscos relacionados com a infra-estrutura de Tecnologia da Informação e Comunicação (TIC) seja apresentado de forma objetiva ao conselho administrativo, ao longo do desenvolvimento de seu planejamento estratégico. Uma revisão de literatura, sobre governança de TIC, foi realizada para a identificação de modelos que pudessem oferecer contribuições.

1. Governança de Tecnologia da Informação e Comunicação

A informação é reconhecida pelas organizações nos últimos anos como sendo um importante recurso estratégico, que necessita ser gerenciado (Weill & Ross, 2004). Os sistemas e os serviços de Tecnologia da Informação e Comunicação (TIC) desempenham um papel vital na coleta, análise, produção e distribuição da informação, indispensável à execução do negócio das organizações. Dessa forma, tornou-se essencial o reconhecimento de que a TIC é crucial, estratégica e um importante recurso que precisa de investimento e gerenciamento apropriados.

Esse cenário motivou o surgimento do conceito de governança tecnológica, do termo inglês IT Governance, por meio da qual procura-se o alinhamento de TIC com os objetivos da organização. Governança tecnológica define que TIC é um fator essencial para a gestão financeira e estratégica de uma organização e não apenas um suporte a esta.

Governança de TIC pode ser definida da seguinte forma:

- Uma estrutura de relacionamentos entre processos para direcionar e controlar uma empresa para atingir seus objetivos corporativos, por meio da agregação de valor e controle dos riscos pelo uso da TIC e seus processos (ITGI, 2001);
- capacidade organizacional exercida pela mesa diretora, gerente executivo e gerente

de TIC, de controlar o planejamento e a implementação das estratégias de TIC e, dessa forma, permitir a fusão da TIC ao negócio (Van Grembergen, 2003);

- especificação das decisões corretas em um modelo que encoraje o comportamento desejável no uso de TIC, nas organizações (Weill & Ross, 2004).

A governança envolve direcionamento de TIC e controle da gestão, verificação do retorno do investimento e do controle dos riscos, análise do desempenho e das mudanças na TIC e alinhamento com as demandas futuras da atividade fim – foco interno – e com a atividade fim de seus clientes – foco externo. Essa abrangência é ilustrada na Figura 1. A gestão preocupa-se com o planejamento, a organização, a implementação, a implantação e a manutenção da infra-estrutura de TIC e com o gerenciamento dos processos com foco no suporte e no fornecimento dos serviços (Van Grembergen, 2003).

Para alcançar a governança da tecnologia da informação e comunicação, as organizações utilizam modelos que definem as "melhores práticas" para a gestão de TIC. Entre esses modelos, os de maior aceitação são o COBIT (ITGI, 2000) e ITIL (OGC, 2000).

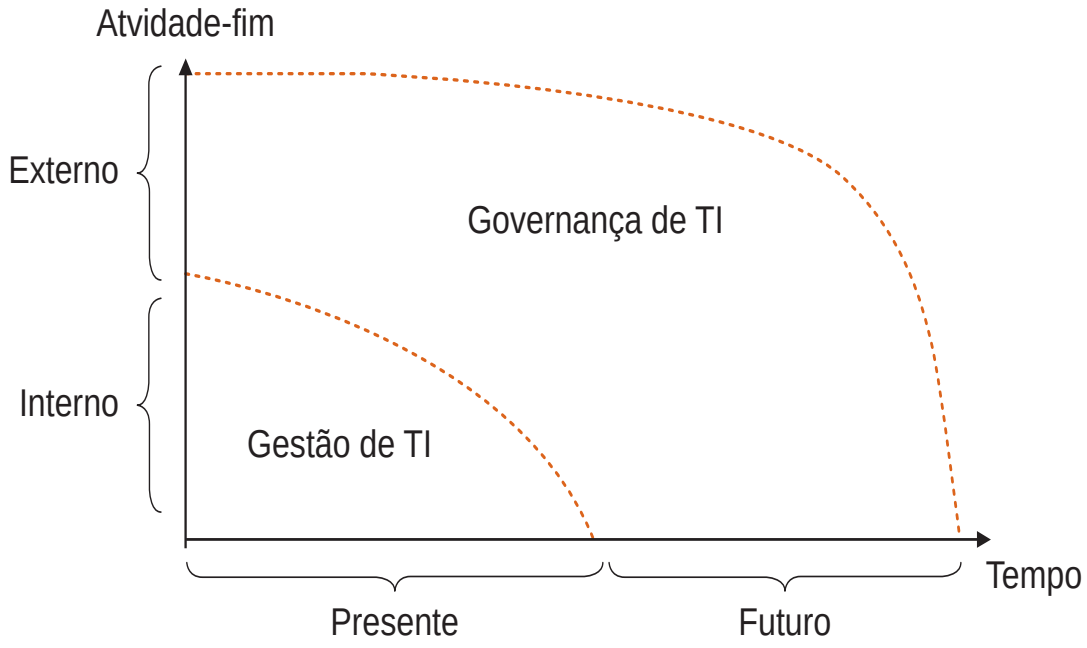


Figura 1 – Abrangência da governança e da gestão de TI (Van Grembergen, 2003).

2. Necessidade de Governança da Segurança da Informação

Seja de forma sistêmica e prática ou de forma científica, o gestor deve sempre buscar a melhor das alternativas para suas decisões. De forma sistêmica, o gestor usa a experiência acumulada e as observações do ambiente para fazer seu cenário decisório ou modelo decisório. É possível considerar que isso seja válido não só para o processo decisório no enfoque organizacional, mas também para o gerenciamento de segurança da informação. Entretanto, em função do grande número de dados provenientes das mais diversas fontes da infra-estrutura de TIC no cenário atual, boa parte das decisões precisa ser tomada de forma estruturada e científica e não mais de forma sistêmica. Isso é válido tanto para as questões de segurança computacional, quanto para o processo de tomada de decisões estratégicas nas organizações.

No enfoque organizacional, de forma científica, o gestor pode utilizar modelos de governança organizacional apoiados por ferramentas disponíveis na teoria da decisão, que, por sua vez, utiliza ferramental de outras ciências, tais como matemática, estatística, filosofia, administração, etc.

Considerando a dependência atual das organizações do correto funcionamento de sua área de TIC, para a realização de sua missão, as ações relacionadas com a segurança computacional estão deixando cada vez mais de ser tratadas apenas como uma responsabilidade da área de TIC e estão sendo vistas como um desafio para os gestores das organizações. Os gestores atuais estão cada vez mais necessitados de incorporar as responsabilidades relacionadas com a segurança computacional em seu processo de tomada de decisão.

Além disso, os administradores atuais necessitam que não só a TIC esteja alinhada com as estratégias da organização, mas que estas estratégias estejam tirando o melhor proveito da infra-estrutura de TIC existente. Eles terão que assumir cada vez mais a responsabilidade de garantir que as organizações estejam oferecendo aos seus usuários e clientes um ambiente de TIC seguro e confiável.

As organizações necessitam de proteção contra os riscos inerentes ao uso da infra-estrutura de TIC e simultaneamente obter indicadores dos benefícios de ter essa infra-estrutura segura e confiável. Dessa forma, além da governança de TIC, as organizações precisam estruturar especificamente a governança da segurança da informação.

3. Algumas Iniciativas Relacionadas com a Governança da Segurança da Informação

É possível encontrar estudos que apontem a necessidade de um modelo, para que as organizações possam alcançar a governança da segurança da informação (BSA, 2003) (ITGI, 2001) (IIA, 2001) (CGTFR,2004) (NCSP, 2004) (Caruso, 2003) (OGC, 2001B) (CERT, 2005b).

Em um estudo recente, o Coordination Center (CERT/CC), um centro especializado em segurança na internet, localizado no Software Engineering Institute-Carnegie Mellon University, aponta a atual necessidade de as organizações estabelecerem e manterem a cultura de uma conduta organizacional para a segurança da informação. Eles procuram motivar as organizações a expandirem seus modelos de governança, incluindo questões de segurança computacional, e incorporar o pensamento sobre segurança por toda a organização, em suas ações diárias de governança corporativa (CERT, 2005b).

Como resultado de uma força tarefa formada nos Estados Unidos, em dezembro de 2003, para desenvolver e promover um framework de governança coerente, para direcionar a implementação de um programa efetivo de segurança da informação, foi apresentado ao público um documento descrevendo a necessidade de governança da segurança da informação (CGTFR, 2004). Esse trabalho apresenta também recomendações do que é necessário ser implementado e uma proposta para avaliar a dependência das organizações em relação à segurança computacional.

O IT Governance Institute apresenta também a necessidade de ter um modelo para governança da segurança da informação (ITGI, 2001). Nesse trabalho é apresentada a necessidade de as diretorias das organizações envolverem-se com as questões de segurança computacional.

4. Modelos em Auxílio à Governança da Segurança da Informação

Um modelo para governança da segurança da informação pode ser estruturado como um subconjunto da governança de TIC e, conseqüentemente, da governança organizacional. Esse modelo será responsável pelo alinhamento das questões de segurança computacional com o plano estratégico da organização.

Ao descrever o cenário atual para o gerenciamento de segurança computacional, muitas fontes na literatura apontam a necessidade e a importância de alcançar um modelo de governança da segurança da informação, que possa ser utilizado pelas organizações, de modo que a segurança computacional não seja tratada apenas no âmbito tecnológico, mas reconhecida como parte integrante do planejamento estratégico das organizações no processo de tomada de decisão. O The Institute of Internal Auditors (IIA) publicou um trabalho onde destaca que, uma vez que os diretores são responsáveis pelos bons resultados e pela continuidade da organização que governam, eles precisam aprender a identificar, atualmente, as questões corretas sobre segurança computacional e, ainda, considerá-las como parte de sua responsabilidade (IIA, 2001).

Atualmente, as responsabilidades acerca da segurança computacional são, freqüentemente, delegadas ao gerente de segurança (Chief Security Officer) das organizações, gerando

conflitos em relação ao orçamento destinado a essa área e à necessidade de impor medidas que vão além de seu escopo de atuação. Dessa forma, é muito comum observar um cenário, em que as questões de segurança computacional não são tratadas em um nível de gestão da organização, tendo, como conseqüência, a falta de recursos para minimizar os riscos existentes no patamar exigido pela estratégia organizacional. A responsabilidade pelo nível correto de segurança computacional deverá ser uma decisão estratégica de negócios, tendo como base um modelo de governança da segurança da informação que contemple uma análise de risco.

Em um relatório do Corporate Governance Task Force é proposto que, para proteger melhor a infra-estrutura de TIC, as organizações deveriam incorporar as questões de segurança computacional em suas ações de governança corporativa (CGTFR, 2004).

Em um trabalho publicado em 2003, o Business Software Alliance (BSA) chama a atenção para a necessidade de desenvolver um modelo de governança da segurança da informação, que possa ser adotado imediatamente pelas organizações (BSA, 2003). Esse trabalho sugere que os objetivos de controle contidos na ISO 27000 devam ser considerados e ampliados para o desenvolvimento de um modelo, em que governança da segurança da informação não seja considerada apenas no plano tecnológico, mas parte integrante das "melhores práticas corporativas", não deixando de cobrir aspectos relacionados com as pessoas, processos e tecnologia.

Para que as organizações obtenham sucesso na segurança de sua informação, os gestores precisam tornar a segurança computacional uma parte integrante da operação do negócio da organização (ENTRUST, 2004). A forma proposta para se conseguir isso é utilizar um modelo de governança da segurança da informação como parte do controle interno e políticas que façam parte da governança corporativa. Considerando-se esse modelo, segurança computacional deixaria de ser tratada apenas como uma questão técnica, passando a ser um desafio administrativo e estratégico.

Um modelo de governança da segurança da informação deverá considerar as observações apresentadas anteriormente e apresentar-se fortemente acoplado ao modelo de governança de TIC, detalhando e ampliando seu escopo de atuação na área de interseção com a segurança computacional.

5. Requisitos para um Modelo de Governança da Segurança da Informação

Uma vez que as organizações possuem necessidades distintas, elas irão apresentar abordagens diversas para tratar as questões relacionadas com a segurança da informação. Dessa forma, um conjunto principal de requisitos deve ser definido para guiar os mais diversos esforços. Identificados esses requisitos, deve-se correlacioná-los em um modelo de governança da segurança da informação.

Um modelo de governança da segurança da informação poderá ser desenvolvido tendo em mente os seguintes requisitos:

1. Os Chief Executive Officers (CEOs) precisam ter um mecanismo para conduzir uma avaliação periódica sobre segurança da informação, revisar os resultados com sua equipe e comunicar o resultado para a mesa diretora.
2. Os CEOs precisam adotar e patrocinar boas práticas corporativas para segurança computacional, sendo municiados com indicadores objetivos que os façam considerar a área de segurança computacional como um importante centro de investimentos na organização e não apenas um centro de despesas.
3. As organizações devem conduzir periodicamente uma avaliação de risco relacionada com a informação, como parte do programa de gerenciamento de riscos.
4. As organizações precisam desenvolver e adotar políticas e procedimentos de segurança com base na análise de risco para garantir a segurança da informação.
5. As organizações precisam estabelecer uma estrutura de gerenciamento da segurança para definir explicitamente o que se espera de cada indivíduo em termos de papéis e responsabilidades.
6. As organizações precisam desenvolver planejamento estratégico e iniciar ações para prover a segurança adequada para a rede de comunicação, para os sistemas e para a informação.
7. As organizações precisam tratar segurança da informação como parte integral do ciclo de vida dos sistemas.

8. As organizações precisam divulgar as informações sobre segurança computacional, treinando, conscientizando e educando todos os envolvidos.
9. As organizações precisam conduzir testes periódicos e avaliar a eficiência das políticas e procedimentos relacionados com a segurança da informação.
10. As organizações precisam criar e executar um plano para remediar vulnerabilidades ou deficiências que comprometam a segurança da informação.
11. As organizações precisam desenvolver e colocar em prática procedimentos de resposta a incidentes.
12. As organizações precisam estabelecer planos, procedimentos e testes para prover a continuidade das operações.
13. As organizações precisam usar as melhores práticas relacionadas com a segurança computacional, como a ISO 20000 (antiga ISO 17799), para medir a performance da segurança da informação.

Tendo como base a estrutura de tomada de decisão em sistemas de informação gerenciais, os princípios citados podem ser organizados em três níveis: operacional, tático e estratégico. A organização nesses níveis irá permitir a evolução de dados do nível operacional em informação do nível tático e, posteriormente, em conhecimento do nível estratégico, que possa ser útil aos gestores no planejamento estratégico das organizações.

Estruturado dessa forma, o modelo poderá ser utilizado para prover conhecimento necessário para motivar os administradores a patrocinar a utilização das melhores práticas de segurança computacional em todos os níveis da organização. Dessa forma, o modelo deverá ainda ser capaz de apontar as melhores práticas a serem seguidas em cada um dos níveis da organização, contemplando três pontos principais em cada um desses níveis:

- O que se espera de cada indivíduo: o que deve e o que não deve ser feito.
- Como cada indivíduo poderá verificar se está cumprindo o que é esperado: indicadores de produtividade.
- Quais métricas devem ser utilizadas para medir a eficiência dos processos executados e para apontar ajustes que necessitem ser aplicados.

Uma revisão de literatura sobre práticas de gerenciamento de segurança computacional aponta, pelo menos, quatro pontos chaves a serem considerados na definição de um modelo para a governança da segurança da informação, a saber:

- Necessidade de uma avaliação de risco. Os riscos precisam ser conhecidos e as medidas de segurança correspondentes devem ser identificadas.
- Necessidade de uma estrutura organizacional de segurança computacional, tratada em todos os níveis da organização.
- Necessidade de criar, endossar, implementar, comunicar e monitorar uma política de segurança por toda a organização, com comprometimento e apoio visível dos gestores.
- Necessidade de fazer com que cada indivíduo da organização conheça a importância da segurança computacional e treiná-los, para que possam utilizar as melhores práticas neste sentido.

Embora esses quatro pontos chave sejam os mais comuns apontados pela literatura, os seguintes pontos são citados com freqüência:

- Necessidade de monitorar, auditar e revisar as atividades de forma rotineira.
- Necessidade de estabelecer um plano de continuidade de negócio que possa ser testado regularmente.

6. Processos e Controles para um Modelo de Governança da Segurança da Informação

Para atender a todos os requisitos necessários a um modelo de governança da segurança da informação, é proposto, neste artigo, a combinação das potencialidades dos modelos COBIT e ITIL e da norma ISO 20000. Esses modelos vêm sendo utilizados isoladamente pelas organizações nos últimos anos e representam as melhores práticas desenvolvidas, testadas e aprovadas por especialistas ao redor do mundo.

Uma visão geral da norma ISO 27000, dos modelos COBIT e ITIL serão apresentados a seguir.

6.1 Código de Prática para a Gestão da Segurança da Informação - ISO 27001

Para atender aos anseios de grandes empresas, de agências governamentais e de instituições internacionais em relação ao estabelecimento de padrões e normas que refletissem as melhores práticas de mercado relacionadas com a segurança dos sistemas e informações, o British Standards Institute (BSI) criou uma das primeiras normas sobre o assunto. Denominada BS 7799 - Code of Practice for Information Security Management, ela foi oficialmente apresentada em primeiro de dezembro de 2000, após um trabalho intenso de consulta pública e internacionalização. A BS 7799 foi aceita como padrão internacional pelos países membros da International Standards Organization (ISO), sendo então denominada ISO/IEC 17799:2000 (ISO, 2000). No ano 2001, a norma foi traduzida e adotada pela Associação Brasileira de Normas Técnicas (ABNT), como NBR 17799 - Código de Prática para a Gestão da Segurança da Informação (ABNT, 2001).

A norma ISO/IEC 17799, com base na parte 1 da BS 7799, fornece recomendações para gestão da segurança da informação, a serem usadas pelos responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança, e prover confiança nos relacionamentos entre organizações Atualmente, essa norma evoluiu para um conjunto de normas organizadas pelo ISO, como ISO 27000 (ISO, 2000).

O conjunto de normas ISO 27000, que substituiu a norma 17799:2005, define 127 objetivos de controle que poderão ser utilizados para indicar o que deve ser abordado no modelo de governança da segurança da informação a ser adotado na organização, enfocando o processo sob o ponto de vista do negócio da empresa. A norma trata, dentre outros, dos seguintes aspectos: Política de Segurança, Plano de Continuidade do Negócio, Organização da Segurança, Segurança Física e Ambiental, Controle de Acesso e Legislação.

Essa norma considera a informação como um patrimônio que, como qualquer importante patrimônio da organização, tem um valor e, conseqüentemente, precisa ser adequadamente protegido. A conformidade dos processos corporativos com a norma ISO 27001 pode ser utilizada pelas empresas, para demonstrar aos seus parceiros de negócio e clientes o seu comprometimento com as informações por ela manipuladas em relação aos seguintes conceitos básicos da segurança da informação:

- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

Nesse contexto, a segurança da informação está relacionada com a proteção da informação contra uma grande variedade de ameaças, para permitir a continuidade do negócio, minimizar perdas, maximizar o retorno de investimentos e capitalizar oportunidades.

Para a seleção dos objetivos de controle apropriados para a organização, a norma recomenda que seja realizada uma Análise de Risco, que irá determinar a necessidade, a viabilidade e a melhor relação custo/benefício para a implantação desses controles.

6.2 Modelo COBIT

A missão maior relacionada com desenvolvimento do modelo Control Objectives for Information and Related Technology (COBIT) é pesquisar, desenvolver, publicar e promover um conjunto atualizado de padrões internacionais e de melhores práticas referentes ao uso corporativo de TIC para os gerentes e auditores de tecnologia (ITGI, 2000).

Desenvolvido e difundido pelo Information System Audit and Control (ISACA) e pelo IT Governance Institute (a partir da terceira edição do modelo), o COBIT é um modelo considerado por muitos a base da governança tecnológica. O COBIT funciona como uma entidade de padronização e estabelece métodos formalizados para guiar a área de tecnologia das empresas, incluindo qualidade, níveis de maturidade e segurança da informação.

O COBIT está estruturado em quatro domínios, para que possa refletir um modelo para os processos de TIC. Esses domínios podem ser caracterizados pelos seus processos e pelas atividades executadas em cada fase de implementação da

governança tecnológica. Os domínios do COBIT são os seguintes:

a) Planejamento e Organização: esse domínio possui onze objetivos de controle que dizem respeito às questões estratégicas associadas a como a TIC pode contribuir, da melhor forma possível, para alcançar os objetivos da organização.
b) Aquisição e Implementação: possui seis objetivos de controle que definem as questões de identificação, desenvolvimento e aquisição da infra-estrutura de TIC, conforme as diretivas estratégicas e de projeto predefinidos no Plano Estratégico de Informática da empresa, também conhecido como Plano Diretor de Informática (PDI).
c) Entrega e Suporte: esse domínio, com treze objetivos de controle, define as questões ligadas ao uso da TIC, para atendimento dos serviços oferecidos para os clientes, a manutenção e as garantias ligadas a estes serviços.
d) Monitoração: com quatro objetivos de controle, esse domínio define as questões de auditoria e acompanhamento dos serviços de TIC, sob o ponto de vista de validação da eficiência dos processos e evolução destes em termos de desempenho e automação.

O modelo COBIT define objetivos de controle como sendo declarações de resultado desejado ou propósito a ser atingido, pela implementação de procedimentos de controle numa atividade de TI em particular.

A Figura 2 ilustra os quatro domínios do COBIT, os objetivos de controle para cada domínio e seus inter-relacionamentos.

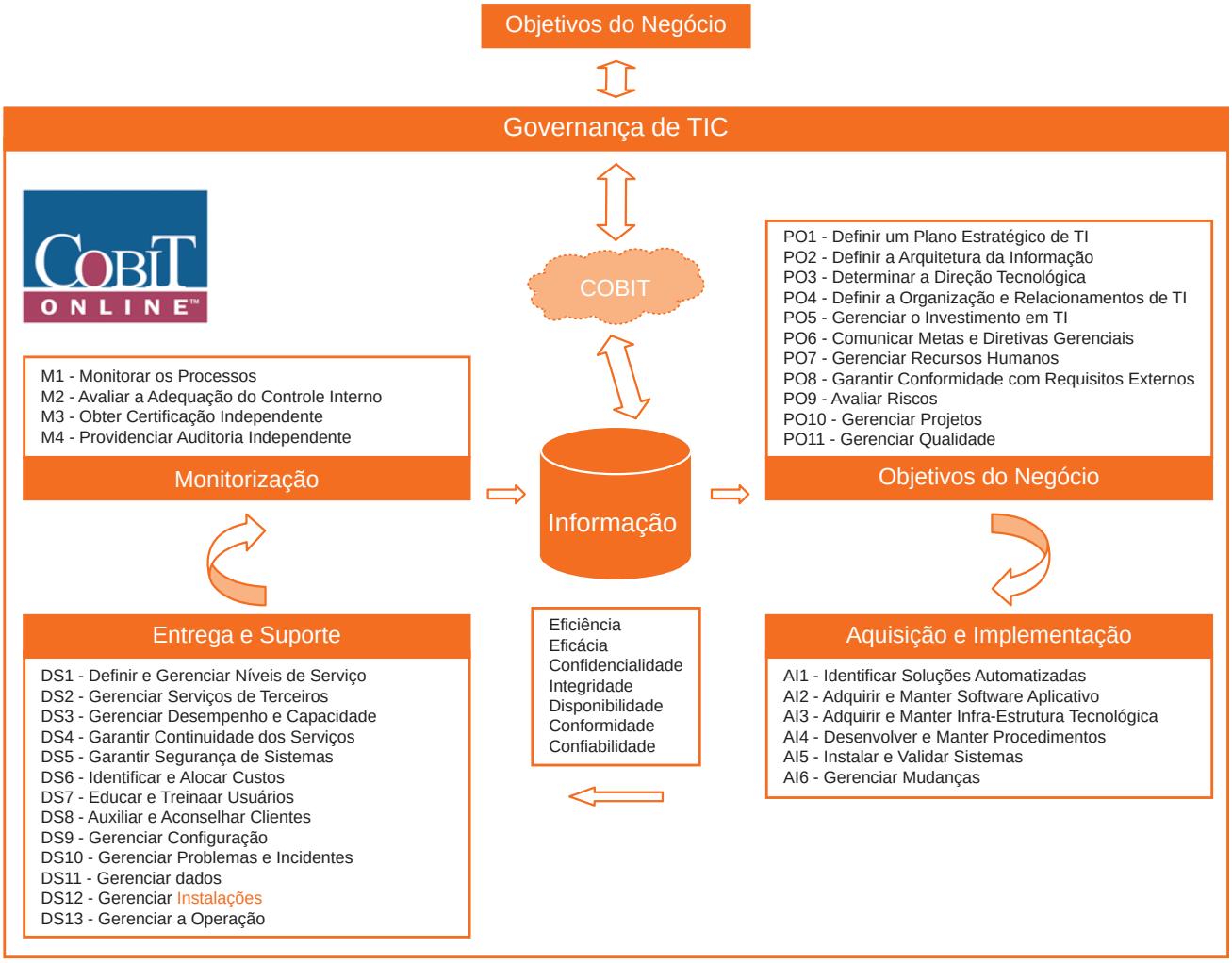


Figura 2 – Os domínios de processo do COBIT (ITGI, 2000).

Além dos quatro domínios principais, que guiam o bom uso da tecnologia da informação na organização, existe também a questão de auditoria, que permite verificar, por meio de relatórios de avaliação, o nível de maturidade dos processos da organização. O método de auditoria segue o modelo do Capability Maturity Model for Software (CMMS) (Paulk et al., 1993) e estabelece os seguintes níveis:

0) Inexistente: Significa que nenhum processo de gerenciamento foi implementado.
1) Inicial: O processo implementado é realizado sem organização, de modo não planejado.
2) Repetitível: O processo implementado é repetido de modo intuitivo, isto é, depende mais das pessoas do que de um método estabelecido.
3) Definido: O processo implementado é realizado, documentado e comunicado na organização.
4) Gerenciado: Existem métricas de desempenho das atividades, de modo que o processo implementado é monitorado e constantemente avaliado.
5) Otimizado: As melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos envolvidos.

O resultado da auditoria da metodologia COBIT, para a avaliação do nível de maturidade, ajuda a área de TIC a identificar o nível atual e como evoluir para melhorar os processos da organização, permitindo a evolução gradativa desses.

O resultado da auditoria permite identificar o nível de evolução dos processos na organização, de modo concreto, com base em relatórios confiáveis de auditoria e parâmetros de mercado. O sumário executivo do relatório gerado pela auditoria traz as seguintes informações: se existe um método estabelecido para o processo; como o método é definido e estabelecido; quais os controles mínimos para a verificação do desempenho do método; como pode ser feita a auditoria no método; quais as ferramentas utilizadas no método e o que avaliar no método para sua melhoria. A partir desse ponto, a organização define os objetivos de controle a serem atingidos.

6.3 Modelo ITIL

O modelo Information Technology Infraestructure Library (ITIL) foi desenvolvido pelo governo britânico no final da década de 80 e tem como foco principal a operação e a gestão da infra-estrutura de TIC na organização, incluindo todos os pontos importantes no fornecimento e manutenção dos serviços de TIC (OGC, 2000). O ITIL, composto por um conjunto das melhores práticas para auxiliar a governança de TIC, vem sendo um modelo amplamente utilizado atualmente (RUDD, 2004).

O princípio básico do ITIL é o objeto de seu gerenciamento, ou seja, a infra-estrutura de TIC. O ITIL descreve os processos que são necessários para dar suporte à utilização e ao gerenciamento da infra-estrutura de TIC. Outro princípio fundamental do ITIL é o fornecimento de qualidade de serviço aos clientes de TIC a custos justificáveis, isto é, relacionar os custos dos serviços de tecnologia de forma que se possa perceber como estes trazem valor estratégico ao negócio. Por meio de processos padronizados de gerenciamento do ambiente de TIC é possível obter uma relação adequada entre custos e níveis de serviços prestados pela área de TIC.

O ITIL consiste em um conjunto de melhores práticas, que são inter-relacionadas, para minimizar o custo, ao mesmo tempo em que aumenta a qualidade dos serviços de TIC entregues aos usuários. Como destacado na Figura 3, o ITIL é organizado em cinco módulos principais, a saber: A Perspectiva de Negócios, Gerenciamento de Aplicações, Entrega de Serviços, Suporte a Serviços e Gerenciamento de Infra-estrutura. Embora o modelo ITIL não tenha um módulo dedicado ao gerenciamento de segurança computacional, ele faz referência a esse tema descrevendo, em um documento, como este poderia ser incorporado, por meio dos processos descritos, nos módulos de Suporte a Serviços e Entrega de Serviços.

Dentre os cinco módulos citados, os mais utilizados são o Suporte a Serviços e Entrega de Serviços.

Apesar de o modelo ITIL possuir processos bem definidos para auxiliar na governança de TIC, neste trabalho identifica-se a necessidade de algumas adaptações para que possa ser utilizado para implementar todos os requisitos de um modelo de governança da segurança da

informação. Essas adaptações estão relacionadas, principalmente, com a forma de tratar incidentes de segurança computacional.

Considerando a estrutura de tomada de decisão em sistemas de informação, este trabalho propõe ainda um mapeamento dos módulos Suporte a Serviços e Entrega de Serviços do modelo ITIL, no nível operacional e no nível tático, conforme descrito a seguir.

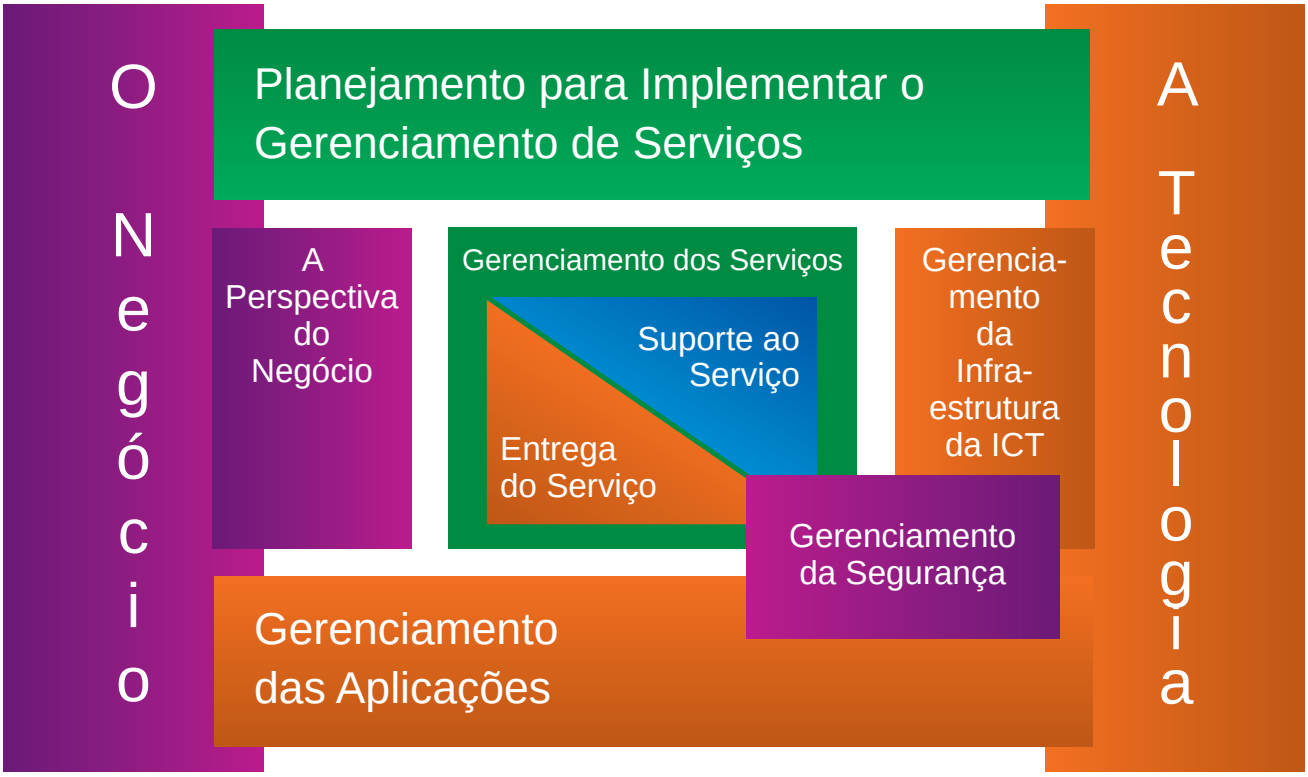


Figura 3 – Modelo para Gerenciamento de Serviços ITIL (OGC, 2000).

7. Considerações Finais

Neste artigo apresentaram-se a necessidade de um modelo para governança da segurança da informação e os requisitos para isto. Para atender todos os requisitos necessários a um modelo de governança da segurança da informação, propõe-se a utilização integrada dos modelos COBIT e ITIL e da norma ISO 27002.

O modelo COBIT e a norma ISO 27002 irão fornecer os objetivos de controle necessários para atender aos requisitos apresentados. Os processos descritos no modelo ITIL serão utilizados para guiar a implementação desses objetivos de controle.

Por meio de uma correlação desses objetivos, presentes no modelo COBIT e na norma ISO 27002, com os processos descritos no modelo ITIL, neste trabalho identificou-se que os módulos de Suporte a Serviços e Entrega de Serviços do modelo ITIL não estão estruturados para implementar todos os objetivos de controle apresentados para o nível operacional e tático.

Para que o modelo ITIL seja capaz de implementar todos os objetivos de controle apresentados pela norma ISO 27002 e pelo modelo COBIT, para os níveis operacional e tático, este trabalho propôs, no Capítulo 6, uma expansão de seus processos.

A combinação do modelo COBIT com a norma ISO 27002 e o modelo ITIL permitirá a utilização das potencialidades de cada uma dessas

propostas para o desenvolvimento de um modelo único que facilite identificar: o quê, quem, como e que recursos tecnológicos utilizar, para o alcance da governança da segurança da informação.

Referências

(ABNT, 2001) ABNT. *Tecnologia da informação – Código de prática para a gestão da segurança da Informação.* NBR ISO/IEC 17799. 30/09/2001. (Atualmente substituída pela ISO 27002)

(BSA, 2003) BUSINESS SOFTWARE ALLIANCE. *Information Security Governance: Toward a Framework for Action.* Disponível on-line em http://www.bsa.org.Visitado em 12/12/2004.

(CARUSO, 2003) CARUSO, J.B. *Information Technology Security: Governance, Strategy and Practice in Higher Education.* EDUCASE Center for Applied Research, September, 2003. Disponível on-line em http://www.educause.edu/ecar/. Visitado em 16/03/2005.

(CERT, 2005b) CERT CORDINATION CENTER, *Governing for Enterprise Security.* (2005) Disponível on-line em http://www.cert.org/governance/ges.html. Visitado em 01/03/2005

(CGTRF, 2004) CORPORATE GOVERNANCE TASK FORCE REPORT. *Information Security Governance: A Call to Action.* April, 2004. Disponível on-line em: www.cyberpartnership.org/InfoSecGov4_04.pdf. Visitado em 15/11/2004.

(ENTRUST, 2004) ENTRUST. *Information Security Governance (ISG): An Essential Element of Corporate Governance.* April, 2004. Disponível on-line em: http://www.entrust.com/governance/. Visitado em 16/03/2005.

(IIA, 2001) THE INSTITUTE OF INTERNAL AUDITORS. *Information Security Governance: What Directors Need to Know.* (2001). The Critical Infraestructure Assurance Project. ISBN 0-89413-457-4. Disponível on-line em www.theiia.org/eSAC/pdf/ISG_1215.pdf. Visitado em 14/01/2005.

(ISO, 2000) International Organization for Standardization / International Eletrotechnical Committee. *Information technology- Code of practice for information security management. Reference number* ISO/IEC 17799:2000(E). (*Atualmente substituída pela ISO 27002*)

(ITGI, 2000) THE IT GOVERNANCE INSTITUTE.*COBIT: Control Objectives for information and related Technology.* Printed in the United States of America, 2000. ISBN: 1-893209-13-X.

(ITGI, 2001) THE IT GOVERNANCE INSTITUTE. *Information Security Governance: Guidance for Boards of Directors and Executive Management.* Printed in the USA, 2001. ISBN 1-893209-28-8. Disponível on-line em: http://www.itgi.org/template_ITGI.cfm?template=/ContentManagement/ContentDisplay.cfm&ContentID=6672. Visitado em 02/02/2005.

(NCSP, 2004) NATIONAL CYBER SECURITY PARTNERSHIP. *Information Security Governance Assessment Tool for Higher Education.* 2004. Disponível on-line em: http://www.cyberpartnership.org. Visitado em 15/03/2005.

(OGC, 2000) Office of Government Comerce (OGC). *ITIL: The Key to Managing IT Services – Best Practice for Service Support.* Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330015 8,

(OGC, 2001a) Office of Government Comerce (OGC). *ITIL: The Key to Managing IT Services – Best Practice for Service Delivery.* Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330017 4.

(OGC, 2001b) Office of Government Comerce (OGC). *ITIL: The Key to Managing IT Services – Best Practice for Security Management.* Printed in the United Kingdom for the Stationery Office, 2001. ISBN0 11 330014 X.

(PAULK et al, 1993) PAULK, M.C.; CURTIS, B; CHRISSIS, M.B.;WEBER, C.V. *Capability Maturity Model for Software, version 1.1.* Technical Report, Carnegie Mellon Software Engeneering Institute, CMU/SEI-93-TR-024, February 1993. Disponível on-line em: http://www.sei.cmu.edu/cmm/. Visitado em 12/01/2005.

(RUDD, 2004) RUDD, Colin. *An Introductory Overview of ITIL*. Publicado por iTSMF ltd, Webbs Court, United Kingdom, 2004. Version 1.0a. Disponível on-line em: http://www.itsmf.com/publications/ITIL/Overview.pdf. Visitado em 13/03/2005.

(van GREMBERGEN, 2003) VAN GREMBERGEN, Wim. *Strategies for Information Technology Governance.* Idea Group Publishing, 2003. ISBN 1-591140-140-2.

(WEILL&ROSS, 2004) WEILL, Peter; Ross, Jeanne W. *IT Governance: how top performers manage IT decision rights for superior results.* Harvard Business School Publishing, 2004. ISBN 1-59139-253-5.

Wagner Antônio / Sucesu

Ações de segurança da informação no governo mineiro – 2005/2007

Marconi Martins de Laia

Graduado em Administração pela Universidade Federal de Minas Gerais (1999), e em Administração Pública, pela Fundação João Pinheiro (1997). Possui mestrado em Ciências da Informação, pela Universidade Federal de Minas Gerais (2002) e, atualmente, é doutorando do Programa de Pós-graduação em Ciência da Informação da UFMG. Diretor da Superintendência Central de Governança Eletrônica do Governo de Minas Gerais.
marconi.laia@planejamento.mg.gov.br

Divulgação

Rodrigo Diniz Lara

Diretor Central de Gestão da Informação da Secretaria de Estado de Planejamento e Gestão, graduado em Administração Pública, pela Fundação João Pinheiro, especialista em Gestão Estratégica da Informação pela UFMG.
rodrigo.diniz@planejamento.mg.gov.br

RESUMO

A segurança da informação é hoje uma atividade essencial em qualquer tipo de organização, principalmente do setor público que, além de ter que proteger as informações do seu negócio, é responsável pela custódia das informações de cidadãos e empresas. O objetivo deste artigo é apresentar a concepção do Plano Corporativo de Segurança da Informação do Governo do Estado de Minas Gerais e seus principais resultados. Serão apresentadas as duas fases do Plano, sendo que a primeira contemplou a sua elaboração e contou com a participação da Secretaria de Estado de Fazenda (SEF), Secretaria de Estado de Planejamento e Gestão (Seplag) e a Companhia de Tecnologia da Informação de Minas Gerais (Prodemge). Já a segunda fase refere-se à implementação do Plano e os resultados, aqui apresentados, restringem-se à Seplag.

Palavras-chave: Segurança da Informação. ABNT NBR ISO/IEC 27001:2006. Gestão de Riscos

1. Introdução

A sociedade da informação vem sendo discutida e apresentada como uma nova era, em que a informação pode fluir a velocidades e quantidades até há pouco tempo inimagináveis, além de assumir valores sociais e econômicos centrais (Brasil, 2000). A base instrumental para esse novo paradigma encontra-se no desenvolvimento sem precedentes das Tecnologias da Informação e Comunicação (TICs), que permitem a troca de dados por meio dos fios de telefone, linhas de fibra-ótica, transmissões via satélite, dentre outros, e formam uma estrada virtual capaz de interligar e conectar países, comunidades e pessoas em qualquer lugar do planeta. Embora com base no desenvolvimento das TICs, não se resume ao desenvolvimento tecnológico.

No contexto supramencionado, a informação adquiriu o status de recurso fundamental para as organizações. O desenvolvimento da TIC tornou a informação cada vez mais difusa nas últimas décadas (Akutsu; Pinho; 2002; Castells, 2003), o que ensejou um novo conjunto de riscos e oportunidades para organizações privadas, públicas ou não-governamentais.

Para as organizações públicas, o desenvolvimento das TICs ensejou grandes desafios. Como destaca Araújo (2006), a década de 80 testemunhou o início dos processos de Reforma do Estado, que transformaram radicalmente o papel e a gestão das organizações públicas. Não por acaso, a aplicação e a utilização das Tecnologias da Informação figuram sempre nas experiências recentes de reforma administrativa em todo o mundo.

Sêmola (2003) afirma que a crescente valorização da informação como principal ativo das organizações, somada a alguns fatores como: a dependência dos processos organizacionais em relação aos sistemas de informação; o crescimento contínuo da digitalização das informações; o crescimento exponencial da conectividade da organização; o crescimento do compartilhamento das informações; a maciça utilização da internet; a grande diversidade e compartilhamento de técnicas de ataque e invasão; a carência de mecanismos legais de responsabilização em ambiente virtual; e a diversificação dos tipos de ameaças como, funcionários insatisfeitos, hacker[1], vírus[2], spams[3], engenharia social[4], tem influenciado para que a segurança da informação seja considerada uma real necessidade e um requisito estratégico, que interfere na capacidade das organizações de realizarem suas atividades com eficiência e eficácia.

No âmbito público, Brasil (2006, p. 4) afirma que:

> As informações sob custódia do Estado sempre exigiram um trato especial para sua proteção. No entanto, com o aumento da complexidade das organizações que realizam as tarefas de suporte à gestão de Estado, aliada à crescente demanda de informações, das quais dependem, tornou-se vital prover a proteção a essa massa informacional com uma abordagem moderna e suficientemente abrangente.

Diante desse cenário, o Governo do Estado de Minas Gerais, em consonância com o Programa de Governança Eletrônica, sob a coordenação da Secretaria de Estado de Planejamento e Gestão (Seplag) e em parceria com a Secretaria de Estado de Fazenda (SEF) e da Companhia de Tecnologia da Informação de Minas Gerais (Prodemge) iniciou, em 2005, a elaboração e a implantação do Plano Corporativo de Segurança da Informação com o objetivo de preparar as referidas organizações a alcançar o nível de segurança desejável.

A implantação de controles de segurança da informação eficazes garantirá que o Governo do Estado adote novas tecnologias, principalmente a internet, como recurso estratégico

1 *Hacker* é "indivíduo que se especializa em estudar os ativos tecnológicos (computadores, sistemas, redes) e testar seus limites, explorando suas fraquezas e falhas. Tem grande facilidade de assimilação e estuda exaustivamente algo até dominar o assunto" (MOREIRA, 2001, p. 65)

2 Vírus "é um programa capaz de infectar outros programas e arquivos de um computador. Para realizar a infecção, o vírus embute uma cópia de si mesmo em um programa ou arquivo, que, quando executado, também executa o vírus, dando continuidade ao processo de infecção". (NIC BR Security Office, 2007, §1)

3 Spam "é o termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês Unsolicited Commercial Email)". (NIC BR Security Office, 2007, §1)

4 Engenharia Social é o "método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações. (NIC BR Security Office, 2007, §1)

para disseminação de informações e canal de comunicação junto a outros Órgãos do Governo, fornecedores e cidadão, preservando os princípios básicos de segurança da informação: confidencialidade, integridade e disponibilidade.

O Plano Corporativo de Segurança da Informação foi estruturado em etapas, conforme o modelo PDCA aplicado aos processos do Sistema de Gestão de Segurança da Informação (SGSI), definido pela ABNT NBR ISO/IEC 27001:2006[5]. Primeiramente, foi realizada uma ampla fase de diagnóstico, que contou com a parceria da Consultoria Módulo. Nessa etapa foi identificado um conjunto de áreas prioritárias para aplicação das ações de segurança. Após o diagnóstico foi estruturado o Plano Diretor de Segurança. No segundo momento, cada um dos órgãos participantes – Seplag, SEF e Prodemge – passou à implementação das diretrizes expostas no Plano. Atualmente, o Plano Corporativo de Segurança da Informação encontra-se na terceira etapa (Fig. 1).

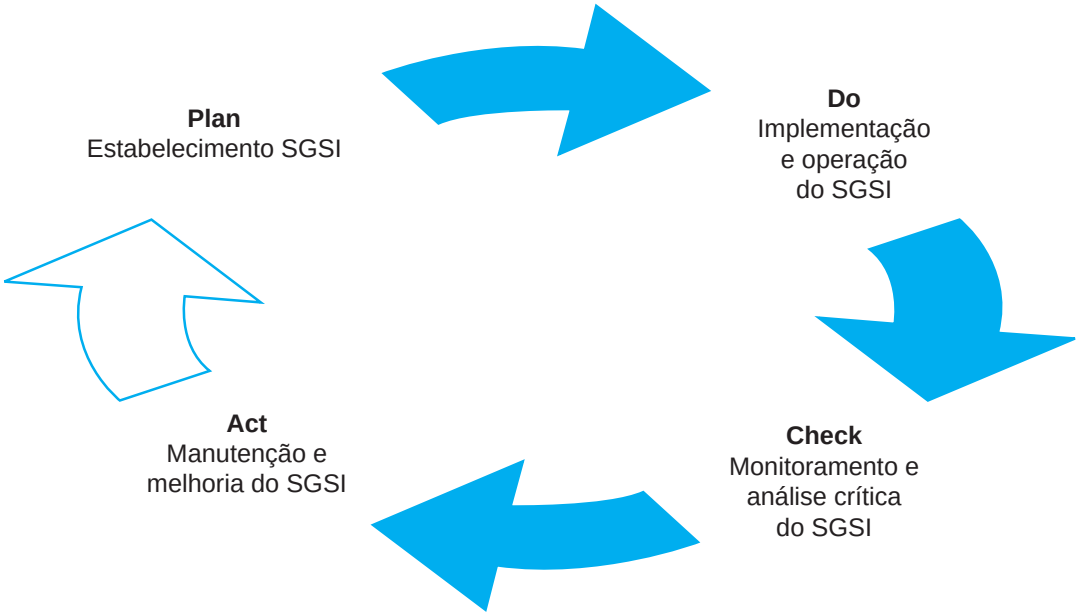


Figura 1 – Situação da aplicação do Modelo PDCA aplicado aos processos do SGSI do Plano Corporativo de Segurança da Informação do Governo do Estado de Minas Gerais – 2007
Fonte: Adaptado de: ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança –Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006. vi p.

O objetivo desse artigo é apresentar o Plano Corporativo de Segurança da Informação do Governo do Estado e os seus principais resultados. Além desta seção introdutória, o artigo é composto de mais três seções. A Seção 2 apresenta a primeira fase que contemplou a elaboração do Plano Corporativo de Segurança da Informação da SEF, Seplag e Prodemge. A Seção 3 apresenta os produtos que foram gerados após a implementação do Plano Corporativo de Segurança da Informação na Seplag, que corresponde à fase de implantação das diretrizes do Plano. A Seção 4 tece considerações finais sobre os desafios do Governo do Estado, na área de segurança da informação.

5 A norma ABNT NBR ISO/IEC 27001:2006 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação.

2. 1ª Fase – Elaboração do Plano Corporativo de Segurança da Informação – SEF Seplag e Prodemge – 2005/2006

A primeira fase do Plano Corporativo de Segurança da Informação da SEF, Seplag e Prodemge contemplou as atividades para o estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI), que representa a primeira etapa na implementação de um Modelo PDCA aplicado aos processos do SGSI, conforme explicitado pela norma ABNT NBR ISO/IEC 27001:2006. Essa primeira etapa possui o objetivo de:

> Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. vi)

Os projetos dessa primeira etapa serão descritos a seguir.

2.1 Análise de Riscos

A análise de riscos identificou os riscos e vulnerabilidades dos ativos tecnológicos, físicos e humanos, que suportam os processos críticos e sensíveis das três organizações, estabelecendo ações para a preparação do ambiente, para implementação de medidas de segurança. Sêmola (2003, p.109) reafirma o papel da análise de riscos ao mencionar que ela é um "[...] instrumento perfeito para dimensionar a situação da segurança atual (da organização), tornando-a consciente dos riscos e orientando-a na busca de soluções que a conduzam para o patamar de risco aceitável."

A análise de riscos contemplou em seu escopo cerca de um conjunto de servidores, computadores/notebooks, contratos/regulamentações, ativos de conectividade, gestores/usuários e os ambientes físicos e os Data Centers da SEF, Seplag e Prodemge. O mais importante é que a análise do Governo de Minas Gerais não focou somente ativos tecnológicos. A metodologia identificou um conjunto de processos críticos para as organizações. A partir daí, os ativos que suportam os processos foram analisados. Para realização dos trabalhos foi utilizado um software de Gestão de Riscos denominado Risk Manager, que possui uma base de conhecimento vasta sobre segurança da informação.

2.2 Plano Diretor de Segurança da Informação

A partir da análise de risco, o Plano Diretor de Segurança (PDS) definiu os projetos e investimentos em segurança em um horizonte de tempo de três anos, que serão executados para conduzir o ambiente da SEF, Seplag e Prodemge – infraestrutura física, tecnologia e pessoas – a um nível de segurança definido como aceitável pelas três organizações.

A criação do PDS contou com o desenvolvimento das seguintes atividades:

a) Mapeamento dos processos críticos de negócio e dos seus gestores.
b) Mapeamento da relevância dos processos críticos, para o funcionamento global do negócio.
c) Classificação da sensibilidade de Confidencialidade, Integridade, Disponibilidade e Legalidade (CIDAL) de cada processo de negócio, referente a uma provável quebra de segurança.
d) Identificação das características de cada processo, em função das dimensões Gravidade, Urgência e Tendência (GUT).
e) Identificação e planejamento dos projetos de segurança que devem ser implementados, indicando os objetivos, escopo, benefícios, produtos básicos, atividades, recursos necessários, prioridade, prazo e estimativa de investimentos.

2.3 Política de Segurança da Informação

A Política de Segurança da Informação estabeleceu, formalmente, as diretrizes, normas, procedimentos/instruções de trabalho de segurança a serem cumpridos por todos os servidores e prestadores de serviço das

três organizações, além de fornecer orientação e apoio às ações de gestão de segurança.

As diretrizes da Política de Segurança foram elaboradas em conjunto e foram as mesmas para a SEF, Seplag e Prodemge. As normas, procedimentos e instruções de trabalho foram desenvolvidos tendo em vista o ambiente de cada organização. Ao final do trabalho foram desenvolvidas 15 normas de usuários, 15 normas técnicas, 15 procedimentos e 15 instruções de trabalho, além de um modelo de termo de sigilo desenvolvido para cada organização.

Os principais benefícios dessa ação foram a determinação dos valores de segurança da informação para as organizações, a criação de uma linguagem comum, no que se refere à segurança da informação e a padronização e normatização dos processos e tecnologias em segurança. Ademais, a Política de Segurança da Informação mostrou-se como um exemplo exitoso de política realizada de forma corporativa. Não são raros os casos em que a administração pública precisa lidar, como os problemas e as dificuldades de fazer com que agências autônomas trabalhem de forma cooperativa para buscar objetivos comuns de uma política, evitando que cada uma fique insulada em seu próprio contexto. O projeto de segurança foi bem-sucedido ao criar uma estrutura de gestão descentralizada coordenada, que permitiu a criação de uma Política única para os três órgãos em questão.

2.4 Programa de Sensibilização em Segurança

O elemento humano é apontado por vários autores, entre eles, Moreira (2001), Sêmola (2003), Ramos (2004) e Teófilo (2002), como o elo mais fraco na implementação do processo de gestão da segurança da informação. O programa de sensibilização em segurança teve o propósito de formar uma cultura de segurança que se integre às atividades de rotina dos colaboradores das organizações, a partir de uma ampla divulgação da Política de Segurança e dos seus conceitos principais.

A campanha de segurança da informação da Seplag utilizou como mote "Segurança da Informação. Adote essa idéia" (Fig. 2). O processo de conscientização contou com a realização de 11 palestras de sensibilização com a peça teatral "As velhas e o dia de chuva", para 800 servidores públicos, contratados e estagiários. Essa peça teatral já havia sido utilizada pela Companhia Energética de Minas Gerais (Cemig) e aborda, de forma lúdica, os problemas dos velhos hábitos de segurança da informação adotados pelas pessoas. Nas palestras foram distribuídas cartilhas e brindes, como camisas, cordas de crachás e canetas. Na intranet da Seplag foi criada uma área de segurança da informação e foram divulgados 12 cartazes sobre o tema, ao longo do ano de 2006.

A campanha de segurança da informação da SEF utilizou como mote "Segurança da Informação. Segure essa idéia" (Fig. 3) e contou também com um mascote chamado "Segurito". A campanha conscientizou cerca de 7.683 servidores e terceirizados distribuídos por todas as regionais da SEF no Estado.

Figura 2 – Mote da Campanha de Segurança da Informação – Seplag (2006)

Figura 3 – Mote da Campanha de Segurança da Informação – SEF (2006)

2.5 Plano de Continuidade de Negócios para os Ativos de Tecnologia da Informação

O Plano de Continuidade de Negócios (PCN), para os ativos de tecnologia da informação, foi elaborado com o objetivo de estabelecer as ações para garantir a continuidade dos processos vitais de negócio identificados no PDS das três organizações em caso de desastre nos ativos de TI, que suportam esses processos.

A primeira etapa do trabalho foi a realização de uma análise de Impacto ao Negócio também conhecida por Business Impact Analysis (BIA), que procurou ordenar os processos de negócio de acordo com a sua criticidade e requisitos de continuidade. A partir do BIA foi elaborada a estratégia de recuperação e os planos: Gestão da Continuidade, Administração de Crises, Recuperação do Desastre, Validação e Testes para serem implementados.

3. 2ª fase – Implantação do Plano Corporativo de Segurança da Informação na Seplag – 2006/2007

A 2ª fase do Plano Corporativo de Segurança da Informação contemplou as atividades de Implementação e Operação do SGSI (Do) e Monitoramento e análise crítica do SGSI (Check), que representam, respectivamente, a segunda e a terceira etapas na implementação de um Modelo PDCA aplicado aos processos do SGSI, conforme explicitado pela norma ABNT NBR ISO/IEC 27001:2006. A segunda etapa possui o objetivo de "implementar e operar a política, controles, processos e procedimentos do SGSI" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. vi). Já a terceira etapa do ciclo PDCA tem o intuito de

> Avaliar e, quando aplicável, medir o desempenho de um processo diante da política, objetivos e experiência prática do SGSI e apresentar os resultados para a análise crítica pela direção. (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2006, p. vi)

Por se tratar de etapas que dependem das análises de riscos de cada ambiente, essa segunda etapa foi realizada separadamente em cada organização. Para fazer frente às recomendações e às necessidades estabelecidas na Análise de Riscos e no Plano de Segurança, a Seplag empreendeu um conjunto de projetos, cujos resultados podem ser vistos de forma sumária a seguir:

Primeiramente, em função das vulnerabilidades encontradas nos ativos tecnológicos na primeira fase do projeto, foram realizadas implementações e configurações, de modo que os ativos fiquem protegidos das ameaças que possam causar algum impacto para a Seplag, visando um aumento de performance e segurança para os usuários. Nessa primeira etapa foram implementados os controles relacionados com os riscos classificados como alto e muito alto.

Ademais, um segundo projeto focou a realização de uma especificação para os requisitos constantes na Política de Segurança da Informação da Seplag, indicando as ações a serem tomadas para a efetiva implementação da política publicada.

A primeira ação a ser executada foi a adesão a um registro de preços realizado pela Prodemge, para aquisição de uma ferramenta de administração centralizada de antivírus e de anti-spam. A ferramenta de anti-spam reduziu drasticamente o número de e-mails indevidos que giram em torno de 70% do total de e-mails recebidos pelos funcionários da Seplag, atualmente.

O terceiro projeto foi criar o escritório de projetos de Segurança da Informação Security Project Management Office (SPMO), que ficou subordinado à Superintendência Central de Governança Eletrônica, apoiando diversos projetos simultaneamente como um centro de competência em segurança da informação. A razão da escolha foi por acreditar que as funções de segurança, assim como outras, são parte de um projeto amplo de utilização das TICs na

administração pública. Um manual de gerenciamento de projetos em segurança da informação foi criado estabelecendo os processos e os indicadores para uma gestão eficiente.

Atrelada à criação do escritório, uma das ações mais importantes foi realizar o treinamento de todos os componentes do Security Project Management Office (SPMO). Além destes, um conjunto com mais 32 gestores de outras organizações públicas do Poder Executivo Estadual também foi qualificado. O treinamento foi constituído de dois módulos, sendo que o primeiro focou os fundamentos dos aspectos de gestão da segurança da informação e o segundo focou os aspectos de gestão das tecnologias da segurança da informação. Todos os três servidores do SPMO da Seplag, responsáveis pela implementação da segurança da informação no órgão, realizaram a prova de certificação e receberam o certificado Módulo Certified Security Officer.

Também foi criado o projeto de classificação da informação, que teve como objetivo, em um processo-piloto, classificar as informações para indicar a necessidade, prioridades e o nível esperado de proteção, quando do tratamento da informação. O processo-piloto escolhido foi o de concursos públicos, gerenciado pela Diretoria Central de Provisão, que possui informações críticas e bastante visadas até o momento da publicação do edital do concurso.

As atividades do projeto contemplaram a criação de uma norma que estabeleceu três níveis de classificação: sem restrição, restrito e confidencial; treinamento dos gestores responsáveis por esse processo, com o intuito de garantir a continuidade da classificação; informações do processo classificadas a partir da data da implantação da norma.

Após a execução das atividades previstas na fase 2 do Plano Corporativo de Segurança da Informação da Seplag foi realizada uma nova Análise de Riscos, no mesmo escopo de ativos, e constatados resultados positivos descritos a seguir:

a) Evolução do índice de segurança médio em estações de trabalho de 82,7%.
b) Evolução do índice de segurança médio em servidores de 41%.
c) Evolução do índice de segurança médio em ativos de conectividade de 205%.
d) Evolução do índice de segurança médio em pessoas de 17%.

4. Considerações finais

A Administração Pública do Poder Executivo Estadual, por meio das ações do Plano Corporativo de Segurança da Informação da SEF, Seplag e Prodemge, iniciou a trajetória para implementação de um nível satisfatório de proteção das suas informações.

O Plano Corporativo de Segurança da Informação está sendo realizado por fases, para alcançar níveis de segurança progressivos em períodos limitados, conforme expostos nas fases 1 e 2. Após essas fases, as organizações deverão avaliar a necessidade de execução de outras e, assim, sucessivamente, pois a gestão de segurança da informação é contínua e permanente. Esse modelo permite a evolução por fases, atingindo cada vez maior escopo e maior nível de segurança, sem que haja concentração antecipada de investimentos que concorreriam com as atividades diárias das organizações.

Além dos resultados da Seplag, descritos no artigo, SEF e Prodemge também empreenderam um conjunto de ações para elevar a segurança das informações governamentais. Não obstante os avanços, o próximo desafio do Governo do Estado de Minas Gerais é a expansão dos projetos de segurança da informação para o restante dos órgãos e entidades da Administração Pública do Estado de Minas Gerais, principalmente a publicação de uma Política Corporativa de Segurança da Informação e a consolidação de um Modelo de Gestão de Segurança da Informação para o futuro Centro Administrativo do Governo do Estado[6], previsto para o início de 2010, que concentrará todas as Secretarias de Estado e outros órgãos da Administração Direta e Indireta.

Embora os desafios sejam grandes, a breve descrição, neste artigo, mostra o compromisso e a responsabilidade do Governo de Minas Gerais com a gestão pública, fato que o referencia como modelo de gerenciamento de políticas públicas em todo o Brasil.

6 Informações adicionais sobre a implantação do Centro Administrativo do Governo do Estado de Minas Gerais podem ser obtidas por meio do site www.codemig.com.br.

Referências

ARAÚJO, L. A. D. *A correspondência eletrônica do empregado e o poder diretivo do empregador*. *In*: Revista de direito constitucional

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27 002:2005 – Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p.

_____. ABNT NBR ISO/IEC 27001:2006 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2006. 40 p.

AKUTSU, Luiz; PINHO, José Antônio Gomes de. Sociedade da informação, accountability e democracia delegativa: investigação em portais de governo no Brasil. Revista de Administração Pública, Rio de Janeiro, v. 36, n. 5, p. 723-745, set/out. 2002.

ARAÚJO, Wagner Frederico Gomes de. A Avaliação de Sítios Governamentais como um Instrumento para Melhoria dos Serviços e Informações On-line: da concepção aos resultados. Trabalho premiado em 1º Lugar no **1º Prêmio Excelência em Gestão Pública do Estado de Minas Gerais**. Belo Horizonte, Junho de 2006.

BRASIL. **Livro Verde da Sociedade da Informação no Brasil**. Brasília: Ministério da Ciência e Tecnologia, (2000).

BRASIL. Gabinete de Segurança Institucional. **Metodologia para gestão de segurança da informação para a administração pública federal.** 30 maio. Brasília. 2006 14 p. Disponível em: < https://www.governoeletronico.gov.br/anexos/metodologia-para-gestao-de-seguranca-da-informacao> Acesso em: 08 dez. 2007.

CASTELLS, Manuel. A sociedade em rede. 7.ed. São Paulo: Paz e Terra, 2003. p.1 –118. (A era da informação: economia, sociedade e cultura, v.1)

MOREIRA, Nilton Stringasci. **Segurança mínima:** uma visão corporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001. 240 p.

NIC BR Security Office. **Cartilha de Segurança para Internet**. Versão 3.1. [s.l]. 11 set. 2007. Disponível em: <http://www.nbso.nic.br/docs/cartilha/>. Acesso em: 06 dez. 2007.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Elsevier, 2003. 156 p.

TEÓFILO, Álvaro. Treinamento e conscientização: fatores essenciais para o sucesso de uma política de segurança. **Módulo Security Magazine**, São Paulo, 15 out. 2002. Disponível em: <http://www.modulo.com.br/pt/page_i.jsp?page=3&catid=2&objid=304&pagecounter=0&idiom=0>. Acesso em 8 out. 2007.

Divulgação

O monitoramento eletrônico e as relações trabalhistas

Alexandre Atheniense

Advogado graduado pela UFMG, com especialização em Internet Law e Propriedade Intelectual (Berkman Center - Harvard Law School). Sócio do escritório Aristoteles Atheniense Advogados. Presidente da Comissão de Tecnologia da Informação do Conselho Federal da OAB. Coordenador e professor do curso de pós-graduação de Direito de Informática da Escola Superior de Advocacia da OAB/SP. Coordenador da Comissão de Estudos da Associação Brasileira de Direito de Informática e Telecomunicações (ABDI) em Minas Gerais. Autor do livro Internet e o Direito e co-Autor dos livros Internet Legal e Manual de Direito Eletrônico e Internet. Atua nas áreas de Direito Empresarial e Direito de Informática. Editor do blog "DNT - O Direito e as Novas Tecnologias" (www.dnt.adv.br).

RESUMO

A utilização de vários dispositivos de comunicação no ambiente empresarial por meio eletrônico pode resultar na transmissão ou acesso de dados sigilosos pelos empregados. Este problema resulta na necessidade de monitoramento eletrônico por parte dos empregadores. Este recurso vem suscitando discussões controversas sobre a violação ao direito de privacidade dos empregados. Neste artigo, serão analisados os fundamentos da licitude e dos limites do monitoramento eletrônico.

A atividade empresarial moderna está inserida em um contexto de extrema competitividade, com demandas crescentes por soluções rápidas e eficazes. O advento e a conseqüente consolidação das tecnologias de informação propiciaram o instrumental necessário para responder adequadamente a estas exigências apontadas. Somado a este fator, observa-se o decréscimo no custo de tais ferramentas, bem como a sua simplificação, permitindo, dessa forma, uma abrangência dilatada de usuários, devido à sua maior acessibilidade.

Nesse diapasão, o implemento da tecnologia adentrou-se não somente nas linhas de produção, mas também em todos os setores da empresa. Esta incorporação deu-se de forma irreversível ao ponto de se constatar a dependência de atividades estritamente secundárias da empresa aos meios de informática e à tecnologia da informação em geral.

O correio eletrônico, especificamente, exerce papel imprescindível nesse cenário delineado. A comunicação veloz e eficaz que ele propicia, permitindo inclusive a incorporação de diversos documentos digitalizados, enseja benefícios imediatos e um prisma de possibilidades que não podem ser desprezados. Salienta-se ainda o baixo custo e o alcance que tal meio de comunicação se reveste, acarretando a adesão em massa em todo o ambiente empresarial.

A tecnologia como um todo é apta a fornecer inúmeras comodidades, mas não se pode ignorar que seu uso inadequado pode gerar danos de amplitudes consideráveis. No que tange às tecnologias da informação, desvios de finalidade podem ser facilmente constatados no âmbito das relações de trabalho, tanto no pólo do empregador, quanto no do empregado.

Sob a ótica do trabalhador, o meio de comunicação eletrônico pode ensejar a transmissão de dados sigilosos a competidores, bem como pode ser um mecanismo para a prática de diversos ilícitos, na seara cível e criminal. Em resguardo a esta constatação, o empregador utiliza variados instrumentos para viabilizar o monitoramento das atividades dos seus prepostos.

O chamado monitoramento eletrônico corresponde justamente à consecução dos meios disponíveis de vigilância com emprego de recursos tecnológicos. Este procedimento é plenamente viável quanto às mensagens eletronicamente transmitidas. Basicamente pode-se distinguir o monitoramento eletrônico em duas modalidades de controle. A vigilância pelo controle formal concretiza-se em programas que analisam aspectos externos da mensagem, tais como o destinatário, o título da mensagem e o registro das páginas visitadas. Via de regra, buscam-se indícios tecnológicos de diversas naturezas que correspondam a ultrapassagem do limite de conduta dos empregados.

Devemos entender que o espectro de monitoramento nas empresas atualmente extrapola o até então restrito controle das mensagens eletrônicas intercambiadas pelos empregados.

O efetivo monitoramento se dá até mesmo antes da efetiva contratação pelo departamento de recursos humanos, que traça um perfil do candidato através da somatória das informações colacionadas a partir de sites de relacionamento. Estas informações cotejadas com os dados dos currículos enviados revelam hábitos inerentes a esfera privada dos candidatos.

Ressalte-se que estas informações tendem a possuir maior credibilidade pois são fornecidas graciosamente pelo usuário, além de fotos e vídeos que compõe este banco de dados interativo, muito mais atraente do que um breve resumo das atividades curriculares.

Nas empresas que se preocupam com a segurança da informação, constitui-se regra a adoção de política de segurança interna onde se impõe a criação de regras sistêmicas somadas às normas legais vigentes, de modo a delimitar com eficiência o limite da conduta no meio digital a ser concedido a cada empregado.

A publicidade desta política reduzida a um termo de adesão obrigatório, será fundamental para conversão em prova inconteste do poder diretivo dos empregados em discussões trabalhistas futuras.

Nesta política não se encontram apenas definidos o conteúdo ou site e serviços que serão vedados aos empregados, mas também o alcance do acesso permitido a rede interna e externa e os recursos que serão utilizados para este fim.

As ferramentas que permitem regular o uso seguro das informações estão se aperfeiçoando com o uso das identidades biométricas e certificação digital, de modo a deixar indícios inequívocos sobre o acesso e compartilhamento de materiais considerados como ilícitos.

Essa política demanda vigília e revisão permanente, seja no aspecto sistêmico quanto legal, uma vez que as ferramentas de interatividade na internet e no ambiente de trabalho se aperfeiçoam a cada dia, não significando que inexista suficiente proteção jurídica para tornar a captura destas informações pelo empregador como meio de prova ilícita a ser produzida em processos judiciais.

Impõe-se que o poder diretivo do empregado no ambiente de trabalho permita que este se traduza no maior numero possível de logs que possam evidenciar todas os atos praticados pelos empregados a partir do momento que se conecta a infra-estrutura tecnológica da empresa.

O monitoramento eletrônico ampara-se em diversos fundamentos legais. Primeiramente, menciona-se o poder de direção atribuído ao empregador (art. 2º da CLT), visando o controle e direcionamento da atividade desenvolvida pela empresa. Esta diretriz advém do próprio direito de propriedade, vinculando a determinação do uso e da fruição ao seu titular.

A influência da propriedade não se restringe àquela supra mencionada. Para a determinação de sua real abrangência, insta distinguir as duas modalidades de correio eletrônico disponibilizadas em um ambiente de empresa.

O chamado e-mail corporativo consiste no correio eletrônico fornecido pela empresa ao seu preposto. Há uma identificação direta com a empresa devido à adoção de nomenclatura do empregador, o chamado domínio na internet (por exemplo: fulano@empresabeltrana.com.br).

Já o denominado e-mail privado é aquele provido por ente alheio ao empregador. Não obstante, o acesso a tal meio de comunicação se concretiza apenas com a utilização da estrutura, do maquinário de propriedade da empresa.

Destarte, o e-mail corporativo pode ser facilmente caracterizado como ferramenta de trabalho, nos

termos do art. 458, §2º da CLT, e, como tal, tem sua função adstrita ao exercício da atividade laboral.

A função da senha e sua respectiva finalidade adquirem relevância neste contexto. A tentativa de descaracterização do e-mail corporativo como ferramenta de trabalho é impulsionada pelo argumento de que a senha fornecida ao empregador teria como propósito a garantia de sua privacidade frente ao seu empregador, bem como a terceiros. Não se pode olvidar o fato de que as senhas, nesta modalidade de correio eletrônico, são criadas e posteriormente fornecidas diretamente pelo empregador aos seus prepostos. O intuito nitidamente perceptível é o resguardo de informações pertinentes à empresa que são transmitidas por tal meio de comunicação, ocorrendo, por conseguinte, a proteção da atividade empresarial desenvolvida em face de terceiros e até mesmo do próprio empregado.

O conhecimento quanto à senha, destarte, decorre logicamente da própria estrutura do e-mail corporativo. Enfatiza-se que posicionamento contrário poderia até mesmo gerar obstáculos consideráveis à realização da atividade empresarial. Basta salientar o transtorno que o impedimento do empregado poderia causar. Seu afastamento, por qualquer motivo, poderia ensejar, no mínimo, a interrupção do curso normal do trabalho e a ausência de acesso a dados imprescindíveis.

São também fundamentos para a determinação da licitude do monitoramento eletrônico as inúmeras hipóteses legais de responsabilização do empregador pela conduta de seus prepostos. Nesta seara, menciona-se o art. 932, III do Código Civil que atribui a responsabilidade objetiva do empregador por fato de terceiro. O tipo penal previsto no art. 241, §1º, III do Estatuto da Criança e do Adolescente quanto à transmissão de material envolvendo pedofilia por meio eletrônico. O crime de violação de direitos autorais disposto no art. 12 da Lei 9.609/98, também pode ser mencionado.

A atribuição de crime à conduta do empregado que viola segredo profissional (art. 154 do Código Penal), assim como o delito de concorrência desleal (art. 195 da Lei 9.279/96), da mesma forma incluem-se no rol de legítimos fundamentos para o monitoramento eletrônico. No entanto, o monitoramento eletrônico pode esbarrar em garantias fundamentais do cidadão, acarretando conflitos que passam a ser observados no Judiciário brasileiro.

Os argumentos formulados contrariamente ao monitoramento residem basicamente na proteção dada pela Constituição ao sigilo das comunicações (art. 5º, XII). Esta proteção constitucional é decorrência lógica de outra garantia fundamental: a privacidade (art. 5º, X).

A fixação da possível antinomia deve ser realizada com cautela. Os supostos óbices constitucionais ao monitoramento eletrônico cingem-se à vedação ao controle material das mensagens. A vigilância desenvolvida por meios de controle meramente formais não atinge a inviolabilidade tutelada pela Magna Carta e, portanto, nesta modalidade, não há que se falar em conflito de valores constitucionais.

Quanto ao controle material, diversas variáveis devem ser levadas em consideração. Inicia-se perquirindo a natureza jurídica do correio eletrônico. A controvérsia quanto a este ponto é presente na doutrina. Sua caracterização como correspondência torna-se pressuposto essencial para a corrente que pugna pela inviolabilidade de seu conteúdo.

Relevante a consideração de Kildare Gonçalves Carvalho (2004: 390) que assevera:

> *"Quanto à inviolabilidade de correspondência, embora não haja, quanto a ela, previsão expressa no texto constitucional permitindo seja interceptada, deve-se entender possa ser quebrada naqueles casos em que venha a ser utilizada como instrumento de práticas ilícitas"*.

A perspectiva do citado constitucionalista encontra fulcro no princípio da proporcionalidade. Uma norma constitucional não deve prevalecer de forma abstrata e apriorística em relação à outra. Constatada a antinomia, esta se resolve por meio do princípio da proporcionalidade.

Contudo, a caracterização do correio eletrônico como correspondência não abrange o cerne da questão, podendo até mesmo ser considerada inócua. Mesmo que se repute o correio eletrônico como correspondência, os limites de sua proteção estão determinados na Lei 9.296/96, que regulamentou o aludido dispositivo constitucional.

O artigo 10 da mencionada lei ordinária estatui: "*Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei*". A exegese da norma aponta a permissividade do monitoramento desde que haja autorização judicial ou se esteja munido por uma finalidade legalmente tutelada. Neste ponto urge o reforço dos inúmeros fundamentos legais apresentados para o monitoramento eletrônico, atribuindo legitimidade ao seu implemento, desde que adstrito aos objetivos apresentados.

O Tribunal Superior do Trabalho manifestou-se quanto ao tema no RR 613, publicado em 10/06/2005. Esta importante decisão reconhece a legalidade do monitoramento do e-mail

corporativo. Pertinente a vinculação do monitoramento ao controle realizado "de forma moderada, generalizada e impessoal". O desvio destes objetivos configura abuso de direito (art. 187 do Código Civil), viabilizando inclusive a reparação civil.

A garantia da inviolabilidade das comunicações nos termos supra descritos funda-se na proteção ao direito à privacidade, como já assentado. Portanto, sua correta definição torna-se imprescindível para a solução do conflito posto. Costumeiramente, aborda-se o tema da privacidade pela delimitação de sua abrangência, deslocando-se do ponto essencial da questão.

Mesmo a doutrina que procede à perspectiva do direito adstrita a sua amplitude reconhece a relativização de seu conteúdo, moldado segundo algumas especificidades. Alexandre de Morais (2000: 74) estabelece os parâmetros para tal restrição: *"Essa necessidade de interpretação mais restrita, porém, não afasta a proteção constitucional contra ofensas desarrazoadas, desproporcionais e, principalmente, sem qualquer nexo causal com a atividade profissional realizada"*.

Da mesma forma, pondera José Afonso da Silva (1996: 204) ao distinguir os aspectos da vida da pessoa: *"A vida exterior, que envolve a pessoa nas relações sociais e nas atividades públicas, pode ser objeto das pesquisas e das divulgações de terceiros, porque é pública"*.

O conteúdo abrangido pela privacidade é de relevante determinação, entretanto, a limitação a este aspecto foge do núcleo do problema. A privacidade consiste em essência, não ao seu conteúdo em si. Refere-se ao poder atribuído ao seu titular de autodeterminar a exteriorização do conteúdo que abrange o próprio conceito de privacidade. O conceito colacionado por José Afonso da Silva (1996: 202) é de precisão irreparável, caracterizando a privacidade como *"o conjunto de informação acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito"*.

Nestes termos, não se cogita de violação à privacidade pelo simples fato de ocorrer o conhecimento de terceiro quanto a elemento intrínseco à esfera íntima do indivíduo. A ofensa à privacidade exige o cerceamento na faculdade do titular em determinar os destinatários de tais informações[1].

Esta noção, aplicada à problemática do monitoramento eletrônico, produz efeitos imediatos em sua resolução. Fixa-se a premissa que o e-mail corporativo, como ferramenta de trabalho que é, restringe-se à transmissão de mensagens pertinentes à atividade laboral desenvolvida. Admitido este pressuposto, tem-se que o monitoramento eletrônico é legítimo, pois seu objeto de incidência não alcança conteúdo da esfera privativa do empregado.

Assim, o ambiente proporcionado pelo e-mail corporativo é desprovido de qualquer expectativa de privacidade. O envio de mensagens com conteúdo íntimo não caracteriza violação da privacidade, devido à cognição do empregado, quanto à natureza do meio de comunicação utilizado. Não ocorreu, neste caso, subtração ao poder de autodeterminação do preposto como já ressaltado, restando, incólume, a sua privacidade.

Não obstante a predisposição do e-mail corporativo como ferramenta de trabalho e as já expostas conseqüências advindas de tal imputação, a conduta das partes é elemento idôneo à modificação destas características. O contrato de trabalho demanda que a atuação de seus figurantes seja pautada pela boa-fé. O dever de informação insere-se plenamente neste instituto.

A vedação expressa ao uso particular do e-mail corporativo e a previsão do monitoramento eletrônico de tal meio de comunicação, disposta no contrato de trabalho ou em termo aditivo (art. 444 da CLT), não somente qualifica a conduta do empregador como fiel, mas também torna inequívoco o comportamento esperado do empregado.

É notório que o direito do trabalho (material e processual) possui, como um de seus princípios regentes, o da proteção. A inércia do empregador, acrescida de demais variáveis relevantes, pode caracterizar sua anuência tácita quanto ao uso particular do correio eletrônico, sendo esta perspectiva reforçada pelo princípio acima apresentado.

A repercussão do aludido aceite tácito modifica a própria natureza do correio eletrônico. Admitida sua utilização para fins alheios à atividade laboral, tem-se criada a legítima expectativa do empregado quanto ao respeito de informações pertinentes à sua esfera íntima, suscitando a

1 A título de exemplo menciona-se a seguinte situação: um indivíduo que procede a um diálogo com seu amigo, abordando aspectos de sua intimidade, em um elevador lotado de passageiros não tem sua privacidade violada. Apesar destas informações alcançarem terceiros, este fato ocorreu sem mácula à sua faculdade de autodeterminação.

necessidade de um ambiente de privacidade. Como não há modo de se aferir aprioristicamente a natureza do conteúdo da mensagem, senão pela sua averiguação, o monitoramento eletrônico (material como já enfatizado) neste contexto deve ser reputado ilícito.

Em síntese, o usuário de e-mail privado detém expectativa de privacidade quanto a este meio de comunicação, ensejando assim a proteção do conteúdo das mensagens transmitidas. Já o e-mail corporativo, a princípio, poderia ser objeto de controle material desde que não caracterizada a aceitação tácita pelo empregador para fins distintos da atividade laboral.

Torna-se assim aconselhável que o empregador proíba o uso do correio eletrônico corporativo para fins diversos. Caso a política da empresa deseje permitir o uso privado, o caminho mais sensato seria a exigência de que as mensagens privadas sejam transmitidas por e-mail privado. Este posicionamento é facilmente realizado tendo em vista os inúmeros provedores que oferecem tal serviço gratuitamente na internet.

De todo modo, optando o empregador a permitir seus prepostos a utilizarem o e-mail corporativo para fins privados, o monitoramento eletrônico somente torna-se sustentável caso se estabeleça um horário rígido para a veiculação de tais mensagens. Neste lapso temporal facultado ao empregado, por consectário lógico, o monitoramento eletrônico é veemente proibido.

Quanto a qualificação das provas obtidas com o monitoramento, a licitude daquelas é determinada pela validade deste. Ou seja, o resultado de um monitoramento validamente realizado (nas hipóteses já devidamente arroladas) pode ser perfeitamente utilizado para a instrução probatória em eventual lide.

A despeito de se viabilizar as provas obtidas pelo monitoramento nas hipóteses acima delineadas, o uso de e-mail corporativo para fins privados não acarreta por si só a possibilidade de rescisão do contrato por justa causa. A jurisprudência tem exigido a demonstração de prejuízo ao desenvolvimento normal do trabalho ou idoneidade dos atos para causarem danos à empresa[2].

As questões envolvendo o monitoramento eletrônico ainda podem ser consideradas incipientes. Somado a este fato, tem-se o envolvimento de um complexo de valores de grande apreço no bojo constitucional, o que acaba por acirrar a controvérsia. Inúmeras decisões judiciárias conflitantes foram prolatadas, cenário este que felizmente tende a ser sanado com a já mencionada decisão do Tribunal Superior do Trabalho quanto ao tema. Espera-se a observância deste precedente para que se estabeleça maior segurança jurídica nas relações de trabalho.

Referências

ARAÚJO, L. A. D. *A correspondência eletrônica do empregado e o poder diretivo do empregador*. In: Revista de direito constitucional e internacional. v.40. São Paulo: 2002.

BARROS, A. M. *Curso de direito do trabalho*. São Paulo: LTr, 2005.

BELMONTE, A. A. *O controle da correspondência eletrônica nas relações de trabalho*. In: Revista LTr, v. 68, n.9. São Paulo: LTr, 2004.

CARVALHO, K. G. *Direito constitucional*. 10 ed.. Belo Horizonte: Del Rey, 2004.

FERRAZ JR, T.S. *Sigilo de dados*: o direito a privacidade e os limites à função fiscalizadora do Estado. In: Cadernos de direito constitucional e ciência política. n. 19. São Paulo: 2002.

LEITE, C. H. B. *Curso de direito processual do trabalho*. 3 ed. São Paulo: LTr, 2005.

MORAES, A. *Direito constitucional*. 7 ed. São Paulo: Atlas, 2000.

PECK, P. *O mau uso da tecnologia e a falta de observância da arquitetura legal geram riscos desnecessários para as empresas*. Disponível em: http://www.serpro.gov.br/noticiasSERPRO/200521406. Acesso: 25/08/2006.

SILVA, J. A. da *Curso de direito constitucional positivo*. 11 ed. São Paulo: Malheiros, 1996.

SOUZA, M. c. m. de. *E-mail (... net) na relação de emprego*: poder diretivo do empregador (segurança) & privacidade do empregado. Kplus. Disponível em: http://kplus.cosmo.com.br.materia.asp?co= 46&rv=Direito. Acesso em: 29/11/2006.

2 *"Justa causa. Email não caracteriza-se como correspondência pessoal. O fato de ter sido enviado por computador da empresa não lhe retira essa qualidade. Mesmo que o objetivo da empresa seja a fiscalização dos serviços, o poder diretivo cede ao um único email enviado para fins particulares, em horário de café, não tipifica justa causa"* (TRT-SP n. 2000034734, rel. Fernando Antônio Sampaio da Silva).

Aplicação de ontologias em segurança da informação


Divulgação

Mauricio B. Almeida

Doutor em Ciência da Informação (UFMG), atualmente é professor adjunto do departamento de Teoria e Gestão da Informação da UFMG, onde está integrado à linha de pesquisa Gestão da Informação e do Conhecimento. Mantém pesquisas nas áreas de Representação do Conhecimento e Ontologias, Sistemas de Informação, Memória Organizacional e Preservação Digital.

RESUMO

Segurança da informação é um assunto relevante em praticamente todas as organizações. Ao mesmo tempo em que sentem necessidade de implementá-la, os gerentes não possuem clareza sobre o que deve ser protegido e como fazê-lo. Este artigo apresenta uma visão geral da pesquisa na área e descreve iniciativas diversas. Destaca a importância de classificar a informação no ambiente corporativo e conclui que existem benefícios na aplicação de ontologias em segurança da informação. Espera-se contribuir com uma revisão de literatura, sem a pretensão de que seja exaustiva e com um roteiro para construção de ontologias, bem como sua integração aos recursos corporativos.

1. Introdução

A expressão segurança da informação representa um conceito amplo. Em geral, nas empresas e nas instituições, está associada a sistemas informatizados e a dados que estes manipulam. Entretanto, uma organização não possui apenas dados em formato digital. Considere-se que muita informação sobre uma empresa está armazenada fora dela (governo, conselhos, fornecedores, etc.). Considere-se, ainda, a complexidade do ciclo de vida da informação, desde sua produção até sua disseminação, e as influências do fator humano. Mesmo se observado apenas o contexto das organizações, não parece tarefa trivial definir segurança da informação.

Os problemas de muitas organizações na implementação de segurança da informação estão relacionados com a dificuldade em definir o que deve ser protegido, qual o nível de proteção necessário e quais ferramentas utilizar no ambiente corporativo. A dificuldade começa na própria definição do objeto a proteger, ou seja, na definição da informação. Wilson (2002) alerta para o uso indistinto dos termos dado e informação. Para o autor, dados são fatos e estão fora da mente de uma pessoa. Informações consistem de dados aos quais se incorpora um contexto relevante para o indivíduo. Cabe então à organização descobrir em quais

contextos a informação crítica se manifesta e quais as necessidades corporativas em relação à segurança, e não apenas buscar proteção para dados em computadores e em redes.

A despeito da discussão, a expressão segurança da informação é amplamente utilizada no ambiente corporativo e envolve uma série de possibilidades, muitas delas, associadas à Tecnologia da Informação (TI): controle de acesso a recursos (dispositivos ou documentos); segurança em comunicação; gestão de riscos; políticas de informação; sistemas de segurança; diretrizes legais; segurança física; criptografia; arquivística; dentre outros (Krause e Tipton, 1997). Para o Legal Information Institute (2005), segurança da informação diz respeito a proteger a informação e os sistemas de informação de acesso não autorizado, uso, divulgação, modificação ou destruição. Está relacionada a três aspectos: integridade, confidencialidade e disponibilidade. Integridade diz respeito à proteção contra alteração indevida ou destruição, assegurando a autenticidade e o não-repúdio. Confidencialidade significa preservar restrições de divulgação e de acesso, garantindo meios para proteção da privacidade pessoal. Disponibilidade significa assegurar o acesso e o uso da informação de forma confiável.

Este artigo destaca a importância da classificação da informação em questões de segurança. Apresenta uma abordagem com base em ontologias para segurança da informação. O termo ontologia nasceu na filosofia, mas tem sido utilizado para designar uma estrutura de organização da informação que se baseia em conceitos e em suas relações. Esperam-se duas contribuições principais ao leitor: i) informar sobre as abordagens disponíveis na literatura, proporcionando uma visão geral da área; ii) apresentar a ontologia como um importante instrumento passível de utilização em iniciativas de segurança.

O restante do presente artigo está dividido em quatro seções: a seção dois apresenta considerações sobre segurança da informação nas organizações, com destaque para iniciativas governamentais e iniciativas normativas; a seção três destaca as iniciativas que envolvem a TI; a seção quatro enfatiza as iniciativas que envolvem a TI e, ao mesmo tempo, utilizam ontologias como ferramenta de classificação, além de apresentar um roteiro sobre como construir ontologias para fins de segurança da informação; e a seção cinco apresenta as considerações finais.

2. Visão geral sobre segurança da informação

Para muitas organizações, a segurança da informação é uma necessidade de negócio. Ainda assim, nem sempre se implementam práticas para tal, visto que os projetos necessários são caros, complexos, demandam tempo e não têm garantia de sucesso. Segundo Fowler (2005), os principais mecanismos para proteger as informações corporativas são: as políticas de segurança da informação, a análise de riscos e a classificação da informação.

Uma política de segurança é um plano de alto nível que estabelece como esta segurança deve ser praticada na organização, que ações são aceitáveis e que nível de segurança a organização está disposta a aceitar. A análise de riscos consiste da prática de confrontar o valor da informação e as ameaças com perdas, bem como identificar meios de proteção que possam reduzir riscos. Os procedimentos de classificação da informação agrupam objetos similares em categorias, o que possibilita implementar medidas de proteção que vão garantir a confidencialidade da informação.

Existem diversos tipos de iniciativas para lidar com problemas de segurança da informação, dentre os quais se destacam: iniciativas governamentais; iniciativas normativas; iniciativas tecnológicas.

No contexto da Federation of American Scientists (FAS), associação formada em 1946 pelos cientistas atômicos do Projeto Manhattan[1], Quist (1993) discute a necessidade de uma classificação da informação, para fins de segurança e descreve as três ações principais para tal: i) determinar se a informação deve ser classificada; ii) determinar o nível de classificação; iii) determinar a duração da classificação. O autor também apresenta procedimentos para avaliar, se a informação deve ser classificada: i) definir precisamente a informação, descrevendo-a em linguagem sem ambigüidades; ii) verificar a existência de classificação específica

1 Projeto em que os Estado Unidos tentavam desenvolver a primeira arma nuclear durante a 2º Guerra Mundial.

para o setor da organização, onde a informação foi obtida; iii) verificar se a informação é controlada pelo governo; iv) determinar se a divulgação da informação causará danos à segurança nacional; v) especificar, precisamente, porque a informação é classificada.

O ISOO (2003) estabelece um sistema de classificação da informação para segurança no âmbito do governo norte-americano. São descritas algumas regras sobre classificação de documentos, como, por exemplo: i) apenas pessoas autorizadas podem classificar documentos originais; ii) existem apenas três níveis de classificação: supersecreto, secreto e confidencial; iii) informações não devem ser classificadas pelo sistema de classificação, caso não sejam de interesse da segurança nacional. O ISOO (2003) descreve ainda marcas obrigatórias, aplicadas aos documentos originais, para identificação dos níveis de segurança a adotar: i) marcas em partes do documento, caso tais partes tenham diferentes classificações; ii) classificação do documento como um todo, com o nível mais restrito de classificação presente dentre as partes do documento; iii) inserção dos campos *classificados por, razão da classificação e data final da classificação* no documento.

No Canadá, o Government of Alberta (2005) dispõe de um sistema de classificação de documentos que tem por objetivos: i) proteger a informação pessoal; ii) proteger a informação confidencial contra acesso não autorizado; iii) proteger a propriedade intelectual do governo; iv) dar suporte à disseminação de informação; v) possibilitar cooperação intergovernamental e para segurança pública. O sistema de classificação identifica quatro níveis de segurança para a informação: irrestrita, protegida, confidencial e restrita. Existem casos em que a informação é de interesse nacional e, assim, classificada como: confidencial, secreta e supersecreta. Na prática, a implementação da classificação envolve os seguintes procedimentos: i) marcar a informação; ii) armazená-la; iii) transmiti-la; iv) descartar a informação desnecessária; v) permitir o acesso e a divulgação apropriados; vi) estabelecer responsabilidades.

Baker (2004) estabelece categorias para informação e para sistemas de informação, no âmbito do National Institute of Standards and Technology (NIST)[2]. As categorias propostas – *baixa*, *moderada*, *alta* – têm como base o impacto potencial para a organização, quando ocorrem eventos que colocam em risco a informação e os seus sistemas. A avaliação do impacto em categorias fundamenta-se nos objetivos de segurança para informação e para sistemas de informação (confidencialidade, integridade, disponibilidade) especificados pelo Legal Information Institute (2005).

Baker (2004) apresenta um conjunto de procedimentos para mapeamento entre a informação e os níveis de impacto que pode provocar: i) identificar sistemas de informação; ii) identificar tipos de informação; iii) selecionar níveis de impacto temporários; iv) rever e ajustar níveis de impacto temporários; v) atribuir categoria do sistema de segurança. O autor descreve, ainda, outro conjunto de procedimentos para identificar os tipos de informações: i) identificar as áreas de negócio fundamentais; ii) identificar, para cada área de negócio, as operações que descrevem o propósito do sistema em termos funcionais; iii) identificar as subfunções necessárias para conduzir cada área; iv) selecionar tipos de informações básicas associados com as subfunções identificadas; v) identificar qualquer tipo de informação que receba manipulação especial por ordem superior ou agência regulatória.

As iniciativas citadas apresentam considerações sobre segurança da informação, sem, entretanto, definir exatamente a qual objeto se refere, quando citam o termo "informação". Além disso, também não é citado o meio onde a informação é disseminada na organização. Uma importante forma para disseminação é o meio digital, representado por documentos em formato digital, sistemas de informação automatizados, dentre outros recursos de TI.

3. Segurança da informação no contexto da TI

Em muitas organizações, os gerentes encarregam as equipes de TI de solucionar questões de segurança da informação. Tal prática tem conduzido a planos de segurança fundamentados em soluções puramente tecnológicas e, dessa forma, ineficientes em atender às necessidades da organização. A comunidade de

2 Parte do U.S. Department of Defense.

negócios é quem realmente sabe da importância de determinada informação no contexto organizacional e deve participar ativamente do planejamento da segurança.

A ISO/IEC-15408-1 (2005) é a principal referência para avaliação de atributos de segurança em produtos e em sistemas de TI, os quais são denominados *objetos de avaliação*. Usuários de TI, sejam consumidores, desenvolvedores ou avaliadores, nem sempre possuem conhecimento ou recursos para julgar questões de segurança. Para atender a esses usuários, a ISO/IEC-15408-1 (2005) estabelece um critério comum para a avaliação, o que possibilita que o resultado seja significativo para audiências variadas. O resultado das avaliações da ISO/IEC-15408-1 (2005) auxilia os consumidores de TI a decidirem se um produto ou sistema atende aos requisitos de segurança. Do ponto de vista do desenvolvedor, a norma descreve as funções de segurança, que devem ser incluídas no projeto do *objeto de avaliação*. Do ponto de vista dos avaliadores e de outros membros da organização, a norma determina as responsabilidades e as ações necessárias para a avaliação do objeto.

No âmbito da internet, cabe destacar o papel do Computer Emergency Response Team/Coordination Center (CERT/CC), criado pelo Defense Advanced Research Projects Agency (ARPA), após o incidente worm[3], em 1988. O objetivo é centralizar a coordenação de respostas a incidentes de segurança. Além disso, o CERT ainda é responsável por publicar informes, pesquisar sobre segurança e manter um banco de dados sobre segurança em redes e na internet.

Além das referências principais, uma grande diversidade de iniciativas para segurança da informação, na área de TI, vem surgindo desde os anos 80: roteiros para avaliações e para auditorias (Kraus, 1980; GAO, 1988; Garfinkel e Spafford, 1996; ISACF, 2000; ISSEA, 2003); listas de verificação (Wood, et al. 1987; CIAO, 2000); diretrizes e critérios (OECD, 1992; Wood, et al. 1990; NIST/CSD, 1998), listas de termos e taxonomias (Neumann e Parker, 1989; Meadows, 1992; Levine, 1995; Howard e Longstaff, 1998).

Dentre essas iniciativas, destaca-se a taxonomia de incidentes de segurança proposta por Howard e Longstaff (1998). Os autores advogam a necessidade de uma linguagem comum sobre segurança, que permita o intercâmbio e a comparação de dados sobre incidentes de segurança. Tal linguagem é composta por termos de alto nível, ou seja, genéricos, estruturados em uma taxonomia.

Na linguagem de Howard e Longstaff (1998), um evento corresponde a uma alteração no estado do sistema ou dispositivo. A alteração é resultado de ações (autenticar, ler, copiar, etc.) direcionadas a objetos (conta, processo, dado, rede, etc.). Um evento pode ser parte de um conjunto de processos, que objetivam ocorrências não autorizadas. Esse evento é, então, parte de um ataque. Um ataque utiliza uma ferramenta (ataque físico, comando, script, etc.), para explorar a vulnerabilidade de um dispositivo, que corresponde a uma falha no sistema e permite ação não autorizada. A vulnerabilidade pode ser de projeto, de implementação ou de configuração. Além disso, provoca um evento e gera um resultado não autorizado (acesso indevido, roubo de recursos, etc.). Um grupo de ataques que envolve diferentes agentes, objetivos, locais ou horários, é denominado incidente. Um incidente é um ataque mais um objetivo, o qual pode ser ganho político ou financeiro, danos ou prejuízos, etc.

O uso de uma linguagem única, com significados consensuais, possibilita a construção de modelos sobre um domínio do conhecimento e pode incrementar a forma com que os indivíduos da empresa aprendem novas práticas, compartilham conhecimento e o armazenam com um nível de ambigüidade reduzido (Von Krogh e Roos, 1995; Eccles e Nohria, 1994). As linguagens informais, como a linguagem natural, são expressivas, mas geram interpretações ambíguas. As linguagens formais proporcionam a criação de modelos com nível de ambigüidade reduzido e com significados consistentes para o contexto da organização. Uma ontologia pode operacionalizar a linguagem formal, visto que possui conceitos, relações e atributos semanticamente bem definidos e pode variar em grau de formalidade, conforme a necessidade.

A linguagem representada pela ontologia precisa estar restrita apenas a um vocabulário sobre segurança da informação. Pode abranger conceitos significativos para uma organização naquele domínio, além de permitir a classificação da informação registrada, ou seja, a classificação dos documentos corporativos pelos próprios membros da organização.

3 Robert T. Morris, estudante da *Cornell University*, criou, em 1988, um *worm* para um experimento de acesso a computadores. O programa deveria detectar a existência de cópias de si mesmo e não reinfectar computadores. Um bug impediu a detecção e sistemas foram infestados com centenas de cópias do worm, cada uma delas tentando acesso e se replicando em mais worms. (Menninger, 2005)

4. Ontologias aplicadas à segurança da informação

O termo ontologia é originário da filosofia e tem sido utilizado desde o início dos anos 80, em Ciência da Computação e em Ciência da Informação, para designar uma estrutura de organização da informação, com base em um vocabulário representacional. Segundo Borst (1997), uma ontologia é uma especificação formal e explícita de uma conceitualização compartilhada. Nessa definição, formal significa legível por computadores; especificação explícita diz respeito a conceitos, relações e a axiomas explicitamente definidos; compartilhado quer dizer conhecimento consensual; conceitualização diz respeito a um modelo abstrato de algum fenômeno do mundo real[4].Com aplicações em diversas áreas, as ontologias também servem a propósitos de segurança da informação, conforme comprovam exemplos apresentados na seção 4.1. A seção 4.2 apresenta um breve roteiro sobre como construir uma ontologia organizacional, para classificação da informação em projetos de segurança da informação.

4.1 Pesquisa anterior significativa sobre ontologias em segurança

Segundo Raskin et al. (2001), a pesquisa em segurança da informação pode se beneficiar da adoção de ontologias. Os autores apresentam duas propostas para utilização da ontologia na pesquisa em segurança da informação.

A primeira proposta enfatiza a possibilidade de reunir um conjunto de termos e relações representativos do domínio de segurança da informação. Uma ontologia sobre segurança da informação auxilia os usuários de produtos e sistemas de informação ao proporcionar intercâmbio, organização e comparação de dados sobre incidentes de segurança, bem como melhorias na capacidade de tomada de decisão diante de um incidente.

A segunda proposta consiste em incluir fontes de dados em linguagem natural na aplicação de ações em segurança da informação. Dessa forma, seria possível especificar formalmente o know-how da comunidade de segurança, possibilitando o incremento de medidas para prevenção e para reação a ataques. O Processamento de Linguagem Natural (PNL)[5] pode ser aplicado, por exemplo, no processamento de logs de sistemas, os quais são escritos em uma sublinguagem da linguagem natural.

Para Martiniano e Moreira (2007), o grande volume de dados gerado por diferentes fontes, tais como logs de sistemas, de firewalls[6], alertas de vulnerabilidade, etc., tem causado problemas aos administradores. O principal problema está relacionado com a dificuldade em acumular conhecimento para a tomada de decisão e para a solução de incidentes de segurança.

Apesar dos esforços em classificar dados sobre segurança, as iniciativas, em geral, não contemplam a semântica dos dados armazenados. Sem o significado dos dados, um administrador ou um agente de software não é capaz de fazer correlações sobre os incidentes de segurança. Nesse contexto, Martiniano e Moreira (2006) propõem uma ontologia de incidentes de segurança, a qual define um vocabulário único. A maioria dos conceitos da ontologia sobre incidentes de segurança foi obtida de glossários e taxonomias sobre segurança da informação (Howarde Longstaff, 1998; NSCS, 1988; Shirley, 2000), em recursos sobre vulnerabilidade (NVD-National Vulnerability Database[7], CVE-Common Vulnerabilities and Exposures Project[8]). Para avaliar se é representativa, a ontologia foi confrontada com o SNORT[9].

Fenz et al. (2007) também propõem a construção de uma ontologia,

4 Para um estudo comparativo das diversas definições de ontologias e suas aplicações ver Almeida (2003).

5 *Processamento da linguagem* natural é um campo da lingüística computacional que estuda os problemas de compreensão e geração automática de linguagens naturais.

6 Um *firewall* é uma aplicação que analisa o tráfico em uma rede, dando permissão ou não para a passagem de dados a partir de um conjunto de regras.

7 O NVD é um repositório de padrões do governo norte-americano voltado para questões de vulnerabilidade. Disponível na internet em http://nvd.nist.gov/.

8 CVE é um dicionário público com informações sobre vulnerabilidades. Disponível na internet em http://cve.mitre.org/.

9 SNORT é uma rede com recursos sobre prevenção e detecção de invasões em sistemas, a partir de uma linguagem com base em regras. Disponível na internet em http://www.snort.org/.

em Ontology Web Language (OWL), de suporte à certificação ISO/IEC-27001 (2005), com informações para criação e manutenção de políticas de segurança. O mapeamento ontológico do padrão ISO aumenta o grau de automação do processo, reduzindo custos e o tempo para a certificação. A ontologia de suporte é criada a partir da combinação de três recursos principais: i) a CC Ontology (Ekelhart et al., 2007), a qual contempla o domínio Common Criteria[10] (CC) e enfatiza requisitos de garantia de segurança para a avaliação; ii) a Security Ontology (Ekelhart et al., 2006), que contém dados sobre ameaças e respectivas medidas de proteção; iii) o próprio padrão ISO/IEC-27001 (2005). A Figura 1 apresenta um fragmento de uma ontologia sobre segurança.

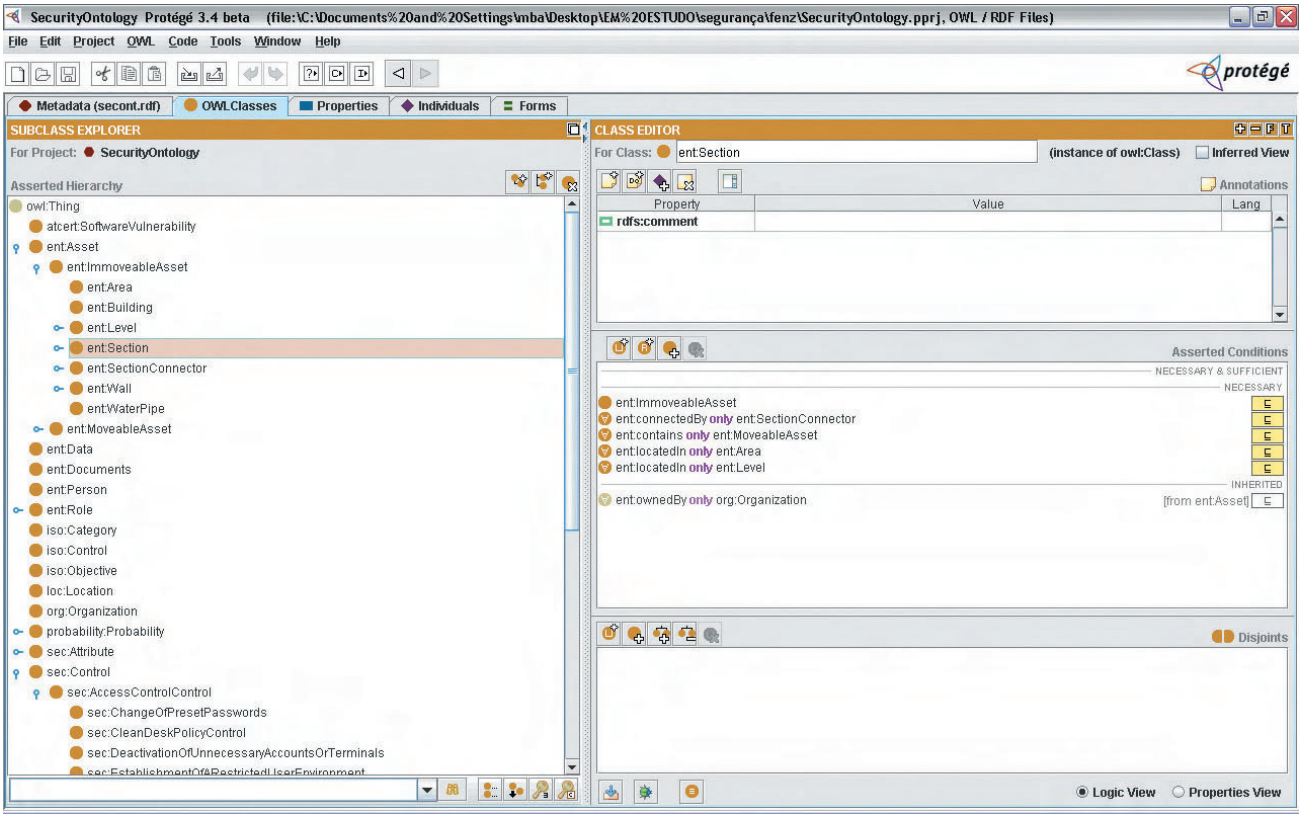


Figura 1 – Ontologia de incidentes em um editor de ontologias (Fenz et al., 2007).

4.2 Construção de ontologia organizacional para segurança da informação

Existem aplicações com base em ontologias para segurança da informação, conforme comprovam as iniciativas apresentadas na seção 4.1. Tais iniciativas estão relacionadas com a criação de um vocabulário consensual, de alto nível, com termos sobre segurança da informação. Pretende-se apresentar uma abordagem que enfatize duas ações principais: i) agrupamento dos termos sobre segurança em uso no dia-a-dia da

10 O *CC-Common Criteria for Information Tecnhnology Secutity Evaluation* fornece diretrizes para avaliação e certificação de segurança.

organização e dos termos obtidos em ontologias de alto nível, os quais representam padrões aceitos no domínio; ii) integração do vocabulário sobre segurança a um vocabulário mais amplo, representativo da informação registrada e compartilhado por todos os membros da organização. As duas contribuições podem ser operacionalizadas em uma ontologia.

Apresenta-se, a seguir, um conjunto de procedimentos e uma breve descrição sobre como construir ontologias para classificação de informação registrada (documentos). O processo foi dividido em duas etapas, apresentadas de forma genérica: 1- Ontologia e 2- Recursos corporativos.

Etapa 1 – Ontologia

i. Aquisição de conhecimento: o objetivo dessa etapa é obter, com os membros de um setor, informações sobre suas atividades, sobre documentos que utilizam, sobre conceitos e relações relevantes para o entendimento das práticas organizacionais. As técnicas mais utilizadas para isso são as entrevistas e a análise de documentos.
ii. Conceitualização: os dados são organizados em uma taxonomia corporativa composta por classes representativas de conceitos, bem como por relações entre as classes; em ontologias, classes representam uma categoria de objetos similares, denominados instâncias.
iii. Construção da ontologia[11]: a ontologia é então construída por meio de um editor de ontologias e em duas camadas: a primeira, de alto nível (reaproveitamento de outras ontologias, como as da seção 4.1); a segunda, com termos específicos do ambiente de trabalho, levantados na fase de aquisição de conhecimento e organizados na fase de conceitualização.

Etapa 2 – Recursos corporativos

i. Organização dos documentos: a partir de princípios da arquivística, organizam-se os documentos, conforme sua origem, registram-se a tipologia de documentos e seu ciclo de vida e elegem-se os documentos vitais[12] para as atividades corporativas.
ii. Padronização dos documentos: a partir de princípios da Organização, Sistemas e Métodos (OSM), os documentos são padronizados formalmente e é acrescentada uma folha de rosto a cada um, na qual são registrados dados como autor, data de emissão, data de revisão, autorização, dentre outros.
iii. Classificação dos documentos: os membros dos setores são orientados e treinados para classificar documentos, conforme as classes definidas na ontologia, assim que estes são produzidos; a classificação é feita na folha de rosto e pode ocorrer, a partir de um sistema de informação automatizado, que a consulta à ontologia seja um documento em formato digital ou em papel.

Com esses procedimentos, apresentados de forma simplificada, os documentos, que correspondem a uma grande parte da informação registrada na organização, são classificados e relacionados entre si. A ontologia permite a inserção de atributos, os quais podem apresentar características especiais de um documento, como por exemplo, sua confidencialidade, temporalidade, dentre outros. Além de permitir a classificação, a ontologia pode armazenar, ainda, as *instâncias* de tipos de documentos, ou seja, referências aos próprios documentos utilizados na rotina organizacional.

A ontologia resultante é um modelo consultado por um sistema, que pode ser, por exemplo, de gestão de documentos. Sugere-se que a interface de classificação seja integrada a outra interface já em uso, de forma que o usuário não tome a tarefa como um trabalho adicional. A ontologia passa a ser a referência única para qualquer sistema de informação em uso na organização em questões que dizem respeito à segurança da informação.

11 Para um levantamento abrangente sobre ferramentas, linguagens e metodologias para a construção de ontologias ver Almeida (2003).

12 Documentos vitais são aqueles essenciais para atestar uma atividade em um contexto organizacional, ou seja, documentos sem os quais os processos não teriam início, continuidade, e os agentes não contariam com instrumental para exercer avaliações e gestão.

5. Considerações Finais

Este artigo apresentou considerações sobre segurança da informação, destacando iniciativas governamentais, normativas e tecnológicas. Sem pretensão de abranger toda a pesquisa em segurança da informação, apresentou-se apenas o suficiente para uma visão geral da área. Introduziu-se, então, a ontologia como importante instrumento para projetos de segurança nas organizações, e descreveu-se um breve roteiro para a sua construção.

Vários benefícios podem ser contabilizados com o uso de ontologias em projetos de segurança: i) criar modelos conceituais que tornam possível a organização saber mais sobre o domínio de incidentes de segurança; ii) facilitar a interoperabilidade entre diferentes ferramentas de segurança; iii) criar um padrão para estruturar dados sobre segurança e possibilitar que termos diversos sejam mapeados para a ontologia; iv) possibilitar a reutilização de dados sobre segurança, por meio da importação e exportação de ontologias; v) auxiliar os administradores de sistemas nas decisões sobre gestão de segurança, com possibilidades de consultas e de inferências automáticas.

Apesar das vantagens com o uso de ontologias, cabe destacar a influência do fator humano. Tal influência é marcante pelo fato de que grande parte dos problemas de segurança é gerada por ações, intencionais ou não, de pessoas em suas atividades rotineiras. A classificação da informação registrada em uma ontologia pelos próprios usuários, a partir de suas necessidades, é uma primeira resposta ao problema do fator humano. Ao tornar as pessoas parte do processo, orientá-las, treiná-las e deixar que decidam sobre a classificação das informações que manipulam rotineiramente, pode-se esperar por colaboração nas iniciativas de segurança da informação. Sem essa participação, fomentada pela abordagem distribuída de conhecimento consensual da teoria das ontologias, nenhum sistema tecnológico de segurança poderá ser considerado eficiente, a partir de uma abordagem sistêmica.

Referências

ARAÚJO, L. A. D. *A correspondência eletrônica do empregado e o poder diretivo do empregador*. *In*: Revista de direito constitucional ALMEIDA, M.B.; BAX, M.P. Uma visão geral sobre ontologias: pesquisa sobre definições, tipos, aplicações, métodos de avaliação e de construção. *Ciência da Informação*. v. 26, n. 1. p. 39-45, set./dez. 2003.

BAKER, W. *Information security*; volume I. (2004). Available from Internet: <http://csrc.nist.gov/publications/nistpubs/800-60/SP800-60V1-final.pdf >. Access: 02 May 2006.

CIAO-Critical Infrastructure Assurance Office. *Practices for Securing Critical Information Assets*. (2000). Available from Internet: <http://www.infragard.net/library/pdfs/securing_critical_assets.pdf> . Access: 02 Dec. 2007.

ECCLES, R.G.; NOHRIA, N. *Assumindo a responsabilidade*; redescobrindo a essência da administração. Rio de Janeiro: Campus, 1994. 287p.

EKELHART, A. et al. Ontological Mapping of common criteria's security assurance requirements. INTERNATIONAL INFORMATION SECURITY INFORMATION, 2007, Sandton, *Proccedings*… Springer: [s.n.], 2007.

EKELHART, A. et al. *Security ontology*; simulating threats to corporate assets. (2006). Available from Internet: <http://www.springerlink.com/index/w530v5081301j833.pdf>. Access: 30 July 2007.

FENZ, S. et al. I*nformation security fortification by ontological mapping of the ISO/IEC 27001 Standard*. (2007). Available from Internet: <http://www.ifs.tuwien.ac.at/node/4274 >. Access: 19 Nov. 2007.

FOWLER, S. *GIAC Security essentials certification*. (2003). Available from Internet: <http://www.sans.org/reading_room/whitepapers/auditing/846.php>. Access: 13 April 2005.

GAO-General Accounting Office of United States. *GAO Audit Guide*. (1988). Available from Internet: <http://www.gao.gov/index.html>. Access: 15 Nov. 2007.

GARFINKEL, S.; SPAFFORD, G. *Practical Unix and Internet Security*, 2 ed. 1996. Sebastopol : O'Reilly. 1000 p.

GOVERNMENT OF ALBERTA. *Information Security Classification*. (2005). Avalaible from Internet: <http://www.im.gov.ab.ca/publications/pdf/InfoSecurityClassification.pdf>. Access: 20 Oct. 2006.

HOWARD, J.D.; LONGSTAFF, T. A. *A common language for computer security incidents*. (1998). Avalaible from Internet: <http://www.cert.org/research/taxonomy_988667.pdf>. Access: 13 Dec. 2006.

ISACF-Information Systems Audit and Control Foundation. *COBIT-Control Objectives for Information and Related Technology*. (2000). Available from Internet: <http://www.isaca.org/>. Access: 01 Dec. 2007.

ISSEA-International Systems Security Engineering Association. *SSE/CMM-System Security Engineering/Capability Maturity Model, V3.0*. (2003). Available from Internet: <http://www.sse-cmm.org/>. Access: 02 Dec. 2007.

ISO/IEC 15408-1. *Internacional Standard – Information Technology – Security Techniques*; Evaluation Criteria for IT Security – part 1. (2005). Available from Internet : <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40612> . Access: 21 April 2006.

ISO/IEC-27001. *International Standard – Information Technology – Security Techniques*; information security management systems – requirements. (2005). Available from Internet : <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103> . Access: 21 April 2006.

ISOO-*The Information Security Oversight Office*; Marking classified national security information. (2003). Avalaible from Internet: <http://www.archives.gov/isoo/training/marking-booklet.pdf>. Access: 12 Jan. 2006.

KRAUSE, M.; TIPTON, H.F. *Handbook of Information Security Management*. 3 ed., 1997. Boca Raton: Auerbach. 729 p.

KRAUSS, L. I. *SAFE*; security audit and field evaluation for computer facilities and information systems. New York : Amacom, 1980. 336 p.

LEVINE, D. E. Auditing Computer Security. In: HUTT, A. E. et al. (Ed.). *Computer Security Handbook*. 3 ed. New York : Wiley, 1995.

LII-Legal Information Institute of Cornell University. *U.S. Code collection*; 3452 Definitions. (2005). Available from Internet: <http://www.law.cornell.edu/uscode/html/uscode44/usc_sec_44_00003542----000-.html>. Access: 8 Dec. 2007.

MARTINIANO, L.A.F.; MOREIRA, E. S. *An OWL-based security incident ontology*. (2007). Available from Internet: <http://protege.stanford.edu/conference/2005/submissions/posters/poster-martimiano.pdf >. Access: 20 Nov. 2007.

MARTINIANO, L.A.F.; MOREIRA, E. S. *The evaluation process of a computer security incident ontology*. (2006). Available from Internet: <http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-199/wonto-06.pdf >. Access: 20 Nov. 2007.

MEADOWS, C. *An outline of a taxonomy of computer security research and development*. (1992). Available from Internet: <http://portal.acm.org/citation.cfm?id=283770>. Access: 2 Jan.2005.

MENNINGER, M.R. *The birth of incident response*; the story of the first Internet worm. (2005). Available from Internet: <http://www.selfseo.com/story-9757.php >. Access: 20 Nov. 2006.

NCSC-National Computer Security Center. *Glossary of computer security itens*. (1988). Available from Internet: <http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt >. Access: 15 Nov. 2007.

NEUMANN, P.; PARKER, D. *A summary of computer misuse techniques*. (1989). Available from Internet: <http://www.emeraldinsight.com/Insight/ViewContentServlet?Filename=Published/EmeraldFullTextArticle/Pdf/0460110503_ref.html>. Access: 8 July 2007.

NIST/CSD-Nacional Institute of Standards and Technology/Common Criteria/Computer Security Division. *Common Criteria for Information Technology Security Evaluation*. (1998). Available from Internet: <http://csrc.nist.gov/nissc/1999/proceeding/papers/p15.pdf >. Access: 01 Dec. 2007.

OECD-Organization for Economic Cooperation and Development. *Guidelines for the Security of Information Systems*. (1992). Available from Internet: <http://www.oecd.org/ >. Access: 01 Dec. 2007.

QUIST, A. S. *Security Classification of Information*; volume 2, principles and techniques for classification of information. (1993). Available from Internet: <http://fas.org/sgp/library/quist2/index.html>. Access: 02 Dec. 2007.

RASKIN, V. et al. *Ontology in information security*; a useful theoretical foudation and methodological tool. (2001). Available from Internet: <http://portal.acm.org/ft_gateway.cfm?id=508180&type=pdf&dl=portal&dl=ACM>. Access: 16 Aug. 2005.

SHIREY, R. *RFC 2828*; Internet Security Glossary. (2000). Available from Internet: <http://rfc.dotsrc.org/rfc/rfc2828.html>. Access: 19 Nov. 2007.

VON KROGH, G.; ROOS, J. Conversation Management. *European Management Journal*. [online].v. 13, n. 4, p. 390-394, 1995a. Available from Internet: <http://www.sciencedirect.com>. Access: 10 March 2005.

WILSON, T.D. *The nonsense of 'knowledge management'* . (2002). Available from Internet: <http://informationr.net/ir/8-1/paper144.html#non95>. Access: 03 April 2006.

WOOD, C. C. *Principles of Secure Information Systems Design*. (1990). Available from Internet: <http://portal.acm.org/citation.cfm?id=85089.85091>. Access: 22 Sept. 2007.

WOOD, C. C. et al. *Computer Security*; a comprehensive controls checklist. New York : Wiley, 1987. 214 p.

Divulgação

Protegendo os inocentes

Mário Augusto Lafetá Velloso

Consultor em Segurança da Informação, especialista em Gestão de Tecnologia da Informação, analista de Sistemas e professor do curso de Sistemas de Informação do Departamento de Ciências Exatas e Tecnológicas da Universidade Estadual de Montes Claros/MG (Unimontes). Certificado em Segurança da Informação MCSO, pela Módulo Security Solutions S/A. Pós-graduado em Gestão de Tecnologia da Informação pela Universidade Federal de Minas Gerais (UFMG). Pós-graduado em Tecnologias na Educação e bacharel em Sistemas de Informação pela Unimontes.

Divulgação

Paulo César Lopes

Bacharel em Computação, Administração e Direito pela UFMG. Pós-graduado em Ciência da Computação (UFMG), com ênfase em Redes de Computadores. Analista de Suporte Técnico da Companhia de Tecnologia da Informação do Estado de Minas Gerais (Prodemge), especialista em sistemas operacionais e redes. Coordenador do projeto de reestruturação tecnológica e migração dos sistemas legados para a plataforma aberta na Prodemge.

RESUMO

Este artigo propõe uma reflexão sobre as mudanças sociais provocadas pelo desenvolvimento das tecnologias da informação e comunicação e seus reflexos nos hábitos e formas de relacionamento entre as pessoas, com foco nas crianças e adolescentes. Identifica os principais riscos a que estão expostos na internet e propõe recursos auxiliares e práticas usuais que visam a colaborar no processo de monitoramento e acompanhamento desses usuários da rede mundial de computadores. O aspecto da educação de crianças e adolescentes é enfatizado como o mais eficaz instrumento para preservação da segurança e privacidade. Este artigo não tem a pretensão de esgotar a questão, mas de contribuir para que os jovens se tornem usuários conscientes das vantagens e dos riscos da internet.

Introdução

Já foi o tempo em que os pais apenas limitavam-se a orientar seus filhos sobre os perigos de aceitarem presentes de pessoas estranhas, de conversarem com quem não se conhece, de esquecer o portão ou a porta aberta ou de entrar em lojas ou bares no caminho de casa. Muitas destas recomendações estão entrando em desuso e algumas já podem ser consideradas até mesmo desnecessárias. Grande parte das crianças e muitos adolescentes não podem mais brincar nas ruas, caminhar para ir à padaria do bairro ou retornar da escola sozinhos. Hoje, para a maioria das famílias com algumas posses, a infância deve ser protegida por quatro paredes, por veículos automotores, por acompanhantes e extenso monitoramento. Jogos e brincadeiras como esconde-esconde, rouba-bandeira, garrafão, pega-ladrão e outros, realizados nas ruas, foram substituídos por jogos eletrônicos em videogames ou computadores e pelo acesso à internet. Muitos pais, por não poder oferecer a infância que tiveram, tentam compensar as restrições físicas, impostas aos seus filhos, com a amplitude e as possibilidades quase ilimitadas da grande rede mundial de computadores.

A internet é, sem dúvida, revolucionária e dona de um potencial educacional sem limites. Mas também apresenta grandes riscos para os inocentes. Tudo na web é ampliado. Tanto o lado construtivo e produtivo, quanto o destrutivo e improdutivo. O mundo virtual advindo da conexão dos computadores – a internet – não possui limites, e limites fazem parte de uma boa educação. Duas perguntas constantes de pais preocupados com o intenso acesso dos seus filhos à web são: quais são os riscos que meus filhos correm ao usarem a internet? O que posso fazer para protegê-los?

Este artigo pretende contribuir, em parte, na elaboração de respostas para estas perguntas simples. Evidentemente, não pretendemos esgotar assunto tão instigante, complexo e polêmico.

Contextualizando

A internet: essa rede que interliga milhões de computadores ao redor do mundo e permite a publicação e a troca de informações de qualquer tipo entre seus usuários é parte inegável do cotidiano dos nossos filhos. É realmente uma tecnologia fascinante. Mas o acesso às "informações de qualquer tipo" precisa ser tratado, já que estamos considerando indivíduos cujo caráter e cuja personalidade estão em processo de formação. Como esse processo se dá a partir dos valores e informações que recebem, bem como do meio e da cultura ao qual estão inseridos, o uso que eles dão à internet deve ser examinado, analisado e controlado, bloqueando-se as informações e experiências negativas que não contribuam para o seu desenvolvimento.

A tendência natural dos pais ou dos responsáveis é de serem otimistas a respeito do uso que seus filhos fazem da internet. Essa tendência teria como pressuposto o fato de essa rede ser considerada o "caminho do futuro", pois estariam cientes de que essa nova tecnologia encontra-se em estágio de formação e aperfeiçoamento e, por este motivo, poderiam influenciar a maneira como as crianças irão usá-la. A partir dessa tendência otimista, poderíamos inferir que esses pais e responsáveis gostariam que seus filhos usassem a internet de modo seguro e responsável. Daí, a necessidade de estratégias para administrar esse uso, além da necessidade de estabelecer controles e restrições de conteúdo, caso julguem necessário. Em outras palavras, poderíamos afirmar que é necessário ir além da responsabilidade de supervisionar e administrar as "atividades on-line" das crianças: é preciso torná-las sábias, responsáveis e conhecedoras de alguns dos riscos aos quais ficam expostas, enquanto usuárias dessa tecnologia.

Apesar do alarde acerca dos riscos do uso da internet, ainda há uma tendência de acreditar que ela seja uma fonte estática de informações ao invés de uma ferramenta extremamente dinâmica de comunicação, com possibilidades de implicações positivas e negativas para as crianças. Trata-se de um equívoco primário e perigoso. Essas pessoas costumam acreditar também que as crianças usam a internet primordialmente para atividades educacionais e de pesquisa. Portanto, é importante estar atento para uma possível discrepância entre o que os pais acreditam que as crianças estejam fazendo e o que elas realmente fazem na internet. Como pai ou responsável, como você se classifica como usuário de internet: leigo, intermediário, avançado ou especialista ?

Alguns aspectos precisam também ser considerados para o adequado tratamento do problema: normalmente suas crianças acessam a internet a partir de qual(is) ponto(s) de acesso: de casa? Da escola? Da casa de um(a) amigo(a) ? De uma biblioteca pública? De um computador em seu local de trabalho? De um ponto de acesso comunitário? De uma lan-house? Do seu celular? Um outro aspecto: até onde você sabe, qual é o principal uso que sua(s) criança(s) faz(em) da internet? Tarefas da escola? Pesquisa por informações? Jogos? Troca de mensagens instantâneas? Salas de "bate-papo"? E-mails? Encontrar novos amigos? Criar seu "site" pessoal (blog)? Pegar/ouvir músicas? Todas as alternativas anteriores? Há mais alguma que você ainda não saiba? O desafio está ficando cada vez maior.

Apesar dos tantos benefícios dessa tecnologia, precisamos ressaltar a existência de conteúdos na internet que poderíamos classificar como inapropriados. Apenas para exemplificar, citamos a pornografia, a violência, o racismo, além das questões sobre a segurança nas "interações on-line" com outras pessoas quanto à divulgação de informações pessoais e sigilosas. Diante dessa realidade, poderíamos dizer que não possuímos nenhuma preocupação com o uso que nossas crianças fazem da internet?

Afinal, como poderíamos conciliar o uso da internet com níveis de segurança satisfatórios? Poderíamos apresentar em algumas sugestões iniciais: colocar o computador que as crianças usam em uma área de uso comum do lar; haver sempre um adulto por perto, enquanto as crianças estiverem usando a internet; educá-las a sempre pedir permissão antes de enviar informações ou participarem de atividades na internet; ensiná-las a contornar adequadamente qualquer situação desconfortável que ocorra enquanto elas estiverem on-line; orientá-las sobre como proteger sua privacidade diante dessa inovadora ferramenta de comunicação. Ou seja, o primeiro passo a ser dado deve ser a definição clara e objetiva das regras básicas para o uso adequado e seguro de todo o potencial oferecido pela internet, sempre tendo o bom senso como "pano de fundo", no estabelecimento de tais regras. Os passos seguintes seriam o monitoramento do histórico dos endereços de sites visitados, bem como a lista de favoritos ou bookmarks; o uso de softwares de monitoração automática de navegação bem como softwares de bloqueio de conteúdo; o uso de softwares que impedem a instalação de vírus de computador, de programas que espionam e "roubam" dados sigilosos e pessoais ou que representem outros tipos de "ameaças cibernéticas".

Ótimo, agora demos alguns passos na direção da navegação segura das nossas crianças, mas e quanto aos computadores das escolas, das bibliotecas, das lan-houses ou de qualquer outro lugar que estas crianças podem usar para acessar a internet, o que fazer? Como implementar as sugestões que propusemos anteriormente? Para estes locais, é importante que os pais ou os responsáveis verifiquem as respectivas políticas existentes de uso da internet e solicitem a instalação das ferramentas de software já sugeridas, quando for o caso.

Ressaltamos ainda que vivemos em um planeta composto de comunidades distintas, com valores morais e culturais diversos. Partindo desse contexto, percebemos que, enquanto comunidade, precisaremos ainda nos envolver com outras questões mais amplas, porém que também dizem respeito aos riscos a que nossas crianças estão expostas. São questões como: os provedores de acesso à internet devem ser administradores e supervisores de conteúdo? Ou nossa comunidade entende que isso seria invasão de privacidade e prefere deixar esta responsabilidade como sendo apenas dos pais? O governo deveria desempenhar algum tipo de papel no controle de conteúdo da internet? Qual? Até que ponto estaríamos dispostos a deixar o governo entrar na vida pessoal de nossas famílias com esse tipo de controle? Seria melhor atribuir a uma organização independente tal responsabilidade? Ou deveríamos deixar a internet sem administração ou supervisão – como atualmente está – e trataríamos os riscos com ações positivas e educativas voltadas para nossas crianças, dentro dos limites que julgamos adequados, sem a interferência de terceiros ou de estranhos em nossa liberdade de "surfar na rede mundial de computadores"?

Ameaças mais comuns

Podemos dividir as ameaças da internet em dois grandes grupos: as ameaças por pessoas e as ameaças por softwares. As ameaças por pessoas têm como pré-requisito a interação de um usuário (nossos filhos, por exemplo) com um terceiro com más intenções. Já as ameaças por softwares englobam os programas de computador que executam tarefas, cujas conseqüências são negativas.

Ameaças por Pessoas

Parte das ameaças da internet proporcionadas por pessoas é a mesma que motivava nossos pais e avós a sempre nos recomendarem, quando éramos pequenos, a "não falar com estranhos". A web permite a comunicação com estranhos de todo tipo e de qualquer parte do mundo. O problema é que manter o anonimato nesses diálogos é muito simples. Se passar por outras pessoas também. Um terceiro mal intencionado pode usar o anonimato ou o disfarce criado, explorando a inocência das crianças. Pode ainda seduzi-las com propostas atraentes, com a finalidade de encontrá-las para cometer qualquer tipo de abuso (inclusive os sexuais), planejar seqüestros ou "apenas" extrair informações pessoais e sigilosas.

Mas há também aquelas ameaças oriundas não só dos diálogos on-line que acontecem via internet. São aquelas que recebemos por meio de e-mails, que estão presentes em alguns sites inidôneos ou em algumas daquelas janelas que se abrem, enquanto estamos navegando (pop-ups), sempre com propostas sedutoras e atraentes. Ao clicarmos naqueles links, acabamos por cair em uma armadilha e, caso não haja uma ação corretiva e bloqueadora no devido tempo, nos tornamos mais uma vítima de uma "fraude eletrônica".

Ameaças por Softwares[1]

Os primeiros programas invasores de computadores foram os vírus. Criados no início da década de 80, normalmente propagavam-se por meio de disquetes contaminados, alterando as informações de inicialização do computador (*Master Boot Record* ou MBR). Desde então, sua capacidade destrutiva vem aumentando exponencialmente. Eles se propagam infectando, ou seja, criando cópias deles mesmos, tornando-se parte de outros programas de computador. Dependem da execução do programa hospedeiro para tornarem-se ativos e dar continuidade ao processo de infecção e também podem acessar sua lista de endereços de e-mails, enviando cópias de si mesmo, provocando verdadeiras epidemias. Alguns desses programas podem apagar arquivos, desconfigurar sistemas operacionais ou mesmo inutilizar todos os dados de um disco rígido.

Os worms são programas que enviam cópias de si mesmos para outros computadores. Diferentes dos vírus, os worms não embutem cópias em outros programas e não necessitam ser executados para se propagar. Eles exploram vulnerabilidades ou falhas nas configurações de softwares instalados em computadores. Eles são programas autônomos, criados para cumprir determinadas missões, como enviar spams ou atacar sites. Outra tarefa típica é abrir portas na máquina invadida para a entrada de outros worms.

Os bots, termo derivado de "robot", ou robô, em português, é um tipo de worm que possui dispositivos de comunicação com o invasor, permitindo seu controle a partir de outros computadores. Os bots são normalmente utilizados para atacar sites, retirando-os do ar, e enviar e-mails não solicitados em grandes quantidades.

O Trojan, ou "cavalo de tróia", chega até nossos computadores como uma espécie de "presente": um álbum de fotografias interessantes, um protetor de tela bacana, um cartão virtual, jogo ou algo que possa despertar o interesse do destinatário. Além de executarem as ações para as quais foram aparentemente projetados, os Trojans realizam outras ações malignas sem o conhecimento do usuário, como instalar vírus ou abrir portas que podem ser acessadas à distância por um invasor.

Os spywares compõem a categoria de software que tem como objetivo monitorar as atividades de um sistema e enviar as informações coletadas para um terceiro. Normalmente, são capturadas informações pessoais e privadas, tais como nome completo do usuário, nome da esposa e filhos, idades, números de documentos oficiais como RG e CPF, bancos e

1 As informações referentes às ameaças por softwares basearam-se no vídeo "Os Invasores", criado pelo Comitê Gestor da Internet no Brasil – CGI.br, disponível em http://www.antispam.br/videos/.

instituições financeiras com as quais o usuário tem relacionamento.

Há dois subtipos de spywares bem conhecidos: os keyloggers e os screenloggers. Os keyloggers armazenam as teclas digitadas pelo usuário. Normalmente, o início de sua atividade de captura está condicionada a uma ação do usuário como "entrar no site de um banco" ou "entrar em um site de comércio eletrônico". Os keyloggers capturam todas as informações importantes digitadas pelo usuário como senhas, números de conta, identificadores e nomes de usuário. Os screenloggers podem ser caracterizados como uma forma avançada de keylogger: eles capturam as regiões da tela onde o usuário clica com o mouse e armazenam essas imagens para posterior envio a um terceiro.

Tratando o problema

A exposição de crianças e adolescentes às ameaças da internet é uma realidade. Não há como privá-las de uma ferramenta de educação[2] tão dinâmica e útil como esta. Portanto, urge a necessidade de realizarmos algumas ações que minimizem os riscos aos quais elas ficam expostas.

Consideramos que o principal aspecto a ser tratado pelos pais e responsáveis é a educação e a conscientização dos nossos filhos, quanto ao cuidado no relacionamento e interação com pessoas desconhecidas e no envio de informações pessoais ou sigilosas por meio da rede.

Mas é necessário também tratar algumas vulnerabilidades da própria máquina[3]. Para isso, recomendamos o uso de softwares de proteção. Deve-se começar pela instalação ou ativação de um firewall pessoal, de um anti-vírus e de um anti-spyware. Além disso, é necessário manter os programas em uso sempre atualizados, além de instalar todos os pacotes de correções de segurança. Deve-se dar especial atenção à atualização dos programas de proteção e à atualização das assinaturas de vírus do seu anti-vírus.

Podemos, ainda, ressaltar algumas dicas para serem aplicadas no uso cotidiano da internet:

- Não clique em links recebidos por e-mail ou via serviços de mensagens instantâneas.
- Sempre examine os arquivos recebidos por e-mail ou via serviços de mensagens instantâneas com anti-vírus antes de abrí-los. Na dúvida, é melhor apagar o arquivo, sem abri-lo.
- Esteja sempre atento ao navegar na internet.
- Evite entrar em sites com conteúdo suspeito.
- Evite clicar em links das janelas que se abrem automaticamente, enquanto navega (pop-ups).
- Se o computador está se comportando de forma estranha, atualize o seu anti-vírus e acione a opção de varredura completa do equipamento. Se o problema persistir, recomendamos a reinstalação do sistema operacional e dos aplicativos.
- Não forneça informações pessoais na rede, especialmente aquelas referentes a dados cadastrais, cartões de créditos, dados bancários e senhas, a não ser que seja um site de sua inteira confiança.
- Utilize e-mails diferentes para uso pessoal, trabalho, compras on-line e cadastros em sites em geral.
- Evite o "clique compulsivo", ou seja, clique apenas naquilo que realmente lhe interessa, descartando a curiosidade de clicar em links recebidos aleatoriamente.
- Ao receber e-mails promocionais de empresas, evite clicar no link disponível no e-mail. Ao acessar o site da empresa você poderá confirmar a existência da promoção ou mesmo de um golpe que anda "circulando" pela rede.
- Leia com atenção as informações fornecidas em sites, onde você realiza cadastros para evitar que concorde sem querer com opções indesejáveis. Ao realizar esses cadastros certifique-se que a empresa possui uma política de privacidade adequada para resguardar o sigilo das

2 GETSCHKO, Demi. Participação e Presença na Rede. In: CGI.br (Comitê Gestor da Internet no Brasil). *Pesquisa sobre o uso das tecnologias da informação e da comunicação 2006*. São Paulo, 2007, pp. 35-37.

3 Algumas das informações referentes ao resguardo das vulnerabilidades da própria máquina foram extraídas do vídeo "A Defesa" ", criado pelo Comitê Gestor da Internet no Brasil – CGI.br, disponível em http://www.antispam.br/videos/.

informações que você fornece.

- Antes de repassar e-mails que relatam fatos atípicos, procure certificar-se quanto à veracidade das informações ali contidas.
- Mantenha-se atualizado quanto às novas ameaças virtuais que surgem na rede.

Ferramentas e links interessantes

Além das ferramentas já conhecidas para a proteção de um sistema (firewall, anti-vírus, anti-spyware, anti-spam e outras), existe um volume considerável de soluções desenvolvidas especialmente para a proteção das crianças e adolescentes. Geralmente o desenvolvimento de tais soluções busca monitorar e/ou bloquear as atividades de risco na web. Alguns fornecedores estão disponibilizando estas ferramentas junto com seus produtos. Podemos citar a Microsoft que disponibilizou junto ao sistema operacional VISTA[4] o Windows Vista Parental Controls, que permite o ajuste de restrições como limites de tempo, limites de quais programas poderão ser executados, quais jogos poderão ser utilizados e quais sites podem ser visitados por componente da família[5].

A solução da Microsoft é interessante, mas existem diversas outras. Estes programas de computador, com funções semelhantes ao Parental Control, são comuns e fáceis de encontrar. Quatro conjuntos destacam-se para os ambientes domésticos. O primeiro deles são os filtros de conteúdo para acesso à web, instalado nas estações de trabalho, o segundo envolve as soluções que substituem os navegadores web; o terceiro é um conjunto que possui soluções híbridas: são os navegadores com filtros; o último é voltado para o monitoramento das atividades que estão sendo realizadas no computador. A maioria destas soluções é gratuita para uso não corporativo, mas poucas possuem versão em português.

Um bom exemplo de filtro de conteúdo é IProtectYou versão freeware[6]. Este programa é um filtro que pode ser manipulado por leigos, sem muitas dificuldades. Permite bloquear e-mails, chats, serviços de mensagens instantâneas, palavras específicas, e bloquear web sites. É um filtro simples e funcional que permite a instalação de senha para a desinstalação ou mudanças de configuração. O mesmo produto apresenta uma versão Shareware (IProtectYou Pro), que disponibiliza outras funcionalidades, como níveis de restrição para cada membro da família obter informações on-line das atividades dos usuários, restringir o tempo de utilização liberando e proibindo o acesso à web de acordo com horários pré-agendados. Outro bom representante deste grupo de soluções é Blue Coat K9 Web Protection. Este produto é bastante semelhante ao IProtectYou e permite um controle efetivo aos acessos à web. Existem outros representantes deste grupo na versão freeware: são eles Parental Filter e Naomi[7]. Todos permitem controlar alguns tipos de acessos à web e até os acessos às redes ponto a ponto (P2P[8] – Peer to Peer). Existem outros programas semelhantes em versões shareware. Dois exemplos: Advanced Parental Control e Anti-Porn.

O segundo grupo possui vários representantes, mas poucos são gratuitos. Uma solução freeware é Web Browser KidRocket[9]. Esta solução é bastante simples e eficiente. Direcionada para as crianças com menos de oito anos, o KidRocket possui lista de sites, que podem ser utilizados, e algumas funcionalidades que auxiliam no desenvolvimento da criança. Esta solução pode ser configurada de maneira que tome conta do equipamento, inviabilizando a utilização de qualquer outro programa. Outras soluções conhecidas: Frostzone KidSafe; Firefly Web Browser; TUKI Freedom Browser; KidSurf Child Safe Web Browser; My Kids

4 Existe ferramenta semelhante para o Windows XP que implementa estas proteções. A ferramenta é o Windows Live OneCare Proteção para a Família. A solução exige a inscrição no Windows Live. Veja em http://get.live.com/. Acesso em 31/10/2007.

5 Para mais informações veja http://www.microsoft.com/protect/products/family/vista.mspx. Acesso em 31/10/2007.

6 Disponível em http://www.snapfiles.com/get/iprotectyou.html. Acesso em 31/10/2007.

7 Disponível em http://www.naomifilter.org/index.html.

8 Exemplos de soluções P2P: Kazaa, Emule, LimeWire, Morpheus. Disponíveis em http://baixaki.ig.com.br/categorias/cat283_1.htm. Cabe salientar que estas soluções podem tornar os sistemas vulneráveis e contribuem para a transgressão de várias leis, especialmente a de Direitos Autorais.

9 Disponível em: http://kidrocket.org/download.php. Acesso em 21/11/2007.

Browser e Kids Playground Web Browser. Uma solução com design voltado para o público infantil é o navegador BuddyBrowser. Trata-se de uma solução interessante e bastante completa, já direcionada para crianças um pouquinho mais velhas, que inclui várias outras ferramentas e funcionalidades (mas este não é freeware). Possui lista de sites convenientes às crianças, o que viabiliza um controle efetivo das atividades da criança e do pré-adolescente na web, direcionando-os a realizarem conexões mais seguras.

Ressaltamos também que alguns provedores de acesso à internet no Brasil disponibilizam aos pais soluções que permitem o controle das atividades on-line dos filhos. Estas soluções geralmente possuem custos, mas são bem próximos dos valores das soluções disponíveis na modalidade shareware.

Várias soluções licenciadas, disponíveis na web, agregam grande segurança ao seu computador. Estas ferramentas podem ser adquiridas através da própria internet e alguns dos grandes fornecedores tais como Symantec, Computer Associates, Mcafee, Panda, Trend Micro, entre outros, disponibilizam versões para avaliação de seus produtos. Recomendamos que você experimente tais ferramentas antes de adquiri-las. Assim terá certeza quanto à satisfação em relação à ferramenta adquirida, seja ela um firewall, um antivírus, um anti-spyware, anti-trojan ou uma ferramenta qualquer que reduza sua exposição aos riscos existentes.

Outras soluções são disponibilizadas sem ônus e algumas delas são eficientes. Citamos alguns softwares gratuitos importantes para uma melhor proteção do computador que você usa:

- Firewalls: Sygate Personal Firewall (gratuito), disponível em http://microlink.tucows.com/files3/spf.exe, ZoneAlarm Firewall Basic (gratuito), disponível em http://download.zonealarm.com/bin/free/1025_update/zaSetup_en.exe. Comodo é outro firewall sem ônus (Windows XP e 2000). Disponível em http://www.personalfirewall.comodo.com/. Outra opção é o Outpostfree Firewall. Disponível em http://www.agnitum.com/products/outpostfree/.
- Software anti-vírus: AVG Free Edition (gratuito), disponível em http://free.grisoft.com/, avast! Home (gratuito), disponível em http://www.avast.com/index_por.html. Outra opção de antivírus é o Bitdefender Free Edition. Disponível em http://www.bitdefender.com/PRODUCT-14-world--BitDefender-10-Free-Edition.html. O ClamWin é um programa GPL. Disponível em http://www.clamwin.com/.
- Software anti-spyware: Spybot Search and Destroy (gratuito), disponível em http://www.spybot.info/pt/download/index.html, Microsoft Windows Defender (gratuito), disponível em http://www.microsoft.com/athome/security/spyware/software/default.mspx. Free Spyware Removal Forever é outra solução sem ônus. Remove spyware e adware. Disponível em http://free-spyware-removal-forever.microsmarts-llc.qarchive.org/. Outro programa gratuito para uso pessoal ou educacional é o SpywareBlaster 3.5.1. Disponível em http://www.javacoolsoftware.com/spywareblaster.html. Opção também interessante é o Free Anti-SPY Guard. Disponível em http://www.pcguardsoft.com/free-anti-spy.html. O SpywareTerminator é outra solução gratuita. Disponível em http://www.spywareterminator.com/.

Há também alguns sites que são muito úteis, pois apresentam informações interessantes a respeito da segurança no uso da internet. Podemos citar:

- http://www.cgi.br/
- http://cartilha.cert.br/
- http://www.antispam.br/
- http://www.infowester.com/dicaseguranca.php
- http://www.portaldafamilia.org/artigos/artigo054.shtml
- http://www.microsoft.com/brasil/athome/security/children/default.mspx
- http://www.safecanada.ca/link_e.asp?category=3&topic=94
- http://www.internet101.ca/en/index.php
- http://www1.k9webprotection.com/
- http://www.datastronghold.com/security-articles/general-security-articles/the-state-of-kids-internet-safety.html
- http://online-security-for-kids.qarchive.org/
- http://www2.cifop.ua.pt/nonio/seguranet/guia_pais.htm
- http://www.seguranet.crie.min-edu.pt/pais/Default.aspx
- http://www.acmesecurity.org/laboratorio/news/seguranca-na-internet-para-criancas
- http://dotsafe.eun.org/dotsafe.eun.org/eun.org2/eun/index_dotsafe.html
- http://www.fosi.org/icra/

Checklist de segurança

Apresentamos um checklist, desenvolvido pela Media Awareness Network em 2003[10], onde você pode verificar seu grau de envolvimento nas principais ações de proteção das suas crianças e adolescentes, enquanto usuários da internet:

Checklist	SIM	NÃO
Você está envolvido e ciente das atividades on-line das suas crianças? Você sabe o que eles estão fazendo e com quem eles estão conversando enquanto estão na internet?		
A sua família (pai, mãe e filhos) já estabeleceu um conjunto de regras ou um acordo para o uso apropriado da internet?		
Suas crianças já sabem que têm que pedir permissão antes de enviar qualquer tipo de informação pessoal on-line? Isso inclui: enquanto usa o e-mail, as salas de bate-papo ou de mensagens instantâneas, preenchendo formulários em sites, perfis pessoais em sites de relacionamento ou participando de desafios na web.		
Você tenta não fazer tantas críticas negativas sobre as atividades de seus filhos na web e usa as experiências deles como uma oportunidade de discutir conteúdo inapropriado, estabelecimento de confiança entre vocês e responsabilidades advindas de seus atos on-line?		
Você faz do uso da internet uma atividade familiar, guiando suas crianças para sites bons e ensinando-os como fazer pesquisas com segurança e eficácia?		
Você já ensinou seus filhos a não acreditarem em tudo o que lêem na internet e a verificar a veracidade das informações que ali se encontram junto a um adulto ou com uma outra fonte confiável?		
Se sua criança acessa a internet a partir da escola, da biblioteca, de uma lan-house ou de um outro local público, você já avaliou se são adequadas as regras, políticas e restrições de uso da internet impostas por esses locais?		
Você verifica as políticas de privacidade dos sites que suas crianças acessam, para se certificar de quais informações pessoais que são coletadas e se estas informações podem ou não ser vendidas ou repassadas a terceiros?		
Para tornar seu trabalho de monitoramento mais fácil, você já colocou o computador usado pelos seus filhos para o acesso à internet em um local de uso comum da casa, tais como a sala de estar, a sala de TV, a sala de jantar ou a cozinha?		
Se seu filho ou filha possui uma página web pessoal ou um blog, você já verificou se ela não publicou nenhuma informação pessoal que possa expô-la a riscos desnecessários?		
Você já conversou com seus filhos sobre comportamento on-line responsável? Eles entendem que furtar informações de web sites, fazer download de software pirata, criar ou fazer ameaças on-line e hackear e crackear são atividades ilegais?		

Legislação correlacionada

Desde a Constituição de 1988 (art. 227, CF/88), o Brasil já demonstrava o envolvimento com a Doutrina de Proteção Integral da Criança e do Adolescente. Em 1990 oficializou com a adesão a Convenção Internacional sobre Direitos da Criança por meio do Decreto Legislativo 28/1990.

Em 1990 também surge a primeira e única lei efetiva, e em nível infraconstitucional, de proteção à criança e ao adolescente. O Estatuto da Criança e do Adolescente (ECA – Lei 8069/90) é instrumento de efetivação dos direitos fundamentais garantidos pela Constituição. No seu artigo 2º existe a definição de criança e adolescente. Criança, para os efeitos da lei, é pessoa com menos de doze anos de idade, e adolescente é pessoa entre doze e dezoito anos de idade.

Recentemente, o Brasil também ratificou, por meio do Decreto nº 5007/04, o Protocolo Facultativo à Convenção sobre os Direitos da Criança (Nova York 2000), referente à venda de crianças, à prostituição infantil e à pornografia infantil.

O Código Penal, junto ao Estatuto da Criança e Adolescente, propõe a prevenção e a repressão a vários

10 Disponível em http://www.media-awareness.ca/english/resources/tip_sheets/internet_checklists/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=27804. Acesso em 09/12/2007.

delitos que envolvem os jovens. Alguns são conhecidos: estupro, atentado violento ao pudor, corrupção de menores e outros. Alguns são novos como a produção, divulgação e publicação de fotografias com conotação sexual, envolvendo crianças e adolescentes. Apresentamos o artigo do ECA[11]:

> Art. 241. Apresentar, produzir, vender, fornecer, divulgar ou publicar, por qualquer meio de comunicação, inclusive rede mundial de computadores ou internet, fotografias ou imagens com pornografia ou cenas de sexo explícito envolvendo criança ou adolescente.
>
> Pena – reclusão de 2 (dois) a 6 (seis) anos, e multa.
>
> § 1º Incorre na mesma pena quem: (Incluído pela Lei nº 10.764, de 12/11/2003)
>
> I - agencia, autoriza, facilita ou, de qualquer modo, intermedeia a participação de criança ou adolescente em produção referida neste artigo;
>
> II - assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens produzidas na forma do caput deste artigo;
>
> III - assegura, por qualquer meio, o acesso, na rede mundial de computadores ou internet, das fotografias, cenas ou imagens produzidas na forma do caput deste artigo.
>
> § 2º A pena é de reclusão de 3 (três) a 8 (oito) anos: (Incluído pela Lei nº 10.764, de 12/11/2003)
>
> I - se o agente comete o crime prevalecendo-se do exercício de cargo ou função;
>
> II - se o agente comete o crime com o fim de obter para si ou para outrem vantagem patrimonial.

Apesar da possibilidade de interpretação do artigo acima de que o simples armazenamento das imagens e fotografias envolvendo sexo com crianças e adolescentes, mesmo sem ciência do usuário do equipamento computacional, seja crime, para grande parte dos penalistas, o ordenamento jurídico brasileiro é incipiente e tímido no combate à pedofilia[12].

Conclusão

Os recursos e considerações aqui apresentadas não esgotam todos os problemas ocasionados pela intensa exposição das crianças e adolescentes à web. São apenas alguns recursos auxiliares e práticas usuais que visam colaborar no processo de monitoramento e acompanhamento dos jovens enquanto usuários da internet. A educação infantil e do adolescente exige tempo, dedicação, diálogo e confiança. Mecanismos implementados por programas de computador nunca darão plena segurança às crianças e aos adolescentes. As soluções computacionais não darão maturidade, discernimento, bom senso, virtuosidade, astúcia e sabedoria. Não há tecnologia capaz de substituir a relação aberta, o diálogo franco e a educação dada pelos pais aos seus filhos.

O grande dilema da educação de crianças – quando liberar e quando proibir – é a questão basilar que envolve esta discussão dos riscos existentes no acesso delas à internet. É evidente que a independência e a autonomia das crianças e adolescentes são características que devem ser construídas e incentivadas, como afirmava Piaget[13]. Mas todo pai sabe que o cotidiano exige proximidade, acompanhamento, participação e monitoramento. A presença dos pais é simplesmente insubstituível. As crianças e os adolescentes devem experimentar e aprender. Daí a dificuldade em decidir quando "liberar" e quando "proibir". Trata-se de um dilema individual, que, em parte, é respondido quando lembramos que educar é antes de tudo amar profundamente. Concluímos com a fala de Paulo Freire[14]: "Educar é um ato de amor e para educar crianças é necessário, sobretudo, amá-las profundamente" e com a sintetização de Içami Tiba[15]: "Quem Ama, Educa!".

11 ECA disponível em http://www.planalto.gov.br/ccivil_03/Leis/L8069.htm. Acesso 27/12/2007.

12 Para denúncias de crimes virtuais que afetem toda a sociedade, como é o caso da PEDOFILIA, utilize a Central Nacional de Denúncias de Crimes Cibernéticos. Disponível em http://www.safernet.org.br/twiki/bin/view/SaferNet/WebHome. Para outros casos o site apresenta algumas orientações interessantes. Acesso em 30/11/2007.

13 http://pt.wikipedia.org/wiki/Piaget

14 http://pt.wikipedia.org/wiki/Paulo_Freire

15 http://pt.wikipedia.org/wiki/I%C3%A7ami_tiba

Governança de TICs e Segurança da Informação


Divulgação

João Luiz Pereira Marciano

Bacharel e mestre em Ciência da Computação, doutor em Ciência da Informação, consultor de programas da TecSoft e SofTex, do Departamento de Polícia Federal e da Organização das Nações Unidas. Ex-professor do programa de pós-graduacão da Universidade Católica de Brasília e ex-professor substituto da Universidade de Brasília, atualmente Analista Legislativo da Câmara dos Deputados.
Áreas de interesse: segurança da informação, políticas de informação, epistemologia e hermenêutica, análise estatística. marciano@unb.br

RESUMO

Os padrões e modelos direcionados à correta gerência dos temas relacionados com as tecnologias de informação e de comunicação (TICs), no meio organizacional, têm-se proliferado continuamente, tanto no tipo, quanto no número de utilizações. Em conseqüência ao grande volume de informações de diversas fontes e categorias, que permeiam as redes e os demais recursos digitais, somam-se as informações acerca da gestão desses mesmos recursos, as quais têm seus próprios requisitos de sensibilidade e ciclos de vida. As metodologias de segurança da informação muito têm a contribuir neste contexto, ao se aliarem às práticas de gestão em busca de soluções que devem se adequar, ao mesmo tempo, ao negócio e às estratégias de governança da informação.

Palavras-chave: Governança da informação. Segurança da informação. ITIL. COBIT. TICs.

1. Introdução

Muito tem-se falado acerca da necessidade de implementação de modelos e metodologias destinados à governança das tecnologias de informação e de comunicação (TICs). Na literatura, diversas acepções são apresentadas ao termo "governança" (Van Grembergen; De Haes; Guldentops, 2004, p. 5), sendo que, de modo geral, quanto à governança corporativa, elas estão relacionadas com a capacidade da organização realizar atividades voltadas ao seu desempenho e à vantagem competitiva. Esta capacidade pode variar conforme o negócio e a localização geográfica da organização, o que constitui um problema à parte para as organizações globais. Em especial, o trabalho de Ayogu (2001, p. 309), acerca do tema, introduz uma observação fundamental, ao notar que, do ponto de vista prático, o problema da governança corporativa está relacionado com o delineamento de instituições (entendidas como o conjunto de procedimentos, normas, rotinas e convenções, formais ou informais, que norteiam as ações coletivas (North, 1991; Ostrom, 1999, p. 36-37) que orientam o corpo de gerentes em suas ações, levando em consideração o bem-estar dos stakeholders (investidores, empregados, comunidades, fornecedores e clientes).

No tocante às TICs, a governança assume aspectos necessariamente mais localizados, inseridos em um contexto delineado pelas

próprias tecnologias que se propõe aplicar e gerenciar. Pode-se entender a governança das TICs como sendo a responsabilidade desempenhada pela alta gerência para garantir que tais tecnologias suportem adequadamente o negócio, em toda a sua extensão interna *corpore* e no relacionamento com os parceiros, aqui entendidos como aqueles que se relacionam com a organização ao longo da sua cadeia produtiva.

Torna-se, então, essencial a construção de um mapeamento adequado entre os objetivos organizacionais e os objetivos das TICs. Este alinhamento estratégico entre a governança organizacional e a governança das TICs, o qual se mostra em diferentes estágios de maturidade, apresenta, via de regra, profundo impacto sobre as atividades da organização. Desse modo, a governança das TICs assume papel essencial, agora não mais restrito ao subconjunto tecnológico, mas expandido ao próprio *locus* da organização em sua rede de relacionamentos.

Diversas abordagens podem ser aplicadas à modelagem do mapeamento entre os dois tipos de governança (Peterson, 2004): baseiam-se no estabelecimento de prioridades e objetivos, na obediência a determinações legais e governamentais, nos pontos de vista dos principais agentes da cadeia de valor, etc. Porém, a título de marco inicial, deve-se observar que existe um aspecto da governança das TICs que também se insere firmemente no ambiente organizacional: a segurança da informação, que percorre (idealmente) todos os meandros da vida da organização e que se utiliza de ferramentas de observação de diversos comportamentos de usuários, clientes e parceiros. Além disso, a segurança da informação, adequadamente norteada por políticas, busca os mesmos objetivos do alinhamento estratégico já citado, a saber, atender a prioridades e objetivos organizacionais, basear-se firmemente na aderência a padrões e determinações legais e inserir-se no ambiente organizacional de modo a apoiar os ativos com os quais se relaciona, não só no tocante ao valor monetário de tais ativos, mas, principalmente, na preservação do conhecimento organizacional.

2. O contexto da segurança da informação diante da governança de TICs

Os mecanismos de análise e de formalização de políticas de segurança atualmente em voga, tais como a norma ISO/IEC 27001 (ISO, 2006), ou a descrição de recomendações de institutos de tecnologia e de padrões (Bass, 1998), partem de pressupostos representados por "melhores práticas" (Wood, 2002b), ou seja, adota-se um conjunto de procedimentos *ad hoc*, definidos de forma empírica e geralmente voltados a aspectos técnicos, por vezes deslocados do contexto humano e profissional no qual se inserem.

Cumpre observar que os sistemas de informação, mormente aqueles digitais, em ampla voga no contexto da Sociedade da Informação, encontram-se, naturalmente, envoltos por completo em ambientes do mundo real, estando sujeitos a várias formas de ações afeitas à sua segurança, tais como negações de serviço, fraudes, roubos, tentativas de invasão, corrupção e outras atividades hostis (Schneier, 2000; Wood, 2002a; Bosworth; Kabay, 2002).

Em resposta a estas hostilidades, a segurança da informação, em seu sentido mais abrangente, envolve requisitos voltados à garantia de origem, uso e trânsito da informação, buscando certificar todas as etapas do seu ciclo de vida. Estes requisitos podem ser resumidos na forma dos três primeiros itens a seguir (ISO, 2006), aos quais algumas abordagens agregam ainda os dois últimos (Krutz; Vines, 2002; Krause; Tipton, 1999):

Confidencialidade: garantia de que a informação é acessível somente por pessoas autorizadas a realizarem tal acesso (Jonsson, 1998).

Integridade: garantia de não-violação da informação e dos métodos de seu processamento[1].

Disponibilidade: garantia de que os usuários, devidamente autorizados, obtenham acesso à informação e aos recursos computacionais correspondentes, sempre que necessário.

Autenticidade: garantia de que a informação é de fato originária da procedência alegada.

1 É comum confundir-se integridade com corretude, mas um exemplo banal ilustra a distinção entre ambas: imagine-se uma mensagem cujo conteúdo original seja "2+2=5"; caso, ao ser transmitida, tal mensagem chegue ao seu destino com esta mesma disposição, ela se mostra íntegra, porém, não é correta. Isto salienta também a distinção entre estrutura e significado, aos quais, conforme já se disse, a segurança não está afeita. Note-se que esses dois conceitos pertencem a domínios distintos de representação: sintático e semântico.

Irretratabilidade ou não repúdio: garantia de que não se pode negar a autoria da informação ou o tráfego por ela percorrido.

Desse modo, a segurança faz-se presente nas arquiteturas e modelos da informação, inserindo-se em todos os níveis. Entretanto, observa-se um número crescente de ocorrências de incidentes relativos à segurança da informação. Fraudes digitais, furtos de senhas, cavalos de tróia (códigos de programas aparentemente inofensivos, mas que guardam instruções danosas ao usuário, ao software ou ao equipamento), vírus e outras formas de ameaças têm-se multiplicado vertiginosamente, conforme ilustra a Figura 1.

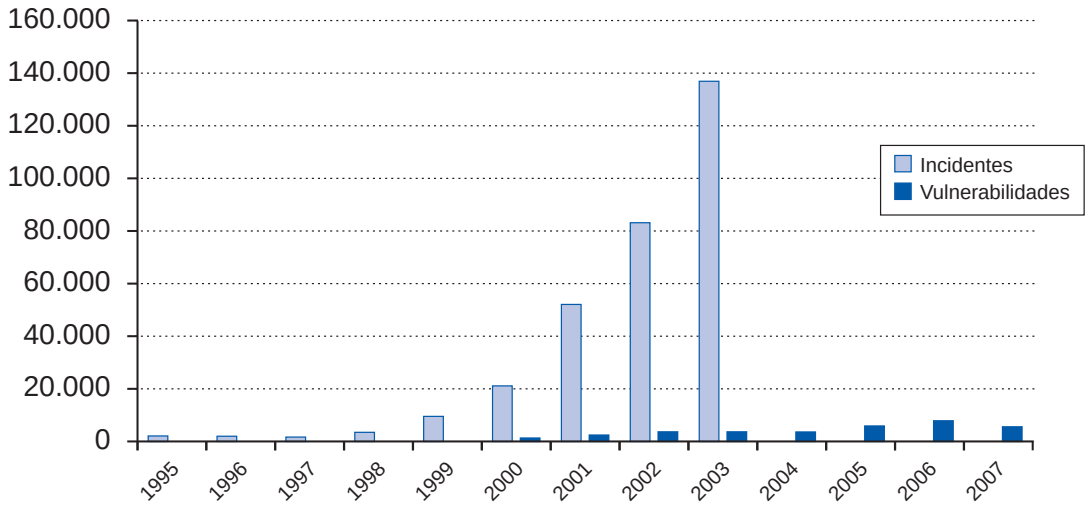


Figura 1 – Vulnerabilidades e incidentes de segurança da informação em sites no mundo, reportados no período de 1988 a 2003. Fonte: (CERT, 2006).

Na imagem apresentada pela Figura 1, mostra-se o aumento do número de vulnerabilidades, ou seja, potenciais falhas de mecanismos computacionais (implementados em software ou em hardware), as quais, uma vez exploradas ou em virtude de fatores não tecnológicos, como humanos, dão ensejo à ocorrência dos incidentes. Estes, por sua vez, apresentam-se em número e crescimento muito superiores às vulnerabilidades, mesmo porque a reiterada exploração de uma mesma vulnerabilidade pode ocasionar múltiplos incidentes. Observa-se, ainda, que um mesmo incidente que atinja diversas instalações (como a infecção por um mesmo vírus em centenas de milhares de computadores, por exemplo) é contabilizado como um único caso para a confecção do gráfico.

Tabela 1 – Ranking de países por acesso à internet (Fonte: e-Commerce.Org (2006)).

País	Usuários da internet (milhões)	População (est. 2006, milhões)	Adoção da internet (%)	Usuários no mundo (%)
EUA	203,8	299,0	68,1	20,0
China	111,8	1.307,0	8,5	10,9
Japão	86,3	128,4	67,2	8,5
Índia	50,6	1.112,2	4,5	5,0
Alemanha	48,7	82,5	59,0	4,8
Reino Unido	37,8	60,1	62,9	3,7
Coréia do Sul	33,9	50,6	67,0	3,3
Itália	28,9	59,1	48,8	2,8
França	26,2	61,0	43,0	2,6
Brasil	25,9	184,3	14,1	2,5

3. Alguns organismos e padrões relacionados com a governança das TICs e com as políticas de segurança da informação

Tal como a governança de TICs, as políticas de segurança da informação, para serem eficazes, devem aderir à legislação e às regulamentações vigentes sobre o contexto organizacional. Leis e normas nacionais ou mesmo internacionais, além de padrões reconhecidos, contribuem para esta prática.

Os Estados Unidos da América, como grande pólo gerador de inovações tecnológicas e como um dos países de mais alta taxa percentual de uso computacional por habitante, conforme ilustra a Tabela 1, ditam muitas normas utilizadas pela comunidade internacional no tocante à SI. Muitas dessas normas e procedimentos são gerados tendo em vista o contexto cultural e econômico daquele país, sendo criados por órgãos governamentais como o General Accounting Office (GAO) (GAO, 1998), com o objetivo de embasar ou atender à sua legislação. Em outras situações, organismos de alcance global propõem e discutem modelos de normas e procedimentos a serem aplicados a todo o contexto da internet. Neste âmbito destacam-se, dentre várias organizações, o NIST, o CERT e o SANS Institute.

3.1 NIST

O National Institute of Standards and Technology (NIST) é uma organização voltada à normatização e padronização de instrumentos e práticas no âmbito do governo e das organizações públicas nos Estados Unidos. O órgão realiza periodicamente conferências voltadas à SI, cujos resultados são publicados e disponibilizados ao público. Como exemplo, cite-se o texto de Bass (1998), o qual apresenta um modelo de política de segurança, que abrange aspectos gerenciais, de operação e de implementação. Por sua vez, King (2000) discorre sobre algumas das chamadas "melhores práticas" da SI, ou seja, estratégias heurísticas que se baseiam em casos reais, não necessariamente corroboradas pela teoria. Por fim, Raggad (2000) propõe uma estratégia de defesa corporativa, semelhante aos moldes adotados pelo Department of Defense (DoD).

3.2 CERT

O Computer Emergency Response Team (CERT) (CERT, 2004) é uma organização sem fins lucrativos, sediada na Universidade Carnegie-Mellon, na Pennsylvania, cujos relatórios estatísticos anuais constituem uma referência global para o acompanhamento de vulnerabilidades, ameaças e incidentes no âmbito da internet. Além disso, o CERT realiza estudos e desenvolve instrumentos e metodologias, como a OCTAVE, voltados ao incremento da segurança da informação, que são aplicados em larga escala, e, ainda, disponibiliza correções para falhas encontradas em diferentes softwares.

3.3 SANS Institute

O SysAdmin, Audit, Network, Security Institute (SANS Institute) é uma organização de pesquisa e educação estabelecida em 1989, que conta, atualmente, com mais de 165 mil profissionais de segurança entre seus afiliados. Além de uma grande gama de cursos e textos técnicos sobre a segurança da informação, o SANS Institute publicou e tornou disponíveis na internet diversos modelos templates de pequenas normas de segurança, voltadas para correio eletrônico, uso de computadores, controle de acesso e muitas outras. Além disso, sua lista das 20 principais vulnerabilidades dos sistemas Windows e Unix é bastante conceituada (SANS, 2004). O SANS Institute publicou ainda um modelo para a elaboração de políticas de segurança de nível organizacional (GUEL, 2001), além de uma lista de verificação (checklist) para validação da conformidade ao padrão ISO/IEC 17799 (Thiagarajan, 2003).

3.4 ITSEC

O Information Technology for Security Evaluation Criteria (ITSEC) foi um dos primeiros padrões propostos para a interoperabilidade de sistemas computacionais com requisitos de segurança, principalmente criptografia de chaves simétricas. Seu desenvolvimento ocorreu como resultado de um esforço conjunto dos governos da França, Alemanha, Reino Unido e Holanda. Em meados da década de 80, foi apresentado como um padrão proposto para aquisição e desenvolvimento de sistemas governamentais e comerciais (Ford, 1994). Nos últimos tempos, tem sido substituído por outros padrões, como COBIT e Common Criteria.

3.5 COBIT

Em 1998, foi criado o Information Technology Governance Institute (ITGI), organismo com base nos Estados Unidos, com o objetivo de realizar pesquisas e estudos sobre o tema da governança, proteção e segurança de TI. Um dos principais produtos desses estudos é o guia conhecido como Control Objectives for Information and related Technology (COBIT), totalmente compatível com a norma ISO/IEC 17799, que tem como público-alvo gestores de organizações, auditores e responsáveis pela segurança da informação (IT Governance Institute, 2005).

Os componentes do COBIT são os seguintes (IT Governance Institute, 2004):

- sumário executivo, que detalha os conceitos fundamentais do guia (IT Governance Institute, 2000b);
- framework, que é a base e o suporte para os demais componentes, organizando o modelo de processos em quatro grandes domínios (IT Governance Institute, 2000c):
  - planejamento e organização;
  - aquisição e implementação;
  - entrega e suporte;
  - monitoração e avaliação.
- objetivos de controle, provendo mais de 300 enunciados que definem o que precisa ser gerenciado em cada processo de TI, a fim de atingir os objetivos da organização, inclusive quanto à gestão de riscos (IT Governance Institute, 2000a);
- práticas de controle, que indica quais controles e práticas são necessários para atingir os objetivos estabelecidos;
- linhas mestras de gestão, com ferramentas para dar suporte aos gestores de TI (IT Governance Institute, 2000e);
- linhas mestras de auditoria, que delineiam 34 objetivos da auditoria de TI, com atividades e um guia para a sua realização.

Além desses componentes, provê-se ainda um guia rápido (COBIT QuickStart), para a adoção gradual e orientada dos elementos do COBIT (IT Governance Institute, 2000d).

3.6 Common Criteria

O projeto Common Criteria (CC), originalmente patrocinado por sete organizações de seis países distintos, foi padronizado sob o código ISO/IEC 15408. Seu objetivo é ser usado como base para avaliação de propriedades de segurança de produtos e sistemas de TI, permitindo a comparação entre os resultados de avaliações independentes de segurança, por meio de um conjunto de requisitos padronizados a ser atingido. O processo de avaliação estabelece níveis de confiabilidade de que as funções avaliadas atingem os requisitos estabelecidos, ajudando os usuários a determinar se tais sistemas ou produtos possuem os níveis desejados de segurança e se os riscos advindos de seu uso são toleráveis. Seu público-alvo são os desenvolvedores, avaliadores e usuários de sistemas e produtos de TI que requerem segurança.

O padrão está dividido em três partes (NIAP, 2003a):

- introdução e modelo geral, onde são definidos os conceitos e princípios seguidos pelo modelo, além de uma nomenclatura e uma diagramação, que se baseiam na orientação a objetos, específicas para a formulação de objetivos de segurança, selecionar e definir seus requisitos e o alto nível de produtos e sistemas;
- requisitos funcionais de segurança, que estabelecem um

conjunto de elementos funcionais para a padronização dos requisitos, divididos em classes, como gestão de segurança, privacidade e comunicação; em famílias, como funções e mensagens; e em componentes, como as bibliotecas de definições (NIAP, 2003b);

- requisitos da garantia de segurança, que estabelecem um conjunto de elementos para a padronização da garantia da segurança, também divididos em famílias, classes e componentes, ao longo do ciclo de desenvolvimento dos produtos ou sistemas. Um exemplo de classe é a gestão de documentação do produto ou sistema, com as famílias "guia do administrador" e "guia do usuário", contendo componentes como um que determine que "o guia do administrador deve ser consistente com toda a documentação suprida para avaliação" (NIAP, 2003c).

3.7 ITIL

A Information Technology Infrastructure Library (ITIL) compreende um conjunto de melhores práticas destinadas ao provimento da qualidade de serviços em TI, originalmente patrocinadas pelo Office for Government Commerce da Inglaterra. Posteriormente, originou a norma BS 15000, que, por sua vez, tornou-se um anexo da norma ISO 20000.

A biblioteca ITIL divide-se em dois grandes segmentos, sendo o primeiro o Service Support, dividido em (Inform-IT, 2007):

- gestão de incidentes: destinada a reduzir a indisponibilidade dos serviços;
- gestão de problemas: destinada a minimizar o impacto de incidentes e problemas causados por falhas de TI;
- gestão de configuração: destinada a identificar e controlar os ativos de TI na organização, estabelecendo suas relações com os serviços por eles prestados;
- gestão de mudanças: destinada a minimizar o impacto das mudanças eventualmente requeridas por incidentes ou problemas, garantindo o nível de qualidade dos serviços;
- gestão de instalações: destinada a garantir que instalações de versões de hardware e software estejam consoantes com testes e requisitos de segurança.

O segundo segmento é o Service Delivery, dividido em:

- gestão do nível de serviços: destinada a garantir o acordo de nível de serviços – Service Level Agreements (SLA) – com o cliente;
- gestão financeira para serviços de TI: destinada à formação, negociação e exibição de custos dos serviços;
- gestão de disponibilidade: destinada à garantia de disponibilidade, com vistas à satisfação do cliente e manutenção do negócio;
- gestão de capacidades: destinada à observância de demandas, sua adequação e consonância com tempos e custos;
- gestão de continuidade de serviços de TI: destinada a assegurar a recuperação dos ativos de TI, quando necessário.

3.8 Brasil

No Brasil, principalmente a partir do final da década de 90, tem-se dado importância específica a eventos da segurança da informação, no tocante aos aspectos legais e jurídicos que os envolvem. Até então, os incidentes eram enquadrados sob a óptica do contexto, em que se inseriam, por exemplo, fraude ou falsificação, conforme o caso e a visão do jurista responsável.

Nos últimos anos, leis têm sido propostas para tratar especificamente de temas relacionados com a segurança da informação em formato digital, como o comércio eletrônico, mas tais projetos ainda encontram-se em tramitação no Congresso Nacional. A legislação brasileira, como se sabe, é bastante abrangente; porém, em diversos casos, carece de atualizações essenciais à sua formalização e implementação. Exemplos que merecem destaque, no tocante à segurança da informação, são o texto publicado pelo Tribunal de Contas da União (TCU), com melhores práticas sobre o tema (TCU, 2003), e recomendações dispostas pelo Network Information Center do país (NIC-BR) (NBSO, 2005).

4. Comentários finais

Evidencia-se a inter-relação entre os modelos de governança de TICs e os modelos voltados à segurança da informação. Um não pode subsistir sem o outro. Enquanto as TICs devem-se adequar perfeitamente à governança institucional, a segurança da informação deve dar-lhe suporte, a fim de garantir o exato alinhamento com as políticas e práticas dos ativos da informação, os quais são o principal insumo para as organizações da Sociedade da Informação.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001* : Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação - requisitos. Rio de Janeiro, 2006.

AYOGU, M. D. Corporate governance in Africa: the record and policies for good corporate governance. *African Development Review*, v. 13, n. 2, p.308_330, Dec. 2001.

BASS, F. T. Security policy: target, contents and links. In: *Proceedings of the 21st National Information Systems Security Conference*. NIST National Institute of Standards and Technology, 1998. Disponível em: <http://csrc.nist.gov/nissc/1998/proceedings/paperG4.pdf>. Acesso em: 2 jun. 2003.

BOSWORTH, S.; KABAY, M. E. (Eds.). *Computer Security Handbook*. 4th. ed. New York: John Wiley & Sons, 2002.

BRASIL. TRIBUNAL DE CONTAS DA UNIÃO. *Boas práticas em segurança da informação*. Brasília: Tribunal de Contas da União, 2003. Disponível em: <http://www.tcu.gov.br>. Acesso em: 8 jul. 2003.

COMPUTER EMERGENCY RESPONSE TEAM. Site oficial. Pittsburgh, 2004. Disponível em: <www.cert.org>. Acesso em: 9 maio 2003.

COMPUTER EMERGENCY RESPONSE TEAM. *CERT/Coordination Center Statistics*. Pittsburgh, Carnegie Mellon University, Jan. 2006. Disponível em: <http://www.cert.org/stats/cert_stats.html>. Acesso em: 9 jan. 2006.

E-COMMERCE.ORG. *Dados estatísticos sobre a internet e comércio eletrônico*. São Paulo, 2006. Disponível em: <http://www.ecommerce. org.br/STATS.htm>. Acesso em: 9 maio 2006.

FORD, W. Standardizing information technology security. StandardView, ACM, v. 2, n. 2, p. 64_71, 1994. Disponível em: <http://doi.acm.org/10.1145/202949.202951>. Acesso em: 2 ago. 2004.

GENERAL ACCOUNTING OFFICE. *Information Security Management* : learning from leading organizations.Washington - General Accounting Office, 1998. Disponível em: <http://www.gao.gov/special.pubs/ai9868.pdf>. Acesso em: 05 abr. 2004.

GUEL, M. D. *A short primer for developing security policies*. Bethesda, Maryland, 2001. Disponível em: <http://www.sans.org/resources/policies/Policy_Primer.pdf>. Acesso em: 25 abr. 2002.

INFORM-IT. *Foundations of IT Service Management Based on ITIL V3*. Zaltbommel, Netherlands: Van Haren Publishing, 2007.

IT GOVERNANCE INSTITUTE. *COBIT Control Objectives*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Executive Summary*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Framework*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Implementation Tool Set*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT Management Guidelines*. 3rd. ed. Chicago, 2000. Disponível em: <www.isaca.org>. Acesso em: 3 ago. 2004.

IT GOVERNANCE INSTITUTE. *COBIT security baselines*. Chicago, 2004. Disponível em: <http://www.isaca.org>. Acesso em: 17 jan. 2005.

IT GOVERNANCE INSTITUTE. *COBIT*. Chicago, 2005. Disponível em: <http://www.isaca.org>. Acesso em: 17 jan. 2005.

JONSSON, E. An integrated framework for security and dependability. In: *Proceedings of the 1998 workshop on New security paradigms*. Charlottesville, Virginia, United States: ACM, 1998. p. 22_29. Disponível em: <http://doi.acm.org/10.1145/310889.310903>. Acesso em: 2 ago. 2004.

KING, G. Best security practices: an overview. In: *Proccedings of the 23rd National Information Systems Security Conference*. NIST National Institute of Standards and Technology, 2000. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/022.pdf>. Acesso em: 18 jul. 2003.

KRAUSE, M.; TIPTON, H. F. *Information Security Management Handbook*. New York: CRC Press - Auerbach, 1999.

KRUTZ, R. L.; VINES, R. D. *The CISSP Prep Guide: Gold edition*. New York: John Wiley & Sons, 2002.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) – v 2.2.*: Part 1 - introduction and general model. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/_les/ccpart1v2.2.pdf>. Acesso em: 9 jul. 2004.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) – v 2.2* : Part 2 - security functional requirements. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/_les/ccpart2v2.2.pdf>. Acesso em: 11 jul. 2004.

NATIONAL INFORMATION ASSURANCE PARTNERSHIP. *Common Criteria for Information Technology Security Evaluation (ISO 15408) – v 2.2* : Part 3 - security assurance requirements. Washington, 2003. Disponível em: <http://www.commoncriteriaportal.org/public/_les/ccpart3v2.2.pdf>. Acesso em: 11 jul. 2004.

NBSO. Site oficial do Network Information Center Security Office. Rio de Janeiro, 2005. Disponível em: <http://www.nbso.nic.br/>. Acesso em: 13 fev. 2005.

NORTH, D. C. Institutions. *The Journal of Economic Perspectives*, v. 5, n. 1, p. 97_112, Winter 1991.

OSTROM, E. Institutional rational choice: an assessment of the institutional analysis and development frameworks. In: SABATIER, P. (Ed.). *Theories of the policy process*. Boulder - Colorado: Westview Press, 1999. p. 35_71.

PETERSON, R. R. Integration strategies and tactics for information technology governance. In: VAN GREMBERGEN, W. (Org.). *Strategies for information technology governance*. Hershey, PA: Idea Group Inc. Publishing, 2004. p. 37_80.

RAGGAD, B. G. Corporate vital defense strategy: a framework for information assurance. In: *Proccedings of the 23rd National Information Systems Security Conference*. NIST-National Institute of Standards and Technology, 2000. Disponível em: <http://csrc.nist.gov/nissc/2000/proceedings/papers/029.pdf>. Acesso em: 9 jul. 2003.

SANS. *The Twenty Most Critical Internet Security Vulnerabilities* . Bethesda, Maryland, 2004. Disponível em: <http://_les.sans.org/top20.pdf>. Acesso em: 10 dez. 2004.

SCHNEIER, B. *Secrets and Lies: digital security in a networked world*. New York: John Wiley & Sons, 2000.

THIAGARAJAN, V. *Information Security Management : BS 7799.2:2002 Audit Check List*. Bethesda, Maryland, 2003. Disponível em: <http://www.sans.org/score/checklists/ISO_17799_checklist.pdf>. Acesso em: 3 ago. 2004.

VAN GREMBERGEN, W.; DE HAES, S.; GULDENTOPS, E. Structures, processes and relational mechanisms for IT governance. In: VAN GREMBERGEN, W. (Org.). *Strategies for information technology governance*. Hershey, PA: Idea Group Inc. Publishing, 2004. p. 1_36.

WOOD, C. C. Don't let the role of information security policies in the Arthur Andersen/Enron case go without mention to your Chief Executive Officer. *Computer Fraud & Security*, v. 2002, n. 5, p. 11_13, May 2002.

WOOD, C. C. *Information Security Policies Made Easy* : Version 9. Boston: Baseline Software Press, 2002.

Esteganografia: a arte das mensagens ocultas[1]


Divulgação

Célio Albuquerque

Ph.D. (2000) em Informação e Ciência da Computação, pela University of California, Irvine, e atua como professor do DCC/UFF, desde 2004.


Divulgação

Eduardo Pagani Julio

Mestre em Computação (2007), pela UFF, e atua, desde 2004, como professor da Universidade Salgado de Oliveira e da Faculdade Metodista Granbery, ambas em Juiz de Fora.


Divulgação

Wagner Gaspar Brazil

Mestre em Computação (2007), pela UFF, e atualmente trabalha na Petrobrás, na área de Segurança da Informação, sendo responsável por projetos de criptografia, análise de risco e certificação digital.

RESUMO

Esteganografia deriva do grego, em que estegano significa esconder, mascarar, e grafia significa escrita. Logo, esteganografia é a arte da escrita oculta. Durante toda a história, as pessoas buscam inúmeras maneiras de esconder informações dentro de outros meios, para, de alguma forma, obter mais privacidade para seus meios de comunicação. As abordagens mais comuns de inserção de mensagens em imagens incluem técnicas de inserção no bit menos significativo, filtragem e mascaramento e algoritmos de transformações. Cada uma destas técnicas pode ser aplicada a imagens, com graus variados de sucesso.

1 Uma versão estendida deste trabalho encontra-se disponível em [20].

1. Introdução

A segurança digital é uma área com grande potencial para pesquisa e desenvolvimento. Sistemas de detecção de intrusão, anti-vírus, proxies e firewalls, ultimamente, aparecem muito na mídia em geral e estão se tornando ferramentas de uso doméstico. É cada vez maior o número de pessoas que tentam ludibriar as defesas, para ter acesso a um dos bens mais preciosos da sociedade moderna: a informação. Por outro lado, existem outras pessoas que buscam o desenvolvimento e o estudo de técnicas para proteção das comunicações. As ferramentas e técnicas que provêem a segurança da informação são inúmeras. A criptografia está entre elas há milhares de anos.

Um dos ramos da criptografia é a esteganografia. De origem grega, a palavra significa a arte da escrita escondida (estegano = esconder e grafia = escrita). A esteganálise, por sua vez, é a arte de detectar mensagens escondidas nos mais diversos meios de comunicação. A esteganografia inclui um amplo conjunto de métodos e de técnicas, desenvolvido ao longo da história, para prover comunicações secretas. Dentre as técnicas destacam-se: tintas invisíveis, micropontos, arranjo de caracteres, assinaturas digitais e canais escondidos [1,2,3].

As aplicações de esteganografia incluem identificação de componentes dentro de um subconjunto de dados, legendagem, rastreamento de documentos e certificação digital e demonstração de que um conteúdo original não foi alterado. Entretanto, como qualquer técnica, a esteganografia pode ser usada correta ou incorretamente. Há indícios recentes de que a esteganografia tem sido utilizada para divulgar imagens de pornografia infantil na internet [4,5], além das mensagens de redes terroristas.

Há um interesse cada vez maior, por diferentes comunidades de pesquisa, no campo da esteganografia, marcas d'água e seriação digitais. Com certeza, isso leva a uma certa confusão na terminologia. A seguir, encontram-se alguns dos principais termos utilizados nestas áreas:

- dado embutido ou embedded data – é o dado que será enviado de maneira secreta, normalmente em uma mensagem, texto ou figura;
- mensagem de cobertura ou cover-message – é a mensagem que servirá para mascarar o dado embutido. Esta mensagem de cobertura pode ser de áudio, de texto ou uma imagem;
- estego-objeto ou stego-object – após a inserção do dado embutido na mensagem de cobertura obtém-se o estego-objeto;
- estego-chave ou stego-key – adicionalmente pode ser usada uma chave para inserir os dados do dado embutido na mensagem de cobertura. A esta chave dá-se o nome de estego-chave;
- número de série digital ou marca fingerprinting – consiste em uma série de números embutidos no material que será protegido, a fim de provar a autoria do documento.

Os sistemas de marcação visam proteger a propriedade intelectual sobre algum tipo de mídia (eletrônica ou não). Estes sistemas de marcação são conhecidos também como watermarking (marca d'água). Apesar de aparecer quase sempre em conjunto com a esteganografia, os sistemas de marcação não pertencem a esse ramo. Ambos fazem parte de uma área de pesquisa conhecida como ocultamento da informação ou information hiding.

O sistema de marcação tipo marca d'água refere-se a métodos que escondem informações em objetos que são robustos e resistentes a modificações. Nesse sentido, seria impossível remover uma marca d'água de um objeto sem alterar a sua qualidade visual. Por outro lado, a esteganografia propõe-se a esconder uma informação em uma imagem de cobertura. Se a imagem for destruída ou afetada, a mensagem é perdida. Uma outra diferença clara entre esteganografia e técnicas de marca d'água é que, enquanto o dado embutido da esteganografia nunca deve ficar aparente, a marca d'água pode ou não aparecer no objeto marcado, dependendo da aplicação que se queira atender.

Nesse sentido, podem-se classificar os sistemas de marcação segundo sua robustez e sua aparência. Quanto à robustez, podem ser classificados como robustos ou frágeis. Já quanto à aparência, os sistemas de marcação podem ser classificados como de marcação imperceptível ou de marcação visível.

2. Aspectos históricos

A esteganografia é uma arte antiga. Suas origens remontam à antiguidade. Os gregos já a utilizavam para enviar mensagens em tempos de guerra [6]. Alguns reis raspavam as cabeças de escravos e tatuavam as mensagens nelas. Depois que o cabelo crescesse, o rei mandava o escravo pessoalmente com a mensagem. Os egípcios usavam ilustrações para cobrir as mensagens escondidas. O método de escrita egípcio conhecido como hieróglifo era uma técnica comum para esconder mensagens. Quando um mensageiro egípcio era pego com um hieróglifo que continha algum código, o inimigo não suspeitava e a mensagem podia ser entregue sem problemas ao destinatário.

Durante a Idade Média, a esteganografia foi mais estudada e desenvolvida. Em 1499, um monge chamado Tritheimius escreveu uma série de livros chamados "Steganographia", nos quais descreveu várias técnicas diferentes. Uma delas foi a grade de Cardano, que era uma lâmina que randomicamente definia retângulos. A quantidade e o posicionamento dos retângulos eram o segredo da grade. O remetente escrevia as palavras da mensagem secreta nos retângulos. Depois, a grade era removida e o remetente preenchia os espaços remanescentes com letras ou palavras, para criar a mensagem que seria enviada. Uma vez entregue a mensagem, o destinatário colocava a grade, que era a mesma do emissor, sobre o papel ou superfície que continha a mensagem, e podia ler os caracteres, dentro dos retângulos, sem problemas.

Tintas invisíveis também foram muito usadas em esteganografia nos tempos mais modernos e são utilizadas até hoje. Essas tintas foram utilizadas por espiões durante a Primeira e a Segunda Guerra Mundial, com o desenvolvimento de reagentes químicos específicos para cada uma. Outros métodos modernos de esteganografia incluem cifradores nulos, que são mensagens nas quais certas letras devem ser usadas para formar a mensagem e todas as outras palavras ou letras são consideradas nulas. Para o seu uso, ambos os lados da comunicação devem manter o mesmo protocolo de uso das letras que formam a mensagem. Este método é difícil de implementar, pois a mensagem de cobertura deve ter algum sentido, do contrário, um inimigo desconfiará e quebrará o código. Um exemplo de um código utilizando cifrador nulo é mostrado a seguir [7].

"News Eight Weather: tonight increasing snow. Unexpected precipitation smothers eastern towns. Be extremely cautious and use snowtires especially heading east. The highways are knowingly slippery. Highway evacuation is suspected. Police report emergencies in downtown ending near Tuesday".

Usando as primeiras letras de cada palavra o texto que aparece é:

"Newt is upset because he thinks he is president".

Novas técnicas de esteganografia são produzidas atualmente para ser utilizadas nos novos meios de comunicação. Por exemplo, hoje em dia muitos artistas e gravadoras usam a marca d'água para proteger suas obras. Com o crescente aumento da pirataria e de sites na internet, onde se podem baixar filmes, músicas e vídeos, esta técnica tem se mostrado uma aliada na proteção dos direitos autorais. O uso de esteganografia em software tem um grande potencial, pois pode esconder dados em uma infinidade de mídias. Nas técnicas que utilizam o último bit de um byte para esconder mensagens, uma mensagem de 64kbytes pode ser escondida em uma figura de 1.024 x 1.024 em tons de cinza ou imagens coloridas. Esta e outras novas técnicas representam o estado da arte da esteganografia atual e são apresentadas a seguir.

3. Técnicas de esteganografia

As abordagens mais comuns de inserção de mensagens em imagens incluem técnicas de inserção no bit menos signicativo, técnicas de filtragem e mascaramento e algoritmos e transformações. Cada uma destas técnicas pode ser aplicada a imagens, com graus variados de sucesso. O método de inserção no bit menos signicativo é, provavelmente, uma das melhores técnicas de esteganografia em imagem [1,9].

3.1 LSB

Estas técnicas baseiam-se na modificação dos bits menos significativos (Least Significant Bit) dos valores de pixel no domínio espacial. Em uma implementação básica, estes pixels substituem o

plano LSB inteiro com o stego-dados. Com esquemas mais sofisticados, em que locais de inclusão são adaptativamente selecionados, dependendo de características da visão humana, até uma pequena distorção é aceitável. Em geral, a inclusão de LSB simples é suscetível a processamento de imagem, especialmente a compressão sem perda.

Técnicas com base em LSB podem ser aplicadas a cada pixel de uma imagem codificada em 32bits por pixel. Estas imagens possuem seus pixels codificados em quatro bytes. Um para o canal alfa, outro para o vermelho, outro para o verde e outro para o azul. Seguramente, pode-se selecionar o LSB de cada byte do pixel para representar o bit a ser escondido sem causar alterações perceptíveis na imagem. Estas técnicas constituem a forma de mascaramento em imagens mais difícil de ser detectada, pois podem inserir dados em pixels não seqüenciais, tornando complexa a detecção [1,9,12].

3.2 Filtragem e mascaramento

As técnicas de esteganografia que se baseiam em filtragem e mascaramento são mais robustas que a inserção LSB. Estas geram estego-imagens imunes à compressão e ao recorte. No entanto, são técnicas mais propensas à detecção [9]. Ao contrário da inserção no canal LSB, as técnicas de filtragem e mascaramento trabalham com modificações nos bits mais significativos das imagens. As imagens de cobertura devem ser em tons de cinza, porque estas técnicas não são eficazes em imagens coloridas [12]. Isto deve-se ao fato de que modificações em bits mais significativos de imagens em cores geram muitos artefatos, tornando as informações mais propensas à detecção.

Estas técnicas são semelhantes à marca d'água visível, em que valores de pixel em áreas mascaradas são aumentados ou diminuídos por um pouco de porcentagem. Reduzindo o incremento por um certo grau faz a marca invisível. No método de retalhos (patchwork), pares de remendos (patches) são selecionados pseudo-aleatoriamente. Os valores de pixel em cada par são aumentados por um valor constante pequeno em um remendo e diminuídos pela mesma quantia no outro.

3.3 Algoritmos e transformações

As técnicas de esteganografia, que se baseiam em algoritmos e transformações, conseguem tirar proveito de um dos principais problemas da inserção no canal LSB, que é a compressão. Para isso, são utilizadas: a transformada de Fourier discreta, a transformada de cosseno discreta e a transformada Z [13].

Sendo embutido no domínio de transformação, os dados escondidos residem em áreas mais robustas, espalhadas através da imagem inteira, e fornecem melhor resistência contra processamento de sinal. Configuram-se como as mais sofisticadas técnicas de mascaramento de informações conhecidas [12], embora sofisticação nem sempre implique em maior robustez aos ataques de esteganálise. A inclusão de dados apresentados no domínio de transformação é amplamente usada para marca d'água robusta.

De forma geral, estas técnicas com base em algoritmos e transformações aplicam uma determinada transformação em blocos de 8x8 pixels na imagem. Em cada bloco, devem ser selecionados os coeficientes redundantes ou de menor importância. Posteriormente, estes coeficientes são utilizados para atribuir a mensagem a ser escondida em um processo, em que cada coeficiente é substituído por um valor pré-determinado para o bit 0 ou 1 [12].

A transformada de cosseno discreta (DCT) é muito utilizada nas compressões dos padrões JPEG e MPEG. Para imagens em que as variações dos tons são graduais, a técnica de DCT mostra excelentes resultados e, por isso, é adotada nos padrões mais usados hoje em dia. O padrão MPEG usa para a compressão de áudio uma variante da DCT conhecida como MDCT (Modified DCT). Maiores detalhes podem ser obtidos em [14].

3.4 Outras técnicas

Na técnica de espalhamento de espectro (como o espalhamento de freqüência), os dados escondidos são espalhados ao longo da imagem de cobertura. Uma estego-chave é usada para selecionar randomicamente os canais de freqüência. A White Noise Storm é uma ferramenta popular que usa esta técnica. Em [15],

dados embutidos como objeto a ser transmitido, a imagem de cobertura é visualizada como interferência em um framework de comunicação de cobertura.

No mundo digital atual, há grande quantidade de áudio e vídeo circulando principalmente pela internet. Quando informações são escondidas dentro de um vídeo, normalmente é usado o método da DCT. Sendo assim, esteganografia em vídeo é muito similar à esteganografia em imagens, exceto pelo fato de que as informações são escondidas em cada frame do arquivo de vídeo.

Esconder imagens em sinais de áudio é algo desafiante, pois o sistema auditivo humano (SAH) pode trabalhar em uma faixa muito grande de freqüências. A sensitividade a ruído é muito apurada. Apesar de ser tão poderoso para captar sinais e freqüências, o SAH não consegue fazer diferenciação de tudo que recebe. Sendo assim, sons mais altos tendem a mascarar sons mais baixos. Além disso, o SAH não consegue perceber um sinal em fase absoluta, somente em fases relativas. Também existem algumas distorções do ambiente muito comuns, que são simplesmente ignoradas pelo ouvido na maioria dos casos. Para desenvolver um método de esteganografia em áudio, a representação do sinal e o caminho de transmissão devem ser considerados na escolha de um método de esteganografia. A taxa de dados é muito dependente da taxa de amostragem e do tipo de som que está sendo codificado. Um valor típico de taxa é 16 bps, mas este valor pode variar de 2 bps a 128 bps.

4. Técnicas de esteganálise

Grande parte das técnicas de esteganografia possui falhas ou insere padrões que podem ser detectados. Algumas vezes, basta um agressor fazer um exame mais detalhado desses padrões gerados, para descobrir que há mensagens escondidas. Outras vezes, o processo de mascaramento de informações é mais robusto e as tentativas de detectar ou mesmo recuperar ilicitamente as mensagens podem ser frustradas. A pesquisa de métodos para descobrir se há alguma mensagem escondida por esteganografia é chamada esteganálise.

Recuperar os dados escondidos está além da capacidade da maioria dos testes atuais, uma vez que muitos algoritmos de mascaramento utilizam geradores aleatórios muito seguros para esconder a informação durante o processo de mascaramento. Muitas vezes, os bits são espalhados pelo objeto de cobertura. Dessa forma, os melhores algoritmos de esteganálise podem não ser capazes de dizer onde está a informação, mas devem dizer se há dados escondidos.

Existem diversas abordagens para detectar a presença de conteúdo escondido em imagens digitais. Estas abordagens podem ser divididas em três tipos [16]:

- **ataques aurais –** estes ataques consistem em retirar as partes significativas da imagem como um meio de facilitar aos olhos humanos a busca por anomalias nessa imagem. Um teste comum é mostrar os bits menos significativos da imagem. Câmeras, scanners e outros dispositivos sempre deixam alguns padrões nos bits menos significativos.
- **ataques estruturais –** a estrutura do arquivo de dados algumas vezes muda assim que outra mensagem é inserida. Nesses casos, um sistema capaz de analisar padrões estruturais seria capaz de descobrir a mensagem escondida. Por exemplo, se mensagens são escondidas em imagens indexadas (paletas de cores), pode ser necessário usar diferentes versões de paletas. Este tipo de atitude muda as características estruturais da imagem de cobertura, logo, as chances de detecção da presença de uma mensagem escondida aumentam [9].
- **ataques estatísticos** – os padrões dos pixels e seus bits menos significativos freqüentemente revelam a existência de uma mensagem secreta nos perfis estatísticos. Os novos dados não têm os mesmos perfis esperados. Estas técnicas estatísticas também podem ser usadas para determinar se uma dada imagem e/ou som possui alguma mensagem escondida. Na maioria das vezes, os dados escondidos são mais aleatórios que os substituídos no processo de mascaramento ou inserem padrões que alteram as propriedades estatísticas inerentes do objeto de cobertura [9,17,18]. Dentre as técnicas de esteganálise, que se baseiam em ataques estatísticos existentes, podem ser citadas: esteganálise por teste do χ^2(Chi-Square Test Approach), análise RS, métricas de qualidade de imagens, métricas de tons contínuos e análise de pares de amostragem.

5. Aplicações

Em atividades militares, a descoberta de comunicações secretas pode levar a um ataque imediato do inimigo. Mesmo com a criptografia, a simples detecção do sinal é fatal, pois descobre-se não somente a existência de inimigos, mas também a sua posição. Unindo o conceito de ocultamento de informação com técnicas como modulação em espalhamento de espectro torna-se mais difícil de os sinais serem detectados ou embaralhados pelo inimigo.

Várias técnicas relacionadas com o ocultamento de informação levam em consideração sistemas com níveis de segurança. Um vírus ou um programa malicioso propaga-se dentro do sistema passando de níveis de segurança inferiores para os superiores. Uma vez que alcança seu objetivo, tenta passar informações sigilosas para setores de nível de segurança menores. Para isso, utilizam-se de técnicas de ocultamento para esconder informações confidenciais em arquivos comuns de maneira que o sistema lhe permita ultrapassar níveis de segurança diferentes.

Existem situações em que se deseja enviar uma mensagem sem que seja possível descobrir quem a enviou. Geralmente, esse tipo de situação é mais uma característica de atividades ilegais. Entretanto, essa situação também tem aplicações em atividades legais, em que se deseja que a privacidade do remetente seja mantida. Alguns exemplos dessas situações são: registros médicos ou votações on-line.

Existem também grandes aplicações na área da indústria médica no que diz respeito a imagens médicas. Normalmente, é usada uma forma de comunicação padrão chamada DICOM, que separa a imagem das informações relativas ao paciente e ao exame como o nome, a data e o médico. Em alguns casos, a ligação entre os dados e a imagem é perdida. Então, se as informações fossem ocultadas dentro da própria imagem, não haveria risco de a imagem se separar dos dados [19].

Em alguns casos, deseja-se monitorar um dado arquivo, com direitos autorais, que está sendo distribuído na internet, por exemplo. Pode-se também inserir pedaços de informações dentro dos dados que estão sendo transmitidos, para que o público que as receba possa usá-las. Como exemplo, podem-se ter informações de um dado produto anunciado por uma rádio, em que o cliente, com um simples apertar de botão, pode descobrir o preço, o local de venda mais próximo ou fabricante. Atualmente, a esteganografia tem sido também explorada em ramos de sistemas de detecção de intrusão [10] e em sistemas de arquivos [11]. Outras aplicações de esteganografia incluem as técnicas de autenticação, criptografia e rastreamento de documentos, que podem ser utilizadas normalmente em conjunto com a técnica de marca d'água.

5.1 Marcas d'água

O grande crescimento dos sistemas de multimídia interligados pela rede de computadores nos últimos anos apresenta um enorme desafio nos aspectos propriedade, integridade e autenticação dos dados digitais. Para enfrentar tal desafio, o conceito de marca d'água digital foi definido.

Uma marca d'água é um sinal portador de informação, visualmente imperceptível, embutido em uma imagem digital. A imagem que contém uma marca é dita imagem marcada ou hospedeira. Apesar de muitas técnicas de marca d'água poderem ser aplicadas diretamente para diferentes tipos de dados digitais, as mídias mais utilizadas são as imagens estáticas.

Existe uma certa confusão entre as marcas d'água imperceptíveis e as visíveis utilizadas em cédulas de dinheiro, por exemplo. As visíveis são usadas em imagens e aparecem sobrepostas, sem prejudicar muito a sua percepção. São usadas geralmente para expor imagens em locais públicos, como páginas na internet, sem o risco de alguém copiá-las e usá-las comercialmente, pois é difícil remover a modificação sem destruir a obra original. É possível também inserir digitalmente marcas visíveis em vídeo e até audíveis em música.

As marcas d'água digitais são classificadas, de acordo com a dificuldade em removê-las, em robustas, frágeis e semifrágeis. Normalmente, esta classificação também determina a finalidade para a qual a marca será utilizada.

As marcas robustas são projetadas para resistir à maioria dos procedimentos de manipulação de imagens. A informação embutida em uma imagem, por meio de uma marca robusta, poderia ser extraída mesmo que a imagem hospedeira sofresse rotação, mudança de escala, mudança de brilho/contraste, compactação com perdas com diferentes níveis de compressão, corte das bordas, etc. Uma boa marca d'água robusta deveria ser impossível de ser removida, a não ser que a qualidade da

imagem resultante deteriore a ponto de destruir seu conteúdo visual. Por esse motivo, as marcas d'água robustas são normalmente utilizadas para a verificação da propriedade das imagens.

As marcas frágeis são facilmente removíveis e corrompidas por qualquer processamento na imagem. Este tipo de marca d'água é útil para checar a integridade e a autenticidade da imagem, pois possibilita detectar alterações nesta. Às vezes, esta propriedade é indesejável. Por exemplo, ajustar brilho/contraste para melhorar a qualidade da imagem pode ser um processamento válido, que não deveria ser detectado como uma tentativa de adulteração maliciosa. Ou então, compactar uma imagem com perdas em diferentes níveis de compressão deveria ser uma operação permitida. Ainda, imprimir e escanear uma imagem não deveria levar à perda da autenticação. Assim, foram criadas as marcas d'água semifrágeis.

Uma marca semifrágil também serve para autenticar imagens. Diferentemente, estas procuram distinguir as alterações que modificam uma imagem substancialmente daquelas que não modificam o conteúdo visual da imagem. Uma marca semifrágil normalmente extrai algumas características da imagem que permanecem invariantes por meio das operações permitidas e as insere de volta na imagem de forma que a alteração de uma dessas características possa ser detectada.

Podem-se subdividir as marcas de autenticação em três subcategorias: sem chave, com chave secreta e com chave pública/privada. Com relação à extração da marca d'água, têm-se três tipos de sistemas diferentes. Cada um deles diferencia-se pela sua natureza ou combinação de entradas e saídas:

- **marcas d'água privadas (também chamadas não-cegas) –** esse sistema requer a marca d'água original. Dentro desse esquema, existem dois tipos. No primeiro, é necessário o arquivo original para achar pistas de onde se localiza a marca dentro do arquivo marcado. O sistema do segundo tipo necessita das mesmas informações do anterior, mas somente tenta responder se o arquivo contém a marca d'água. Espera-se que este sistema seja mais robusto, já que transporta pouca informação e requer acesso a dados secretos;
- **marcas d'água semiprivadas ou semicegas –** diferente do anterior, não utiliza o arquivo original na extração. Algumas aplicações onde poderia ser utilizado esse esquema seriam para provar a propriedade em corte ou em mecanismos de controle de cópia como em aparelhos de DVDs;
- **marcas d'água públicas ou cegas –** não requer nem o arquivo original nem a marca. A intenção do esquema é tentar retirar a marca do dado sem pistas de onde este se localiza ou como seria.

6. Aplicativos existentes

As redes de computadores, atualmente, provêem um canal de fácil utilização para a esteganografia. Vários tipos de arquivo podem ser utilizados como imagem de cobertura incluindo imagens, sons, texto e até executáveis. Por isso, é grande o número de aplicativos já criados para tentar usar esta facilidade. Por outro lado, existem também alguns softwares de esteganálise que tentam localizar os dados embutidos nas diversas mensagens de cobertura. Tais aplicações podem ser encontradas facilmente na internet e funcionam em várias plataformas.

As ferramentas Ezstego e Stego On-line trabalham com imagens indexadas de 8bits no formato GIF. Outra aplicação é o Revelation, que esconde arquivos em imagens de cobertura no formato bitmap de 24bits. Por ser escritas em Java, estas ferramentas são altamente portáveis.

As ferramentas Hide and Seek e Jphide and Seek são capazes de inserir uma lista de arquivos em uma imagem no formato JPEG. O Jphide and Seek utiliza criptografia de chave simétrica e o usuário é obrigado a fornecer uma pass phrase. É interessante notar que o aplicativo analisa a imagem de cobertura e diz qual o tamanho máximo que o arquivo de entrada deve ter para que o processo seja seguro.

O Outguess propõe-se a melhorar o passo da codificação da imagem JPEG por meio de um gerador de números pseudoaleatórios. Os coeficientes da DCT são escolhidos também de maneira randômica para ser substituídos pelos números gerados aleatoriamente. O LSB dos coeficientes selecionados é substituído pela mensagem cifrada. Testes estatísticos de primeira ordem não são capazes de detectar mensagens mascaradas com o Outguess.

Os softwares de esteganálise dispõem-se a descobrir se os arquivos usados como mensagem de cobertura contêm algum dado embutido e se é possível identificar o software utilizado no processo de esteganografia. Um destes softwares é o StegSpy,

que permite a identificação de um arquivo que serve como mensagem de cobertura. O programa detectará a esteganografia e o software utilizado para esconder o dado embutido. A versão atual do software também identifica a localização da mensagem embutida dentro do arquivo de cobertura. O StegSpy, atualmente, identifica os programas Hiderman, JPHide and Seek, Masker, JPegX e Invisible Secrets.

Outra ferramenta de esteganálise é o StegDetect. Este software propõe-se a detectar o conteúdo esteganográfico gerado pelos softwares Jsteg, JP Hide and Seek, Invisible Secrets, versões mais antigas do Outguess, F5, AppendX, e Camouflage. A versão mais atual do StegDetect suporta análise discriminante linear (LDA), para detectar qualquer estego sistema.

No campo das marcas d'água, existem vários softwares para gerar marcas em diversos tipos de mídias, tais como TeleTrax, Alpha Tec, Syscop e DataMark. O ponto fundamental de todos os programas é a robustez da marca produzida. Nesse sentido, é preciso testar esta robustez de alguma forma. O StirMark é uma ferramenta para testes de robustez de algoritmos de marca d'água. Com o StirMark foi possível realizar o primeiro *benchmarking* de algoritmos de marca d'água, em 1999.

O programa SignIt da AlpVision é de fácil utilização para esconder números de série IDDN em imagens de vários formatos. Este número é escondido em todos os lugares na imagem e não pode ser visto a olho nu. Além disso, é impossível remover o número de inscrição embutido sem alterar a imagem em um modo visível. Para controlar sua utilização, o software conecta-se com a empresa desenvolvedora pela internet, que armazena o IDDN de todos os usuários registrados, o que torna esse identificador único, podendo ser utilizado para proteger os direitos autorais de imagens e localizar cópias ilegais.

O software GWatermarker insere tanto a marca d'água de forma visível a olho nu, quanto de maneira invisível de forma robusta. O software utiliza algoritmos próprios para a inserção e remoção das marcas visíveis e invisíveis (algoritmo RC4 para a inserção da chave secreta e o algoritmo hash MD5).

7. Considerações finais e tendências

Tanto a esteganografia quanto a marca d'água descrevem técnicas que são usadas na intenção de ocultar uma comunicação dentro de uma informação disfarce. Entretanto, esteganografia refere-se tipicamente a uma comunicação ponto-a-ponto. Por isso, o método geralmente não é robusto contra modificações ou tem somente uma robustez limitada que a protege de pequenas alterações que possam ocorrer em termos de transmissão, armazenamento, mudanças de formato, compressão ou conversões digital-analógicas.

Em marcas d'água, por outro lado, o foco está na robustez. Não existe comunicação ponto-a-ponto, mas deseja-se que a marca inserida em um dado seja recuperada de algum modo depois da imagem circular por quaisquer canais típicos da aplicação. Por exemplo, pode-se marcar uma imagem que se deseja proteger contra cópias sem autorização. Caso alguém a copie e utilize técnicas de processamento de imagem para tentar apagar a marca, ainda assim deve ser possível decodificar a marca da imagem alterada. Isso provaria quem é o verdadeiro autor ou proprietário da imagem. A questão da detecção não é tão importante, apesar de que, se o observador não perceber a marca, talvez nem tente removê-la.

Um exemplo de aplicação oposta seria marcar uma imagem para verificar se esta sofrerá alterações. Caso a imagem seja modificada de alguma forma, a marca será destruída, mostrando que o ato realmente aconteceu. A robustez ou a sua ausência define a aplicação da marca utilizada. As marcas d'água robustas devem resistir a ataques e alterações na imagem. As marcas frágeis devem ser destruídas, caso a imagem sofra alterações.

Atualmente, existem estudos para proteger a esteganografia das técnicas de esteganálise. Em [8] são apresentados novos métodos que permitem esconder mensagens de forma segura e resistente à análise estatística.

Técnicas esteganográficas têm uso legal e ilegal. Como uso legal no presente e no futuro, esteganografia tem sido usada e será cada vez mais utilizada na proteção de direitos intelectuais, principalmente quando se consideram as novas formas de comercialização que utilizam a mídia digital. Nesse sentido, as técnicas de marca d'água parecem ser um campo profícuo de pesquisa e aplicações no futuro.

Por outro lado, há o uso ilegal de técnicas esteganográficas, que cresce cada vez mais, em virtude da facilidade de acesso à internet. Usar esteganografia para transitar mensagens ou até pequenas imagens de pornografia ou pedofilia é possível e provável. Um relatório de crimes de

tecnologia lista alguns tipos de crime comuns utilizando alta tecnologia:

- comunicações criminosas;
- fraudes;
- hacking;
- pagamentos eletrônicos;
- pornografia e pedofilia;
- ofensas à propriedade intelectual;
- propagação de vírus e cavalos de tróia.

Um exame preliminar desta lista mostra vários casos de mau uso da esteganografia, principalmente no que se refere à comunicação criminosa. Em termos de segurança da informação há também outras áreas de interesse. Uma área com uso potencial em várias aplicações é o desenvolvimento de protocolos que usam esteganografia para burlar censura. Há também a possibilidade de ataques de vírus utilizarem técnicas de esteganografia. As técnicas e ferramentas esteganográficas podem ser utilizadas em conjunto com outras aplicações para, automaticamente, extrair informações escondidas sem a intervenção do usuário. Um cenário possível para um ataque de vírus poderia ser o envio de uma mensagem escondida em uma imagem enviada por e-mail. Um cavalo de tróia instalado na máquina poderia então extrair o vírus da imagem e infectar várias máquinas.

Finalizando, a esteganografia, quando bem utilizada, fornece meios eficientes e eficazes na busca por proteção digital. Associando criptografia e esteganografia, as pessoas têm em mãos o poder de comunicar-se em segredo pela rede mundial de computadores mantendo suas identidades íntegras e secretas.

Referências

[1] PETITCOLAS, F. A. P.; ANDERSON, R. J.; KUHN, M. G. Information hiding — A survey. *Proceedings of the IEEE*, v. 87, n. 7, p. 1062–1078, 1999.

[2] PETITCOLAS, F. A. P.; KATZENBEISSER, S. *Information hiding techniques for steganography and digital watermarking*. 1st. ed. [S.l.]: Artech House Books, 1999.

[3] JOHNSON, N. F.; JAJODIA, S. Exploring steganography: Seeing the unseen. *IEEE Computer*, v. 31, n. 2, p. 26–34, 1998.

[4] MORRIS, S. *The future of netcrime now (1) -threats and challenges*. Home Office Crime and Policing Group, USA, 2004. Technical Report 62.

[5] HART, S. V.; ASHCROFT, J.; DANIELS, D. J. *Forensic examination of digital evidence: a guide for law enforcement*. Department of Justice -Office of Justice Programs, USA, April 2004. Technical Report NCJ 199408.

[6] KAHN, D. The history of steganography. In: *Proceedings of the First International Workshop*. Cambridge, UK: [s.n.], 1996.

[7] JOHNSON, N. *Steganography*. George Mason University, 1998.

[8] MEERWALD, P. *Digital Image Watermarking in the Wavelet Transform Domain*. Dissertação (Mestrado) — Department of Scientific Computing, University of Salzburg, Austria, January 2001.

[9] WAYNER, P. *Disappearing Cryptography: Information Hiding: Steganography and Watermarking (2nd Edition)*. San Francisco, CA, USA: Morgan Kaufmann Publishers Inc., 2002. ISBN 1558607692.

[10] SIEFFERT, M. et al. Stego intrusion detection system. AFRL/ASU Assured Information Security, Rome, NY, USA, 2004.

[11] HIROHISA, H. Crocus: a steganographic filesystem manager. In: *ASIACCS '07: Proceedings of the 2nd ACM symposium on Information, computer and communications security*. New York, NY, USA: ACM Press, 2007. p. 344–346. ISBN 1-59593-574-6.

[12] POPA, R. *An analysis of steganography techniques*. Dissertação (Mestrado) — The Polytechnic University of Timisoara, Timisoara, Romênia, 1998.

[13] GONZALEZ, R. C.; WOODS, R. E. *Digital Image Processing*. 2nd. ed. Boston, MA, USA: Prentice-Hall, 2002.

[14] SALOMON, D. *Data Compression: The Complete Reference*. Segunda edição. Nova Iorque: Springer, 2000.

[15] MARVEL, L.; BONCELET, C.; RETTER, J. *Spread spectrum image steganography*. 1999.

[16] ROCHA, A. de R. *Randomização Progressiva para Esteganálise*. Dissertação (Mestrado) — Universidade Estadual de Campinas, Campinas, Brasil, 2006.

[17] WESTFELD, A.; PFITZMANN, A. Attacks on steganographic systems. In: *IH '99: Proceedings of the Third International Workshop on Information Hiding*. London, UK: Springer-Verlag, 2000. p. 61–76. ISBN 3-540-67182-X.

[18] PROVOS, N.; HONEYMAN, P. Hide and seek: An introduction to steganography. *IEEE Security and Privacy*, IEEE Educational Activities Department, Piscataway, NJ, USA, v. 1, n. 3, p. 32–44, 2003. ISSN 1540-7993.

[19] FILHO de L. et al. Electrocardiographic signal compression using multiscale recurrent patterns. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, v. 52, n. 12, p. 2739–2753, 2005.

[20] JULIO, E. P. ; BRAZIL, W. ; Albuquerque, C. Esteganografia e suas Aplicações. Em: Livro de Minicursos do SBSEG. Rio de Janeiro: Sociedade Brasileira de Computação, 2007, v. VII, p. 54-102.

[21]WANG, H.; WANG, S., Cyber warfare: steganography vs. steganalysis. Commun. ACM, ACM Press, New York, NY, USA, v. 47, n. 10, p. 76–82, 2004. ISSN 0001-0782.

Você sabe com o quê está falando?


Divulgação

Luís Carlos Silva Eiras
luiscarloseiras@gmail.com

Em "Jogos de guerra"[1], David (Mathew Broderick) é um garoto que vai mal na escola. Numa das muitas vezes em que é chamado na diretoria, depois de uma ótima piada sobre reprodução assexuada em sala de aula, descobre a senha do sistema de notas. "Pencil" está escrito num papel colado na mesa retrátil da secretária. É suficiente para que ele, em casa, entre no sistema e aumente sua nota e a de sua namorada.

Essas cenas resumem um dos problemas da segurança de qualquer sistema: senhas óbvias, guardadas em lugares óbvios. Enfim, não adianta sofisticar o acesso nas máquinas e nos sistemas, se a "engenharia social" – eufemismo para roubo de senhas – tem sempre êxito. Quem, num centro de um centro de processamento de dados, não ouviu alguém gritando: "Ô, fulano, qual que é mesmo a senha?". E quem não conhece alguém cuja senha do banco está anotada no próprio cartão magnético?

Além das senhas, outras invenções para identificação podem ser vistas em filmes. Em "2001, Uma odisséia no espaço"[2], Dr. Heywood Floyd (Willian Sylvester) tem que falar seu destino, nacionalidade e nome para ser identificado na estação espacial[3]. James Bond (Sean Connery) é erradamente identificado pelas digitais por uma complicada máquina escondida dentro de um guarda-roupa (!) em "007 - Os diamantes são eternos"[4].

Às vezes, há um nítido avanço na imaginação dos roteiristas. Em "Blade Runner, O caçador de andróides"[5] o reconhecimento é feito por meio de um teste chamado Voight-Kampff, que mistura análise da íris com perguntas idiotas. Já em "Minority Report"[6] a mesma análise é feita por aranhas-robôs sem as perguntas. A identificação em "Gattaca"[7] é mais complicada: os personagens são submetidos, toda hora, a testes de DNA, o que não impede que sejam burlados.

Os filmes dão apenas uma idéia[8]. Na prática já podemos ser identificados por meios biométricos (impressões digitais, formato da mão e do rosto, altura, cor dos olhos e dos cabelos, íris, voz etc.), pelo registro e análise automática da imagem nas câmeras de segurança (de noite, por infravermelho na fronteira do México com os Estados Unidos), por rastreamento de cartões de débito, crédito, de identificação e passaporte, no uso de celulares e no acesso à internet, pelas escutas telefônicas, braceletes e "grampos" rastreados por GPS etc. Quanto ao DNA, exames estão sendo implantados na França para controle dos imigrantes.

Mas nessa história de segurança, legal mesmo são os captchas. Ao invés de o usuário submeter sua identidade ao computador, é o computador que submete o usuário a um teste para certificar se ele é mesmo gente ou uma máquina. Captcha é Completely Automated Turing Test To Tell Computers and Humans Apart ou Teste de Turing Completamente Automático para Diferenciar Computadores e Humanos e foi inventado em 2000.

Um captcha é formado de números e letras distorcidas e, às vezes, riscadas, que aparecem nas páginas iniciais de certos sistemas. Como ainda os computadores são incapazes de ler essas distorções e repeti-las, todo usuário que faz a solução correta é presumidamente humano. Isso tem impedido que sistemas consigam, por tentativas automáticas, entrar em outros sistemas[9].

Os captchas tocam em outro problema. Num mundo onde máquinas, sistemas e pessoas estão cada vez mais conectadas, como saber quem é quem? Quando o mundo do Second Life dominar a internet, como saber se os avatares são de gente ou de máquinas? Com quem ou com o quê você estará falando?

1 John Badham, 1983.
2 Stanley Kubrick, 1968.
3 Mas ele já não teria sido identificado na Terra quando embarcou? Ah, a burocracia espacial!
4 Guy Hamilton, 1971.
5 Ridley Scott, 1982.
6 Steven Spielberg, 2002.
7 Andrew Niccol, 1997.
8 Uma lista de 50 filmes que utilizam biometria para identificação pode ser encontrada em http://www1.folha.uol.com.br/folha/informatica/ult124u21492.shtml.
9 Nesta história de captcha é possível deparar com humor involuntário. O texto na Wikipédia em português sobre o assunto está escrito numa língua muito estranha. http://pt.wikipedia.org/wiki/CAPTCHA.

Há 40 anos, a Prodemge
desenvolve soluções
tecnológicas que
auxiliam o Estado
a prestar serviços
à população
com mais
transparência, agilidade
e modernidade.

40 ANOS conectando Minas

Planejamento • Finanças •
Segurança • Trânsito •
Justiça • Saúde •
Agricultura • Educação •
Cultura • Turismo •
Meio Ambiente • Ação Social •
Desenvolvimento Econômico

prodemge

www.prodemge.gov.br

COM O SHERLOCK,

TI E NEGÓCIO SE CONECTAM EM TEMPO REAL.

O Sherlock é uma suíte de produtos e serviços que apresenta uma visão multidimensional do ambiente de Tecnologia da Informação e sua interferência nos negócios da empresa. Além disso, gerencia o desempenho da infra-estrutura de TI e das aplicações que suportam as áreas produtivas, contribuindo para a saúde do processo empresarial.

SHERLOCK. A MAIS COMPLETA VISÃO DO AMBIENTE DA REDE E APLICAÇÕES DISPONÍVEL NO MERCADO.

AS VANTAGENS DO SHERLOCK TI & BUSINESS.

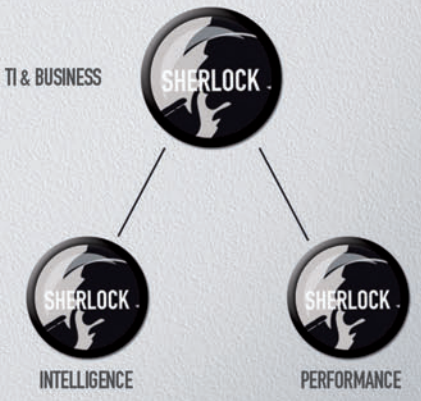
- Gerenciamento centralizado dos serviços;
- Completo entendimento dos problemas de TI e Negócios;
- Planejamento de capacidade;
- Maior disponibilidade das atividades críticas de TI;
- Construção de cenários em função das metas;
- Redução de custos.

MAIS BENEFÍCIOS PARA A ÁREA DE TI DA EMPRESA.

- Melhoria da produtividade;
- Registro de Base de Dados;
- Maior cooperação entre a área de rede, aplicação e negócios;
- Gerência proativa;
- Visão integrada de TI com Negócio.

INTEGRAÇÃO TOTAL COM OS MÓDULOS INTELLIGENCE E PERFORMANCE.

- Sherlock Intelligence: utiliza o conceito de gerência por Unidade de Negócio (UN), permitindo avaliar o impacto de TI no desempenho dessas unidades.
- Sherlock Performance: permite capturar e monitorar dados em tempo real, além de identificar informações importantes para o negócio da empresa.



tel.: (31) 2125 4200
sherlock@microcity.com.br
www.sherlockmicrocity.com.br

MICROCITY
Outsourcing de Infra Estrutura de T.I.