CTIR Gov

Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal - CTIR Gov

http://www.ctir.gov.br

O CTIR Gov é um órgão subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC - do Gabinete de Segurança Institucional da Presidência da República – GSIPR. O CTIR Gov tem como finalidade precípua o atendimento aos incidentes em redes de computadores pertencentes à Administração Pública Federal.

Entrevista do Coordenador Geral de Tratamento de Incidentes de Segurança do Governo Federal Brasileiro (CGTIR Gov) ao Boletim Eletrônico da Organização dos Estados Americanos - OEA

Por José Luis Tesoro

Outubro de 2010

Disponível em http://www.suboletin.com/contentsoea/docs/Boletin_58/Wallieportugues.htm

1. Quais são os principais riscos e ameaças à segurança em relação ao governo eletrônico?

Manter a segurança informacional de uma organização no ambiente computacional interconectado nos dias atuais é tarefa diária, permanente e que exige muito estudo e dedicação. Assim como nas organizações privadas, as organizações públicas sofrem constantes e diferentes formas de ataques quando disponibilizam serviços e informações para a sociedade em geral, por meio do uso intensivo das tecnologias da informação e da comunicação (governo eletrônico ou simplesmente e-gov).

Nesse contexto, observa-se que alguns fatores vêm contribuindo para o aumento da insegurança na área de e-gov:

- os lançamentos de novos produtos e serviços para a Internet, que são adotados quase que de imediato, sem a devida avaliação mínima dos requisitos de segurança;
- a facilidade na obtenção e na utilização de ferramentas de ataques, com o uso de interfaces gráficas e scripts pré fabricados para invasão e desenvolvimento de artefatos maliciosos (malwares), vem ampliando a quantidade de invasores que não precisam mais dispor de complexos e sólidos conhecimentos computacionais;
- a ampliação da capacidade de causar prejuízos dos novos malwares e das técnicas de ataque como, por exemplo, a disseminação/utilização em larga escala de redes de máquinas infectadas (Botnets);
- a disseminação de páginas falsas, muito semelhantes às originais do e-gov, induzindo o cidadão a entregar seus dados pessoais e empresariais a indivíduos não credenciados e mal intencionados; e

- a crescente utilização da Internet como ferramenta de manifestação de desagravos políticos, sociais, econômicos, religiosos etc.

2.- Poderia mencionar, de forma genérica, alguns problemas de segurança e as suas conseqüências?

Dentro de um verdadeiro universo de problemas, podemos destacar alguns fatos que facilitam a ação (por exemplo: desfiguração de sites institucionais, indisponibilidade dos serviços, redirecionamento para páginas falsas ou aceso indevido a base de dados governamentais) de indivíduos mal intencionados.

No anseio de prontamente responder aos anseios e pressões da sociedade, percebese que a velocidade de desenvolvimento das aplicações e programas voltados para a Internet não é acompanhada por medidas de segurança adequadas e robustas. Em muitos casos, em prol da rapidez na prestação ou disponibilização de algum serviço ou informações, as soluções não são exaustivamente testadas e validadas, apresentando vulnerabilidades no seu desenvolvimento, na sua implementação ou não recebendo a devida manutenção/atualização periódica de segurança.

Outro fator relevante refere-se às constantes atualizações dos conteúdos informacionais que são realizadas diretamente pelos conteudistas (normalmente não possuidores de conhecimentos técnicos em TI ou em segurança), o que implica na abertura de compartilhamentos e acessos privilegiados aos sistemas, com a conseqüente geração de vulnerabilidades.

Por último, cabe ressaltar que, apesar de já estar em prática o uso do certificado pessoal digital (CPF eletrônico) para o acesso a vários dados sensíveis (por exemplo: https://cav.receita.fazenda.gov.br/scripts/CAV/login/login.asp), a maior parte dos acessos aos serviços disponibilizados do e-gov são realizados sem a obrigatoriedade de uma identificação inequívoca por parte dos usuários (anonimato virtual).

3. Quais são as linhas de ação mais difundidas que contribuem para a segurança em relação ao governo eletrônico?

Neste aspecto gostaria de destacar o funcionamento do Grupo de Trabalho sobre Segurança (GT Segurança), componente da arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico Brasileiro (http://www.governoeletronico.gov.br/acoese-projetos/e-ping-padroes-de-

interoperabilidade).

A e-PING define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) no governo federal brasileiro, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

A arquitetura e-PING foi segmentada em cinco partes (“Interconexão”, “Segurança”, “Meios de Acesso”, ”Organização e Intercâmbio de Informações” e “Áreas de Integração para Governo Eletrônico”). Para cada um dos segmentos foi criado um grupo de trabalho específico, composto por especialistas atuantes em órgãos governamentais, responsável pela elaboração de políticas/especificações técnicas a serem adotadas pelo governo federal. Este ano, como integrante do GT Segurança, tenho observado um real desenvolvimento dos padrões de segurança de TIC, particularmente no que se refere a: ao uso seguro do Protocolo de Internet (IP), segurança no uso de Correio Eletrônico, desenvolvimento de Sistemas e serviços de Rede.

Outro destaque é a ampliação do uso de certificados digitais pelas empresas públicas e privadas. Assim sendo, com validade jurídica assegurada por Lei, as empresas podem realizar suas transações com segurança pela Internet, possibilitando que diversos documentos trafeguem por meios eletrônicos com reconhecimento legal, dispensando a conversão para papel e o reconhecimento de firma em cartórios tradicionais**.**

4. Na sua opinião, onde mais avança a segurança da informação na área de governo eletrônico?

Nesse aspecto temos duas atividades distintas, porém complementares e ligadas diretamente à segurança da informação e ao e-gov.

A primeira trata da construção de um marco civil para a Internet brasileira. Basicamente esse projeto está sendo construído com a participação de toda a sociedade (foi aberto do processo colaborativo de discussão e debates pela Internet, ver em http://culturadigital.br/marcocivil/) e, com força de Lei, organizará juridicamente a utilização da Internet no país. Em outras palavras, o atual projeto de Lei reunirá regras para determinar direitos, deveres e responsabilidades de internautas, provedores de acesso, bem como a atuação do Estado no ambiente virtual.

A segunda atividade, oriunda do governo federal, via de regra por meio do Gabinete de

Segurança Institucional da Presidência da República (GSIPR), busca regulamentar a Gestão de Segurança da Informação e Comunicações no âmbito dos órgãos e entidades da Administração Pública Federal, direta e indireta. Essa regulamentação tomou impulso a partir de 2008 e já abrange diversas áreas afetas a segurança da informação como: Elaboração de Política de Segurança, Gestão de Riscos, Tratamento e Respostas a Incidentes em Redes Computacionais, Controles de Acesso dentre outras (exemplos de algumas normas em http://dsic.planalto.gov.br/legislacaodsic/53).

5. Qual a importância da conscientização e da capacitação em segurança da informação na relação governo e cidadãos?

Permita-me embasar a resposta com dois fatos recentes do contexto virtual brasileiro:

a. Constatou-se que 93% dos pequenos e médios empreendedores do Brasil utilizam a Internet em suas atividades administrativas empresariais.

b. O Plano Nacional de Banda Larga (PNBL), lançado pelo Governo Federal em maio do corrente ano, tem por objetivo universalizar a Internet rápida no País, ou seja, levar banda larga de baixo custo e alta velocidade a mais de 4000 municípios (afastados dos principais centros urbanos), ampliando dos atuais 13,5 milhões de domicílios com Internet para 35 milhões em 2014 e atingindo quase 90% da população brasileira.

Sem dúvida, são excelentes notícias em relação a inclusão digital, mas trazem enormes desafios para a área de segurança. De forma sintética, basta inferir que grande parte desses novos entrantes no ambiente virtual e por conseqüência, potenciais utilizadores do governo eletrônico, são carentes de conhecimento no tocante ao uso seguro da Internet. Acredito que programas de conscientização, treinamentos específicos e campanhas de sensibilização, por parte do governo e das empresas provedoras de Internet, sejam ferramentas fundamentais para que esses novos usuários não se tornem potenciais vítimas de indivíduos e grupos mal intencionados.

6.- Deseja adicionar mais algum aspecto?

Gostaria de agradecer essa oportunidade de expressar algumas idéias sobre segurança da informação e concluir ratificando que, nos últimos anos, os órgãos públicos brasileiros vêm implementando e consolidando redes de computadores cada vez mais amplas, como exigência para suportar o fluxo e a demanda crescente de informações. O objetivo é permitir que seus

colaboradores e a sociedade acessem os serviços disponibilizados por meio da rede mundial de computadores de forma a desempenharem suas funções e satisfazerem suas necessidades como cidadãos.

Como já foi declarado por várias autoridades brasileiras, acredito que promover a cidadania, por meio de uma vasta gama de serviços, orientações e informações relevantes ao cidadão como pode ser verificado no portal http://www.e.gov.br/ , seja o principal foco do governo eletrônico.

Entretanto, com olhar mais técnico e crítico, percebe-se que o e-gov tornou-se também, sinônimo de modelo de competência e de governança estatal, inclusive com relatórios de entidades internacionais, classificando os países de acordo com os serviços de e-gov oferecidos aos seus cidadãos. Tal fato, de certa forma, pressiona os administradores públicos a acelerarem demasiadamente a acessibilidade dos serviços à população, em detrimento da complexidade da máquina pública e de especificidades técnicas de segurança. Em conseqüência, por vezes e infelizmente, verifica-se na área de governo eletrônico o comprometimento de alguns pilares básicos da segurança da Informação: disponibilidade, confidencialidade, autenticidade e integridade da informação.

***