TCU: Disseminando as boas práticas em Segurança da Informação

Luis Fernando Rocha

Nas últimas semanas, a velocidade de criação e a disseminação em massa das variantes dos vírus Netsky e Bagle demonstraram o poder das atuais ameaças eletrônicas. Porém, esse é apenas um os exemplos de riscos que envolvem sistemas ligados em redes e que demonstra a necessidade do aumento de conscientização em Segurança da Informação.

Diante desse cenário, o Tribunal de Contas da União (TCU) resolveu investir na disseminação do conhecimento como ferramenta de prevenção e combate a esta realidade. Estamos falando da cartilha de "Boas Práticas em Segurança da Informação", documento criado pelo Tribunal com o objetivo de despertar a atenção para importância desse assunto em organizações governamentais.

"Os episódios envolvendo segurança que temos visto nos últimos tempos passam quase sempre pela falta de cultura em segurança da informação. O TCU, juntamente com outros órgãos, busca, cada um em seu campo de atuação, criar essa cultura que permitirá que os sistemas informatizados do governo federal sejam mais seguros e que os dados e informações neles armazenados sejam íntegros e estejam protegidos de acessos indevidos e disponíveis para seus usuários", explica Daniel Dias Pereira, Diretor da Diretoria Técnica de Auditoria em Tecnologia da Informação da Secretaria Adjunta de Fiscalização do TCU.

Assim, o documento vem sendo distribuído entre diversos órgãos da administração pública federal, estadual e municipal. Daniel Dias ressalta ainda que o órgão já há algum tempo vem editando cartilhas de orientação sobre vários assuntos relacionados com a gestão pública.

"Essas cartilhas têm como objetivo orientar sobre assuntos de grande relevância para a administração pública e para o próprioTribunal. A Cartilha Boas Práticas em Segurança da Informação surgiu da constatação da importância do tema e da necessidade de se criar uma cultura sobre Segurança da Informação na administração pública", diz.

Os assuntos abordados na Cartilha

Nesta primeira versão do documento, Controle de Acesso Lógico, Política de Segurança da Informação e Plano de Contingências foram os principais assuntos abordados. "Além desses assuntos, colocamos um anexo que contém a legislação sobre Segurança da Informação", revela Daniel.

Um dos aspectos mais interessantes deste documento está no fato de um de seus capítulos apontar a importância da elaboração de um plano de contingência, segmento que ainda apresenta investimentos tímidos nas empresas do país.

Para se ter uma idéia, na 9ª Pesquisa Nacional de Segurança da Informação, realizada entre os meses de março e agosto de 2003 pela Módulo, apenas 21% dos entrevistados admitiram que suas empresas possuíam um Plano de Continuidade de Negócios (PCN) atualizado e testado. É importante ressaltar que este levantamento engloba cerca de 50% das 1.000 maiores empresas brasileiras.

Segundo o Diretor do TCU, planos de contingência que realmente funcionem, caso sejam acionados, custam caro e o que se espera deles é que nunca sejam postos em prática. "Essas características fazem com que os administradores públicos e privados não os vejam como essenciais às organizações ou os planos que precisam ser colocados em marcha recebam maiores prioridades e conseqüentemente mais recursos. Infelizmente os planos de contingência recebem mais atenção quando ocorrem grandes desastres como o do World Trade Center, por exemplo", alerta.

Para ele, dois motivos podem aumentar os investimentos nesses planos: aumento da cultura de Segurança da Informação e quando as organizações enxerguem a informação como um ativo importante a ser protegido.

"As áreas técnicas envolvidas com Segurança da Informação devem buscar mecanismos para criar e difundir uma cultura na área. Só assim será possível sensibilizar a alta direção para esse assunto. Outro instrumento adequado para isso, sem dúvida, é a análise de risco da área de TI", orienta.

ISO 17799 como referência

Quando consultamos a bibliografia utilizada para criação de tal cartilha, constata-se a presença da norma NBR ISO/IEC 17799. "Essa norma é um guia de boas práticas em Segurança da Informação que, embora de forma genérica, abrange praticamente todos aspectos de controle necessários à proteção da informação dentro dos conceitos de integridade, disponibilidade e confidencialidade", diz Daniel Dias.

Segundo ele, por ser uma norma adotada integralmente no Brasil, por intermédio da ABNT, toda organização que queira implementar uma política de Segurança da Informação poderá fazê-lo seguindo tal norma. "Uma organização, seja pública ou privada, que implemente uma Política de Segurança da Informação baseada na ISO/IEC 17799 conseguirá criar as condições necessárias para proteger esse ativo tão importante que é a informação", afirma.

Outros documentos importantes

Além da cartilha, Daniel Dias cita outras normas e metodologias aplicáveis na área, que podem ser utilizadas por um órgão público. "Ao nosso ver, se uma entidade adota o COBIT como instrumento de gestão da área de TI, certamente estará estabelecendo bons controles para a Segurança da Informação. Outras normas internacionais, como o Common Criteria (ISO/IEC 15.408) e o CMM, são importantes e devem ser consideradas", explica.

Ele ressalta ainda que o fundamental é que a organização desenvolva uma cultura de Segurança da Informação e ponha em prática os mecanismos necessários à execução de uma Política de Segurança.

Desafios de um profissional de TI

Perguntado sobre os principais desafios dos profissionais de TI dos setores públicos nessa área, Daniel Dias diz que, como em toda organização, esses profissionais enfrentam os desafios da falta de cultura na área e a pouca disposição em investir recursos em sistemas de segurança.

> "Acreditamos que a falta de cultura em segurança ainda é grande dentro dos próprios órgãos de TI e esse talvez seja o maior desafio a ser vencido. A construção de sistemas seguros e que contenham bons controles de acesso lógico, por exemplo, dependem fundamentalmente dessa conscientização", finaliza.

Quem estiver interessado em conhecer a cartilha "Boas Práticas em Segurança da Informação", pode obter uma cópia gratuita, em PDF, no site do TCU.

(Módulo Security Magazine - 15/3)

boas práticas