Ciberseguridad Nacional Argentina: Cracking de Servidores de la Administración Pública

Cristian Borghello[1], Marcelo Temperini[2]

Abstract. Ataques de *Hacking*, *Cracking* y Denegación de Servicio Distribuido (DDoS) son algunos de los delitos informáticos que se cometen a diario en Argentina. Sin embargo, revisten mayor relevancia cuando los objetivos de ataque son sistemas gubernamentales (".GOB.AR"). El presente artículo pretende demostrar, apoyado sobre el análisis de casos de estudio reales, un resumen de las técnicas de intrusión más comunes utilizadas en los últimos años para atacar a los sistemas gubernamentales argentinos, desarrollando sus características y motivaciones. Desde la óptica jurídica, se destacan los diferentes marcos normativos existentes en el ámbito de la seguridad de la información, así como la responsabilidad civil y penal aplicable para los casos de estudio. A modo de conclusión, se brindan una serie de criterios a considerarse por parte del ámbito público, tendientes a mejorar a nivel global la gestión de la seguridad de la información en los organismos gubernamentales.

Abstract. Hacking, Cracking and Distributed Denial of Service (DDoS) are some of the computer crimes committed daily in Argentina. However, they have greater relevance when the targets are systems of the national or local government (".GOB.AR"). This article seeks to demonstrate, resting on the analysis of real case studies, a summary of the most common intrusion techniques used in recent years to attack the Argentinian government systems, developing their characteristics and motivations. From a legal viewpoint, highlights the different regulatory framework in the field of information security, as well as civil and criminal liability applicable to the case studies. In conclusion, there are a few points to be considered by the public admnistration, aimed at improving global security management of information in the government agencies.

Keywords: delitos informáticos, cracking, hacking, cibercrimen, cybercrime, ciberseguridad nacional, argentina,

[1] Licenciado (UTN) en Sistemas y certificado internacional en seguridad de la información. Creador y Director de los sitios Segu-Info –www.segu-info.com.ar– y Segu-Kids –www.segu-kids.org– especializados en Seguridad de la Información Seguridad para la familia. Contacto: cborghello@segu-info.com.ar

[2] Abogado (UNL). Doctorando CONICET con especialización en Delitos Informáticos. Co-director de la Red Elderechoinformatico.com. Analista de Seguridad y Socio Fundador de AsegurarTe – Consultora en Seguridad de la Información. Contacto: mtemperini@asegurarte.com.ar

Introducción

La evolución de las tecnologías de la información brinda herramientas de probada utilidad para mejorar las relaciones interpersonales. Entre dichas relaciones favorecidas, se encuentran aquellas que vinculan a los gobiernos con sus administrados (G2C/*Government to Citizens*) [1]. Los canales de comunicación para el desarrollo y crecimiento de este tipo de relaciones son los portales o sitios gubernamentales, tanto dentro del ámbito municipal, como provincial y nacional, desde los cuales se ofrece a los ciudadanos un nuevo abanico de vínculos con sus respectivos gobiernos, a través de internet. Desde la posibilidad de realizar trámites y consultas online, hasta la de radicar denuncias, consultar el programa cultural o incluso hasta pagar impuestos de manera electrónica.

La situación se vuelve más compleja con el tiempo, puesto que en esta corriente de digitalización de los servicios públicos, no sólo encontraremos los portales oficiales del municipio, provincia o del propio Estado Nacional, sino que además existen una importante cantidad de portales que soportan otros servicios estatales de diferentes dependencias. Motivados en mejorar la publicidad de sus acciones, así como en obtener cierta independencia tecnológica en la disposición y prestación de contenidos y servicios, la cantidad de sitios gubernamentales se ha multiplicado de manera descontrolada, facilitado por la sencillez en los trámites gratuitos de registros de dominios ".GOB.AR" en la Dirección Nacional de Registros de Dominios de Internet[3]. Ese crecimiento desorganizado y carente de controles, es fuente de una estructura de sistemas y datos de marcada complejidad, fomentando el cruzamiento y transferencia de datos constantes entre diferentes dependencias, perjudicando así los niveles de seguridad de la información. Son estos bajos niveles de seguridad, los que permiten que delincuentes de todas partes del mundo accedan, modifiquen y agreguen información en los servidores gubernamentales, incluso poniendo en peligro la protección de los datos personales de una buena parte de la población, como se demostrará en la presente investigación.

Casos de estudio

Una vulnerabilidad es definida como una debilidad que puede proveer al atacante de un acceso no autorizado a un determinado lugar, red, datos, etc. [2]. También puede caracterizarse por la ausencia de una contramedida lo cual, en última instancia, permite el mismo acceso no autorizado. Simplificando, se puede decir que una puerta con la cerradura rota es una vulnerabilidad pero también puede considerarse como tal, el hecho de no destinar un guardia a dicha puerta para cuidarla mientras se repara la cerradura.

[3] NIC.ar es el administrador de los nombres de dominio bajo el código país (ccTLD) .ar, dependiente del Ministerio de Relaciones Exteriores, Comercio Internacional y Culto de la República Argentina. Administra dominios .com.ar, .org.ar, .net.ar, .tur.ar, entre otros. www.nic.ar

La República Argentina tiene un largo historial de ataques a sus sitios web aunque no en la medida de otros países como Rusia, Estonia, Georgia, China o Estados Unidos, los cuáles ya se ven involucrados incluso en algunas de las llamadas "ciberguerras"[4], reflejo de sus enemistades políticas [3].

A continuación se hace un recorrido por los principales tipos de ataques producidos en nuestro país, referenciados a incidentes ya producidos en los últimos años, acompañados de breve desarrollo de sus formas de ataque, consecuencias y motivaciones.

1.1 Caso 1: Modificación de sitios y/o base de datos

Quizás uno de los casos más conocidos y resonantes fue la modificación de un discurso del entonces presidente de la nación Néstor Kirchner en marzo de 2005 [4]. Cada discurso se publica en el sitio oficial de la Presidencia de la Nación y lo que se hizo en esa ocasión fue cambiar partes del mismo por frases soeces. Al momento de la presente investigación, la última modificación al sitio oficial de la Presidencia de la Nación, fue el 11 de diciembre de 2011 [5].

Otro de los casos más difundidos se produjo en junio de 2009 cuando, en plenas elecciones legislativas, se ingresó a la base de datos del padrón electoral [6] y se agregaron leyendas ofensivas sobre algunas provincias. El sitio fue corregido pero, luego de que las primeras leyendas fueran suprimidas, volvieron a ingresar al sitio, perteneciente al Poder Judicial de la Nación, para escribir: *"aumenten la seguridad"* [7].

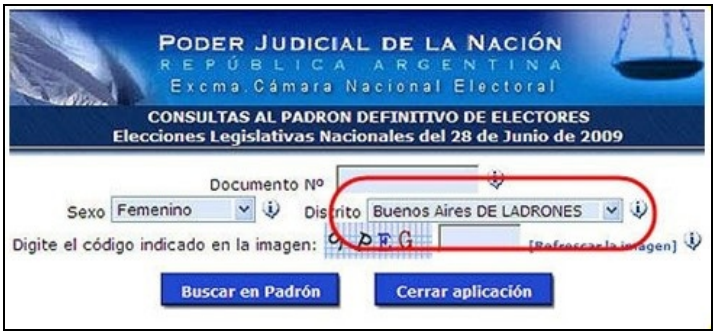

Figura 1 - Ataque el sitio del padrón electoral de Argentina (26/06/2009)

Incidente de aún mayor relevancia (en consideración de sus posibles consecuencias) sucedió con los datos de todos los contribuyentes[5] argentinos a través del sitio web de la Administración Federal de Ingresos Públicos (AFIP) en el año 2010 [8]. Puntualmente, a través de un fallo en la validación de datos, los delincuentes podían acceder al documento nacional de identidad (DNI) escaneado, huella digital, fotografía y firma holográfica de cualquier contribuyente de la República Argentina.

[4] Se refiere a un conflicto bélico que tiene el ciberespacio como escenario.

[5] De acuerdo a la gacetilla oficial de AFIP, más de 7 millones de contribuyentes existen en el sistema, http://www.afip.gob.ar/novedades/docsComunicados/RegistroTributario.htm

1.2 Caso 2: Defacing

En otra categoría de ataques, uno de los más conocidos mediáticamente es el "*defacement*". Este ataque consiste en vulnerar un servidor web a través de distintas técnicas y modificar una o más páginas de los sitios web allí alojados. Generalmente la página modificada corresponde a la primera que visualiza el usuario al ingresar al sitio vulnerado (*"index.xxx"*) y de esta manera se logra una rápida publicidad sobre el éxito del ataque. Esta técnica es observada en aquellos grupos que buscan enviar mensajes de protestas políticas, religiosas o institucionales, siendo los casos más conocidos y recientes, los del colectivo "Anonymous". En determinados casos, simplemente se realizan *defacement* para utilizarlos como trofeo útil para exponer y ganar reconocimiento del propio grupo, que es contextualizado en el sistema de meritocracia que existe entre ellos.

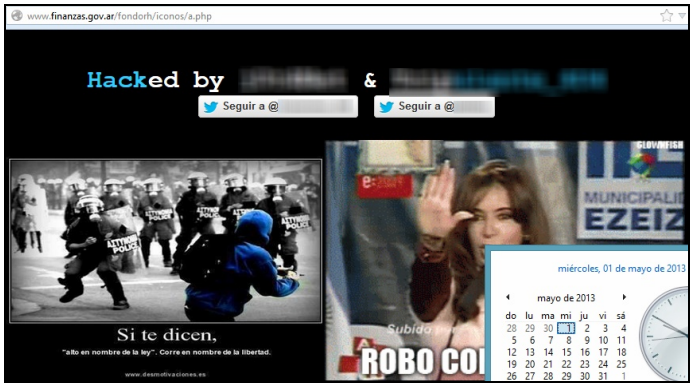

Figura 2 - Ataque Defacing el sitio del Ministerio de Economía, Infraestructura y Servicios Públicos de Salta (02/05/2013)

Según Zone-H[6], en los últimos 5 años ha habido 2.791 ataques de *deface* a sitios gubernamentales argentinos denunciados, pero se debe tener en cuenta que gran parte de los mismos nunca se denuncia, por lo que dicho número sólo debe ser tomado como un índice de referencia, **en relación a la verdadera cifra negra de los delitos informáticos.** Buscando no exceder en los ejemplos y a los fines de la brevedad, a continuación se detallan sucintamente otros casos de relevancia dentro de esta categoría:

- 30/04/2013 - Ministerio de Economía, Infraestructura y Servicios Públicos de la provincia de Salta **(imagen 2)**. El ataque fue realizado el 30 de abril de 2013 y no fue solucionado durante varios días.
- 31/03/2013 - Ministerio de la Producción de la Provincia de Santa Cruz: http://zone-h.com/mirror/id/19571943. Este sitio todavía permanece modificado al momento de desarrollar el presente (40 días después de ocurrido el hecho).
- 07/01/2013 - Ministerio de Relaciones Exteriores y Culto (realizado a sus más de 50 subdominios): http://zone-h.com/mirror/id/18899507

[6] Sitio especializado en *Defacement* en donde cada persona o grupo que realiza un ataque a un sitio web, lo reporta allí, lo que permite llevar un ranking de ataques. http://zone-h.com

- 24/11/2012 - Secretaría de Ambiente y Apoyo Sustentable de la Nación: http://zone-h.com/mirror/id/18641900

1.3 Caso 3: Black Hat SEO[7] y Watering Hole Attack[8]

Estas técnicas, ampliamente utilizadas, están orientadas a motivos económicos y buscan posicionar en las primeros lugares de un buscador cientos o miles de sitios mediante el uso de distintas técnicas. Las técnicas consisten en incluir un código especial (*Javascript*) dentro de los sitios vulnerados para lograr que, sin importar la búsqueda que realice el usuario, lo lleve a uno de estos sitios, en donde se podría resultar infectado con malware o se podrían ofrecer productos generalmente falsos o adulterados. Los servidores gubernamentales (junto a los universitarios) son muy buscados para la inserción de estos códigos porque se intenta aprovechar su reputación positiva en los buscadores: el común de las personas confía en que si el enlace es provisto por un sitio del gobierno, entonces debería ser oficial y real.

Una de las maneras de comprobar rápidamente los sitios vulnerados, es a través de la utilización de buscadores (Google, Bing, etc.), restringiendo los resultados a sitios gubernamentales (.GOB.AR) y buscando[9] por ejemplo ciertas drogas o productos (falsos):

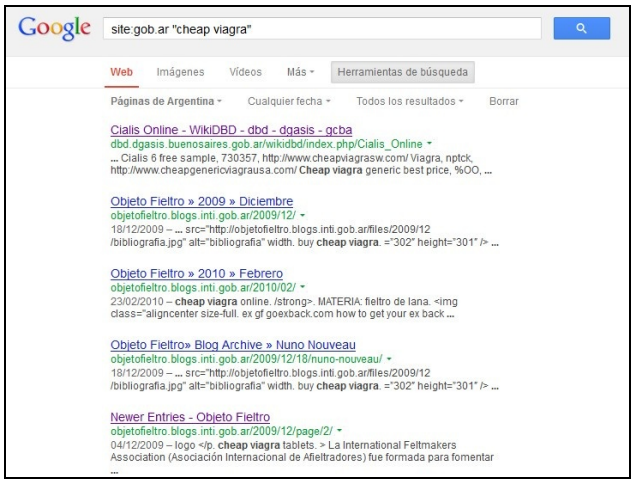

Figura 3 - Búsqueda de Viagra en sitios gubernamentales argentinos (30/04/2013)

A través de este tipo de búsquedas, cualquier atacante podrá acceder a un listado de sitios ya vulnerados por otros, lo cual facilitará la entrada para poder incluir en ellos la promoción de sus productos. Cuanto mayor sea la cantidad de sitios con este tipo

[7] *Black Hat SEO:* técnica no legal para posicionar un sitio web en los buscadores.

[8] *Watering Hole Attack:* el atacante busca infectar o engañar a un grupo en particular (organización, empresa, etc.) e inserta un código dañino en un sitio muy visitado por ese grupo.

[9] La búsqueda se realiza en inglés porque en estos casos los delincuentes son por lo general, extranjeros y, además, de esta manera, se excluyen artículos científicos y oficiales sobre los productos buscados. Las búsquedas GOV.AR y GOB.AR arrojan resultados distintos.

de códigos insertados, mayor es la publicidad y por lo tanto, más rentable se vuelve el negocio, donde la cantidad de *clicks* es directamente proporcional a las ganancias obtenidas.

En la siguiente imagen se puede ver el código fuente del sitio web del Ministerio de Educación vulnerado y cómo se realiza la redirección a la compra de productos farmacéuticos:

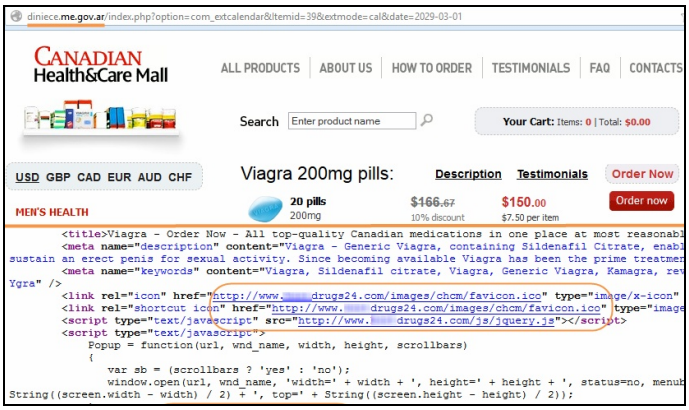

Figura 4 - Ministerio de Educación modificado para alojar publicidad de Viagra (21/04/2013)

Similar ataque existe[10] en varias páginas de un blog oficial del INTI (Instituto Nacional de Tecnología Industrial), donde incluso se ha dejado un hipervínculo expreso de *"buy viagra"* debajo del título de una serie de artículos científicos oficiales de dicho instituto, vínculo que redirige a sitios que permiten comprar viagra.

Figura 5 - INTI (Instituto Nacional de Tecnología Industrial) modificado para alojar publicidad de Viagra (28/04/2013)

[10] A fecha 03/05/2013 aún continúan en línea.

1.4 Caso 4: Denegación de Servicios Distribuidos

Los ataques de Denegación de Servicio Distribuidos (DDoS) [09] son aquellos que mediante la conexión de varios cientos o miles de dispositivos a un mismo recurso, se logra que el mismo salga de servicio o deje de estar disponible.

Durante la realización de la presente investigación, más precisamente en el día 13 de Abril de 2013, desde el grupo Anonymous se llevó adelante una protesta denominada *"OpFuckGobierno"*, en la cuál en menos de 24 hs se atacaron más de 100 sitios del Gobierno Argentino [10], dejando a la mayoría de ellos fuera de servicio, y algunos siendo también víctimas de *cracking* a través del defacement de las mismas.

Cuando un sitio es atacado inmediatamente puede apreciarse que el mismo deja de estar disponible para el resto de los usuarios. A continuación se muestran dos sitios bajo ataque:

Figura 6 - Sitios gubernamentales caídos ante ataques DDoS (13/04/2013)

Debe tenerse en consideración que estos resultados son sólo parte de la realidad ya que la mayoría de las intrusiones producidas no son reportadas y, por lo tanto pasan desapercibidas, sobre todo si persiguen objetivos económicos, dado que su anonimato favorece el hecho de que puedan permanecer en línea más tiempo y se pueden lograr mayores ingresos. Dicha explicación es útil para señalar uno de los grandes inconvenientes que tienen los delitos informáticos, en referencia a que la cantidad real de casos ocurridos en Argentina, es desconocida. Es decir, en esta clase de delitos existe una gran brecha entre la información real sobre la cantidad de casos, y aquella que realmente ha sido reportada por las víctimas, generando una cifra negra del cibercrimen muy importante.

1.5 Otras técnicas

También se aprovechan debilidades en las aplicaciones publicadas en los sitios web como causa de desarrollos que carecen de pruebas de seguridad y de calidad mínimas, que serían capaces de detectarlas y corregirlas a tiempo. Por ejemplo, en el

caso de la figura 1, se utilizó una vulnerabilidad de *SQL Injection*[11] para modificar la base de datos donde se alojan las provincias de la República Argentina.

Otra técnica que vale la pena mencionar es la modificación de un sitio web para agregar miles de enlaces al mismo sitio dañino (*Hiding Text*[12], *Spamming Keywords*[13] y *Keyword Stuffing*[14]), con el objetivo de "engañar" a los buscadores que, al "ver" este sitio enlazado muchas veces, pueden interpretar que el mismo es popular y por lo tanto mostrarlo en las primeras posiciones. Ejemplo de este tipo de ataque puede ser actualmente observado en varias páginas de sitios oficiales de Gobierno de la Ciudad de Buenos Aires.

Figura 7 - Publicidad oculta de Viagra en sitio de Buenos Aires (28/04/2013)

Resumiendo, las técnicas utilizadas para vulnerar cualquier tipo de sitio van desde el simple acceso indebido (*hacking*) a través de usuarios y contraseñas débiles hasta la utilización de intrusiones avanzadas, como la inyección de códigos maliciosos[15] que explotan vulnerabilidades en los sistemas utilizados.

Hasta el momento se ha visto un importante abanico de casos que muestran los diferentes tipos de ataques que sufren las infraestructuras de sistemas del gobierno argentino. Las consecuencias de dichos ataques, dependerá de varios factores, como el nivel de difusión del incidente, la popularidad del organismo o la magnitud del propio ataque. No obstante, es posible determinar sintéticamente las consecuencias más comunes:

- Daño a la imagen de la organización gubernamental afectada.

[11] *SQL Injection:* ataque que consiste en aprovecharse de una vulnerabilidad en una aplicación (un sitio web) para acceder o modificar una base de datos de la entidad atacada.

[12] Texto oculto: colocar palabras claves y enlaces en una página web, con el mismo color de fondo o dentro del código fuente, de modo que pasen desapercibidas para el usuario, pero no para el buscador.

[13] *Spamming Keywords:* técnica que implica formar frases con palabras claves (*keywords*) muy utilizadas, buscando mayor popularidad en la difusión.

[14] *Keyword Stuffing:* técnica que busca abusar de ciertas palabras claves dentro del contenido para hacerlas más populares, incluso no teniendo ningún tipo de relación con el contenido real del sitio o artículo.

[15] Por ejemplo a través de *Cross Site Scripting (XSS)*, que consiste en embeber código HTML peligroso en sitios que lo permitan; incluyendo así etiquetas como <*script*> o <*iframe*>.

- Acceso indebido o modificación de los datos personales de los ciudadanos.
- Posible afectación de los recursos del usuario, simplemente por acceder a códigos maliciosos alojados en los sitios oficiales.
- Afectación a los derechos a la protección de los datos personales de los ciudadanos (casos de accesos a bases de datos).

Seguridad de la Información en las Administración Pública

En septiembre de 2003, la ONTI (Oficina Nacional de Tecnologías de Información) [11] convocó a especialistas en seguridad informática de diversos organismos públicos[16], con el fin de conocer sus opiniones respecto a la necesidad de contar con una estrategia de seguridad de la información para el Sector Público Nacional.

En dicha reunión se convino como primer paso propiciar el dictado de políticas y procedimientos de seguridad por parte de cada organismo que compone el Sector Público Nacional, para lo cual se conformó un grupo de trabajo con el objeto de formular un "Modelo de Política de Seguridad de la Información" que sirviera de base para la elaboración de las políticas correspondientes a cada organismo [12].

A fin de propiciar la adopción de dicho modelo, el día 22 de Diciembre de 2004 se publicó en el Boletín Oficial la Decisión Administrativa 669/2004 (DA), la cuál establece en su artículo 1° que "los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias, deberán dictar o bien adecuar sus políticas de seguridad de la información a la Política de Seguridad Modelo, dentro del plazo de CIENTO OCHENTA (180) días de aprobada ésta última".

Respecto a la implementación de la política, la citada norma establece que las máximas autoridades de los organismos mencionados deberán conformar en sus ámbitos un Comité de Seguridad de la Información, que tendrá entre sus funciones, la de revisar y proponer a la máxima autoridad del organismo para su aprobación, la Política y las responsabilidades generales en materia de seguridad de la información. Asimismo, se establece que se deberán asignar las funciones relativas a la seguridad de sus sistemas de información a un funcionario de su planta, lo cual en modo alguno deberá implicar erogaciones presupuestarias adicionales.

Datos personales bajo ataque

Más allá del daño a la imagen institucional que pueda sufrir el organismo gubernamental atacado, es de hacer notar que en aquellos casos donde exista un **acceso indebido a bases de datos personales**, las consecuencias tienden a ser bastante gravosas, en términos de seguridad de la información. Referenciando a casos concretos que sirvan de ejemplo, se cita el Caso de Estudio Nro. 2, donde queda en

[16] AFIP, SIGEN, ANSeS, DNPDP, AGN, entre otras.

evidencia que los delincuentes han podido acceder, apoderarse de dichas bases de datos personales, e incluso hasta modificarlas, vulnerando así derechos personalísimos de ciudadanos argentinos, como lo son el derecho a la privacidad y el honor, justamente aquellos bienes jurídicos que se pretenden tutelar a través de la Ley de Protección de Datos Personales Nro. 25.326[17]. Además, como más adelante se detallará, dichas acciones en la actualidad constituyen un delito en nuestro país.

Para llevar a cabo muchos de los trámites que realiazan los ciudadanos en los portales, desde tomar una denuncia, un newsletter cultural, hasta la posibilidad de pagar deudas, es necesario almacenar y consultar distintos tipos de bases de datos personales en los sistemas. En consecuencia, los organismos que administran dichos sitios están sujetos a las obligaciones dispuestas a través de la Ley de Protección de Datos Personales Nro. 25.326.

Entre distintas exigencias derivadas de la citada norma, se destaca la existencia del deber de seguridad de los datos, expresamente estipulada en el art. 9[18]. Este deber es traducido a partir de la obligación de adoptar las medidas reguladas por la Dirección Nacional de Protección de Datos Personales, a través de la Disposición 11/2006, [13] donde se definen tres niveles de Seguridad, de acuerdo a la **clasificación de los datos personales y quién es el sujeto obligado. Las medidas serán entonces de nivel básico, medio o crítico.**

De esta manera, todo sistema donde se realice tratamiento de datos personales, deberá cumplir con el nivel básico, debiéndose adoptar las medidas de seguridad que como mínimo incluya:

1. Funciones y obligaciones del personal.

2. Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.

3. Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes.

4. Registros de incidentes de seguridad.

    4.1. Notificación, gestión y respuesta ante los incidentes de seguridad.

5. Procedimientos para efectuar las copias de respaldo y de recuperación de datos.

6. Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso.

7. Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información. La relación entre el usuario autorizado y el/los sistemas de información a los que puede acceder debe mantenerse actualizada. En el caso en que el mecanismo de autenticación utilice contraseña, la misma será asignada por el responsable de seguridad de acuerdo a

[17] Art. 1: La presente ley tiene por objeto la protección integral de los datos personales […] para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.

[18] Art 9º - (Seguridad de los datos) El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar desviaciones, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

un procedimiento que garantice su confidencialidad. Este procedimiento deberá prever el cambio periódico de la contraseña (lapso máximo de vigencia) las que deberán estar almacenadas en forma ininteligible.

8. Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados.

9. Adoptar medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal. Entre otras:

Instalar y actualizar, con la periodicidad pertinente, software de detección y reparación de virus, ejecutándolo rutinariamente;

Verificar, antes de su uso, la inexistencia de virus en archivos recibidos a través de la web, correo electrónico y otros cuyos orígenes sean inciertos.

10. Procedimiento que garantice una adecuada Gestión de los Soportes que contengan datos de carácter personal (identificación del tipo de información que contienen, almacenamiento en lugares de acceso restringidos, inventarios, autorización para su salida fuera del local en que están ubicados, destrucción de la información en desuso, etc.).

Sin embargo, para los casos enunciados en el presente artículo, al tratarse de sistemas administrados por Organismos Públicos, de acuerdo a la Disposición 11/2006 y Disposición 7/2008 deberán siempre cumplimentar como mínimo con el nivel de seguridad medio, de manera que además de cumplir con todos los requisitos del nivel básico, deberán adoptarse otros 7 puntos extras, determinados en el citado Anexo, al cual se remite en honor a la brevedad. Debe además considerarse que es posible que los datos personales tratados por el Estado sean aquellos considerados como sensibles[19] por nuestro sistema jurídico. Si ello fuera así, se deberá cumplir con el nivel más alto de seguridad, el nivel crítico, adoptándose algunas otras medidas extras que aseguren aún más los derechos de los titulares.

En conclusión, todo organismo gubernamental que desee generar un espacio virtual para relacionarse con sus ciudadanos, y que para ello necesite de alguna manera realizar el tratamiento de datos personales, automáticamente se encuentra obligado a las disposiciones normativas anteriormente citadas.

Ataques y Delitos Informáticos

En esta última etapa, se analiza brevemente el marco normativo vigente en la República Argentina en materia de delitos informáticos, a fin de determinar si los casos de estudio descriptos en la presente investigación, pueden ser penalmente sancionados.

La Ley 26.388 de Junio de 2008 sobre Delitos Informáticos [14], modificó el Código Penal Argentino (CPA) incorporando una serie de delitos informáticos. Entre ellos, se encuentra el nuevo art. 153 bis[20], conocido como el delito de *hacking*[21]. Es

19 Son aquellos datos personales que revelen origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual

20 Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

decir, existe sanción penal para el caso del mero acceso no autorizado a cualquier dato o sistema de acceso restringido.

Los legisladores argentinos han optado por condicionar la tipificación de la acción al hecho de que los sistemas o datos, sean de acceso restringido. Sin extendernos en un desarrollo que merece, se esboza que los sistemas deben reunir un mínimo de condiciones de seguridad, para que el mismo pueda alcanzar el estatus de "sistema o dato de acceso restringido". Encontramos entonces aquí otro fundamento más para adoptar las medidas necesarias para proteger los sistemas de información gubernamentales.

En el caso de que el sistema accedido sin contar con legítimas credenciales para ello, contenga bases de datos personales, la pena es agravada, al perfeccionarse el delito tipificado por el art. 157 bis inc. 1[22].

Continuando con su análisis, para el caso que no sólo se haya accedido sin autorización al sistema o dato, sino que además se haya modificado, alterado o suprimido cualquier dato de ese sistema, existe un tipo penal más grave en cuanto a su pena, quedando tipificado bajo la figura del *cracking*[23]. De los casos de estudio analizados ut supra podemos afirmar que en las tres primeras categorías, existen casos de *cracking*, toda vez que en ambos además del mero acceso ilegítimo (*hacking*) existen una alteración o modificación de los datos accedidos.

Por último, en aquellos casos de ataques de Denegación de Servicios Distribuidos, descriptos en el Caso de Estudio Nro. 4, también podría ser penalmente perseguido a partir de la aplicación del nuevo art. 197[24], modificado por la citada Ley Nº 26.388, en consideración que a través de este tipo de ataques se estaría produciendo una interrupción de la normal prestación de un servicio de comunicación electrónica.

A modo de resumen, puede afirmarse que todos los ataques citados en el presente, podrían ser penalmente perseguidos, ya que Argentina cuenta materialmente con legislación penal que los reconoce y tipifica. No obstante, se debe resaltar que la realidad no es correspondida por la teoría, en vista de que incluso cuando las víctimas han sido (y siguen siendo) datos y sistemas gubernamentales, al momento no existen sentencias[25] que tengan por destino sancionar penalmente algunos de estos hechos.

---

[21] El término *Hacking*, que no debería tener una connotación maliciosa, se ha visto bastardeado por personas no especializadas y actualmente se aplica a cualquier actividad, sea esta legal o ilegal.

[22] Art. 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; […]

[23] Segundo párrafo art. 183: En la misma pena (15 días a un año de prisión) incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

[24] Art. 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

[25] De acuerdo a búsquedas en bases de Jurisprudencia de "La Ley Online" e "Infojus", a la fecha 02/05/2013

Responsabilidades

Como ya se ha desarrollado al comienzo del presente trabajo, la diversidad de ecosistemas informáticos y en consecuencia, de los diferentes niveles de seguridad de la información de sus estructuras, dan lugar a los más variados casos de vulneraciones y ataques por parte de terceros. Parte de dicha diversidad encuentra su razón de ser, en la propia descentralización gubernamental existente en Argentina, producto de la adopción de un sistema federal que permite la convivencia de los distintos estamentos de poder, con la consecuente subdivisión de responsabilidades.

En Argentina, dependiente de la Jefatura de Gabinetes de Ministros, se ha creado el ICIC (ex ArCERT), como el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad" [15], mediante la Resolución JGM Nº 580/2011. El mismo tiene como finalidad "*impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran […]*".

A fin de que los distintos estamentos gubernamentales (y ahora también existe la posibilidad de adhesión para el ámbito privado) puedan participar de dicho programa, el mismo establece la posibilidad de adhesión a través de unos formularios puestos a disposición en la Resolución de la Jefatura de Gabinete de Ministros Nº 3/2011 [16].

Es útil destacar que el concepto de CSIRT/CERT[26] (*Computer Emergency Response Team*) [17] fue inicialmente creado en 1988 por la Universidad de Carnegie Mellon como respuesta al gusano de Internet Morris[27]. Existen diferentes CERT públicos y privados en muchos países y, según FIRST (*Forum of Incident Response and Security Teams*) [18], la entidad que actualmente agrupa y coordina los CERT Internacionales, en Argentina existe un sólo CSIRT/CERT afiliado[28]: CSIRT-BANELCO para entidades bancarias privadas.

Si bien actualmente existe el ICIC, se desconoce cuáles son los organismos adheridos que participan del mismo, siendo menester preguntarse por la responsabilidad asumida por aquellos organismos que administran y generan los sistemas ¿Estarían incurriendo en algún tipo de negligencia en materia de seguridad de la información? ¿Cumplen los sistemas de los distintos niveles de gobierno con las medidas de seguridad que son obligatorias según la normativa vigente? ¿Quién evalúa la importancia de la información expuesta y el daño que causan los ciberataques a las

[26] Un CSIRT es un centro de respuesta a incidentes de seguridad en tecnologías de la información. Se trata de un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, pública alertas relativas a amenazas y vulnerabilidades y ofrece información que ayude a mejorar la seguridad de estos sistemas.

[27] En Noviembre de 1988 Morris fue el primer ejemplar de malware auto replicable que afectó a Internet.

[28] A fecha 02/05/2013, según información brindada en FIRST http://www.first.org/members/teams

organizaciones y a los ciudadanos? ¿Que herramientas tienen los ciudadanos para reclamar por el cuidado de sus datos por parte de sus propios gobernantes?

Conclusiones y Propuestas

Las vulnerabilidades en sitios gubernamentales existen, son muchas y variadas y, como se ha expuesto, el objeto de la presente investigación es hacer un llamado de atención con fines de información y educación en materia de Seguridad de la Información. Un llamado que deben atender especialmente aquellos profesionales que son personal responsable y autorizado de los sistemas del Estado Argentino pero, sobre todo, el mismo Estado Argentino (en sentido general, en todos sus niveles de poder).

La autonomía tecnológica de cada estamento gubernamental, si bien trae consigo elementos positivos -independencia en la gestión de contenidos, mejor visibilidad para los ciudadanos-, también acarrea el inconveniente de la heterogeneidad en el nivel de calidad de la administración, incluyendo a la seguridad de la información.

Estas filtraciones por parte de terceros desconocidos, han permitido y siguen permitiendo que delincuentes con distintos intereses se apoderen de la administración de los sistemas, con total libertad para robar datos personales, modificar una página con un mensaje alegórico, o hasta incluir la venta de productos comerciales como el viagra en sitios oficiales.

Desde el punto de vista legal, se ha observado que más allá de la necesidad lógica de dotar a los sistemas informáticos con medidas de seguridad, en virtud de la Decisión Administrativa 669/2004 existen obligaciones legales vigentes de adoptar una Política de Seguridad adecuada a la institución que se trate, incluso estableciéndose la obligación de definir un persona encargada de la Seguridad de la Información de dicho organismo. A ello, deben sumarse las obligaciones de seguridad exigibles para todos aquellos organismos en cuyos sistemas exista algún tipo de tratamiento de datos personales, de acuerdo a la Ley Nº 25.326 y toda su reglamentación vigente.

En relación a la legislación penal, se ha comprobado que todas las acciones analizadas en los casos de estudios actualmente se encuentran tipificadas como delitos informáticos, sin embargo, ninguno de ellos ha tenido como consecuencia el dictado de una sentencia condenatoria. De este dato, se puede inferir y denotar las falencias en materia de investigación y persecución eficaz que existe en este tipo de delitos en nuestro país, incluso en aquellos casos donde los sistemas atacados, son del propio Estado.

Para finalizar, y con la determinada intención de sumar un aporte tendiente a un cambio positivo en el estado de cosas en materia de ciberseguridad nacional, se destacan las siguientes acciones a realizar:

- Creación de un organismo único que se encargue de analizar las posibles vulnerabilidades, administre los incidentes y facilite su solución, que disponga de recursos, tiempo y personal capacitado para brindar soluciones a los incidentes, así como en ejecutar las investigaciones pertinentes.

- Creación de áreas dedicadas a la Seguridad de la Información dentro de cada organismo, o en el caso de no justificarse, determinar al menos un responsable a cargo de los sistemas de información y bases de datos personales.
- Mayor coordinación entre diferentes niveles de organismos para llevar adelante la publicación responsable de cualquier sitio gubernamental.
- Realizar auditorias y análisis de penetración y de vulnerabilidades con personal autorizado y capacitado, con el fin de detectar errores en la infraestructura y las aplicaciones instaladas.
- Exigir recaudos mínimos sobre seguridad implementada en los sistemas al momento de solicitarse la registración los dominios ".GOB.AR".
- Exigir por parte de los organismos encargados de las auditorías de los organismos públicos (SIGEN), mayores esfuerzos para instar al cumplimiento de la normativa vigente en Argentina que obliga a adoptar medidas y nombrar responsables en materia de Seguridad de la Información.
- Solucionar incongruencias tales como que existen sitios "GOV.AR" y "GOB.AR" o desarrollos sobre software libre y software privativo, sin un lineamiento claro al respecto, más allá de los recursos propios ad-hoc con los que cuenta cada delegación.

Muchas de estos puntos son, en definitiva, consecuencias de la falta de planeamiento y aplicación de un verdadero Sistema de Gestión de la Seguridad de la Información (SGSI).

La explotación de las vulnerabilidades informáticas por parte de delincuentes, no hace otra cosa que expresar al mundo la fragilidad del Estado Argentino en materia de ciberseguridad. En un país dividido por diferentes motivos sociales, económicos y políticos, ¿es posible pensar la Seguridad de la Información como parte de la Seguridad Nacional?

Referencias

[1] Wikipedia; G2C, http://en.wikipedia.org/wiki/Government-to-citizen

[2] Wright, Joe; Jim Harmening (2009). "15". *Computer and Information Security Handbook*. Morgan Kaufmann Publications. Elsevier Inc. p. 257. ISBN 978-0-12-374354-1

[3] Informe de ciberguerra de la OCDE, http://blog.segu-info.com.ar/2011/01/informe-de-ciberguerra-de-la-ocde.html

[4] "Atacan sitio oficial de la Presidencia de la Nación Argentina", http://www.pergaminovirtual.com.ar/revista/cgi-bin/hoy/archivos/00001914.shtml

[5] Zone-H, Reportes de incidentes publicados, http://www.zone-h.net/mirror/id/12686576

[6] Web del Padrón Electoral, Poder Judicial de la Nación, http://www.padrones.gov.ar/

[7] "Ataque al sitio del padrón electoral", http://edant.clarin.com/diario/2009/06/26/um/m-01947145.htm

[8] Filtración de información privada en AFIP (solucionado), http://blog.segu-info.com.ar/2011/01/filtracion-de-informacion-privada-en.html

[9] Modificación de sitios web (Defacing), http://www.segu-info.com.ar/articulos/96-defacing-objetivos-economicos.htm

[10] Anonymous, "OpFuckGobierno", 104 Sitios del Gobierno Argentino Tango Down, http://pastebin.com/TPXX0scD

[11] ONTI (Oficina Nacional de Tecnologías de Información), http://www.jgm.gov.ar/sgp/paginas.dhtml?pagina=27

[12] Maresca, Fernando. "La Seguridad de la Información en la Administración Pública Nacional" 2005 http://www.mmabogados.com.ar/LaseguridaddelainformacionenlaAPN.pdf

[13] Dirección Nacional de Protección de Datos Personales (DNPDP), Disposición 11/2006, www.jus.gov.ar/media/33445/disp_2006_11.pdf

[14] Ley 26.388 de Delitos Informáticos, http://www.infoleg.gov.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

[15] ICIC - Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad http://www.icic.gob.ar

[16] Disposición Nº 3/2011 - Jefatura de Gabinete de Ministros (ONTI), http://www.infoleg.gov.ar/infolegInternet/anexos/185000-189999/187698/norma.htm

[17] Wikipedia, http://es.wikipedia.org/wiki/CERT

[18] CERT miembros de FIRST en Argentina, http://www.first.org/members/map/