CTIR Gov

Centro de Tratamiento de Incidentes de Seguridad en Redes de Computadores de la Adminstración Pública Federal

http://www.ctir.gov.br

El CTIR Gov, subordinado al Departamento de Seccuridad de Información y Comunicaciones del Gabinete de Seguridad Institucional de la Presidencia de la República, tiene como finalidad principal el atendimiento a los incidentes en redes de computadores que pertenecen a la Adminstración Pública Federal (APF).

Entrevista con el Responsable por el Tratamiento de Incidentes de Seguridad en Redes de Computadores del Gobierno Federal de Brasil (CGTIR Gov)

Por José Luis Tesoro

Octubre 2010

Disponible en http://www.suboletin.com/contentsoea/docs/Boletin_58/Principal58.htm

1.- ¿Cuáles son los principales riesgos y amenazas para la seguridad en el ámbito del Gobierno Electrónico?

El preservar la seguridad de la información en organizaciones insertas en ambientes interconectados implica hoy una tarea cotidiana y permanente que exige gran estudio, análisis y dedicación. Tanto las organizaciones públicas como las privadas padecen constantes y diferentes formas de ataques cuando ponen servicios e informaciones a disposición de la sociedad a través del uso intensivo de las TIC.

En ese contexto, pueden verificarse algunos factores que contribuyen a acrecentar la inseguridad en el ámbito del e-Gobierno.

- lanzamiento de nuevos productos y servicios para Internet que son adoptados casi inmediatamente sin la debida evaluación mínima de los requisitos de seguridad;
- facilidad para obtener y utilizar herramientas de ataque, con uso de interfaces gráficas y scripts prefabricados para invasión y desarrollo de "artefactos" de software malicioso (*malwares*), lo que resulta en un significativo aumento de la cantidad de invasores que no necesitan ya siquiera disponer de conocimientos computacionales avanzados;
- ampliación y potenciación de la capacidad de causar perjuicios de los nuevos *malwares* y de las técnicas de ataque, por ejemplo la diseminación/utilización en gran escala de redes de máquinas infectadas (*botnets*);
- diseminación de páginas falsas, muy semejantes a las originales de e-Gobierno, induciendo al ciudadano a entregar sus datos personales y empresariales a individuos no acreditados y malintencionados; y

- creciente utilización de Internet como herramienta de manifestación de reclamos y desagravios políticos, sociales, económicos, religiosos etc;

2.- ¿Podría hacer una referencia genérica a algunos casos de problemas de seguridad y sus consecuencias?

Dentro de un verdadero universo de problemas, podemos destacar algunos hechos que facilitan la acción de individuos malintencionados; por ejemplo: desfiguración de sitios web institucionales, indisponibilidad de servicios, re-direccionamiento hacia páginas falsas o acceso indebido a bases de datos gubernamentales.

Cabe señalar que, debido a las ansias por responder prontamente a las presiones de la sociedad y alinearse al contexto internacional, la velocidad de desarrollo de las aplicaciones y programas para Internet no es acompañada comúnmente por medidas de seguridad adecuadas y robustas. En muchos casos, la presión por implementar rápidamente la prestación de un servicio o de determinada información no permite probar ni validar exhaustivamente las soluciones, las cuales exhiben frecuentemente vulnerabilidades en su desarrollo e implementación, así como un deficiente mantenimiento y actualización en términos de seguridad.

Otro factor relevante se asocia a la constante actualización de los contenidos informativos directamente por parte de los *contenidistas,* lo que implica habilitar compartimentos y accesos privilegiados a los sistemas a personas que normalmente carecen de conocimientos técnicos de TIC y de seguridad, con la consecuente generación de vulnerabilidades.

Por último, cabe resaltar que, aun cuando es ya es una práctica habitual el uso del certificado personal digital (CPD electrónico) para acceder a ciertos datos sensibles (por ejemplo: https://cav.receita.fazenda.gov.br/scripts/CAV/login/login.asp), en la actualidad cualquier usuario puede acceder a la mayor parte de los servicios de e-Gobierno sin necesidad de identificación inequívoca (anonimato virtual).

3.- ¿Cuáles son las líneas de acción más difundidas para contribuir a la seguridad en el ámbito del Gobierno Electrónico?

En este aspecto deseo destacar la puesta en marcha del Grupo de Trabajo sobre Seguridad (GT Seguridad), como componente de la arquitectura e-PING (Patrones de Interoperabilidad de

Gobierno Electrónico Brasileño). La arquitectura e-PING define un conjunto mínimo de premisas, políticas y especificaciones técnicas que regulan la utilización de las TIC en el Gobierno Federal Brasileño, estableciendo las condiciones de interacción con los demás Poderes y esferas de gobierno y con la sociedad en general.

Con la finalidad de organizar la definición de los patrones, la arquitectura e-PING fue segmentada en cinco componentes ("Interconexión", "Seguridad", "Medios de Acceso", "Organización e Intercambio de Información" y "Áreas de Integración para e-Gobierno"), creándose para cada uno un grupo de trabajo específico compuesto por técnicos actuantes en órganos del gobierno federal. Esos especialistas en cada asunto son responsables por la elaboración de políticas y especificaciones técnicas para ser adoptadas por el gobierno federal. Como integrante del GT Seguridad, estoy observando, durante este año, un real desarrollo de los patrones de seguridad de TIC, particularmente en lo relativo a:

- Seguridad de IP.
- Seguridad de Correo Electrónico.
- Desarrollo de Sistemas.
- Servicios de Red.

Cabe destacar también la ampliación del uso de certificados digitales como un documento electrónico por parte de las empresas (personas jurídicas). Con dicha constancia digital -cuya validez jurídica está sustentada por Ley- las empresas pueden realizar sus transacciones por Internet con plena seguridad, canalizando por vía electrónica diversos documentos con reconocimiento legal y reconocimiento de firma, sin necesidad de convertirlos a soporte papel.

4.- ¿Hacia dónde avanza en Brasil la Seguridad de la Información en el ámbito del Gobierno Electrónico?

En ese aspecto tenemos dos actividades distintas pero complementarias y asociadas directamente a la seguridad de la información y al e-Gobierno.

La primera es la construcción de un "Marco civil de Internet" en Brasil. Básicamente ese proyecto se está construyendo con la participación de toda ello se abrió un proceso colaborativo de discusión y debates por Internet (ver http://culturadigital.br/marcocivil/) y se organizará

jurídicamente –con fuerza de ley- la utilización de la Internet en el país. El proyecto de ley resultante del proceso reunirá reglas para determinar derechos, deberes y responsabilidades de internautas, proveedores de acceso, así como la actuación del Estado en el ambiente virtual.

La segunda actividad, originada en el gobierno federal, a través del Gabinete de Seguridad Institucional de la Presidencia de la República (GSIPR), se dirige a regular la Gestión de Seguridad de la Información y Comunicaciones en el ámbito de los órganos y entidades de , directa e indirecta. Esta reglamentación tomó impulso a partir de 2008 y ya abarca diversas áreas vinculadas a la seguridad de la información; por ejemplo: Elaboración de Políticas de Seguridad, Gestión de Riesgos, Tratamiento y Respuesta a Incidentes en Redes de Computación, Controles de Acceso, entre otras.

5.- ¿Cuán importante es la concienciación y la capacitación en materia de Seguridad de la Información en los gobiernos y en su relación con los ciudadanos?

Permíteme basar mi respuesta en dos hechos recientes del contexto brasileño:

a. En relación a los pequeños y medianos emprendedores de Brasil, se constató que el 93% utilizan Internet, lo que muestra una elevada inclusión digital por parte de las pequeñas empresas.

b. El Plan Nacional de Banda Ancha (PNBL), lanzado por el Gobierno Federal en mayo del corriente año, tiene por objetivo universalizar en el país el acceso a la Internet de banda ancha -de bajo coste y alta velocidad- llevándola a 4.278 municipios, aumentando el número de domicilios con Internet desde los actuales 13,5 millones a 35 millones en 2014, lo que implica alcanzar prácticamente al 90% de la población brasileña.

Estas excelentes noticias implican enormes desafíos para el área de seguridad. Sintéticamente, basta inferir que gran parte de esos nuevos ingresantes al ambiente virtual y -como consecuencia- potenciales usuarios del e-Gobierno, carecen de conocimiento sobre el uso seguro de que los programas de concienciación, entrenamientos específicos y campañas de sensibilización, por parte del gobierno y de las empresas proveedoras de Internet, serán herramientas fundamentales para que esos nuevos usuarios no se constituyan en potenciales víctimas de individuos y grupos malintencionados.

6.- ¿Desea agregar algún aspecto adicional?

Deseo agradecer esta oportunidad de expresar algunas idas sobre seguridad de la información y concluir ratificando que, en los últimos años, los órganos públicos vienen implementando y consolidando redes locales cada vez más amplias de computadores, como exigencia para sustentar el flujo creciente de informaciones, así como para que sus colaboradores y la sociedad accedan a los servicios disponibles por Internet para desempeñar sus funciones y para satisfacer sus necesidades como ciudadanos.

Creo, como ya fue declarado por varias autoridades brasileñas, que el principal foco del e-Gobierno debe ser promover la ciudadanía mediante una vasta gama de servicios, orientaciones e informaciones relevantes para el ciudadano, como puede verificarse en el portal http://www.e.gov.br/.

Sin embargo, con una mirada más técnica y crítica, puede percibirse también que el e-Gobierno se ha constituido en sinónimo de modelo de competencia y de gobernanza estatal, incluso con informes de entidades internacionales en los que se clasifica y califica a los países de acuerdo con los servicios de e-Gobierno ofrecidos a sus ciudadanos. Estos hechos, en cierta forma, presionan a los administradores públicos para acelerar excesivamente la accesibilidad de servicios a la población, en detrimento de la complejidad de la maquinaria pública y de las especificidades técnicas de seguridad. En consecuencia, a veces se verifica –lamentablemente- en el área de e-Gobierno cierto descuido de algunos pilares básicos de la seguridad de la información: disponibilidad, confidencialidad, autenticidad e integridad de la información.

***