Guerra virtual bate recordes de invasões

Data: 04/07/2011
Veículo: Jornal Semanário

Uma guerra virtual vem crescendo assustadoramente. Nas duas últimas semanas de junho, invasões a sites se intensificaram. Desta vez, os alvos foram os órgãos públicos: prefeituras, presidência da República, Receita Federal, Instituto Brasileiro de Geografia e Estatística (IBGE), Câmaras de Vereadores e até o e-mail da presidente do Brasil, Dilma Rousseff, aumentaram a lista de invasões.

O grupo de hackers Fatal Error anunciou que tirou do ar 500 sites de prefeituras. E Bento está entre as cidades atacadas. A Diretora do Centro de Tecnologia e Comunicação (Cetec), Rita de Cássia dos Santos, disse que o site foi tirado do ar por prevenção e que os problemas de inoperância identificados em outros municípios podem estar relacionados aos ataques assumidos por hackers, uma vez que a estrutura do site é armazenada na Confederação Nacional dos Municípios (CNM).

Esta semana o ministro da justiça, José Eduardo Cardozo se pronunciasse quanto ao caso. Para ele, o Brasil precisa tipificar o crime de hackers para permitir à Polícia Federal e ao Poder Judiciário coibir esse tipo de ataque.

Qual será a melhor forma de se precaver contra ataques e invasões de hackers? O Semanário entrevistou a diretora do Cetec e também o professor do curso Técnico Integrado de Informática do Instituto Federal do Rio Grande do Sul (IFRS), campus de Bento, Rafael Jaques. Confira:

Jornal Semanário - Você concorda que cada vez mais estamos vulneráveis a esse tipo de ataque? Por quê?

Rafael Jaques - Na verdade, sempre estivemos vulneráveis. O que aconteceu recentemente foi a externalização de uma revolta antiga. Ataques como esses têm acontecido há anos, só que agora a mídia resolveu escancarar. Com o crescimento no número de máquinas infectadas, os invasores estão conseguindo maior poder de fogo na hora de tentar uma investida contra alguma entidade.

Outro fator de risco é o choque que há entre a busca incessante de novas tecnologias por parte dos mal intencionados e o descaso de muitos administradores em relação aos seus serviços.

Desse ponto de vista, podemos afirmar que estamos cada vez mais vulneráveis a esse tipo de ataque, pelo menos enquanto não houver uma conscientização global.

JS - Qual o melhor procedimento para se precaver contra esses ataques?

Rita de Cássia dos Santos - Para corporações, órgãos públicos e empresas em geral, o fundamental são os investimentos em infraestrutura de computadores e rede, assim como, os softwares relacionados a segurança digital. Não esquecendo da aplicação de regras e políticas de segurança, com isso, identifica-se e acompanha-se cada um dos usuários que fizerem uso das aplicações disponíveis. Dependendo dos interesses de cada empresa e de suas capacidades de investimento, é possível terceirizar a armazenagem de dados, conexões e filtros de conteúdo, mantendo os mais elevados índices de segurança.

Para nós usuários domésticos, as dicas são muitas. Manter sempre um anti-vírus instalado, jamais abrir arquivos recebidos através de e-mails desconhecidos, utilizar os filtros de anti-spam disponíveis nos serviços de e-mail, em sites bancários observar a presença do cadeado fechado no canto inferior direito do navegador, não utilizar senhas baseadas em informações pessoais ou sequenciais, modificar as senhas constantemente.

Leituras sobre estes assuntos e cursos específicos, também são indicados.

Rafael - Basicamente muito estudo e atualização. Os responsáveis por essas máquinas devem estar em constante busca de melhores maneiras de se evitar o caos. Não existe uma fórmula mágica para barrar todos os intentos malignos contra um determinado agente, apenas trabalho duro, responsabilidade e foco no que se está fazendo.

O ataque que foi usado nesses sites é conhecido como DDoS - Distributed Denial of Service (Negação de Serviço Distribuída). Essa modalidade utiliza diversas máquinas de localidades diferentes para fazerem requisições ao site incessantemente até que o mesmo se sobrecarregue e saia do ar. É praticamente impossível de se evitar um ataque desses, pois seria a mesma coisa que criar um sistema que impeça que milhares de ladrões invadam a sua casa ao mesmo tempo.

Conforme eu já havia comentado, com bastante pesquisa, estudo e dedicação ao trabalho que se está fazendo é possível minimizar os estragos causados por esses ataques, mas não evitá-los por completo.

JS - O site da prefeitura foi retirado do ar em função de ataques realizados a outras prefeituras ou por prevenção para não ser surpreendido?

Rita - O site da Prefeitura esta hospedado na Confederação Nacional dos Municípios e o domínio - wwww.bentogoncalves.rs.gov.br - é disponibilizado pela Procergs. Os dois órgãos sofreram instabilidades em seus servidores de dados, mas nenhum se pronunciou ou identificou oficialmente ataques ao site da Prefeitura de Bento. Até mesmo porque, o site ficou algum tempo sem acesso, mas retornou ao normal sem nenhum indicativo de invasão, toda sua estrutura estava preservada.

Devido aos diversos ataques, o corte de acesso aos sites ou aos domínios, poder ser sim, uma maneira de prevenir invasões.

Lembrando que os sistemas que são acessados através do site da Prefeitura, como atendimento ao cidadão, registro de preços, saúde online, entre outros, estão armazenados em servidores de dados da própria Prefeitura, com os mais rigorosos serviços de segurança digital, e nestes servidores, nenhuma instabilidade ou ataque foi identificado.