NOTÍCIAS ZECA DIRCEU

Brasil lança defesa contra ataque de hackers

13/06/2011

O governo brasileiro começou a colocar em prática medidas para proteger o país no ciberespaço. As ações, que já vinham sendo planejadas há mais de um ano, ganharam corpo em meio à recente escalada dos ataques de hackers a redes públicas, empresas privadas e organismos internacionais, como o FMI.

Brasil inicia plano de proteção no ciberespaço

Segurança: Unidade controlada pelo Exército vai coordenar ações

Moacir Drska e Gustavo Brigatto | De São Paulo

O governo brasileiro não quer que o país entre na lista negra que recentemente passou a incluir do FMI ao Departamento de Comércio dos Estados Unidos, passando por companhias tão diversas como a Sony, o Citigroup e a Lockheed Martin. Esses foram alguns dos alvos recentes da onda maciça de ataques de hackers a redes de computadores.O movimento de defesa do Brasil no ciberespaço começou no fim do ano passado, com o lançamento do "Livro Verde" – um documento que define os parâmetros de proteção das redes governamentais -, mas está ganhando corpo, agora, com a intensificação dos ataques na internet. O cenário é reforçado pela posição dos Estados Unidos em equiparar a sabotagem virtual às ameaças tradicionais, o que permite ao Pentágono responder às ações dos hackers com força militar convencional.

Na prática, o assunto ganhou contornos de segurança nacional no Brasil. Por decisão do governo, a tarefa de efetivar as medidas de defesa e contra-ataque na internet será de uma unidade criada recentemente para esse fim – o Centro de Defesa Cibernética (CDciber). Concebido há um ano, o CDciber está sob o comando do Exército e começa a sair do papel. A ideia é reunir ao redor dele todas as ações de proteção das Forças Armadas em relação ao ciberespaço.

O assunto vem sendo tratado como prioridade pelo governo federal, por meio do Gabinete de Segurança Institucional (GSI) da Presidência da República. Responsável por criar as normas de segurança que devem ser adotadas na administração pública, o órgão está mapeando as vulnerabilidades das redes que controlam sistemas estratégicos no país.

O GSI gerencia 320 grandes redes públicas de computadores, envolvendo 1 milhão de usuários de 37 ministérios e 6 mil entidades governamentais. Segundo Raphael Mandarino Jr., diretor-geral do Departamento de Segurança da Informação e Comunicações do GSI, os ataques que visam o roubo de informações estratégicas são o principal ponto de atenção, apesar de representar apenas 1% das ameaças.

"Registramos 2,1 mil tentativas de invasão a sites do governo por hora. Quanto mais se destaca no cenário internacional, mais o Brasil desperta o interesse dos hackers", afirma Mandarino.

Assim que essas ameaças são identificadas, o sistema em questão é isolado do restante da rede federal; a resolução do problema fica sob responsabilidade de um dos 188 centros de respostas de incidentes do governo.

Em outra frente, Mandarino destaca o desafio de incorporar as melhores práticas de segurança a cada um dos órgãos públicos. Apesar das recomendações do GSI, muitas instituições estão atrasadas na adoção de medidas preventivas. Uma pesquisa recente realizada pelo Tribunal de Contas da União (TCU) mostra, por exemplo, que 64% dos órgãos federais não possuem sequer uma política de segurança da informação.

Para Douglas Viudez, diretor de produção e serviços da Companhia de Processamento de Dados do Estado de São Paulo (Prodesp), a existência de diversas redes que dão estrutura e interconectam diferentes órgãos aumenta os custos de manutenção e cria riscos, principalmente com relação aos usuários. "Em 80% dos problemas de segurança, é o usuário quem deixa a porta aberta para um ataque", diz.

Responsável pelo armazenamento de 70% dos dados do Governo do Estado de São Paulo, a Prodesp vem investindo na certificação de seus funcionários e na colaboração com instituições de pesquisa na área de segurança para proteger os 1,6 mil computadores que compõem seu centro de dados. Só no mês de maio, foram bloqueadas 67 milhões de tentativas de invasão às redes da companhia.

Sob esse cenário de riscos potenciais, um dos principais medos de órgãos de governo é que a recente onda de ataques a empresas, feitos pelos chamados hackers ativistas, migre para os sistemas de infraestrutura dos países.

No início de junho, a Organização do Tratado do Atlântico Norte (Otan) divulgou um relatório sobre a possível extensão desses ataques a novas fronteiras. Para a Otan, "o surgimento de ativistas hackers pode levar a uma nova classe de conflitos internacionais entre esses grupos e nações, ou mesmo a conflitos entre entidades exclusivamente virtuais".

A Otan observa que pelo que se sabe, grupos terroristas como a Al Qaeda ainda não têm a capacidade de executar ataques cibernéticos, mas que no futuro, o crime organizado e grupos de hackers podem vir a vender seus serviços a essas organizações terroristas.

Apesar de não ter um histórico de confrontos bélicos e de movimentos ativistas atuantes, vem crescendo no Brasil a preocupação com a defesa de redes ligadas à prestação de serviços públicos. Responsável por quinze empresas de geração, transmissão e distribuição de energia elétrica, a Eletrobras criou há cerca de um ano um comitê de segurança da informação para identificar e minimizar os riscos de ataques.

Uma das iniciativas do comitê foi separar a rede de tecnologia da informação – ligada à gestão administrativa da Eletrobras – da rede de automação, que controla a operação de usinas e equipamentos de transmissão. "A rede de automação tem o mínimo contato com a internet, o que reduz significativamente os riscos", diz Rodrigo Costa dos Santos, coordenador de segurança de tecnologia e comunicações da Eletrobras.

A estratégia de segregar as redes de automação e TI também vem sendo adotada pela Petrobras. "A probabilidade de uma invasão ter sucesso nesses sistemas ainda é baixa, mas já há casos no mundo que mostram que é preciso se precaver, pois o impacto seria imensurável", diz Flavio Baruzzi, gerente de segurança da informação da companhia.

Fonte: Jornal Valor Econômico