Desafios para a criação de ferramentas de segurança da informação alinhadas à realidade brasileira

Luiz Fernando Rust da Costa Carmo

Hoje em dia nenhuma empresa questiona mais a necessidade de se investir em segurança da Informação. As estatísticas mostram números assustadores. Por exemplo, no último relatório publicado pelo CSI/FBI, relativo ainda a 2005, os prejuízos declarados com incidentes de segurança nos EUA alcançaram cifras da ordem de 130 milhões de dólares. No Brasil, os indicadores publicados pelo CERT BR acompanham as mesmas tendências registradas em âmbito mundial, no que se referem às taxas de crescimento e aos perfis dos incidentes de segurança.

Uma questão fundamental é, se nesse mundo contemporâneo, onde foi desenvolvida uma novíssima cultura própria cibernética extrapolando todas as fronteiras até então estabelecidas por limites geográficos, ainda existiriam especificidades relacionadas a questões culturais, que por sua vez imporiam o desenvolvimento específico de tratamentos (e ferramentas) diferenciados para a Segurança da Informação no Brasil?

Em uma análise essencialmente técnica é quase impossível não apostar em uma inevitável homogeneização dos procedimentos de segurança da informação, haja vista os altos níveis de convergência tecnológica vivenciados atualmente, nunca antes experimentados. Ou alguém ainda questiona que isso é um fato?

Porém, segurança da informação não é apenas tecnologia. Muito pelo contrário, é certamente consenso que o fator humano é o elo mais fraco na corrente de segurança. Por exemplo, os ataques de engenharia social buscam o aproveitamento da negligência, ou da própria desqualificação das pessoas para conseguir obter acesso a informações não autorizadas. Existem ataques de engenharia social diretos, por exemplo, aqueles que se dão por telefone e normalmente exploram a eloqüência de um interlocutor privilegiado; ou os indiretos, que acontecem através de mensagens de correio eletrônico – *phishing* - para convencer as pessoas a revelarem dados confidenciais, ou mesmo promover uma instalação involuntária de algum software que vai deixar a sua máquina vulnerável.

De acordo com *Everardo Rocha (3), "..a cultura marca e é marcada; indivíduo e cultura se influenciam mutuamente; a cultura marca as características que quer nos indivíduos ali formados...*". Ora, se segurança da informação depende do comportamento das pessoas e, se o comportamento das pessoas é influenciado pelas características culturais, resta apenas concluir que segurança da informação é sim fortemente dependente das diferenças culturais.

Segundo *Mônica F. Silva (2),* no Brasil, mais valem as relações pessoais (amizade, parentesco e vizinhança) do que algum contrato ou regulamento; quando o indivíduo se transforma em um simples código de matrícula (como o funcionário em um sistema de

pagamento informatizado), a relação humana desaparece, nossa cultura se ressente desta despersonalização. *Roberto da Matta (1)* explica que existem sociedades focadas nos indivíduos e outras com foco na relação entre estes indivíduos. Estudar o Brasil é estudar a relação entre os indivíduos ou, entre conceitos em oposição, ou ainda, entre as coisas em geral. Para interpretar o Brasil é necessário "estudar aquilo que está **entre** as coisas". Ou seja, o Brasil é relacional.

No Brasil, ao mesmo tempo em que há uma busca desenfreada em mostrar a posse do celular mais moderno, há a rejeição de comprar através de máquinas. Porém, não podemos simplificar a questão sobre como a nossa cultura trata a tecnologia através desta oposição: afeição ou rejeição. A cultura é algo mais amplo e em constante mudança. O ser humano é o agente que constrói a cultura e, ao mesmo tempo, é moldado por ela.

A maioria das "ferramentas" de segurança da informação em voga no Brasil (normas, políticas, análise de riscos/vulnerabilidades...) desconsideram integralmente essas nossas especificidades. Busca-se "conformidade" sem saber o certo o que seria realmente uma referência inquestionável. Diante deste cenário, o que as empresas podem fazer? O primeiro passo é investir em um mapeamento rigoroso das diferenças culturais e seus efeitos. Os aspectos levantados acima permitem perceber com maior clareza como os valores dos indivíduos, herdados da cultura onde estão inseridos, podem afetar sua predisposição ao uso da tecnologia de segurança da informação.

Um outro ponto importante, e também ainda subdimensionado, é a questão da completude funcional das ferramentas de IS face à realidade econômica de nossas empresas. É indiscutível a nossa enorme carência de recursos elegíveis para investimentos em segurança da informação, sem que isso se reflita numa mínima oferta de algum tipo de suporte para a priorização de investimentos. Por exemplo, é necessário que haja uma rápida disseminação de técnicas de priorização de investimento em conjunção com analise de riscos de segurança da informação.

O projeto "AGRIS: Análise e Gerência de Riscos em Segurança" (*financiado pelo Programa FRIDA - Fundo Regional para a Inovação Digital na América Latina e Caribe*) tem como principal objetivo o desenvolvimento de ferramentas costumizadas às práticas organizacionais latino-americanas (enfatizando as brasileiras), levando em conta nossas particularidades culturais e restrições de recursos, mas respeitando integralmente às recentes normas e padrões internacionais correlatos. A ferramenta AGRIS permite que o gestor de Segurança da Informação avalie quais domínios da ISO/IEC 17799 e respectivos controles são relevantes para que a sua organização (análise de conformidade) e, através do mapeamento de seus ativos críticos, venha obter a percepção de suas vulnerabilidades, ameaças, probabilidades de ocorrência, estratégias e custos para mitigação dos riscos identificados (análise de riscos).

Por fim, existe um terceiro e ultimo elemento nesta tríade de fatores críticos às ferramentas de segurança da informação no Brasil: o perene problema de adequação de qualquer procedimento "importado" à legislação brasileira vigente. Por exemplo, faz pouco tempo que a proposição nº 18/2003, de autoria da parlamentar Iara Bernardini e que visa coibir o

anonimato dos responsáveis por páginas e endereços eletrônicos registrados no Brasil, não foi aprovada. Esta proposta carrega em si um nítido desvio do entendimento globalizado sobre o tema, implicando na necessidade imediata de reavaliação dos procedimentos (e ferramentas) de gestão de segurança correlatos.

O fato é que talvez estejamos vivendo a pior das situações, e ainda não nos demos conta. Estamos expostos, como todo o mundo, aos mais cruéis dos ataques cribernéticos, porém não sabemos ainda com maior clareza, como os valores dos indivíduos, herdados da cultura brasileira, podem afetar o processo de segurança da informação, e não temos recursos suficientes nem para implementarmos procedimentos importados, que certamente ainda não foram validados à nossa realidade. É preciso que se façam investimentos em frentes multidisciplinar que alinhem: análise comportamental, gerência de riscos, priorização de investimentos, tecnologia da informação, aspectos jurídicos, etc.

1. *Matta, Roberto. A casa & a rua: Espaço, cidadania, mulher e morte no Brasil. Rio de Janeiro: Editora Guanabara, 1987.*
2. *Rocha, Everardo P. G. O que é etnocentrismo. São Paulo: Brasiliense, 1984.*
3. *Silva, Mônica F.; Dias, Donaldo. Intenção de Uso de Tecnologia de Informação: um estudo sobre a influência do contexto social em uma empresa do setor acadêmico brasileiro, Anais do XXXIX CLADEA, 2004.*

Luiz Fernando Rust da Costa Carmo (Dr. em Informática – LAAS/UPS – FR 1994) é Professor do Núcleo de Computação Eletrônica da UFRJ, sendo coordenador do pós-graduação MSI - Gerência de Segurança da Informação